Introduction to Zero Trust Architecture

Zero Trust Training - Training course study guide

cloud security alliance®

ZTT™
Zero Trust Training

The official location for the Zero Trust Working Group is https://cloudsecurityalliance.org/research/working-groups/zero-trust/

Disclaimer

Cloud Security Alliance designed and created this Zero Trust Training course study guide (the "Work") primarily as an educational resource for security and governance professionals. Cloud Security Alliance makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

About Cloud Security Alliance

The Cloud Security Alliance^{SM} (CSA) (www.cloudsecurityalliance.org) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. Cloud Security Alliance harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. Cloud Security Alliance activities, knowledge and extensive network benefit the entire community impacted by cloud—from providers and customers, to governments, entrepreneurs and the assurance industry—and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA Address

709 Dupont St.
Bellingham, WA 98225, USA
Phone: +1.360.746.2689
Fax: +1.206.832.3513

Contact us: support@cloudsecurityalliance.org
Website: https://cloudsecurityalliance.org/
Zero Trust Training Page: https://knowledge.cloudsecurityalliance.org/page/zero-trust-training
Zero Trust Advancement Center: https://cloudsecurityalliance.org/zt/
Provide Feedback: support@cloudsecurityalliance.org
CSA Circle Online Community: https://circle.cloudsecurityalliance.org/
Twitter: https://twitter.com/cloudsa
LinkedIn: www.linkedin.com/company/cloud/security/alliance
Facebook: www.facebook.com/csacloudfiles
CSA CloudBytes Channel: http://www.csacloudbytes.com/
CSA Research Channel: https://www.brighttalk.com/channel/16947/
CSA Youtube Channel: https://csaurl.org/youtube
CSA Blog: https://cloudsecurityalliance.org/blog/

Acknowledgments

Dedicated to Juanita Koilpillai, a pioneer in software-defined perimeters whose contributions to the Zero Trust Architecture Training and CSA are immeasurable.

The Zero Trust Training was developed with the support of the Cloud Security Alliance Zero Trust Training (ZTT) Expert Group, whose members include volunteers from a wide variety of industries across the globe. Made up of subject matter experts with hands-on experience planning and implementing ZTT, both as cloud service consumers and providers, the ZTT Expert Group includes board members, the technical C-suite, as well as privacy, legal, internal audit, procurement, IT, security and development teams. From cumulative stakeholder input, the ZTT Expert Group established the value proposition, scope, learning objectives, and curriculum of the Zero Trust Training.

To learn more about the Zero Trust Training and ways to get involved please visit: https://cloudsecurityalliance.org/zt/

We would also like to thank our beta testers, who provided valuable feedback on the Zero Trust Training.

Lead Developers:

Abhishek R. Singh, Araali Networks, USA
Agnidipta Sarkar, Group CISO, Biocon, India
Daniele Catteddu, CTO, CISM, Cloud Security Alliance, Italy
Heinrich Smit, CISSP, CISA, CRISC, Semperis, USA
Juanita Koilpilla, CEO, Waverly Labs, USA
Michael Roza, CPA, CISA, CIA, MBA, Exec MBA, CSA Research Fellow, Exec MBA, Belgium
Michael J. Herndon, CCSP, CISSP, CRISC, CGEIT, CIPP/US, CIPT, AWS Certified Solution Architect, Bayer A.G., USA
Michael Shurman, Ravtech, Israel, Inactive member
Prasad T, OSCP, Senior Security Architect, Verse Innovation, India
Richard Lee, CISSP, CCSP, WCP, Citizens Financial Group, USA
Sam Aiello, CISSP CISA CCSK MSc MBA, Verizon Business, USA
Vani Murthy, CISSP, CDPSE, CCSK, CRISC, PMP, ITIL, MBA, MS, Sr. Information Security Compliance advisor at Akamai Technologies, Cambridge, USA

Contributing Editors:

Abbas Kudrati, C|CISO, Forrester ZTX Strategist, CISA, CISM, CSXP, CGEIT, Microsoft, Australia,
Adil Abdelgawad, Security+, 3M, USA
Anna Schorr, Training Program Manager, MBA, CCSK, Cloud Security Alliance, USA
Anusha Vaidyanathan, USA
Hannah Rock, Content Development Manager, Cloud Security Alliance, USA
Jacob Kline, CISSP, The MITRE Corporation, USA
James Lam, CISA, CISM, CRISC, CDPSE, TOGAF, M.S., Accenture Strategy & Consulting, USA
Jenna Morrison, CCSK, USA
Junaid Islam, USA
Lauren Fishburn, USA
Leon Yen, Technical Writer, Cloud Security Alliance, USA
Naresh Kurada, P.Eng, MBA, CISSP, Deloitte, Canada
Remo Hardeman, Security Architect, Cybersecurity Advisor, Omerta Information Security, Petro SA, Vrije University of Amsterdam VU, Netherlands
Shruti Kulkarni, CISA, CRISC, CISSP, CCSK, ITIL v3 Expert, ISO27001 LA, 6point6, United Kingdom
Stephen Smith, Graphic Designer, Cloud Security Alliance, USA

Expert Reviewer:

Alex Sharpe, CRISC, CDPSE, CMMC RP, Sharpe42, USA
Asad Ali, Thales, USA
Matthew Meersman, PhD, CISM, CISSP, CCSP, CDPSE, PMP, MITRE Corporation, USA
Michael J. Herndon, CCSP, CISSP, CRISC, CGEIT, CIPP/US, CIPT, AWS Certified Solution Architect, Bayer A.G., USA
Nishanth Singarapu, CISM, CCSK, ZCEA, Neustar, USA
Rajesh Ingle, PhD, International Institute of Information Technology, Naya Raipur, India
Ravi Adapa, India
Robert D. Morris, CISSP, GDSA, GCIH, MITRE Corporation, USA
Ron Martin, PhD, CPP, Capitol Technology University, USA
Ryan Bergsma, CCSK, Cloud Security Alliance, USA
Shamun Mahmud, Cloud Security Alliance, USA
Shinesa Cambric, CISSP, CISA, CCSP, CISM, Microsoft, USA
Srinivas Tatipamula, C-CISO, CISSP, CISA, AWS CSS/CSA, CDPSE, CISM, CGEIT, CRISC, ISO 27000LA, CCSK, ITIL-F, PMP, Fairfax, USA

Table of Contents

List of Figures

Course Intro

Welcome to *Introduction to Zero Trust* by Cloud Security Alliance. Please note that moving forward we will refer to Zero Trust Architecture as ZTA and to the Cloud Security Alliance as CSA. CSA is dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment across the globe. We hope you are as excited to learn about ZTA as we are about sharing this knowledge with you. This training module is part of a larger series of CSA programs on Zero Trust (ZT) that was created with the support of subject matter experts. If you are interested in volunteering with CSA to help our ongoing research efforts or are just interested in learning more about cloud security, please visit our website at cloudsecurityalliance.org.

In this training, we will provide an introduction to ZTA and ZT. This includes a discussion regarding ZT's relevance, followed by definitions, components, requirements, tenets, pillars, goals, objectives, and benefits of ZT. We'll also cover planning considerations and implementation options for ZTA, as well as use cases demonstrating how different topologies can work together to enhance security in environments assumed to be hostile. Diagrams, explanations, and references are provided to facilitate the learning process.

Course Structure

This introductory course on ZTA consists of seven units, each geared towards helping learners gain competency in a specific area/topic:

- Context of ZTA
- Definitions, Concepts, & Components of ZT
- Objectives of ZT
- Benefits of ZT
- Planning Considerations for ZTA
- ZTA Implementation Examples
- ZT Use Cases

Course Learning Objectives

After completing this course, learners will be able to do the following:

- Understand the foundations of ZT and ZTAs
- Explain ZTA's objectives and benefits
- Discuss possible planning considerations before implementing a ZTA
- Distinguish between the different ZTA implementation options
- Describe ZT use cases and applications

1 Context of ZTA

In this unit, you will learn how the various factors of the evolving technology landscape led to the emergence of ZTA, as well as explore ZT's roots and early approaches in both government and enterprise.

Organizations today are in a cycle of adopting new technologies by leveraging cloud services, either through platforms or by utilizing elastic computing. This means that while transformations are increasingly popular and technology adoption is the strategy for these organizations, their networks and security measures are equally under pressure to keep up with the changing environment and associated new risks.

Changes in the technology landscape, such as cloud computing, edge computing, and IoT, and the evolution of social behavior, such as increased requests for mobility, have led to organizations increasingly adopting distributed environments. Cloud computing, in all its combinations of delivery and deployments models is becoming the leading source of IT services[1]. The result is an increase in complexity for networks and service architectures, due to the need for integrating on-premises IT services with public cloud services, sensors, and actuators. In addition, the need to connect remote offices, remote workers, contractors, smart objects, and others has reinforced the requirement for more flexible, scalable, and secure network capabilities.

Similarly, data often resides in virtual environments outside the organization's premises and its physical control. However, the organization is still responsible and accountable for the data. From a data protection standpoint, traditional security architectures that focus on securing the physical network perimeter are increasingly ineffective in preventing cyber attacks.

This is where ZTA comes into play. ZTA is a model that creates virtual enclaves and grants access to resources inside of that enclave. Every transaction is vetted using the ZT concept of "never trust, always verify". In essence, ZT enables the designing of architectures from the inside out versus outside in.

1.1 History of ZT

ZT was first coined by John Kindervag around 2010 while working as a principal analyst at Forrester[2]. However, this concept was being researched much earlier by the Jericho Forum at the Open Group, and previously by the U.S Defense Information Systems Agency (DISA) and Department of Defense (DOD), with the Black Core project[3]. Kindervag, known as the grandfather of ZT, emphasized that all network traffic is untrusted. His position was that all requests to access data or resources should be verified at each step, with this being termed 'trust but always verify'.

[1] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," 26th, July 2017, https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

[2] John Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," 5th, November 2010, https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

[3] In the CSA's literature on SDP, terms such as "black cloud" or "network darkening" have been discontinued in favor of more neutral terminology.

The earliest concept of ZT was based on a data-centric network design and leveraged micro-segmentation which mandated more granular rules and policies to ultimately limit lateral movement of attackers. As the concept of ZT continued to evolve, it took a more identity-centric approach. This trend accelerated with the adoption of mobility and cloud.

In 2013, Cloud Security Alliance's (CSA) Software-Defined Perimeter (SDP) concept was initiated. SDP was designed to create an invisible perimeter through a security architecture that requires positive identification of network connections from a single packet inspection prior to accessing resources. In 2014, Google implemented ZT for its employees, which motivated it to publish the BeyondCorp model. The approach revolved around the idea that the perimeter had expanded, hence traditional perimeter security and a protected intranet were no longer sufficient to protect against cyber threats. Google's BeyondCorp model shifted the access controls and policies from the perimeter to individual devices and users. It addressed the need to replace the traditional VPN while still allowing users to work securely from any untrusted network with a superior security posture.

Since its inception, the concept of ZT has extended the original security model beyond traditional infrastructure, databases, and network devices to include IoT, cloud environments, big data projects, DevOps environments, containers, and microservices. In 2018, Chase Cunningham and his team at Forrester published the *Zero Trust eXtended (ZTX) Ecosystem* report, which extends the original ZT model beyond its network focus to encompass today's ever-expanding attack surface. In August 2020, NIST announced the final publication of *Special Publication (SP) 800-207, Zero Trust Architecture*, which discusses the core logical components that make up a ZTA[4]. Clearly, ZT is gaining widespread adoption, even as it continues to evolve as a security model.

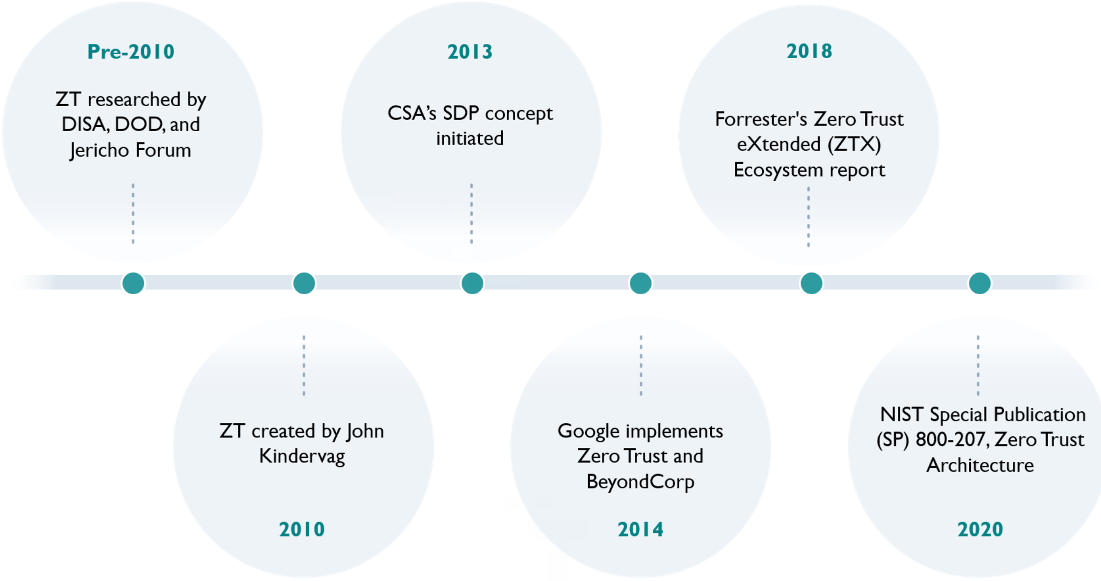

Pre-2010
ZT researched by DISA, DOD, and Jericho Forum
2013
CSA's SDP concept initiated
2018
Forrester's Zero Trust eXtended (ZTX) Ecosystem report
ZT created by John Kindervag
2010
Google implements Zero Trust and BeyondCorp
2014
NIST Special Publication (SP) 800-207, Zero Trust Architecture
2020

Figure 1: *ZT History and Milestones*

[4] NIST, "SP 800-207 Zero Trust Architecture," August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

2 Definitions, Concepts, & Components of ZT

In this unit, you will learn the definitions for key ZT terminology, as well as the concept's main tenets, design principles, pillars, and components and elements.

2.1 Definition[5] of the ZT Concept

ZT is a set of principles and practices designed for reducing cyber risk in today's dynamic IT environments. As a security model, ZT requires strict authentication and verification for each person, device, or service trying to access an IT resource, regardless of whether it is inside or outside the physical network perimeter. Since ZT emphasizes the protection of IT assets rather than network segments, the assessment of a given resource's security posture is not based on its location, but rather on what authentication and authorization controls are in place, and by leveraging risk-based analytics for access verification.

A key aspect of ZT networks is that authentication and explicit authorization must occur prior to network access being granted (e.g., the communication between a requesting entity and the target resource). Encrypting communications between two endpoints will no longer suffice; security practitioners must also ensure that access controls are implemented and each individual flow is confirmed as an authorized connection.

ZT lays out a blueprint for combating both internal and external threat agents trying to access protected assets. Research has shown that 90% of attacks start with a breach via a phishing email[6]. This exploit leads to the creation or compromise of an administrative account, followed by the lateral movement of malware inside the network, finally leading to the exfiltration of enterprise data.

In the context of this training and study guide, CSA defines the ZT concept as a cybersecurity approach that requires the following:

> - Making no assumptions about an entity's trustworthiness when it requests access to a resource
> - Starting with no pre-established entitlements, then relying on a construct that adds entitlements, as needed
> - Verifying all users, devices, workloads, network and data access, regardless of where, who, or to what resource, with the assumption that breaches are impending or have already occurred

Recent trends in enterprise security point to an increasing number of remote users and assets that are based in the cloud versus inside the traditional corporate network[7]. To meet the security

[5] Note: CSA's working definition of ZT and ZTA is based on existing market definitions of ZT (e.g., as defined by Forrester, NIST, etc.). Throughout this study guide, CSA also incorporates material from normative reference documents developed by the ISO/IEC and IEEE.

[6] CISO, "Cybersecurity Threat Trends," 2021, https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

[7] NIST, "SP 800-207 Zero Trust Architecture," August 2020, https://csrc.nist.gov/publications/detail/

challenges brought on by this shift, hardware manufacturers and software vendors are rapidly adopting the ZT model and validating that their products are fit for a ZT implementation.

2.2 Tenets

A tenet is defined as a principle generally held to be true. According to the USA DOD, ZT has five major tenets[8].

1. **Assume a hostile environment:** Malicious actors reside both inside and outside the network. All users, devices, and networks/environments should be untrusted, by default.
2. **Assume breach:** Most large enterprises experience a barrage of attempted cybersecurity attacks against their networks every day and many have already been compromised. Create, manage, and defend resources with vigilance, assuming that an adversary already has a foothold in your environment. Access and authorization decisions should be scrutinized more closely to improve response outcomes.
3. **Never trust, always verify:** Deny access by default. Every device, user, application/workload, and data flow should be authenticated and explicitly authorized using least privilege, multiple attributes, and dynamic cybersecurity policies.
4. **Scrutinize explicitly:** All resources should be consistently accessed in a secure manner using multiple attributes— both dynamic and static— to derive confidence levels for determining contextual access to resources. Access is conditional and can change based on the action and resulting confidence levels.
5. **Apply unified analytics:** Apply unified analytics and behavioristics to data, applications, assets, and services (DAAS), and log each transaction.

