MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

ZERO TRUST ARCHITECTURES: ARE WE THERE YET?

Deirdre Doherty and Brian McKenney
The MITRE Corporation

JUNE 2021

Abstract

The movement towards Zero Trust Architectures (ZTA) aligns with cybersecurity modernization strategies and practices to deter and defend against dynamic threats both inside and outside traditional enterprise perimeters. The "Executive Order on Improving the Nation's Cybersecurity" released from President Biden on May 12, 2021 directs executive agencies to "develop a plan to implement Zero Trust Architecture." The implementation of ZTA requires the integration of existing and new capabilities, as well as buy-in across the enterprise. Successful implementations will require multi-year planning that includes determination of drivers and use cases, policy development, architecture development, technology readiness assessment, pilots, user training, and phasing of deployments. This ZTA Tech Watcher report provides background, applicability and benefits to organizations, outstanding challenges and issues, and recommendations.

Executive Summary

Zero Trust Architectures (ZTA) for enterprise security are gaining momentum across many business sectors and government agencies. The large-scale migration of applications to cloud- hosting platforms and an increasingly mobile workforce cause the current network-centric security architectures, which are dependent on perimeter gateways, to be inefficient at best. These architectures have security vulnerabilities because they assume that once users are admitted to the network, they have wide freedom to access resources.

ZTA seeks to mitigate these problems by distributing protection capabilities closer to sensitive resources and enforcing dynamic end-to-end protections. ZTA provides fine-grained access control to resources based on authenticating identity, device, location, and behavior, and applying least privilege policies. It replaces broad network access policies by authorizing, encrypting, and logging each end-to-end transaction, and reduces lateral movement via micro-segmentation and software-defined perimeters. ZTA can provide several potential benefits in improving security, resiliency, and efficiency.

It is important to recognize that ZTA is both a strategy and architectural approach, not a single product or a technology. A comprehensive architecture requires integration of multiple vendors' products and solutions to address requirements and desired use cases. There has been an upswing of ZTA products and services from commercial vendors and service providers, but large-scale deployments are still few.

The implementation of ZTA is complex and will require multi-year transition plans that include determination of drivers and use cases, policy development, architecture development, technology readiness assessment, pilots, and user training, and phasing of deployments.

To determine ZTA technical readiness, an organization must assess maturity of policy management; data/asset inventory and sensitivity; Identity, Credential, and Access Management (ICAM) tools and processes; network segmentation; device management; application and data security; and security operations.

Implementation must be done incrementally to avoid disruptions to business services and the user experience. ZTA may have to co-exist with current capabilities for a long transition period, requiring additional resources. Existing implementation challenges include:

- Development and management of fine-grained access policies
- Asset inventory and sensitivity analysis
- Interoperability and integration of varied implementation approaches
- Security operations changes, including log collection, situational awareness, and incident response
- Potential new attack surfaces and adversary tactics and techniques
- Scalability and performance for large, federated networks
- Potential changes to existing workflows.

ZTA is a promising new enterprise security strategy and approach, but the integration and transition are complex. Executive support, careful planning, piloting, employee feedback, phased implementation, and investment into addressing the challenges will greatly smooth the transition.

Acknowledgments

The authors would like to thank Mick Costa, Eileen Division, Jacob Kline, and Andy Radle for their insightful contributions to this document.

Contents

List of Figures

Introduction

The adoption of Zero Trust principles for enterprise security architectures continues to garner high interest and momentum across many business sectors and government agencies. Users are increasingly mobile and need to be able to access on-premises and cloud resources efficiently and conveniently from anywhere, subject to appropriate security policies. This migration toward Zero Trust Architectures (ZTA) is a longstanding trend, but the migration has been accelerated by requirements to support a remote workforce per COVID-19 restrictions.

Enterprise infrastructures and resources are moving outside of traditional perimeters as a function of information technology (IT) modernization, including rapid migration to cloud service providers, software-defined networks, and managed security services. The extension of enterprise boundaries and movement of assets represent additional attack surfaces for an adversary to exploit and gain access to resources that may not be adequately protected. Currently, adversaries that successfully breach traditional perimeter defenses can easily move across the enterprise and expand their access and control [1].

The confluence of the above factors drives the need for more effective cybersecurity approaches. ZTA seeks to improve enterprise cybersecurity and operational efficiencies by distributing protection capabilities closer to sensitive resources and enabling added flexibility for securing end-to-end network connections. It is important to recognize that ZTA is a strategy and architectural approach; it is not a product or a technology. No complete ZTA solution is currently available from a single vendor; a comprehensive architecture requires integration of multiple vendors' products and solutions, including application design and development.

> THE EXTENSION OF ENTERPRISE BOUNDARIES AND MOVEMENT OF ASSETS REPRESENT ADDITIONAL ATTACK SURFACES FOR AN ADVERSARY TO EXPLOIT AND GAIN ACCESS TO RESOURCES THAT MAY NOT BE ADEQUATELY PROTECTED.

ZTA guiding principles [2] are:

- Never trust, always verify.
- Employ a least privilege access strategy.
- Assume breach.

To support these principles, ZTA employs technologies to:

- Authenticate and authorize every transaction using least privilege and dynamic access policies based on available data sources (e.g., identity, location, device posture, and user behavior).
- Restrict access to resources based on sensitivity.
- Provide end-to-end encryption of data — both at rest and in transit.
- Distribute perimeter functions closer to applications and data.
- Inspect and log all traffic for visibility and threat-based monitoring.

Additional information on Zero Trust background, concepts, principles, and architectures can be found in several references [2], [3], [4], [5], [6], [7], [8].

Business Drivers and Benefits

Current network-centric security architectures, dependent on perimeter gateways, have security vulnerabilities because they assume that once admitted to the network, users have wide freedom to access resources. It should be assumed that determined adversaries will breach traditional perimeters through various techniques, such as phishing, supply chain, and malicious insiders.

A significant driver for the move to ZTA is the need for infrastructure modernization and migration of applications/services to cloud- hosting services due to their compelling economics, scalability, and flexibility [9]. In addition, workers and other users of organizational resources are increasingly mobile and remote. Perimeter-based security architectures can create inefficient traffic routing and performance/capacity bottlenecks. ZTA's distributed architecture is better adapted to provide connectivity more efficiently, by avoiding routing remote user traffic through the enterprise network before accessing cloud services.

In today's dynamic economy, high workforce turnover and contracting drive the need to quickly provision or revoke user accesses and permissions via agile Identity, Credential, and Access Management (ICAM) processes and tools. Users frequently have multiple devices, both managed and personally owned "Bring Your Own Device" (BYOD). ZTA provides dynamic access policies based on multiple factors and context. This allows for fine-grained access control to resources based on identity, device, context, behavior, and applying least privilege policies.

Growing adversarial sophistication of Tactics, Techniques, and Procedures (TTPs) and threats by insiders, whether malicious or simply careless, require the implementation of least privilege and modernization of the security architecture. ZTA utilizes micro-perimeters and moves security services closer to protected resources. This constrains insiders' or adversaries' ability to execute and perform TTPs that require lateral movement. Least privilege mechanisms, application segmentation, and dynamic access controls further restrict unauthorized access to resources. Central to this capability are policy decision and enforcement points that manage and control access to specific resources.

There is a growing need to protect privacy and intellectual property from unauthorized access. ZTA improves confidentiality of data via end-to-end encrypted transactions and protection of data in transit and at rest.

Capabilities

Instead of assuming that elements of an IT system are inherently trustworthy, ZTA defines characteristics needed for trust and verifies those characteristics before allowing an interaction. Elements of an information system need to demonstrate they satisfy the characteristics required to establish trust according to the six pillars of a Zero Trust security model (Users, Devices, Network, Applications, Automation, and Analytics) [7].

As shown in Figure 1, a target ZTA comprises several capabilities that contribute to overall end-to-end security. The primary components are discussed further below.

Governance and Policy

To implement ZTA, a governance structure needs participation from stakeholders, including senior leaders, system owners, business process stewards, cybersecurity engineers, and risk managers. Achieving Zero Trust requires implementing least privilege policies that support specific business mission objectives. These policies can be complex and time-consuming to develop, especially as policies are defined for each resource. Care must be taken to avoid disrupting existing workflows for access requests.