2.3 Design Principles

Several design principles can be used to guide the creation of a ZTA[9]. These design principles include the following:

- Denying access until the requestor has been thoroughly authenticated and authorized withholding access until a user, device, or even an individual packet has been thoroughly inspected, authenticated, and authorized. The access to resources is temporary and reverification is required. The timespan of the access is defined by policies
- Allowing access to the network changes with ZT; requesters (users, machines, processes) aren't allowed access to anything until they authenticate who they are
- Allowing access to resources only after the requesting entity has been authorized
- Enforcing least privilege, specifically, granting the least amount of access required
- Requiring continuous monitoring of existing security controls' implementation and effectiveness (e.g., controls over access or user behavior)

sp/800-207/final

[8] DOD, "Department of Defense (DOD) Zero Trust Reference Architecture," February 2021, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[9] ISO/IEC/IEEE 42010: 2011 defines "architecture" as: "The fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution."

2.4 Pillars

The ZT concept is a work-in-progress with boundaries and definitions that continue to evolve, especially in terms of scope of applicability and use cases. Even so, the industry has reached a certain level of consensus regarding what the fundamental pillars of a ZTA are. CSA emphasizes these seven pillars of the DOD ZTA[10].

> 1. **Users/identities:** Securing, limiting, and enforcing access for person, non-person, and federated entities' to DAAS, encompasses the use of identity, credential, and access management capabilities, such as multi-factor authentication (MFA) and continuous multi-factor authentication (CMFA). Organizations need the ability to continuously authenticate, authorize, and monitor activity patterns to govern users' access and privileges while protecting and securing all interactions. Role-based access control (RBAC) and attribute-based access control (ABAC) will apply to policies within this pillar in order to authorize users to access applications and data.
> 2. **Device/endpoints:** The ability to identify, authenticate, authorize, inventory, isolate, secure, remediate, and control all devices is essential in a ZT approach. Real-time attestation and patching of devices in an enterprise are critical functions. Some solutions, such as mobile device managers or comply-to-connect (C2C) programs, provide data that can be useful for device confidence assessments. Other assessments (e.g., examinations of compromise state, anomaly detection, software versions, protection status, encryption enablement, etc.) should be conducted for every access request.
> 3. **Network/environment:** When taking a ZT approach, organizations should logically and physically segment, isolate, and control the on-premise and off-premises network/environment with granular access and policy restrictions. As the perimeter becomes more granular through macro-segmentation, it enables micro-segmentation to provide greater protections and controls over DAAS. It is critical to (a) control privileged access, (b) manage internal and external data flows, and (c) prevent lateral movement.
> 4. **Applications and workload:** These should include tasks on systems or services on-premises, as well as applications or services running in a cloud environment. ZT workloads should span the complete application stack from application layer to hypervisor. Securing and properly managing the application layer as well as compute containers and virtual machines should be central to the ZT adoption. Application delivery methods like proxy technologies enable additional protections and therefore should also be an important part of ZT decision and enforcement points. Source code developed in-house and common libraries should be vetted through DevSecOps development practices to secure applications from inception.
> 5. **Data:** ZT protects critical data, assets, applications, and services. A clear understanding of an organization's DAAS is critical for the successful implementation of ZTA. Organizations should categorize their DAAS in terms of mission criticality and use this information to develop a comprehensive data management strategy, as part of their overall ZT approach. This can be achieved through the categorization of data, developing schemas, and encrypting data at rest and in transit. Solutions such as DRM, DLP, software-defined storage and granular data-tagging are crucial for protecting critical data.

[10] DOD, "Department of Defense (DOD) Zero Trust Reference Architecture," February 2021, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

6. **Visibility and analytics:** Vital, contextual details should be included to provide a greater understanding of performance, behavior, and activity baselines across the various ZT pillars. This visibility improves the detection of anomalous behavior and provides the ability to make dynamic changes to security policies and real-time contextual access decisions. Additionally, other monitoring data from sensors, in addition to telemetry, are used to provide situational awareness in the environment. This will aid in the triggering of alerts used for response. A ZT enterprise will capture and inspect traffic, looking beyond network telemetry and into the packets themselves to observe threats and bolster defences more appropriately.
7. **Automation and orchestration:** ZT includes automating manual security processes to take policy-based actions across the enterprise with speed and at scale. Security orchestration, automation, and response (SOAR) improves security and decreases incident response times by automating responses to threats. Security orchestration integrates security information and event management (SIEM) with other automated security tools in the management of disparate security systems. In order to provide proactive command and control, automated security responses require defined processes and consistent security policy enforcement across all environments in a ZT enterprise.

2.5 Components & Elements

At a high level, ZTA requires three core components before any logic can be applied to allow a decision to be made for access:

1. **Communication:** A request for an entity to access a resource, and the resulting access or session
2. **Identity:** The identity of the entity (e.g., user or device) requesting access to the resources
3. **Resources:** Any assets within the target environment

In addition to these three core components, ZT is also composed of two other fundamental elements:

1. **Policy:** The governance rules that define the *who, what, when, how, why* of access to the target resource access
2. **Data sources:** The contextual information providers can use to keep policies dynamically updated

The applicability of all of these components and elements will depend on your use cases and deployment models.

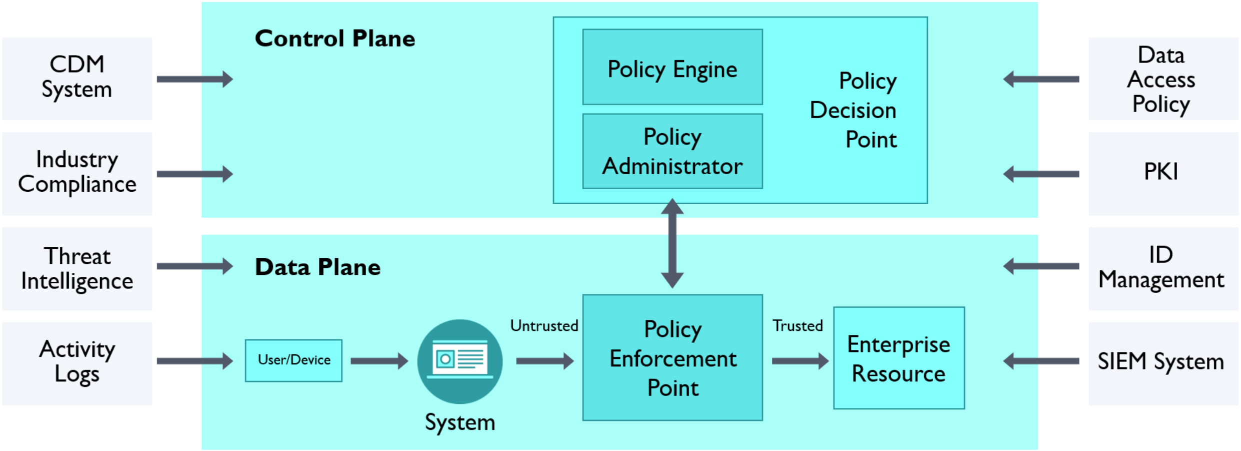


Figure 2: *Key Logical Components of a ZTA*[11]

In the publication, *SP 800-207*, NIST has provided a simple representation of the key logical components of a ZTA (see diagram above). In the NIST ZT workflow the policies are defined, managed, and enforced via the following two mechanisms:

> - Policy decision point (PDP)
> - Policy enforcement point (PEP)

Together, the PDP and PEP regulate access to resources by being placed in the access workflow of traffic.

The PDP is composed of a policy administrator and policy engine (PE). The PDP determines the *rules* and communicates them to the PEP. The PEP acts as a gateway to ensure that access to an approved resource has been granted to the correct entity, with the correct access levels.

NIST defines the following[12]:

> - PDP as the control plane: the component of the logical architecture that has the responsibility to collect, analyze, and transform the data first into intelligence and then into rules to govern the access to resources.
> - PEP as the data plane: the component that, based on input passed by the control plane, has the responsibility to enforce the rules and provide access to the resources (i.e., data).

Data sources serve the purpose of feeding data into the PDP, with the goal of maintaining the rules and keeping the overall decision-making process updated. Various sources of intelligence feed into the policy engine and support the policy administrator in defining and/or refining the access rules.

[11] Figure adapted from NIST, “SP 800-207 Zero Trust Architecture,” August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

[12] NIST, “SP 800-207 Zero Trust Architecture,” August 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

The following is a list of the possible information sources for the policy engine:

- Intrusion detection system (IDS)/Intrusion detection and prevention system (IDPS)
- Network devices (e.g., firewalls, proxies, gateways, routers, etc.)
- Threat intelligence feeds (e.g., third party databases of threats, vulnerabilities, weaknesses, and exploits)
- Information sharing systems
- Denylists and blocklists
- Identity providers and access management systems (e.g., Active Directory [AD] or cloud access security brokers [CASBs])
- Legal and regulatory compliance requirements
- Asset/device management and discovery systems
- Public key infrastructure (e.g., certificate revocation lists)

The figure below provides an alternative representation of the data flows and data sources that feed into the PDPs and PEPs.

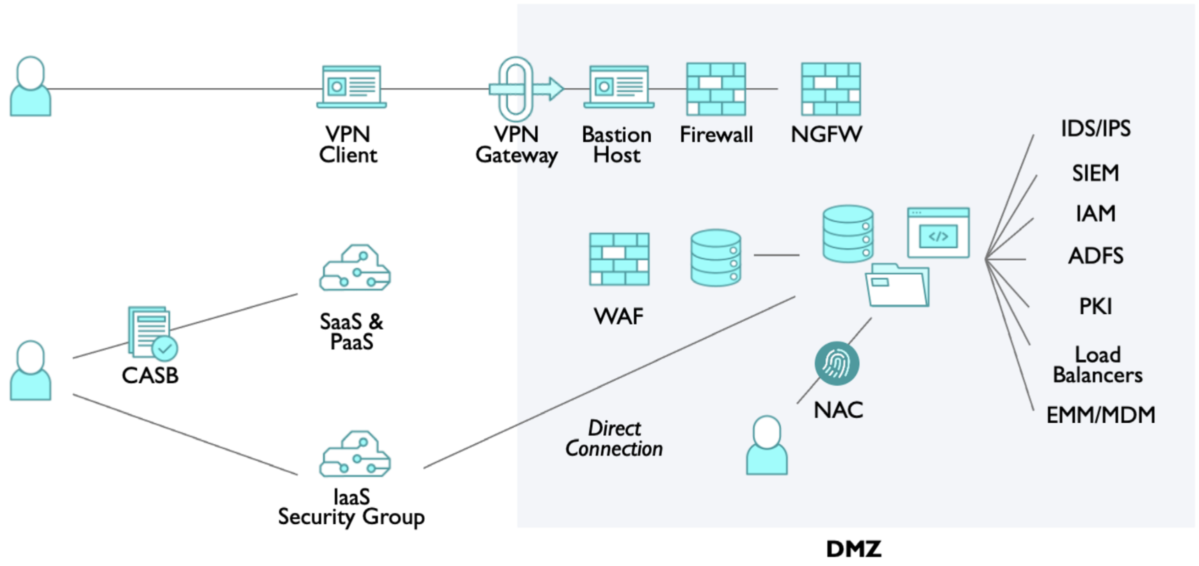


Figure 3: *PDP and PEP Data Flows and Sources*[13]

Security incident and event monitoring databases can be a collection point for any/all of the above sources. Together, these components have telemetry information relating to all the core components of ZTA. This gives enterprises more context to make better informed policy decisions.

Due to the greatly increased number of PEPs, manual management of the access model can be challenging and is not recommended. Instead, automation represents another important characteristic of a ZT environment, as it supports both granular and global control.

[13] Figure adapted from Cloud Security Alliance, "SDP Architecture Guide v2," 7th, May 2019, https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

3 Objectives of ZT

In this unit, you will learn how ZT addresses the main technical and business objectives related to reducing cyber risk in an organization.

As with most security architectures, the primary objective of ZTA is to address security risks inherent in the assumption of trust, and the lack of proper access controls. Typical approaches to addressing these risks include reducing the attack surface and/or improving the effectiveness of security controls.

The motivation behind ZTA is to provide a holistic and consistent security approach for protecting an enterprise against malicious actors both internal and external — threats that exploit inherent or newly-created gaps in conventional protection methods and defense-in-depth controls. The key differentiator in ZTA is the **ephemeral nature of any trust** between data/computing resources and the principals requesting access. This differentiator, combined with capabilities like dynamic policy enforcement and decisioning, bolster an environment's security posture, from the cloud to on premises. This is true for both internal and external attacks that exploit and compromise exposed access mechanisms maliciously.

A ZT approach fulfills both technical and business objectives. Technically, it establishes a framework for protecting resources, simplifies the user experience, reduces the organization's attack surface size and complexity, enforces least privilege, improves control and resilience, and localizes the impact radius of a security failure. From a business perspective, ZT aims to reduce risk, improve governance and regulatory compliance, and align the organization's culture with the risk appetite of its leadership.

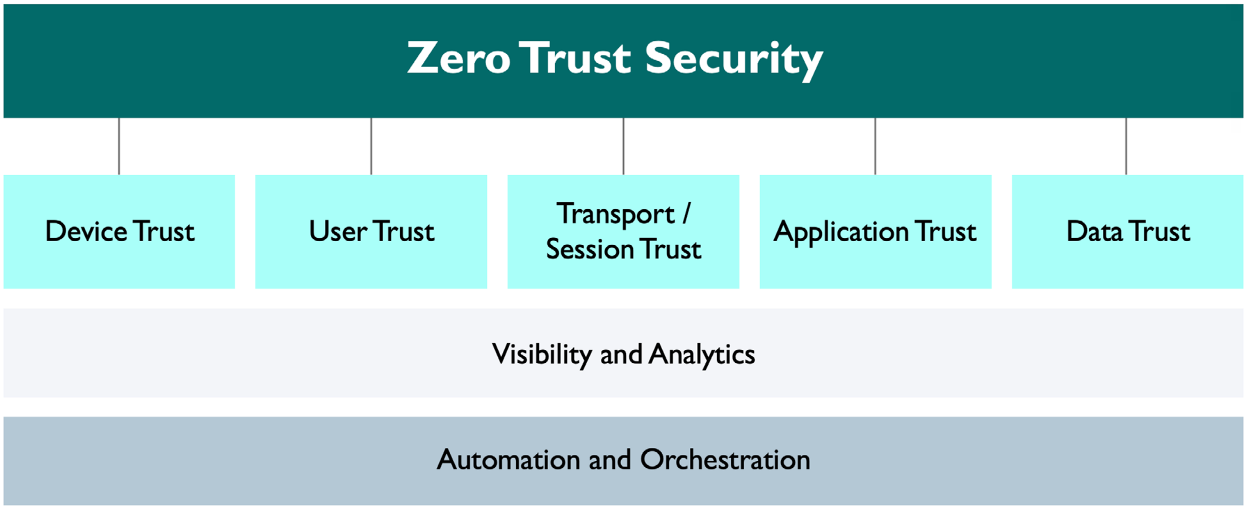


Figure 4: *ZT Concept Framework and Elements*[14]

[14] Figure adapted from ACT-IAC, "Zero Trust Cybersecurity Current Trends,", 18th, April 2019, https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

3.1 Technical Objectives

The following technical objectives serve as critical milestones for organizations looking to adopt ZTA. These objectives include activities and efforts related to the implementation of specific technologies and supporting security frameworks.

- Establish Protective Framework
- Simplified User Experience
- Reduced Attack Surface
- Reduce Complexity
- Principles of Least Privilege
- Security Posture and Resilience
- Incident Containment

3.1.1 Establishing a Protective Framework

The protective framework established by ZT represents a novel approach to cybersecurity. As mentioned previously, ZT's core premise is that an organization should not inherently trust any entity that comes from within or beyond its boundaries. This new protective framework enables a shift of focus to more business oriented goals, with systems designed around the value of the data and their specific protection needs. Many procedures and strategies that were once considered strong security measures are no longer fully effective; as a result, aged cybersecurity techniques and technology will increasingly yield limited results and inadequate protection.

It is no longer practical to use approaches and frameworks based on physical objects and systems, nor is it effective to rely on signature-based threat detection. The increasing frequency and scale of attacks, combined with today's hyper connected world, virtualized environments, and software-based organizations, requires businesses to reconsider everything from network configurations to detection and prevention approaches.

3.1.2 Reduce Management Overhead

ZTA reduces management overhead by applying a consistent access model throughout the environment for all assets, from network devices to virtual servers and applications. Every request for access, whether explicit or implicit, is met with the same interrogation: Who are you? Do you need this access now? Okay, you get this access to this resource for this period.

To support this uniformity, ZTA models are absent of the following:

> - Complicated diagrams of nested groups using legacy access control lists (ACL) with allow and deny parameters producing unexpected results
> - Layers of groups managed by potentially irrelevant decision-makers
> - Stale and orphaned groups whose owners have long since moved on
> - Authorization mechanisms based on antiquated models/labels (e.g., local vs. global)
> - Delays in provisioning, deprovisioning, or access revocation, since every request is handled consistently, just-in-time by the PDPs

3.1.3 Reduce Attack Surface

In a traditional security architecture, access decisions made at the network perimeter either allow or deny access. Denied traffic is dropped outside of the perimeter, while allowed traffic enters the perceived secure environment and travels unencrypted, as it is rare for organizations to encrypt internal traffic. Once inside, an attacker may run port scans, find vulnerabilities, launch denial-of-service attacks, steal additional credentials, eavesdrop on privileged network traffic, and move laterally unobstructed with relative ease. In contrast, with the ZT model the same attacker is no better off than if they had not penetrated the system's external defenses, because each internal resource makes a decision as to whether or not to grant access at any given moment. The organization's attack surface effectively contracts from every resource to only improperly secured resources.

3.1.4 Reduce Complexity

An organization's ever-expanding digital footprint makes for an increasingly complex IT environment, especially with some access decisions being made far in advance of being requested/used or even necessary. Access levels often remain, even as the party granting the access has long since moved on, leaving behind orphaned objects with unmanaged permissions. Such complexity represents one of the biggest security challenges for an organization, as it further reduces visibility, complicates configurations, creates weaknesses and vulnerabilities, and generally makes it easier for malicious actors to gain a foothold in the network.

Additionally, the adoption of newer IT paradigms like hybrid cloud implementations, multi-cloud architectures, and edge computing also further complicates the access control policy management. ZT reduces this complexity by assuming that all parties requesting application access are malicious and should therefore be untrusted. Instead of trying to police all the borders and paths across the network, security professionals need only create islands of applications and data to protect in a more focused manner. This is because ZT strategies require far more attributes than standard security mechanisms. As organizations strive for agility by simplifying networks and consolidating data centers, ZT provides a robust security mechanism to reduce security architecture complexity by creating perimeters around applications and identity. This also reduces the number of access points into an enterprise's IT environment, resulting in tighter control over each identity's level of access and privileges, including third parties like vendors and suppliers.

3.1.5 Enforces the Principle of Least Privilege

ZT enforces the principle of least privilege, which dictates that users and programs should only have the necessary privileges to complete their tasks. Per ZT, users get access to exactly what they need to conduct their business, when they need it. ZT also includes the use of micro-segmentation, or the creation of zones in an IT environment to isolate workloads for better security. This enables users to connect to the right application and use only the services they require. This simplified access provisioning makes it easier to manage security operations and governance teams in a continuously evolving security landscape. ZT also includes the use of purpose based dedicated identities also known as identity personas. Identity persona is created for a group of resources that address a common functionality, which helps in limiting the attack surface created by the compromise of an identity.

3.1.6 Improved Security Posture & Resilience

The objective of ZT is to enhance and bolster the resilience and the security posture of an enterprise's IT infrastructure. From outside of the organization, ZTA ensures that malicious actors have reduced visibility into the enterprise's IT infrastructure and individual assets, thereby reducing the potential attack vectors at their disposal. From within the organization, ZTA restricts lateral movement to minimize the risk of cross-site attacks and damage inflicted by insider threats. Because external users are contained and controlled within a small area of the network, any resulting security issues can be quickly contained and addressed. ZT limits the impact radius of security incidents and enables the swift return of systems to their earlier state.

The reduced attack surface ensures that any source scanning and mapping activities initiated by internal or external actors are not successful unless they are authorized within the ZT implementation. The two-layer architecture consisting of a separated control plane and data plan helps ensure that access is granted to the organization's network only after the users and their devices have been properly authenticated and authorized.

3.1.7 Improved Incident Containment & Management

A primary goal of ZTA is to make the incident management process more effective and efficient; to this end, several of ZTA's core design principles like "never trust, always verify" and the presumption of an ongoing breach require continuous behavioral monitoring of all system entities.

Micro-segmentation and the requirement for continuous network access authorization reduces the impact radius of potential breaches, as it restricts a cyber attacker's ability to move laterally. When a breach does occur, damage is limited to a confined area and containment/eradication and remediation efforts can be carried out with respect to the incident's scope.

The continuous monitoring capabilities included in ZTA allow for more effective identification of anomalies and incidents. The incident-related data is also used to update the PDP, allowing for dynamic policy definition/enforcement critical to limiting the impact across the organization's network.

3.2 Business Objectives

The following key business objectives can serve as critical milestones for organizations looking to align ZT adoption efforts with ongoing, high-level operational needs. These include the overall reduction of both compliance and cyber risk, as well as the fostering of a ZT-based organizational culture.

Risk Reduction

Compliance Management

Organization Improvements

3.2.1 Risk Reduction

A primary business goal of ZTA is the reduction of cyber risk. This is especially critical for organizations dealing with complexity brought on by the proliferation of distributed, open computing infrastructures and the enterprise's migration to the public cloud. The risk reduction objective relates to some of the technical goals and objectives mentioned in the previous section, such as reducing the attack surface and achieving/maintaining an improved and resilient security posture.

Chiefly, ZTA aims to reduce the risk of the following:

- Improper privilege escalation via lateral movement
- Access beyond the need to know requirements
- Access beyond the required time frame
- Access by unsecure devices
- Access via unsecured methods such as unencrypted channels or channels using invalid certificates
- Compromises using methods like brute force, distributed denial-of-service (DDoS), or man in the middle (MITM) attacks
- Unauthorized lateral movement

Additionally, ZT supports the adoption of MFA to protect logins against common brute-force attacks, dictionary attacks, or stolen credentials attacks. In alignment with the ZT model, users and devices are validated before gaining access to protected resources and mutual authentication occurs between the server and client when the connection is being established.

Implemented in all ZTA variants, the principle of least privilege is effective in mitigating the most sophisticated and difficult to detect internal attacks. ZT's level of granularity prevents users from accessing unauthorized resources, as controls and policies are applied separately to every protected resource, for every access request. In addition, all communications between clients and servers flow through mutually authenticated encrypted tunnels, creating extended micro-segmentation systems in lock step.

ZT also includes continuous monitoring as a critical requirement for cyber risk reduction. To maintain a strong security posture, enterprises should continuously monitor all resource access activity and investigate potential signs of compromise. Since ZTA is policy-based, the risk of unauthorized access by compromised accounts can be mitigated, since policies can be conditioned on user and device security posture.

Above all, the ZT model reduces the total risk of running a connected enterprise by using one unified framework, typically provided by a limited number of vendors. This allows an enterprise to mitigate all the major threats that previously required multiple solutions, each with its own drawbacks and security flaws.

3.2.2 Compliance Management

A primary objective of ZT is to help organizations achieve and maintain an optimal compliance posture, reducing both the financial and technical impact of compliance, internal and external. This is mainly achieved through two key ZT features: (1) discovery and (2) mapping out of all networked assets and related access controls. ZT requires that assets are automatically discovered and validated for alignment with the latest compliance requirements since assets and data can only be protected if their presence is known. ZT helps segregate resources based on the relevant legal, regulatory, and contractual compliance requirements.

A proper implementation of ZT verifies authentication and authorization each time traffic moves laterally or inside/outside the network. This approach prevents unauthorized access before data can be accessed, compromised, encrypted for ransom, or exfiltrated. Additionally, it creates an audit trail for satisfying regulatory requirements regarding record keeping and auditing.

The benefits of ZT are instrumental to an organization's efforts in maintaining regulatory compliance. Privacy-related regulations such as General Data Protection Regulation (GDPR)[15] and the California Consumer Privacy Act (CCPA) define stringent requirements for processing and storing personally identifiable information (PII). Organizations must build an accountability framework for maintaining control and visibility over PII: how it is collected, processed, stored, where it resides, for what purpose, how, and by whom; with these components in place, organizations can implement the proper security controls for protecting PII from internal and external threats. ZT enables organizations to better align with standard security practices integrated into existing regulatory requirements' internal controls.

[15] See for instance GDPR Article 30, "Records of processing activities"

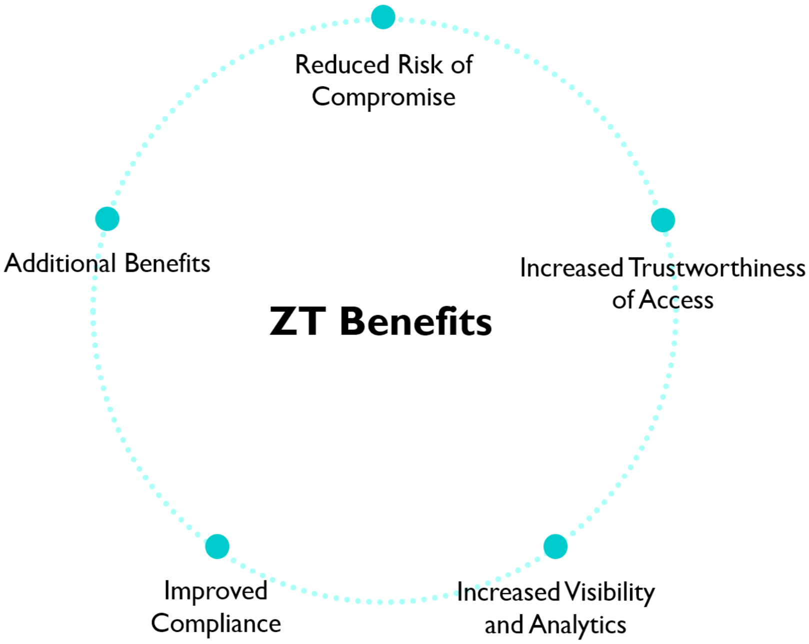
3.2.3 Organizational Improvements

The ZT model's "never trust, always verify" approach results in significant changes to the organization's mindset regarding how resources are accessed, as it requires enterprises to adopt a coordinated, structured approach to cybersecurity. Organizations must shift to a culture based on processes and procedures that support continuous verification — only then can each entity within the company's IT environment be trusted at any given moment in time.

4 Benefits of ZT

In this unit, you will discover the range of benefits that ZT adds to an organization's security efforts, from reducing the risk of compromise to increased visibility and improved compliance.

ZT provides a myriad of benefits for strengthening the cybersecurity posture of an organization, both on-premises and in the cloud. These include, but are not limited to:


Reduced Risk of Compromise
Increased Trustworthiness of Access
Increased Visibility and Analytics
Improved Compliance
Additional Benefits
ZT Benefits

Collectively, ZT's benefits enable organizations to bolster their defenses against internal and external threats, reduce cyber risk and improve adherence to compliance frameworks.

4.1 Reduced Risk of Compromise

One of the main benefits of ZT is that it reduces risk of compromise, primarily through the following:

- Reducing the attack surface and limiting the radius of impact
- Reducing an attacker's ability to move laterally
- Reducing the time to detect and contain breaches

4.1.1 Reduced Attack Surface & Impact Radius

The principle of least privilege and "never trust, always verify" are at the very core of ZT. Resources are accessed based on the attributes of the entity or user, security hygiene of the device, context of the request, and relative risk to the environment. This reduces the risk of unauthorized access and escalation of privileges.

In addition, ZTA implementations leverage the concept of resource hiding, where resources are only visible to authenticated, authorized users. This concept is described in various ways depending on the ZTA implementation technique.

As described in NIST *SP 800-207*[16], a user sends a request from the system (e.g., a laptop) to the PEP to access a resource. The PEP forwards the request to the PDP for authorization, which in turn checks if the user has been authenticated and authorized by policy. The PDP then sends its response to the PEP.

This variation of the agent or gateway deployment model implies the use of vetted, compartmentalized applications or processes (e.g., virtual machines, containers, or some other implementation); regardless of what technology is being used, the goal is the same: to protect the application or application instances from potentially compromised hosts or other applications sharing the same server resources. According to this model, the server only runs approved, vetted applications in a sandbox; these applications can communicate with the PEP to request access to resources, but the PEP will refuse requests from other applications running on the server. In this model, the PEP could be an enterprise service running locally or a cloud service.

4.1.2 Reduced Ability to Move Laterally

ZT calls for the implementation of micro-segmentation to restrict lateral movement inside an enterprise IT environment, thereby reducing the attack surface and potential impact radius. Each access attempt to any resource—internal as well as external—is authenticated and authorized before access is granted, regardless of the requester's origin.

4.1.3 Reduced Time to Detect & Contain Breaches

ZTA's centralized authentication and policy enforcement enables improved visibility into all access attempts across multiple cloud providers and on-premises IT infrastructures. This visibility, in conjunction with dynamic access policies, enables organizations to detect malicious access attempts in real-time and mitigate attacks before they cause damage. By adopting ZTA, organizations increase their level of continuous verification and capability in detecting threats like phishing attempts, privilege elevation for accessing applications and services, and/or the use of stolen credentials. Early detection of these threats can often stop attackers from launching a successful intrusion attempt.

[16] NIST, "SP 800-207 Zero Trust Architecture," August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

4.2 Increased Trustworthiness of Access

ZTA increases the trustworthiness of data by distrusting anyone inside or outside the organization's perimeter. ZTA considers consolidated identity access management (IAM) and policy solutions capable of managing access across the organization's entire environment, providing a single source of truth for identity, and supporting single sign-on (SSO) as a fundamental capability. User authentication is centralized with authentication being strong, dynamic, and strictly enforced before access is allowed. This is supported by MFA, session timeouts, re-authentication requests, and validation. These steps are equally applied to any layer in the stack.

Granular access and permissions are configured based on roles, context, or attributes as applicable. Access to resources is based on the principles of least privilege and need to know. Access to any data is protected cryptographically based on its sensitivity — whether it is at rest, in motion, or being processed.

In summary, from the perspective of access to the resources, some of the benefits of a ZTA are:

- Granular access and permissions, and ability to grant access based on context
- Authentication of device and user before granting access to network and resources
- Enforcement of the least privilege rule
- Strong authentication, including MFA
- Centralized access control
- Continuous validation of identity, authentication, and authorization to resources
- Improved data protection

Additionally, some ZTA methods incorporate single packet authorization (SPA), which also helps increase the trustworthiness of access. SPA uses a next generation passive authentication technology that features no open ports and service listeners; instead, a specialized encrypted packet is used in the following procedure:

- The first SPA packet sent by the client is rejected
- A second service identifies the SPA packet in the IP stack and attempts to authenticate it
- If successful, the server creates an explicit policy to expose the service to the requesting endpoint

For example, the server may open a port in the firewall (e.g., iptables on Linux systems) for the client to establish a secure, encrypted connection with the service in question. The PEP provides the support to enforce the IAM policy of least privilege for the user identity requesting access by communicating with the PDP, preferably executing MFA—only then is a mutual transport layer security (mTLS) session is created for data transfer. Then an mTLS session is created for data transfer. The device is actively validated in context during this process. Frequent and periodic validation can be part of the IAM policy, which can be enforced either manually or by automation.

Another example of how ZTA increases the trustworthiness of access is described in NIST SP 800-207. The enhanced identity governance approach establishes enterprise resource access policies based on identity and assigned attributes. The main requirement for access is a given entity's access privileges (or lack thereof); in addition, the device used, asset status, and environmental factors also come into play, as they will affect the ultimate level of access granted to the subject, regardless of its identity privileges.

The user authenticates to the device (e.g., with a username and password), which in turn authenticates to the network. The user authenticates to the network (e.g., using directory services) and their access request to the resource in question is sent to the gateway or portal. The request is forwarded to the policy administrator/policy engine. After authenticating with the identity provider, the result/decision is returned—if approved, access to the resource is granted to the user.

Consider the example of an IEEE 802.1x implementation using network access control (NAC) coupled with Lightweight Directory Access Protocol (LDAP): all corporate laptops have agents installed, and users authenticate to the laptop, which in turn authenticates to the network via IEEE 802.1x. User requests to access resources are vetted by NAC, LDAP, and potentially other access management applications. The request is authorized if the user is verified as part of the appropriate group.

4.3 Increased Visibility & Analytics

ZTA requires logging, monitoring, and alerting capabilities for increased visibility into users' activity: what actions they took, and when they took these actions. Attempts to access privileged resources as well as administrative or root account activity should always be logged, monitored, and reported. Anomaly detection should also be in place for detecting suspicious patterns in both inbound and outbound traffic.

Varying degrees of automation can be developed for these capabilities, as well as automated workflows for faster, more streamlined response and remediation. For example, alert notifications can be created when certain conditions are met, followed by automatic task assignment to the appropriate parties for further action.

To summarize, ZTA's visibility and analytics-related improvements include the following:

- Granular logging and monitoring for greater visibility across the enterprise
- Monitoring analytics over user entities behavior, leading to user entity behavior analytics
- Network isolation and micro-segmentation for improving the ability to quickly detect and resolve errors
- Continuous monitoring across all attack surfaces, making it easier to detect data breaches and enforce appropriate responses
- Minimization of data exfiltration
- Continuous device posture assessment

The specific visibility and analytics benefits will vary depending on the ZTA implementation.
In the case of CSA's SDP, IAM policies are enforced when access requests are made to a device or host. Granular records of both successful and failed attempts of all components in the path provides increased visibility and the foundation for analytics. Device posture is evaluated during setup of the mTLS sessions. As logs become more granular and descriptive and user entity behavior analytics evolve, security analytics also become more detailed, making it easier to detect breaches or anomalous behavior. This also enables automation of appropriate responses.

Whereas, NIST SP 800-207 specifies that requirement (3) of ZTA is that it enables "the enterprise to observe all network traffic. The enterprise records packets (i.e., OSI layer 3) seen on the data plane, even if it is not able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE as it evaluates access requests."

The DOD ZT Reference Architecture outlines a model for logging, analytics, and automation.

> 1. Historical user behavioral data and current user actions are sent to the analytics engine to be analyzed.
> 2. A user's historical and current actions/behaviors are compared against global baselines or unusual activity indicators that house all acceptable trends. These baselines and unusual activity indicators can then be derived from internal analytics metrics or vendor-supplied feeds.
> 3. The analysis results in a confidence score based on the user's behavior.
> 4. As users traverse the network, their confidence score and historical behavior patterns dictate the level of access they receive.
> 5. Monitoring and analysis is continuously occurring in the background.
> 6. Access to a resource is denied if the users' actions and behavior patterns result in their scores dropping below a certain threshold.
> 7. If the users' actions and behavior patterns do not appear malicious, they can be informed that their scores do not meet the threshold.
> 8. If the users' actions and behavior appear malicious, different handling procedures are initiated depending on the specific actions/behaviors and accessed resources.
> 9. All actions are logged to a SIEM platform, processed by the analytics engine, and handed to a SOAR platform to deploy real time policy access decisions.