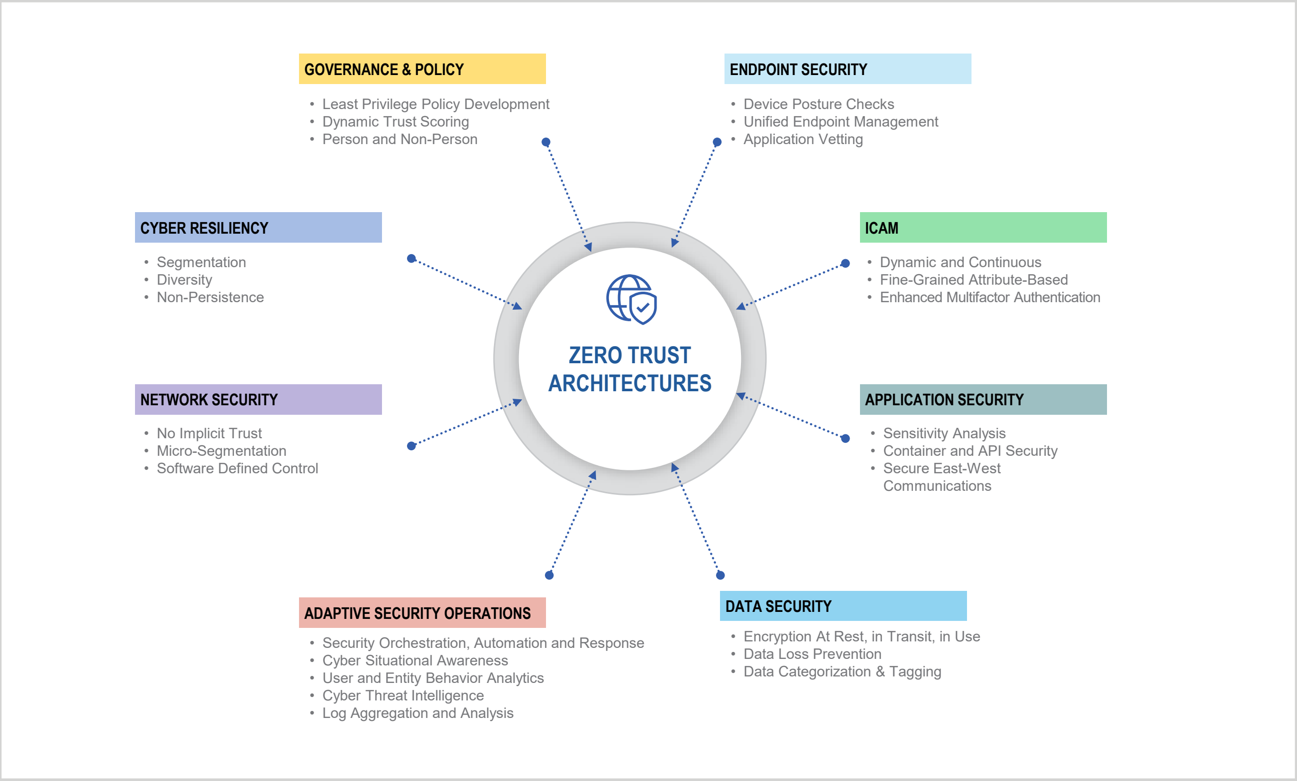

GOVERNANCE & POLICY
• Least Privilege Policy Development
• Dynamic Trust Scoring
• Person and Non-Person
ENDPOINT SECURITY
• Device Posture Checks
• Unified Endpoint Management
• Application Vetting
CYBER RESILIENCY
• Segmentation
• Diversity
• Non-Persistence
ICAM
• Dynamic and Continuous
• Fine-Grained Attribute-Based
• Enhanced Multifactor Authentication
ZERO TRUST ARCHITECTURES
NETWORK SECURITY
• No Implicit Trust
• Micro-Segmentation
• Software Defined Control
APPLICATION SECURITY
• Sensitivity Analysis
• Container and API Security
• Secure East-West Communications
ADAPTIVE SECURITY OPERATIONS
• Security Orchestration, Automation and Response
• Cyber Situational Awareness
• User and Entity Behavior Analytics
• Cyber Threat Intelligence
• Log Aggregation and Analysis
DATA SECURITY
• Encryption At Rest, in Transit, in Use
• Data Loss Prevention
• Data Categorization & Tagging