4.4 Improved Compliance

ZTA has the potential to improve an organization's compliance posture in several ways. For example, ZTA requires organizations to frequently review access policies to ensure they stay in alignment with requirements as their IT environment evolves. To this end, policies are a key element for security governance as they enable organizations to translate their goals and objectives into the rules that drive their approach to security. Polices also support the organization in remaining accountable to its shareholders and stakeholders. In a ZT approach, policies controlling access to resources are carefully enforced, continuously monitored, and frequently updated based on the current situation. These approaches enable organizations to maintain a strong compliance posture in regards to both external (i.e., legal regulations and oversight measures) and internal (i.e., company policy) requirements.

Continuous monitoring is critical for effective policy management, as it enables the alignment of policy definitions with enforcement measures. This is crucial for organizations looking to implement controls for continuous auditing and compliance.

Finally, micro-segmentation strategies apply access controls to each individual resource via fine-grained authorization mechanisms. The requester's trustworthiness is evaluated prior to access being granted. Policies actively determine access levels and may be based on the user's observable state/identity, the requesting system, and other behavioral attributes. By implementing micro-segmentation and the principles of need to know and least privilege, organizations effectively reduce their attack surface/risk exposure, which may in turn limit their liability when it comes to laws and regulations. For example, a fewer number of users/devices with access to sensitive data and/or restricted by location reduces the scope of certain compliance measures (e.g., PCI-DSS or GDPR).

4.5 Additional Benefits

A ZT approach can help organizations identify business processes, data flows, users, data, and associated risks. These insights better equip them to reduce risk in their cloud and container deployments while also improving governance and compliance. Organizations can also gain deeper insights into users and devices, identify threats more quickly, and maintain more comprehensive control across a network. A well-architected ZTA also reduces IT complexity while supporting resiliency and defense-in-depth.

Security benefits aside, the advantages of a ZT security framework are numerous and vary depending on the enterprise's organizational landscape, architecture, and operating model. Utilizing cloud technologies to automate ZT functions helps minimize ongoing operational costs and eases the burden on human resources and staffing.

The ZT model provides a unified access control to data, services, applications, and infrastructure. This enables enterprises to counter major threats with one solution, versus a combination of tools (e.g., firewalls, VPNs, CASBs). By unifying the organization's access controls, ZT reduces security costs while improving efficacy, visibility, manageability, and user experience.

The following is a non-exhaustive list of additional ZT benefits:

- Potential cost reduction
- Simplification of IT management design
- Improved data protection (business critical data and customer data)
- Secure remote access
- Improved user experience

5 Planning Considerations for ZTA

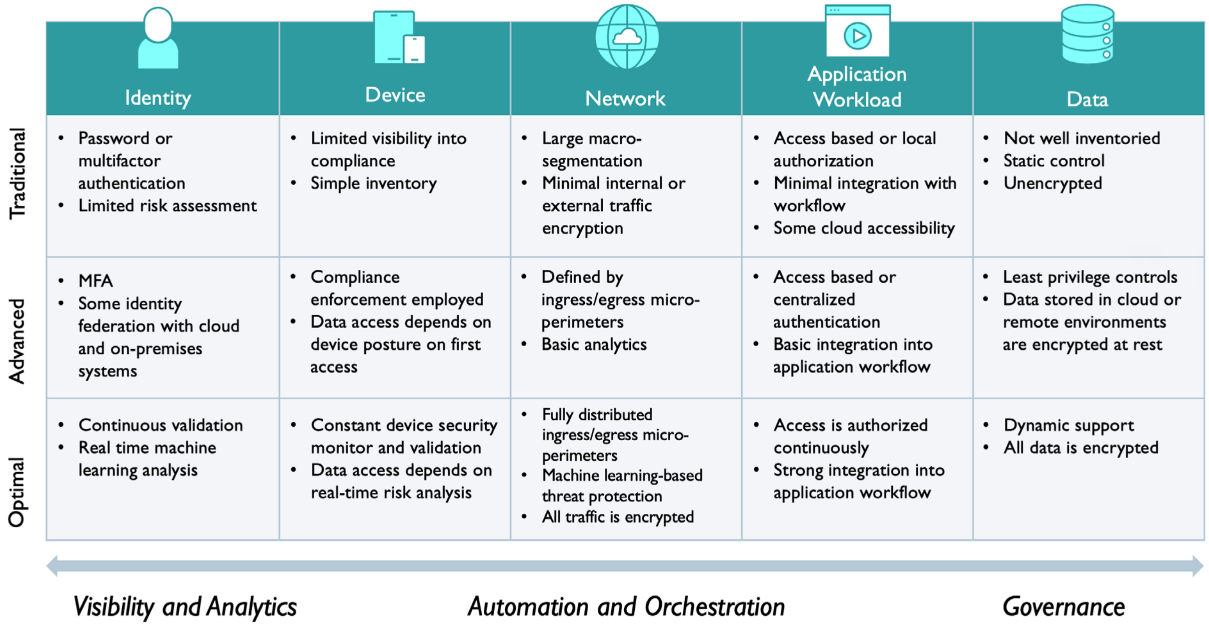
In this unit, you will learn about the preliminary activities required to successfully implement ZTA in an organization, as well as some common tools and frameworks for planning.

As mentioned by leading technology vendors as well as public agencies like NIST, the implementation of a ZTA — and more generally the ZT approach and its design principles — is not a one-off task, but rather a process that depends on a number of different factors, including the following:

- The maturity level of the organization's security approach, especially regarding asset
- mapping and classification and identity and access management
- The existing organizational culture, skills, and expertise
- The amount of existing legacy technology and its criticality
- Existing investments
- Available budget
- The complexity of service architecture and data flows
- The end goal and objectives of the organization

Risk management forms the core of any competent cybersecurity approach; subsequently, ZT migration tactics are highly dependent on the risk profile and risk appetite of the organization in question. For some, the ZT design principle will be applied to a limited set of assets; others will apply ZT to all assets across the organization. In either case, the migration to ZT will follow a risk-based staged approach with numerous iterations culminating in the final transformation into a ZT-driven organization.

For example, CISA's *ZT Maturity Model* provides a reference roadmap that organizations can use for charting their transition towards a ZTA.



	Identity	Device	Network	Application Workload	Data
Traditional	• Password or multifactor authentication • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based or local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based or centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analysis	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted

Figure 5 *CISA High-Level Zero Trust Maturity Model*[17]

The CISA *ZT Maturity Model* consists of five pillars and three cross-functional capabilities that together form the crucial foundations for ZT. Each pillar outlines specific examples of traditional, advanced, and optimal ZTA.

[17] Figure adpated from CISA, "Zero Trust Maturity Model," June 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

5.1 Organizational & Technical Planning

This section describes the high level set of actions each organization is likely to follow when implementing a ZTA.

5.1.1 Understand Your Needs

The first step in the ZT implementation process is the analysis of the organization's needs at a high level. The ZT champion's role is to guide the organization's decision makers in answering the following questions:

- Why should the organization consider adopting ZT?
- What are the critical assets to be protected?
- What is the mission relevance and criticality of ZT to the organization?
- What are the opportunity costs of adopting versus not adopting ZT?
- Is the organization a cultural fit for ZT? What are the existing gaps, if any?
- How urgent is the ZT adoption and migration?
- What are the success metrics?

5.1.2 Identify Key Stakeholders

The identification of key stakeholders is another foundational step in ZT organization and planning. Like other enterprise-wide risk analysis processes, the organization must ensure that all key stakeholders are engaged and surveyed—this ensures that all the perspectives, requirements, pain points, and possible constraints are collected and considered. Additionally, a critical element in ensuring successful adoption of ZT is support from senior leadership in the organization. Without this, ZT adoption efforts are typically disconnected and uncoordinated; while pockets of success may be realized within the organization, a comprehensive and effective enterprise approach cannot be achieved.

The key stakeholders that should be involved include, but are not limited to:

- Business/service owners
- Application owners
- Infrastructure owners
- Service architecture owners
- CISO/security teams
- Legal officers
- Compliance officers
- Procurement officers
- Any other relevant management

5.1.3 Assemble a Team

Effective team collaboration across multiple groups is critical when assessing the application and server access landscape across the organization. Groups must have cross-team communications channels in place, as well as processes for collating their findings for future planning — this may span multiple phases, based on a formalized roadmap. A detailed explanation of the various technical planning aspects is covered in the following section.

5.1.4 Define Current State

At a high level, the organization needs to determine the level of maturity of its internal approaches and processes, specifically in regards to the following:

- Governance
- Risk management
- Compliance
- Asset management
- Identity and access management
- Cybersecurity

Are these processes and approaches already fully optimized and automated, or are they still ad-hoc and informal? The level of maturity will help create a realistic plan for initial adoption of ZT principles, and a roadmap of future incremental evolutionary steps.

The organization should analyze each one of the seven ZTA pillars identified earlier in this training, in respect to existing processes, procedures and technical solutions related to ZT. These include, but are not limited to the following:

- Asset/data inventory and classification
- Authentication and authorization (e.g., MFA, RBAC/ABAC, federated identity)
- Network segmentation (e.g., micro/nano segmentation)
- Encryption and key management (e.g., for data at rest/in transit, confidential computing)
- Secure software development lifecycle (SDLC) management;

- Continuous integration and continuous delivery (CI/CD)
- Monitoring and analytics
- Transaction flows

Organizations with a greenfield and/or cloud-native IT infrastructures have the opportunity to build ZT into the design of their IT and OT systems from the ground up.

5.1.5 Set Goals

The understanding of the organizational and technological status quo will facilitate the definition of realistic short and medium/long-terms goals.

Is it the final objective of the organization to create a complete transformation to ZTA, or to establish a hybrid of ZTA and legacy perimeter-based controls? What's the percentage of resources that will be affected by the ZT migration?

Once the medium/long term expectations have been set, the organization should answer the following questions:

- What are the priorities (e.g, what needs to be addressed immediately)?
- Are there any quick wins/low hanging fruit?
- What are prerequisites or upstream dependencies?
- Are the existing foundations to start from?

Additionally, the following questions are critical for addressing key factors during the goal setting process:

- What is the level of executive mandate?
- What is the strategy?
- What is the budget?
- What is the roadmap?

5.1.6 Define the Use Cases

This step is a critical process to understanding the organization's needs — specifically, in defining an organization's need for ZTA (i.e., its use cases and applications).

5.1.7 Develop Collaboration Plan

Effective team collaboration is crucial for a successful ZTA deployment. To this end, organizations should establish a unified collaboration plan shared among all team members and stakeholders; this can take the form of a Kanban board or software-based collaboration platform. All project communications regarding the ZTA deployment should be centralized on this platform.

Once a collaboration plan is in place, ZTA planning and deployment teams can move on to addressing the following crucial action items and concerns:

> - Determine assets involved (e.g., data or services) and what needs protection– this can be determined through a risk analysis/assessment
> - Identify principals in scope (e.g., humans, machines, and processes)
> - Define IAM approach and methodology
> - Determine processes in scope including both existing processes that need to change and new processes needed
> - Select the service architecture
> - Design the data and process flow
> - Select the ZT implementation model and approach
> - Define policies, both new and changes to existing policies
> - Test/evaluate/select the technology or solution
> - Implement/develop/deploy/deliver the selected approach/solution
> - Monitor the ZT implementation for security and performance issues and plan for routine testing of ZTA security control
> - Adapt/review/improve based on the results of monitoring and continuous testing, adapt/review/improve the ZTA implementation
> - Extend the scope/reiterate the relevant steps of the process

5.2 Risks of Project Implementation

Any project that involves integrating new technologies or adopting novel approaches/methodologies bears some risk of failure; that said, the benefits of ZTA for improving the organization's security posture outweigh any perceived risks.

The following table covers some of the project risks that could arise while implementing a ZTA in an organization, as well as their impact and mitigation tactics.

Description	Implementation Risks	Impact	Mitigation
Failure of the ZTA operational elements such as PDP or PEP	Could hinder users and affected applications from authenticating/ operating properly.	Access to the secured assets could be compromised.	Deploying a high availability system and/or a failover mechanism.
New assessment and review criteria must be applied	Incorrect implementation and compromised operations.	As the new infrastructure solely depends on the architecture, an incorrect assessment of the solution may leave gaps.	A preplanned set of procedures and assessment steps created to validate the ZT implementation.

Security Operations	An interface between two systems in which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).	Security level is reduced, leaving potential gaps in defenses. Responses to security incidents will use incorrect procedures.	Comprehensive analysis of sensitive data and acceptable routes should be performed early in ZTA's design stages.
Remote API calls	Lack of API protocol support, API request inspection, data leakage monitoring, and API discovery (e.g., for shadow or zombie APIs).	Complexity in parsing API requests and the existence of deprecated versions.	Implement support for all relevant parsers. Provide the right controls to protect sensitive data like PII.
Hybrid implementation complexity resulting in environments that require additional effort/resources to operate, maintain, and support	Unforeseen resource misallocations that could significantly increase implementation costs and deadlines.	ZTA adoption and implementation will likely co-exist with legacy or non-ZTA environments, so operations/technology/infrastructure must support hybrid architectures.	Alerts for the same network event may be handled differently by an enterprise SIEM per environment.
ZTA integration with existing network and security infrastructure and operations can be challenging	Incompatibility with the legacy systems must be addressed before implementing the ZTA.	Interoperability with the legacy systems is paramount whilst implementing the ZTA.	ZTA integration can be carried out in incremental phases with validation processes and backout contingencies.

Fielding of partial or incomplete ZTA solutions	Fielding without adopting capabilities through the organizational maturity levels may create vulnerabilities that ZTA was intended to mitigate.	Vulnerabilities present within the ZTA will be targeted by adversaries, potentially resulting in technical and/or reputational exposures to the organization.	Validate that the ZTA adoption strategy is properly conceived to ensure that the intent to execute ZTA adoption through the organizational maturity levels is captured. Additionally, confirm that organizational leadership understands that the initial implementation will not be the final end state and will require continuous, iterative development through the maturity model.
Fielding of ZTA solutions without proper operational sustainment/ maintenance planning	Inconsistent enterprise baselines of fielded technologies, solutions/resources that are deteriorated or expended without effective results.	These risks expose the organization to adversarial threats, resulting in elevated technical and reputational risk to the organization.	Ensure that the ZTA adoption strategy properly covers both the initial deployment as well as long term costs and organizational restructuring necessary to support/ maintain ZTA on a long term basis.

Figure 6 *ZTA Project Implementation Risks*

6 Implementation Options of ZTA

In this unit, you will learn about the various ZTA implementation approaches defined by NIST SP 800-207, as well as some real-world ZTA implementation methods and their main characteristics. The options presented in this unit focus on the network architecture domain and align with the NIST approaches "ZTA Using Micro-Segmentation" and "ZTA Using Network Infrastructure and Software-Defined Perimeters". The primary ZTA implementation options covered in this unit are CSA's SDP, Zero Trust Network Access (ZTNA), and Google BeyondCorp.

6.1 NIST Approach to ZT

Organizations looking to adopt NIST's ZT model have several approaches at their disposal for designing their secure workflows. Each approach implements all of the ZT tenets outlined in Section 2.1 of NIST SP 800-207, and a fully-realized ZT solution will incorporate elements from all of the three NIST ZTA approaches:

> - ZTA using Enhanced Identity Governance
> - ZTA using Micro-Segmentation
> - ZTA using Network Infrastructure and Software Defined Perimeters

Depending on factors such as the organization's existing business flows, requirements, and cybersecurity maturity level, a particular approach may be more suitable for a given environment—in turn, the components used and main sources for policy rules will also vary accordingly.

As mentioned previously, this unit focuses on the NIST approaches for "ZTA Using Micro-Segmentation" and "ZTA Using Network Infrastructure and Software-Defined Perimeters''. Subsequent ZT training courses in this series provide a more comprehensive and expanded overview of NIST's approach to ZT.

6.2 Software-Defined Perimeter

CSA's SDP concept is an approach to enabling and enforcing ZT principles. The SDP architecture is designed to provide on demand, dynamically provisioned air-gapped networks: trusted networks that are isolated from all unsecured networks to mitigate network-based attacks.

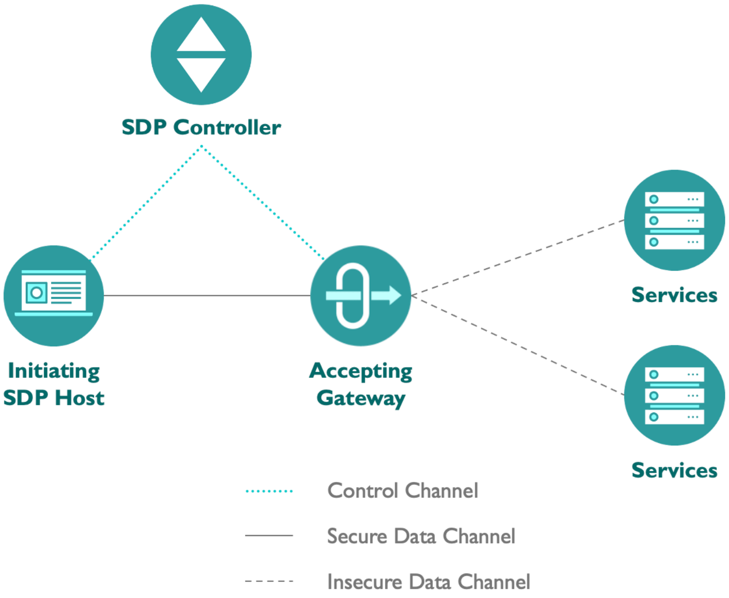


Figure 7: *SDP Pre-Vetting of Connections*[18]

6.2.1 Description

ZT implementations require the verification of anything and everything attempting to access assets, prior to authorization. Additionally, ZT requires continued evaluation of sessions and their risk levels during the entire connection's duration. As described in CSA's *Software-Defined Perimeter (SDP) and Zero Trust*, "a ZT implementation using SDP enables organizations to defend new variations of old attack methods that are constantly surfacing in existing network and infrastructure perimeter-centric networking models. Implementing SDP improves the security posture of businesses that face the challenge of continuously adapting to expanding attack surfaces that are increasingly more complex[19]." The enterprise must monitor the integrity and security posture of the assets. SDP enforces this trust strategy by enabling a default drop-all gateway until users/devices are authenticated and authorized to access the assets hidden by the gateway. By requiring the pre-vetting of connections, SDP enables complete control over who can connect, from which devices to what services, infrastructure, and other conditions and parameters.

As described in the *SDP Architecture Guide v2*, SDP consists of the following major components:

- The client/initiating host (IH)
- The service/accepting host (AH) — also referred to as the PEP per NIST's ZTA model
- An SDP controller to which the AH and IH both connect — also referred to as the PDP per NIST's ZTA model
- An SDP gateway that implements the drop-all firewall

[18] Figure adapted from Cloud Security Allaince, "Software-Defined Perimeter (SDP) Specification v2," 10th, March, 2022, https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2/

[19] Cloud Security Alliance, "Software-Defined Perimeter (SDP) and Zero Trust," 27th, May 2020, https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/

According to the *SDP Architecture Guide v2*, SDP works in the following manner:

> - The **SDP client** software on the IH opens a connection to the SDP. **IH** devices (e.g., laptops, tablets and smartphones) are user-facing, meaning the SDP client software is run on the devices themselves. The network can be outside the control of the enterprise operating the SDP.
> - **AH** devices accept connections from IH and provide a set of SDP-protecting/secured services. AH typically reside on a network under the enterprise's control (and/or under the control of a direct representative).
> - An **SDP gateway** provides authorized users and devices with access to protected processes and services. The gateway can also enact monitoring, logging, and reporting on these connections.

IH and AH host devices connect to an **SDP controller**: a device/appliance or process that secures access to isolated services by ensuring the following:

> 1. Users are authenticated and authorized
> 2. Devices are validated
> 3. Secure communications are established
> 4. User and management traffic remain separate on the network

The controller and AH are protected by SPA, making them invisible and inaccessible to unauthorized users and devices.[20] Six deployment options are available for implementing SDP:

> - Client-to-Gateway
> - Client-to-Server
> - Server-to-Server
> - Client-to-Server-to-Client
> - Client-to-Gateway-to-Client
> - Gateway-to-Gateway

6.2.2 Compliance with ZT Principles

The SDP conforms to the following ZTA principles:

> 1. The IH and users should first be authenticated and authorized by the controller before connecting to the AH. The AH is cloaked from the IH and its users until authentication is completed.
> 2. The SDP gateway applies the drop-all policy until the SPA from the IH is verified. The cryptographic mechanism behind the SPA ensures that only authorized devices can communicate with the AH's controller.
> 3. Every service and AH is protected with its own SDP gateway drop-all policy; communications from the other server should also follow the same access policies. IH and users can therefore only access resources to which they were explicitly granted permissions, ensuring

[20] Cloud Security Alliance, "SDP Architecture Guide v2," 7th, May 2019,: https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2

> adherence to the principle of least privilege.
>
> 4. The SDP controller and SDP gateway are the chokepoints for all access attempts and communications. Subsequently, they can provide continuous monitoring, logging and reporting of all network communications, to include both legitimate and suspicious access attempts.

6.2.3 Implementation Options

Several options are available for implementing a SDP: controllers may reside on-prem or in the public cloud, the gateway can be deployed on the servers (i.e., the AH) or an external node, and the SDP can be configured to protect a single service or multiple services.

The following are some critical best practices for implementing SDP:

> - Because they are single points of failure, controllers should be designed for high availability (HA) in order to withstand DoS/DDoS attacks and other similar malicious activity. HA strategies such as the use of multiple physical server instances with load balancing (e.g., domain name system load balancing) should be considered.
> - Gateways can block a service in the event of a case of failure or overload. Different load-balancing schemas can be used (e.g., the controller can act as a load balancer for gateways). Gateways are stateful SDP entities that can maintain mTLS sessions, so switching over to a different gateway may interrupt sessions across the tunnel.
> - SDP controllers may use an internal user-to-service mapping or a connection to a third party service (e.g., LDAP, directory service, or other on-premises/cloud-based authorization solution). Authorization is typically based on user roles and more fine-grained information, user or device attributes, or even the specific data element/data flow the user is authorized to access. In effect, the access policies maintained by the SDP controller can be informed by other organizational constructs such as enterprise service directories and identity stores. Per NIST, the dynamic ZT policies enforced by the controller are categorized as a ZT tenet.

6.2.3.1 Service Initiated (Cloud-to-Cloud)

An increasingly common use case for deploying a ZTA entails the use of multiple cloud providers. In this scenario, the enterprise manages a local network but uses two or more cloud service providers to host applications/services and data; occasionally, the application/service is hosted on a cloud service separate from the data source.

As depicted below, the application hosted in Cloud Provider A should directly connect to the data source hosted in Cloud Provider B. This enables better performance and ease of management, as the application isn’t forced to tunnel back through the enterprise network.

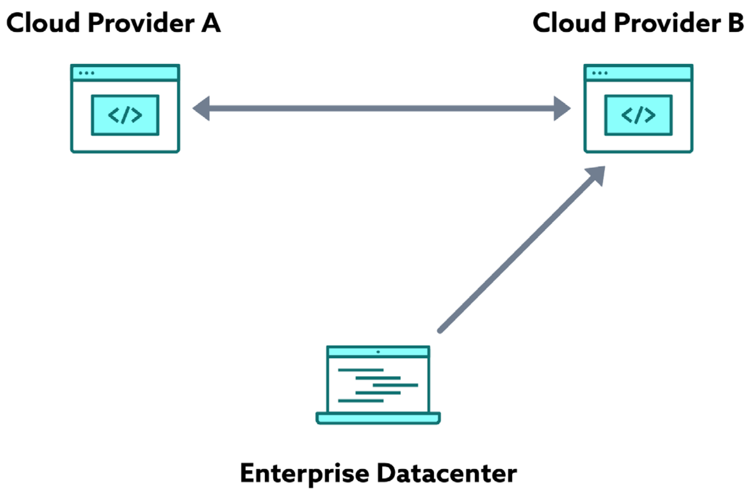


Figure 8: *Cloud-to-Cloud ZTA Service Initiation*[21]

This use case is the server-to-server implementation of the CSA *SDP Specification v2*. A more common example is Cloud Provider A cloud calling Cloud Provider B's LDAP service for authorization/ authentication, as part of SSO.

ZTA services are often set up in a mesh configuration. Meshed services lend themselves well to a multi-cloud environment since they facilitate service-to-service communication (to include micro-services communication) via a proxy.

6.2.3.2 Collaboration Across Boundaries

Cross-enterprise collaboration is another prominent ZTA use case. For example, a hypothetical project may involve employees from Enterprise A and Enterprise B. Enterprise A manages the project database but must allow certain members of Enterprise B to access the data.

To meet this requirement, Enterprise A can set up specialized accounts for Enterprise B employees to access the required data, denying access to all other resources; however, this approach can quickly become difficult to manage. Enrolling both organizations in a federated ID management system streamlines the configuration of these permissions, provided both organizations' PEPs can authenticate subjects in a federated ID community.

6.2.4 Characteristics

SDP's main advantages are its maturity and widespread adoption. Early on, prominent enterprises and leading institutions such as the DOD were supporters/adopters; today, organizations across all industries are implementing different flavors of SDP for varying purposes and environments, to include hybrid and multi-cloud deployments, VPN replacement, and securing IoT. Additionally, regular hackathons that test SDP's attack durability continue to add to its popularity.

[21] Figure adapted from NIST, "SP 800-207 Zero Trust Architecture," August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

SPA and mTLS are highly effective mechanisms for enforcing ZT principles without sacrificing user experience. SDP is in fact capable of providing robust security while simultaneously improving the user experience—especially when replacing legacy solutions. SDP is also relatively easy to implement and can complement existing solutions in place. Organizations are free to adopt a gradual implementation and/or migration to an SDP.

Because SDP is completely distributed and scalable, it can easily protect highly complex deployments (e.g., hybrid and multi-cloud environments). High availability is also built-in to SDP's architecture.

A major disadvantage of SDP is the requirement for client agent installation on each endpoint that connects to the SDP-protected deployment. Additionally, SDP primarily supports traditional user access methods to enterprise resources; API-based, micro-service, and serverless access methods are not well-supported by SDP.

6.3 Zero Trust Network Access

ZTNA is quite similar in spirit and form to CSA's SDP and Google's BeyondCorp, and all three have influenced each other. Though SDP is distinguished by its use of SPA, ZTNA's premise is nonetheless quite similar to SDP. In fact, some literature have ZTNA deriving its origins from SDP.

6.3.1 Description

ZTNA supports a paradigm where neither users nor the applications they access are sitting behind the perimeter. Often considered a VPN replacement, ZTNA allows users to access services from anywhere, anytime, from any device. ZTNA consists of two distinct architectures: endpoint-initiated ZTNA and service-initiated ZTNA.

Endpoint-initiated ZTNA is fairly similar to the original SDP specification. A lightweight agent is installed on the end-user's device and communicates with a controller, which in turn authenticates the user and provisions the necessary connections to the authorized applications. Because of this agent installation requirement, endpoint-initiated ZTNA is difficult to implement on unmanaged devices.

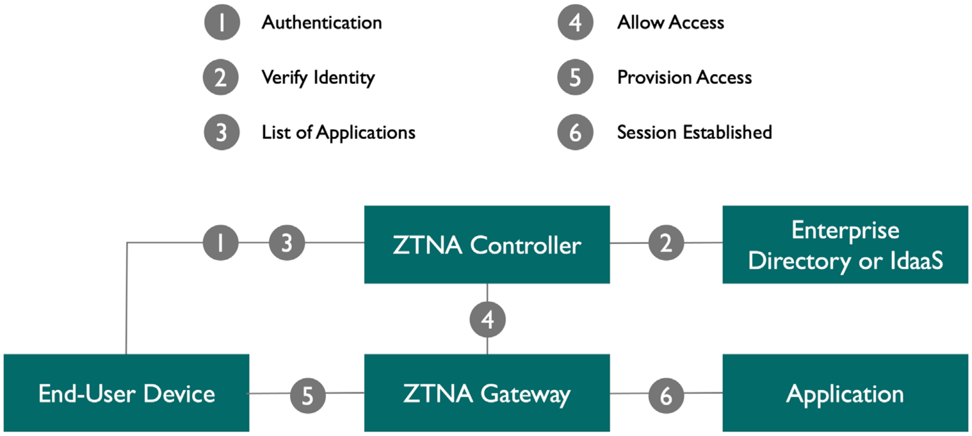


Figure 9: *Endpoint-Initiated ZTNA Communication Flow*[22]

[22] Figure adapted from Gartner, "Market Guide for Zero Trust Network Access (ZTNA)," 8th June, 2020, https://www.gartner.com/en/documents/3986053

On the other hand, service-initiated ZTNA uses a broker between the user and the application. In this case, a lightweight ZTNA connector sits in front of the service, which itself can be located in the data center or in the cloud. The connector establishes an outbound connection from the service to the ZTNA service broker. Upon authentication, traffic passes through the ZTNA broker, isolating services from direct access to unauthenticated users, effectively hiding them and preventing malicious activity like DDoS-type attacks. The service-initiated ZTNA option is suitable for unmanaged devices (e.g., bring your own device [BYOD]) or partner access.

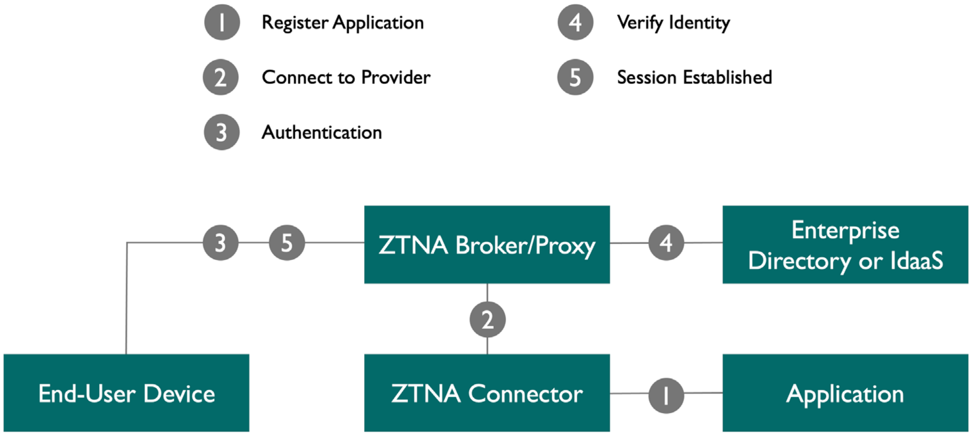


Figure 10: *Service-Initiated ZTNA Communication Flow*[22]

6.3.2 Compliance with ZT Principles

- ZTNA assumes a hostile user access environment. In fact it can operate from unmanaged devices and makes no assumptions about it being pristine.
- ZTNA assumes a breach. The user equipment is unmanaged and can be breached. The authentication and authorization is for a single session between the user and the services.
- Every access to the service is verified in the spirit of "never trust, always verify".
- ZTNA reduces the attack surface by hiding services behind brokers.
- Only authenticated users are allowed access if there is an explicit policy for them to have access.

6.3.3 Implementation Options

ZTNA can be used as a stand-alone product or as a service. In stand-alone mode, the broker runs on the customer's premises, and they are responsible for the deployment and management. Several IaaS cloud providers also offer managed ZTNA services for their customers.

6.3.4 Advantages

ZTNA offers benefits in user experience, agility, adaptability, and simplified policy management. When ZTNA is cloud-based, it has added benefits of scalability and ease of adoption. It is a much favored alternative to traditional VPNs where there is unhindered access once the VPN tunnel is established.

6.3.5 Disadvantages

Endpoint-initiated ZTNA is difficult when the user device is unmanaged (e.g., BYOD). ZTNA cannot guard against malicious actors that are already inside and co-resident with the service. It can only help in cases where the actor is outside of the perimeter where the services are hosted.
Secure access service edge (SASE) is a more recent technology that provides continuous inspection beyond the initial connection authorization and establishment. There is no provision in ZTNA of session revocation based on continuous inspection post establishment.

Policy management (e.g., authorization) is orders of magnitude more complex for programmatic access. The authentication, scale, as well as latency requirements vary significantly. For this reason, ZTNA is mostly applicable for user access and for VPN replacement use cases.

6.4 Google BeyondCorp

As described in the *SDP Architecture Guide v2*: "BeyondCorp is Google's internal network and access security platform, designed to enable their employees access to internal resources." Today, BeyondCorp Enterprise is available to organizations with Google-based IT infrastructures.

6.4.1 Description

The primary component of BeyondCorp is the web proxy: the chokepoint every user/device needs to traverse in order to access the organization's resources.

Some notable features of BeyondCorp include the following:

- Any access to protected resources are done via proxy
- Device and user identities are checked using a device inventory and user/group database
- 802.1x protocol is used to verify the managed devices and provide micro-segmentation
- An access control engine provides authorization for the organization's applications and services
- A data pipeline with additional information such as location, device/user trust levels, and more feeds into the access control engine

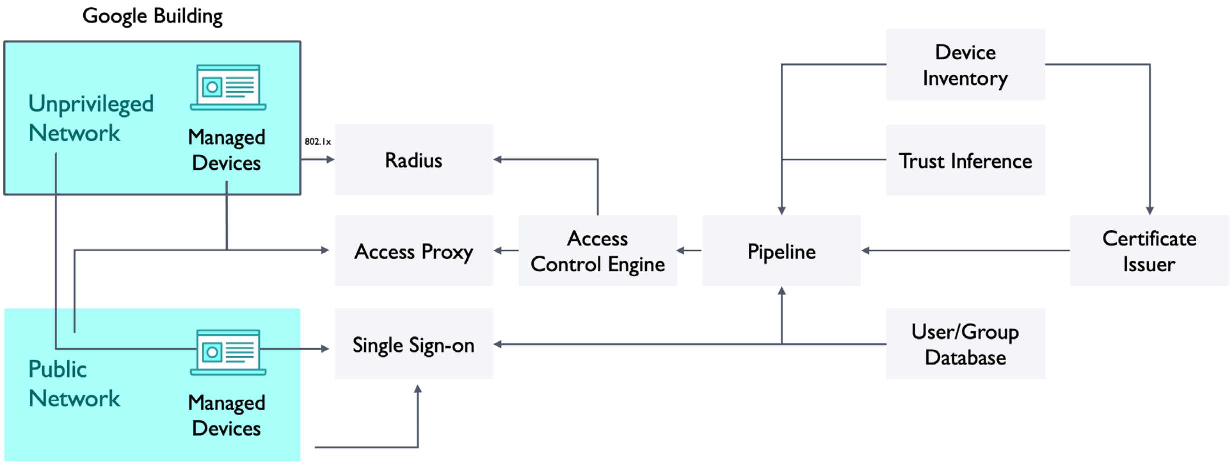


Figure 11: *BeyondCorp Components and Access Flow*[23]

[23] Figure adpated from Google, "BeyondCorp", https://www.beyondcorp.com/

6.4.2 Compliance with ZT Principles

BeyondCorp incorporates ZT principles as follows:

- The device/user should first be authenticated and authorized by the access proxy, prior to establishing a connection to the enterprise application—regardless of whether the device/user is located on the internal or external network.
- The access proxy denies any access request from unauthenticated users or devices.
- Each access request is handled separately by the access proxy, in line with the principle of least privilege.
- The access proxy is the choke point of all access attempts and communication; it should therefore be continuously monitored, with all network communications logged and report—to include both legitimate and illegitimate access attempts.

6.4.3 Implementation Options

As Google's proprietary implementation of ZTA, BeyondCorp offers limited implementation options. Some organizations implement a simplified version of BeyondCorp that only uses an access proxy, leaving out additional components like a device inventory and trust engine.

6.4.3.1 Service Initiated (Remote Application Access)

This implementation approach is in line with BeyondCorp model: a connector is deployed on the same network as the shared applications. Once the connector establishes and maintains a continuous outbound session to the provider's environment, users/devices can authenticate with the provider to access protected applications.

The provider can force the user through an authentication workflow before access is granted. This avoids direct access to the application, as the user/device is allowed to connect to the application server only after the authentication process (e.g., client-initiated ZTNA) is complete. Additionally, this model is agentless (i.e., agent software is not required on the connecting device), with application access over Hypertext Transfer Protocol/Hypertext Transfer Protocol Secure (HTTP/HTTPS)—at layer 7 of the OSI model.

6.4.4 Advantages

BeyondCorp doesn't require client agent installation on connecting devices, though devices should be registered in the device Inventory database and assigned a unique certificate.

6.4.5 Disadvantages

A fully-realized BeyondCorp implementation is less flexible and difficult to integrate with existing security mechanisms such as IAM. Additionally, BeyondCorp's lack of strong cryptographic controls such as SPA and mTLS makes it less secure than SDP, as these controls are required for implementing an *invisible cloud*. Unlike the SDP controller, BeyondCorp's access proxy is an in-line entity that handles both control and data traffic, making for a less scalable/secure model.

7 ZT Use Cases

In this unit, you will learn about various ZT use cases and how they vary — both architecturally as well as in terms of risk mitigation efficacy and limitations/dependencies.

A myriad of ZT use cases can be found across numerous industries. This section provides a non-exhaustive list of example applications. Each use case is broken out by the following:

- Use case description
- Security risks
- ZT mitigation of risks
- Limitations and dependencies

7.1 Remote Access & VPN Replacement

7.1.1 Use Case Description

Enterprises have historically provided employees secure remote access to the corporate network via VPN (i.e., an encrypted tunnel). With the widespread adoption of cloud services, employees now require additional remote access to services residing in one or more clouds and associated environments (e.g., virtual private clouds [VPCs] or virtual networks [VNets]). In the past, secure remote access was limited to applications hosted within the corporate data center. Today, organizations must also provide employees access to applications and services no longer hosted within their corporate data centers.

Traditional VPNs terminate at the organization's perimeter, enabling remote users to access the organization's resources, wherever they are located. The migration of IT resources to the cloud has led to the substantial performance degradation of VPNs. To address this issue and enable optimal access to remote services, organizations are creating encrypted tunnels to external enclaves using new technologies such as cloud proxies and SASE. This allows employees, contractors, and partners to securely access both internal services/applications as well as external IaaS/PaaS/SaaS offerings from other cloud service providers. ZTA bolsters the security posture of remote access processes by including SDP capabilities—namely SPA—in the communications between remote devices/users and external enclaves.

7.1.2 Security Risks

In most VPN solutions, users are allowed into the organizational network via a VPN gateway; once authenticated and granted access, the user has access to enterprise assets. Care must be taken to avoid violating the principle of least privilege. In addition, device authentication should be exercised prior to access, validating that the device has no malicious software or malware. For example, if a remote employee's device is infected with malware, that malware may impact all organizational assets accessible by this user once entering the network.

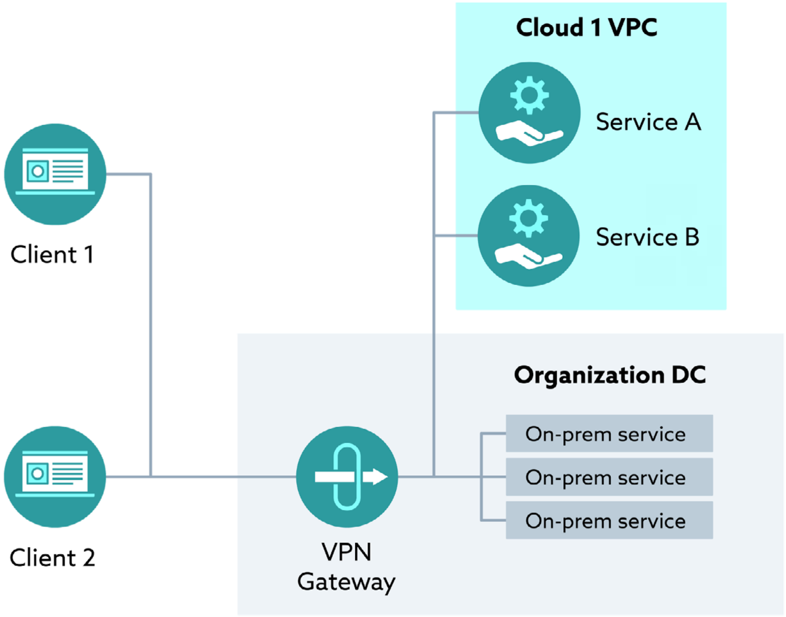


Figure 12: *Traditional VPN Gateway*

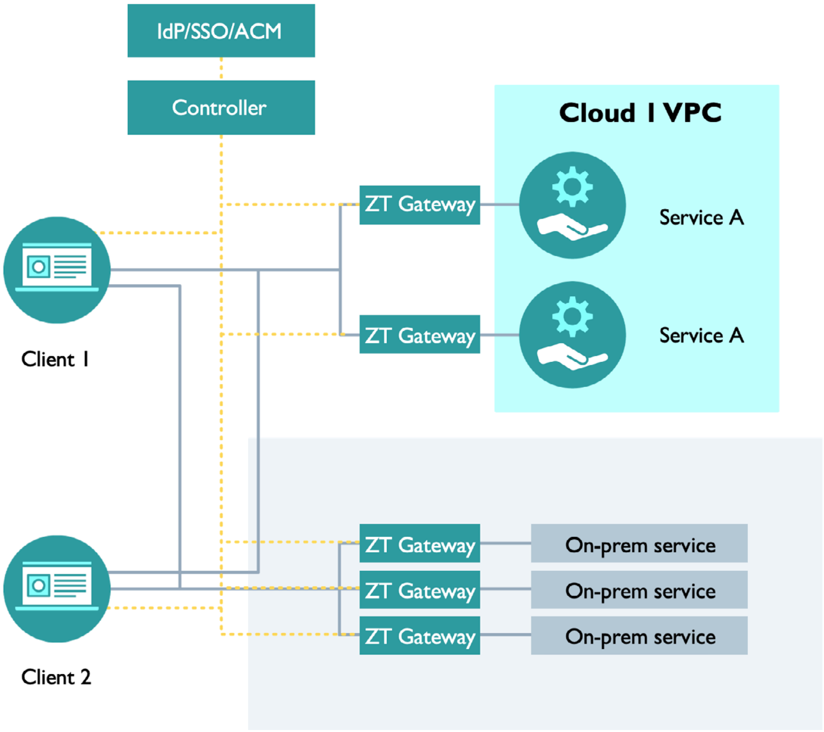


Figure 13: *Protection of Services by ZTA Gateway*

7.1.3 ZT Mitigation of Risks

ZTA effectively avoids or covers many of VPN's inherent security gaps through more granular, contextual security controls. For example, traditional VPN implementations have all user traffic going through a central VPN gateway before reaching a cloud application, creating both high latency as well as a single point of failure/compromise. Additionally, the same policies and security controls are applied to all users regardless of the application and user location.

In contrast, ZTA has each service separately protected by a ZT gateway; each client first connects to the controller, and only after authentication and authorization can they connect to the application over mTLS, via the gateway. Different policies and security controls can also be applied per application.

7.1.3.1 User Experience Impact

With VPN, users — especially mobile users — frequently experience delays, disconnections and connectivity problems. User connectivity to the internet is impacted as well, even if split tunneling is used. Split tunneling is a VPN feature that divides internet traffic and sends some of it through an encrypted VPN tunnel, routing the rest through a separate tunnel on the open network.

7.1.4 Limitations & Dependencies

A ZT environment is flexible and adaptable to change, as the ZT model is based on proven standards including mTLS, SAML, and X.509 certificates, among others. It can be combined with supplemental security systems such as data encryption and remote attestation systems due to its extensible nature. Coupling the evolved encrypted tunnel with the ZTA provides a path for evolution.

7.2 Micro-Segmentation

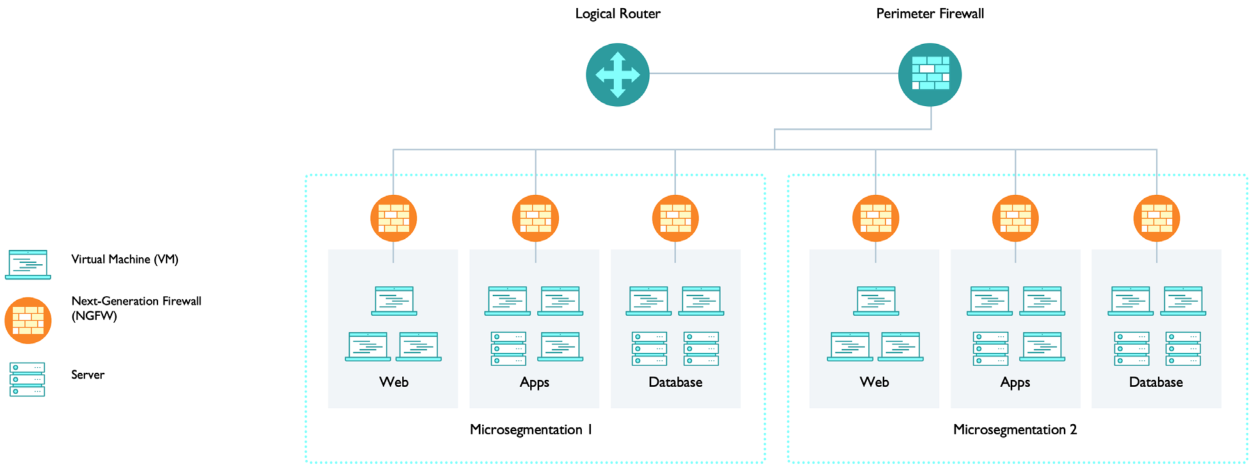


Figure 14: *Micro-Segmentation*[24]

7.2.1 Use Case Description

ZT enforces the separation of connections between the devices on a network. By requiring more granular, policy-based access for device-to-device connections, organizations can prevent the traffic from being visible — even to internal users. This is accomplished by creating dynamic, trusted network zones around applications, effectively hiding them from unauthorized users and devices. On a typical micro-segmented network, each of the connections between servers or devices on a network will be directed through separate layers of authentication and data traffic. Every device must

[24] Figure adapted from TechTarget, "What is Zero Trust? The Ultimate Guide to the Network Security Model," November 2020, https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network

initiate its own encrypted tunnel in order to communicate with servers. Thus, each connection is a separate network impenetrable by other hosts.

Micro-segmentation helps to ensure that device access is limited only to validated, authorized entities, and is highly effective in preventing the spread of a cyber attack across an environment, limiting the impact to the compromised device in question.

Micro-segmentation architectures can be deployed in both cloud environments and on-premise data centers.

7.2.1.1 Types of Micro-Segmentation

Time-based segmentation policies and controls typically become more granular over time. In fact, a direct correlation exists between the granularity of controls and the age of a system's technology stack. Some of the more common micro-segmentation architectural patterns that emerge include the following:

- Traditional network segmentation
- Data center (i.e., east-west) segmentation
- Application micro-segmentation
- Workload micro-segmentation

7.2.2 Security Risks

Once cyber attackers gain a foothold into the network, they typically move laterally in attempts to compromise other machines on the network. Network visibility is usually not restricted to privileged users/devices in VPN and corporate IT environments. The devices themselves are also prone to attacks, since some of these IT assets may be visible from the internet.

7.2.3 ZT Mitigation of Risks

ZT implementations do not implicitly trust any of the devices or applications on the network. Only trusted devices can initiate a connection following a SPA-based request, and later via an encrypted tunnel. The security posture of the IT environment is enhanced by the fact that the devices are completely hidden from unknown users, with users controlled/contained within a tunnel between devices.

7.2.4 Limitations & Dependencies

Because stringent control is maintained over users and devices and their respective access to each application or resource, the architecture and interactions between the devices require careful integration to reduce user/device validation-related latency. Also, the data flowing between devices are not verified/validated, though the connecting device's security posture and identity is verified/validated prior to the connection being granted.

7.3 Software as a Service & ZT

7.3.1 Use Case Description

The rise of the cloud and SaaS deployment models has given organizations access to an unprecedented array of scalable IT resources never before possible. This can fuel innovation and boost productivity, but it also introduces new IT security challenges beyond the traditional corporate firewall. Each SaaS solution in use introduces numerous challenges related to vendor risk management, data protection, access controls, user experience, auditing, monitoring, privileged access management, and more.

7.3.2 Security Risks

In the SaaS shared responsibility model, areas exist where visibility, governance, and control are reduced, leading to varied security risks; SaaS solutions therefore need to be understood, monitored, and reported for risk acceptance. For example, data protection compliance measures apply to SaaS providers, making risk acceptance critical to the implementation process, unless additional controls are added for risk mitigation. Business functions are choosing to procure and use SaaS applications without the knowledge or permission of IT. This phenomenon, also referred to as shadow (or stealth) IT, significantly increases the risk of data breaches and security incidents. Corporate IT should therefore specify in their service level agreements/contracts the requirement for controls with conformance reporting standards.

Due to the rise of the mobile workforce and the proliferation of cloud applications, network-centric security architectures are no longer considered adequate protection. Once a security perimeter is breached using various exploits and attack methods (e.g., phishing, malware, or compromised passwords), threat actors can move freely across other security layers and systems in search of vulnerable data.

Microservices and third-party APIs have also gained widespread adoption in the last decade, enabling SaaS offerings to be integrated with existing systems through publicly supported APIs. Organizations can simply subscribe to these services instead of building them from the ground up; however, this introduces supply chain risk into the ecosystem.

7.3.3 ZT Mitigation of Risks

Adopting the ZT SaaS management model is an effective approach to mitigating cyber risks inherent in SaaS services. This includes the enforcement of policy-based access control in SaaS applications, regardless of the user/device location, as well as the monitoring of all SaaS usage patterns.

In many cases, organizations bolster the security of their SaaS applications with single sign-on security (e.g., SAML) and IP-based access control with a CASB, which may negatively impact the user experience with increased latency and degraded performance. The ZT model adds stronger security to SaaS applications without impacting the user’s experience.

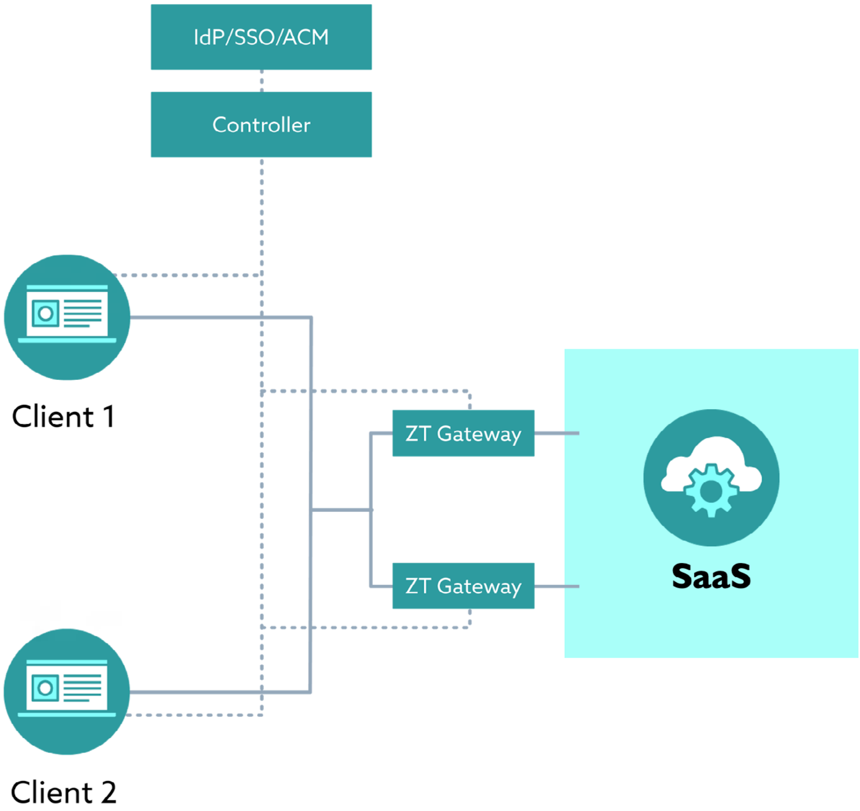


Figure 15: *ZT Model for SaaS Management*

7.3.4 Limitations & Dependencies

ZT SaaS control depends on a SaaS mechanism to control corporate account access. This includes the support of client SSO access lists for a SaaS service — effectively disabling direct access to SaaS services (i.e., bypassing the SSO access mechanism). ZT and SDP are limited in their ability to control the data flow inside a SaaS instance or between different SaaS applications.

7.4 Hybrid, Multi-Cloud, & ZT

7.4.1 Use Case Description

Hybrid clouds combine on-premises solutions or private cloud(s) with one or more public cloud services, with connectivity between each distinct service enabled through technologies like site-to-site VPN and private or dedicated circuits. Many organizations also adopt a multi-cloud strategy in order to leverage several cloud service providers; to this end, organizations can use public, hybrid, or private clouds as part of their overall cloud adoption strategy.

7.4.2 Security Risks

Using multi-cloud, hybrid cloud, or a combination thereof expands the organization's attack surface. Different public cloud providers use varying IAM models, security controls, and connectivity methods between VPCs or between VPCs and private clouds.

The broad level of network access inherent with hybrid and multi-cloud deployments conflicts with ZT's least privilege access model. For example, cloud providers may default to the most open access levels to maintain interoperability—in the case of a site-to-site VPN, the connection between a private and public cloud must be configured for any network access in order for devices on either end to communicate freely.

7.4.3 ZT Mitigation of Risks

If applied across all of an organization's cloud deployments, ZT can mitigate the security risks inherent in publicly exposed cloud services. The following are the guiding principles for accessing an organization's resources across different cloud providers and private clouds:

> 1. A device/users connection point on a particular network should not determine which cloud services are accessible.
> 2. Users should be identified, authenticated, and authorized prior to connecting initially, as well as before any subsequent connections to cloud resources.
> 3. Access to services and resources is granted based on what the organization knows about the user/device, regardless of which cloud service they are connecting to.
> 4. The same security controls (e.g., tunneling and encryption) are applied to both private and public clouds.

ZTA fulfills these requirements by hiding all the services and resources, regardless of their location. Users in turn have no access to those resources prior to completing authentication and authorization.

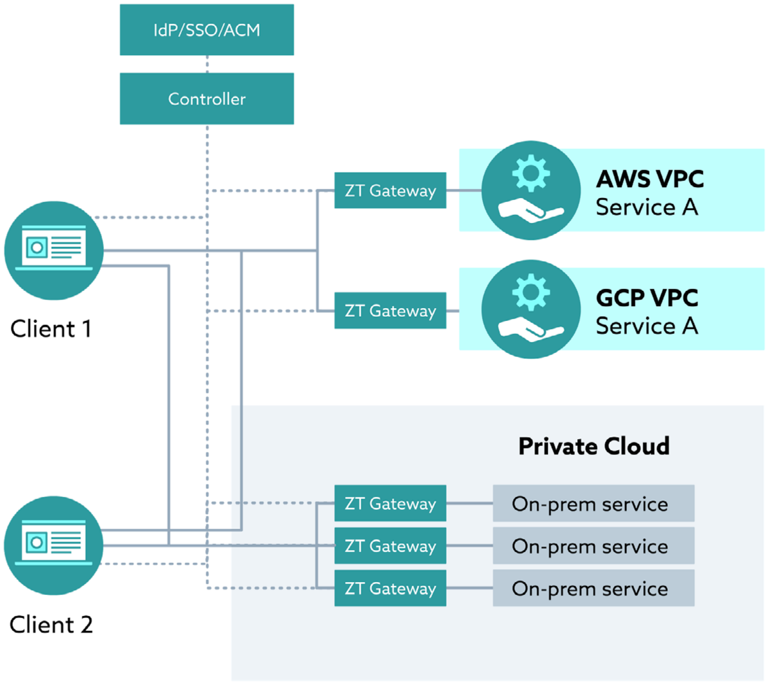


Figure 16: *ZTA Model for VPC and Private Cloud Deployments*

ZTA enforces the use of a mutually encrypted tunnel between the user device and the PEP, per individual service. The least privilege access model is enforced because the access policies are granular and resource/service based, versus network, cloud, or VPC-based.

7.4.4 Limitations & Dependencies

ZT improves the user experience with its distributed architecture, eliminating single choke points that may impose delays and result in single point failures. However, a truly cloud and vendor agnostic implementation of ZT may be difficult to implement due to the varying design patterns of competing cloud providers. For example, the implementation of SSO with Azure AD differs from Azure cloud; similarly, Google Cloud Platform (GCP) differs from an OpenStack-based private cloud.

Lastly, the interconnections between multi-cloud deployments and hybrid-to-public clouds are vendor-dependent. Best practices can be followed, but there isn't one standard protocol or implementation, hence it is not easily designed and implemented.

7.5 Operational Technology

OT primarily exists in industrial environments where processes are carefully regulated and managed to achieve a desired outcome. The systems associated with the OT environment are industrial control systems (ICS) and IIoT devices.

Traditionally, the OT environment was made up of closed, physically air-gapped networks and systems. However, newer OT solutions offer advanced features related to connectivity and automation (e.g., smart OT devices) for an expanding number of industry sectors. Reliance on OT-generated data and features is increasing rapidly, requiring organizations that adopt these new technologies to plan for accessible, secure, and resilient deployments.

Exposing smart OT devices to the internet or public networks can introduce external cyber threats into enterprise networks and environments. For this reason, ZT security best practices mandate that every connected entity has an identity and must be considered an integral part of the ZT Framework—users, devices, virtual infrastructure, and cloud assets[25].

The following section describes several use cases related to ICS and IIoT.

[25] CISA, "Alert (AA20-205A), 23rd, July 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-205a

7.5.1 Use Case Descriptions: CPS, IoT, IIoT, ICS

Per NIST SP 1500-201, cyber-physical systems (CPS) are an integration of physical components, networked systems, embedded computers and software that are linked together for information sharing to make a complete system[26]. CPS serves as the foundation for future smart services, smart cities, smart health care management, and more. As its name implies, CPS are cross-disciplinary in nature and provide seamless integration of cyber and physical systems.

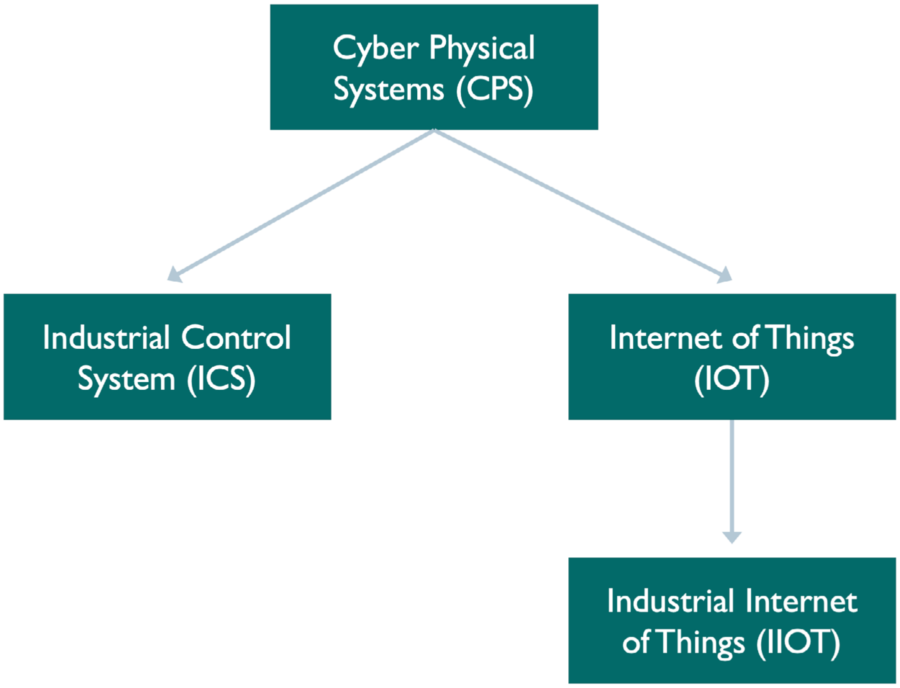

Cyber Physical Systems (CPS)
Industrial Control System (ICS)
Internet of Things (IOT)
Industrial Internet of Things (IIOT)

Figure 17: *Cyber-Physical System Types*

7.5.1.1 IoT & IIoT

IoT consists of a network of devices (i.e., things) equipped with software and/or sensors, connected to the internet via wifi or other wireless/wired technology. IoT devices can range from home devices (e.g., home automation solutions, smart doorbells) to industrial equipment (e.g., smart farming devices, assembly line robots). The IIoT is a subset of the IoT that specifically refers to industrial applications. IIoT systems enable industrial enterprises to realize improvements in efficiency and productivity through automation, continuous monitoring, and analysis.

[26] NIST, "SP 1500-201 Framework for Cyber-Physical Systems v1," June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

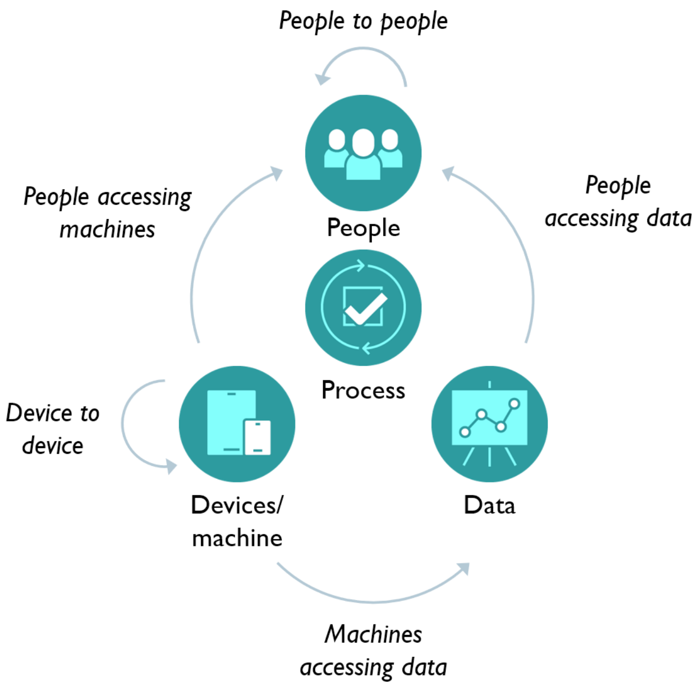


Figure 18: *IoT Entities and Communication Flows*

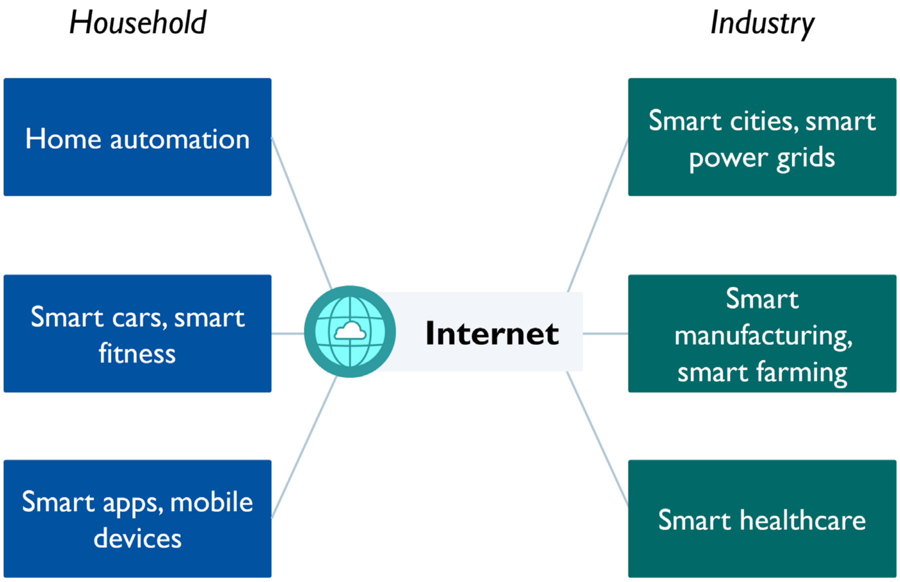

Household
Industry
Home automation
Smart cars, smart fitness
Smart apps, mobile devices
Internet
Smart cities, smart power grids
Smart manufacturing, smart farming
Smart healthcare

Figure 19: *IoT and IIoT Device Types*

7.5.1.2 Industrial Control Systems

Industrial control systems (ICS) encompass several types of control systems used in industrial production, including the following:

- Supervisory control and data acquisition (SCADA) systems
- Distributed control systems (DCS)
- Programmable logic controllers (PLC), often found in industrial sectors and critical infrastructures[27]

Additionally, commercial-off-the-shelf (COTS) networked devices are increasingly used with industrial automation and control systems (IACS). These COTS devices are typically inexpensive, efficient, and highly automated.

ICS systems typically consist of closed systems with components wired to system controllers in a bus topology. However, organizations increasingly require connectivity between their internal IT network and ICS systems — a requirement that introduces cyber-physical risk into the environment, as ICS systems may enable crucial facility processes for power, lighting, air conditioning, and water management. Organizations should therefore leverage ZT, SDP, and SPA to mitigate the cyber risk created by integrating ICS with an organization's TCP/IP networks.

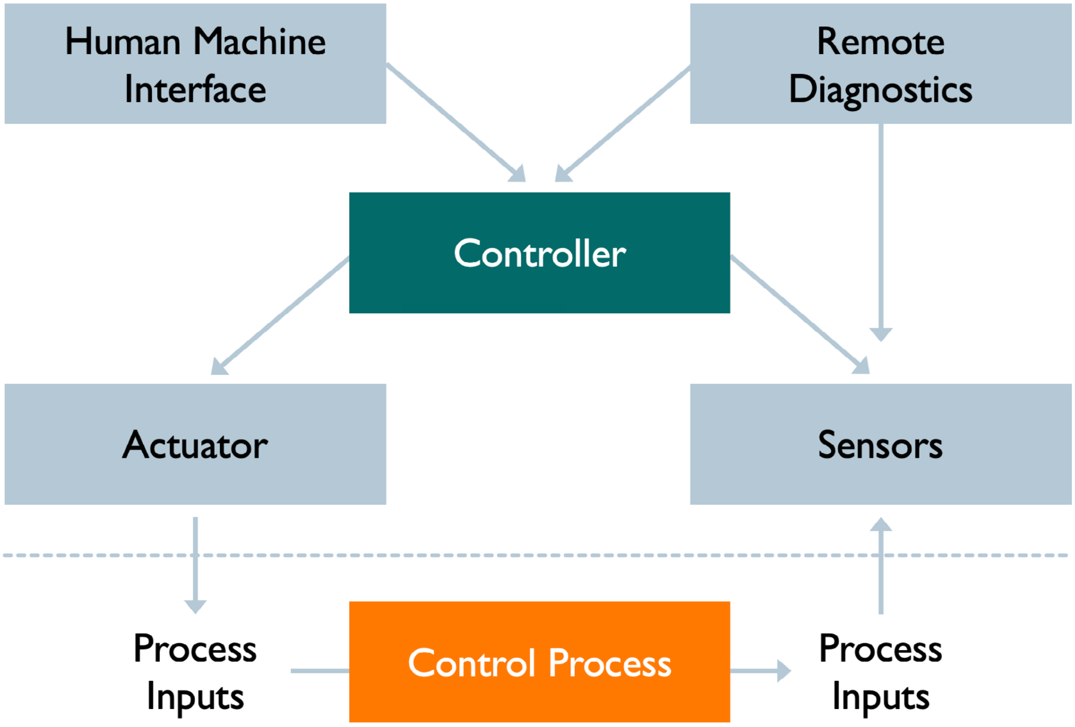


Figure 20: *ICS Communication Flows*[28]

[27] NIST, "SP 800-82 Guide to Industrial Control Systems (ICS) Security," May 2015, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[28] Figure adapted from NIST, "SP 800-82 Guide to Industrial Control Systems (ICS) Security," May 2015, https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

7.5.2 Security Risks

Because IIoT and ICS fall into the domain of industrial or cyber-physical systems, the tenets of confidentiality, integrity and availability (i.e., the CIA Triad) are prioritized differently than traditional IT systems. Instead, availability and integrity take precedence over confidentiality in order to first protect human life and physical assets (e.g., electrical grid). Unfortunately, this lack of confidentiality has led to various high profile incidents in which state-sponsored cyber attackers successfully compromised industrial and cyber-physical systems, causing significant physical damage.

As ICS are widely deployed in critical infrastructure environments such as water, oil/gas, and energy, threats to these systems have a potential for significant harm and loss of life. Subsequently, malicious actors such as terrorists, state-sponsored actors, hacktivists, and criminals have a keen interest in ICS-related vulnerabilities and exploits. To further complicate matters, security hardening and patching is difficult to carry out on these live systems due to their criticality and requirements for high availability.

ICS cyber attacks typically fall into one of the following categories:

> 1. Attacks that plant malicious software (e.g., Mirai malware) into devices to compromise adjacent resources on the internet/network
> 2. Attacks that take control of OT devices to steal data or perform unauthorized actions

Over 400 ICS vulnerabilities were disclosed in 2019[29], with over a quarter resulting from unpatched systems. According to United States Computer Emergency Readiness Team (US-Cert) and National Security Agency (NSA), the most common OT threat vectors and exploits include the following:

> - Spear phishing to gain a foothold into the organization's IT network, prior to pivoting to the OT network
> - Deploying commodity ransomware to encrypt data and adversely impact IT and OT networks
> - Connecting to publicly-accessible PLC that require no authentication for initial access
> - Exploiting weaknesses in commonly used ports and standard application layer protocols to communicate with controllers and download modified control logic
> - Using vendor-supplied engineering software and program downloads compromise systems
> - Modifying control logic and parameters on PLCs

7.5.3 ZT Mitigation of Risks

ZT allows organizations to enforce stronger IIoT device integrity and data confidentiality — at both control and data planes — while ensuring the availability of IIoT devices to overall system operations. Additionally, since IIoT devices are considered part of the ICS ecosystem, the ZT model can be leveraged for securely separating IT and OT using micro-segmentation, effectively isolating the business applications on the data plane from those on the control plane.

[29] DRAGOS, "2019 Year in Review ICS Vulnerabilities," 2019, https://www.dragos.com/wp-content/uploads/Year-in-Review-2019_ICS-Vulnerabilities-.pdf

If deployed and/or managed per ZTA specifications, the following OT device types stand to benefit from significant cyber risk reduction:

- **IIoT**: The SDP using SPA reduces the risk exposure of unauthorized user access and rogue IIoT devices (e.g., devices with hardcoded credentials) by enforcing both IIoT device authentication and adaptive risk-based user authentication (e.g., MFA for privileged actions on authorized IIoT devices). Since IIoT endpoints are largely IP-based with one or more network interfaces, standard monitoring solutions used in conjunction with SIEM/SOAR can be used to trigger alerts and defensive measures.
- **ICS**: By bringing ICS components (e.g., SCADA, human machine interface [HMI], DCS) into the fold of SDP with SPA, organizations can limit the highly vulnerable user access to these systems. More specifically, eliminating the bad practices of hardcoded credentials to enforce risk-based user authentication. Furthermore, ZTA with SDP and SPA affords a mechanism to implement micro-segmentation of the control plane of the ICS components with those of the data plane to mitigate the risks due to the interconnectedness of the business applications.

7.5.4 Limitations & Dependencies

In the context of OT, ZT's limitations primarily stem from device resource constraints and ICS systems' use of legacy and/or non-IP based communication protocols at the cyber-physical interface level. For instance, IIoT devices for utility applications may use ZigBee/IEEE 802.15.4 protocols at one interface to communicate with smart meters, while smart meters in turn may use IP protocols to communicate with utility management systems. Furthermore, ICS systems (e.g., SCADA, PLCs) rely on OT protocols such as ModBus or Profinet for control plane functionality. In these scenarios, applying ZT downstream at the edge of the control plane can be challenging.

Because sensors and IIoT controllers are usually limited in their ability to communicate/authenticate with the SDP, architects need to account for these limitations during the ZTA design phase. Ultimately, it may be necessary to incorporate an agentless micro-segmentation or external proxy-based approach, as an agent-based ZTA may not work with OT and IIoT devices.

Additionally, because OT and IIoT devices are harder to patch and/or upgrade, network-based micro-segmentation is critical for protecting adjacent systems against potentially vulnerable devices. Moreover, continuous scanning of traffic and deep packet inspection can be implemented to detect and block known attack types, even if they come from trusted entities.

7.6 5G

7.6.1 Use Case Description

Fifth generation (5G) wireless technology represents a major shift in communications networks, offering new capabilities and connectivity for applications such as smart cities, autonomous vehicles, remote healthcare, and more. With 5G, billions of devices, sensors, and systems will be able to autonomously connect to networks based on time sensitivity, latency, and processing requirements. In addition to faster speeds, greater capacity, and decreased delays, 5G will deliver improved mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (uRLLC).

5G uses tiny cells in addition to macro towers to function in the low, mid, and high frequency bands. In highly populated areas, the tiny cells function as signal repeaters, resulting in enhanced speed, network capacity, and reliability. The core network — the backbone of the global communications infrastructure — routes data and connects the different portions of the access network.

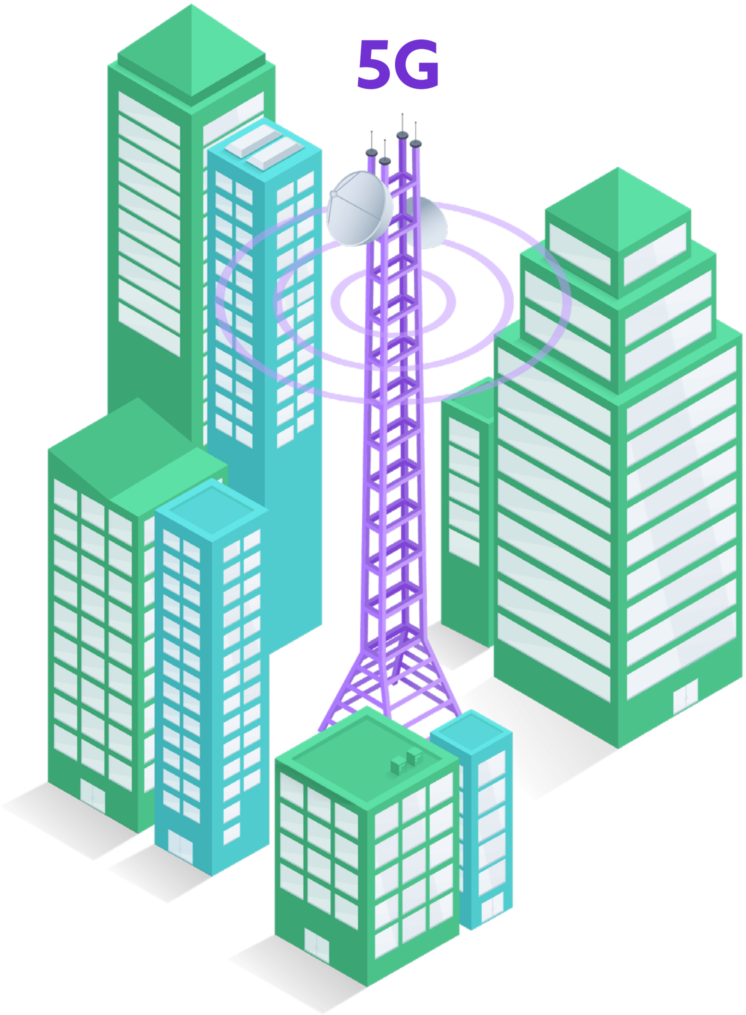


Figure 21: *Fifth Generation*

7.6.2 Security Risks

5G enables several groundbreaking technologies—most notably mobile edge computing (MEC)—that significantly improve application performance and enable unprecedented volumes of real-time data processing. Edge computing places compute and storage resources closer to the customer and/or within the telecommunications network infrastructure. This eliminates performance issues related to backhaul latency (i.e., having to continuously travel back/forth to a central data center).

Unfortunately, these new 5G-enabled configurations also introduce novel security risks into the environment; from the user equipment (UE) to the radio access network (RAN), the mobile edge computing (MEC) to the core nodes, 5G's open architecture makes for an expansive attack surface. Additionally, 5G networks leverage software-defined networking (SDN) technologies; if not properly secured, SDN assets could be compromised by malicious actors, who could in turn reconfigure network devices, monitor all communications, and alter application data.

Also, because 5G brings network devices, storage, computing hardware, and other IT infrastructure closer to the end user, physical security is even more crucial for augmenting ZTA security on the logical layer. It's worth noting this risk factor, along with many others, are common to 4G infrastructures as well, since existing telecommunications devices/equipment operating in remote locations usually lack strong physical security measures for hindering malicious tampering.

7.6.3 ZT Mitigation of Risks

As mentioned previously, 5G networks are software-defined, from the RAN to core and MEC nodes, and are therefore particularly vulnerable to lateral moving malware. ZT device protection can be used to verify the authenticity of software downloads and updates in the system, as well as access to log files.

Because 5G networks support internal compute as well as external cloud resources, they are also vulnerable to MITM attacks. ZT's security model ensures secure connectivity from a 5G UE to a MEC or the cloud. Lastly, ZT data protection can be deployed on IoT-to-5G gateway to ensure only authenticated and authorized systems can access protected data.

7.6.4 Limitations & Dependencies

Integrating ZT requires access to network drivers in 5G infrastructure equipment, which may be difficult to obtain in some vendor implementations. Additionally, ZT's concept of identity and authorization may prove difficult to implement in devices with generic software process names (e.g., store or save). Future ZTA versions will need to support an agentless approach to facilitate the myriad of edge configurations made possible by 5G, as not all edge devices can support agent software installations.

Conclusion

In this introductory ZTA course, we provided learners with an overview of ZT's origins — how it emerged against an increasingly complex technology landscape, why new computing paradigms such as the cloud and virtualization require novel approaches to security, and how early predecessors from both government and enterprise served as models for ZT's foundational concepts. We defined key terminology and principles, followed by an exploration of technical and business benefits that ZT can bring to organizations.

With the historical drivers, early developments, and context of ZTA established, we then outlined planning considerations for ZT adoptions. Learners were given an overview of implementation risks, implementation options, followed by representative use cases to get a sense of how ZTA bolsters security across various industries and application scenarios.

Glossary

For additional terms, please refer to our Cloud Security Glossary, a comprehensive glossary that combines all the glossaries created by CSA Working Groups and research contributors into one place.

Term	Definition	Source
802.1x	An IEEE standard for local and metropolitan area networks–Port-Based Network Access Control. IEEE 802 LANs are deployed in networks that convey or provide access to critical data, that support mission critical applications, or that charge for service. Port-based network access control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.	https://1.ieee802.org/security/802-1x/
Accepting Host (AH)	The SDP policy enforcement points (PEPs) that control access to any resource (or service) to which an identity might need to connect, and to which the responsible enterprise needs to hide and control access. AHs can be located on-premises, in a private cloud, public cloud, etc.	https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2/
Access	To make contact with one or more discrete functions of an online, digital service.	https://csrc.nist.gov/glossary/term/access
Active Directory (AD)	A Microsoft directory service for the management of identities in Windows domain networks.	https://csrc.nist.gov/glossary/term/active_directory
Air-Gapped Networks	An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).	https://csrc.nist.gov/glossary/term/air_gap

Application Programming Interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	https://csrc.nist.gov/glossary/term/application_programming_interface
Attribute-Based Access Control (ABAC)	An access control approach in which access is mediated based on attributes associated with subjects (requesters) and the objects to be accessed. Each object and subject has a set of associated attributes, such as location, time of creation, access rights, etc. Access to an object is authorized or denied depending upon whether the required (e.g., policy-defined) correlation can be made between the attributes of that object and of the requesting subject.	https://csrc.nist.gov/glossary/term/abac
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.	https://csrc.nist.gov/glossary/term/authentication
Authorization	The right or a permission that is granted to a system entity to access a system resource.	https://csrc.nist.gov/glossary/term/authorization
Brute Force Attacks	An attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.	https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
Cloud Access Security Broker (CASB)	On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement.	https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs
Control Plane	Used by various infrastructure components (both enterprise-owned and from service providers) to maintain and configure assets; judge, grant, or deny access to resources; and perform any necessary operations to set up communication paths between resources.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Controller (SDP Controller)	Determines which SDP hosts can communicate with each other. The controller may relay information to external authentication services such as attestation, geo-location, and/or identity servers.	https://downloads.cloudsecurityalliance.org/initiatives/sdp/Software_Defined_Perimeter.pdf
Data Plane	Used for communication between software components. This communication channel may not be possible before the path has been established via the control plane.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
Distributed Denial-of-Service (DDoS)	Involves multiple computing devices in disparate locations sending repeated requests to a server with the intent to overload it and ultimately render it inaccessible.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-15.pdf
Firewall	An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.	https://csrc.nist.gov/glossary/term/firewall
Gateway (SDP Gateway)	Provides authorized users and devices with access to protected processes and services. The gateway can also enact monitoring, logging, and reporting on these connections.	https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/
Hypertext Transport Protocol Secure (HTTPS)	A secure network communication method, technically not a protocol in itself, HTTPS is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.	https://iapp.org/resources/article/hypertext-transfer-protocol-secure/
Identity (ID)	The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.	https://csrc.nist.gov/glossary/term/identity

Identity and Access Management (IAM)	The set of technology, policies, and processes that are used to manage access to resources.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-203.pdf
Identity Provider (IdP)	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A cloud service provider may be an independent third party or issue credentials for its own use.	https://csrc.nist.gov/glossary/term/identity_provider
Initiating Host (IH)	The host that initiates communication to the controller and to the AHs.	https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf
Lightweight Directory Access Protocols (LDAP)	A networking protocol for querying and modifying directory services running over TCP/IP.	https://csguide.cs.princeton.edu/email/setup/ldap
Man-in-the-middle (MITM) attacks	An attack where the adversary positions himself in between the user and the system so that he can intercept and alter data traveling between them.	https://csrc.nist.gov/glossary/term/mitm
Micro-segmentation	Is the technique of creating secure zones within a data center and cloud deployments that allow the organization to separate and secure each workload. This makes network security more granular and effective. These secure zones are created based on business services, and rules are defined to secure information workflow.	https://www.techtarget.com/searchnetworking/definition/microsegmentation
Multi-factor Authentication (MFA)	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).	https://csrc.nist.gov/glossary/term/multi_factor_authentication

Mutual Transport Layer Security (mTLS)	An approach where each microservice can identify who it talks to, in addition to achieving confidentiality and integrity of the transmitted data. Each microservice in the deployment has to carry a public/private key pair and uses that key pair to authenticate to the recipient microservices via mTLS.	https://cheatsheetseries.owasp.org/cheatsheets/Microservices_security.html#mutual-transport-layer-security
Network Access Control (NAC)	A method of bolstering the security of a private or "on-premise" network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
Network Segmentation	Splitting a network into sub-networks, for example, by creating separate areas on the network which are protected by firewalls configured to reject unnecessary traffic. Network segmentation minimizes the harm of malware and other threats by isolating it to a limited part of the network.	https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary
Open Systems Interconnection (OSI)	Qualifies standards for the exchange of information among systems that are "open" to one another for this purpose by virtue of their mutual use of applicable standards.	https://www.ecma-international.org/wp-content/uploads/s020269e.pdf
Phishing	A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.	https://csrc.nist.gov/glossary/term/phishing
Policy decision point (PDP)	Mechanism that examines requests to access resources, and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the particular requester who issued the request under consideration.	https://csrc.nist.gov/glossary/term/policy_decision_point
Policy enforcement point (PEP)	A system entity that requests and subsequently enforces authorization decisions.	https://csrc.nist.gov/glossary/term/policy_enforcement_point

Port	Another essential asset through which security can be breached. In computer science, ports are of two types - physical ports (which is a physical docking point where other devices connect) and logical ports (which is a well-programmed docking point through which data flows over the internet). Security and its consequences lie in a logical port.	https://www.w3schools.in/cyber-security/ports-and-its-security/
Public Key Infrastructure (PKI)	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.	https://csrc.nist.gov/glossary/term/public_key_infrastructure
Role Based Access Control (RBAC)	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.	https://csrc.nist.gov/glossary/term/role_based_access_control
Security Assertion Markup Language (SAML)	A protocol consisting of XML-based request and response message formats for exchanging security information, expressed in the form of assertions about subjects, between online business partners.	https://csrc.nist.gov/glossary/term/security_assertion_markup_language
Security Orchestration Automation and Response (SOAR)	Refers to technologies that enable organizations to collect inputs monitored by the security operations team. SOAR tools allow an organization to define incident analysis and response procedures in a digital workflow format.	https://www.gartner.com/en/information-technology/glossary/security-orchestration-automation-response-soar

Single Packet Authorization (SPA)	Can authenticate a user to a system for simple remote administration. It is a protocol for allowing a remote user to authenticate securely on a "closed" system (limited or no open services) and make changes to or run applications on the "closed" system.	https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-madhat.pdf
Software-Defined Network (SDN)	An approach to computer networking that allows network administrators to manage network services through abstractions of higher-level functionality. SDNs manage the networking infrastructure. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).	https://ieeexplore.ieee.org/abstract/document/6819788
Software-Defined Perimeter (SDP)	A network security architecture that is implemented to provide security at Layers 1-7 of the OSI network stack. An SDP implementation hides assets and uses a single packet to establish trust via a separate control and data plane prior to allowing connections to hidden assets.	https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero-trust/
Transmission Control Protocol (TCP)	A transport protocol that is used on top of IP to ensure reliable transmission of packets. TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets. Since TCP is the protocol used most commonly on top of IP, the Internet protocol stack is sometimes referred to as TCP/IP.	https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:the-internet/xcae6f4a7ff015e7d:transporting-packets/a/transmission-control-protocol--tcp
Transmission Control Protocol/Internet Protocol (TCP/IP)	A set of protocols covering (approximately) the network and transport layers of the seven-layer Open Systems Interconnection (OSI) network model.	https://www.gartner.com/en/information-technology/glossary/tcpip-transmission-control-protocolinternet-protocol

Transport Layer Security (TLS)	A cryptographic protocol, successor to SSL, that provides security for communications over a computer or IP network.	https://csrc.nist.gov/glossary/term/transport_layer_security
Virtual Private Network (VPN)	A virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and IP information transmitted between networks or between different nodes on the same network.	https://csrc.nist.gov/glossary/term/virtual_private_network