FIGURE 1: TARGET CAPABILITIES OF A ZTA

Cyber Resiliency

ZTA incorporates such cyber-resiliency techniques as segmentation, diversity, non-persistence, and privilege restriction. These techniques enable enterprises to better anticipate, withstand, recover from, and adapt to the effects of adversary threat actions [10].

Network Security

ZTA utilizes network security protocols, such as Transport Layer Security (TLS), to implement authentication, confidentiality, and integrity protection. Network micro-segmentation is supported by the ability to further isolate end-to-end transactions between designated users/devices and protected resources. This results in the creation and management of secure logical networks that may run over multiple untrusted networks.

Endpoint Security

Endpoint security is a key component of ZTA because access depends on endpoint attributes, such as device security posture, recognition as part of asset inventory, and ability to vet and applications or services running on the endpoint. Behavior-based detection and threat intelligence may also be employed as part of endpoint security.

Adaptive Security Operations

Due to the dynamic nature and distributed nature of ZTA, security operations will need to leverage Security Orchestration, Automation, and Response (SOAR) concepts and systems [11]. Additionally, security operations are enabled by cyber-situational awareness of events and threat intelligence. User and Entity Behavior Analytics [12] are a potential mechanism for strengthening security by evaluating trust levels based on multiple contextual factors.

Operations should include captures of logs/events for end-to-end monitoring and analytics, which can be enhanced via machine-learning techniques.

ICAM

Identity, Credential, and Access Management (ICAM) [13] is a critical capability for ZTA that should be dynamic, fine-grained, and multi-factor, based on user and device (Non-Person Entity) identities, credentials, state, behavior, and attributes. ZTA leverages and integrates ICAM services to support mutual authentication and dynamic policy enforcement.

Application Security

Applications should be categorized based on sensitivity and user groups that need access. Applications are increasingly containerized and provide application programming interfaces (APIs), which must be secured. Zero Trust access patterns typically support "north-south" communications (e.g., user/device to protected resource); however, "east-west" communications between application components (e.g., cloud-to-cloud, server-to-server) must also be authenticated and secured.

Data Security

ZTA ensures data associated with a protected resource is accessed by only an authenticated and authorized user and device. Encryption for the data at rest and in transit is also addressed. Ideally, data should be categorized and tagged using metadata. Data Loss Prevention [14] may be integrated to detect and prevent the unauthorized transmission of sensitive data.

ZTA Reference Architecture

The core components of the ZTA reference architecture are users and devices connecting to a protected resource over an untrusted network. The protected resource may reside in a cloud, data center, or edge of an enterprise. A ZTA reference architecture is shown in Figure 2 and the main components of the control plane are further described below [6].

The Policy Decision Point (PDP) contains logic to compare dynamic attributes against configured policies to authorize user/device access to resources. The Policy Enforcement Point (PEP) sits in front of the protected resource and uses control information from the PDP to determine whether to allow a connection [6]. Device certificates are typically provisioned for the PDP, PEP, users and devices to ensure communications are fully authenticated and encrypted. The PDP will communicate these policies to the PEP over the control (management) plane.

The PDP may support different policies per type of endpoints, such as non-enterprise owned, non-enterprise managed, and enterprise managed. Endpoints with an agent authenticate to the PDP and communicate via mutual authentication and encryption. The PDP may communicate with an identity provider to validate user credentials, support Multi-Factor Authentication (MFA) [15], and provide attributes that will be used for access decision-making.

The PEP enforces policies from the PDP as the basis of dynamic access management decisions to grant or deny access to a specific resource or a group of resources. The PEP provides granular perimeter protection, enforces network and application policies, and is typically close in proximity to the protected resource.

Managed endpoint access to the protected

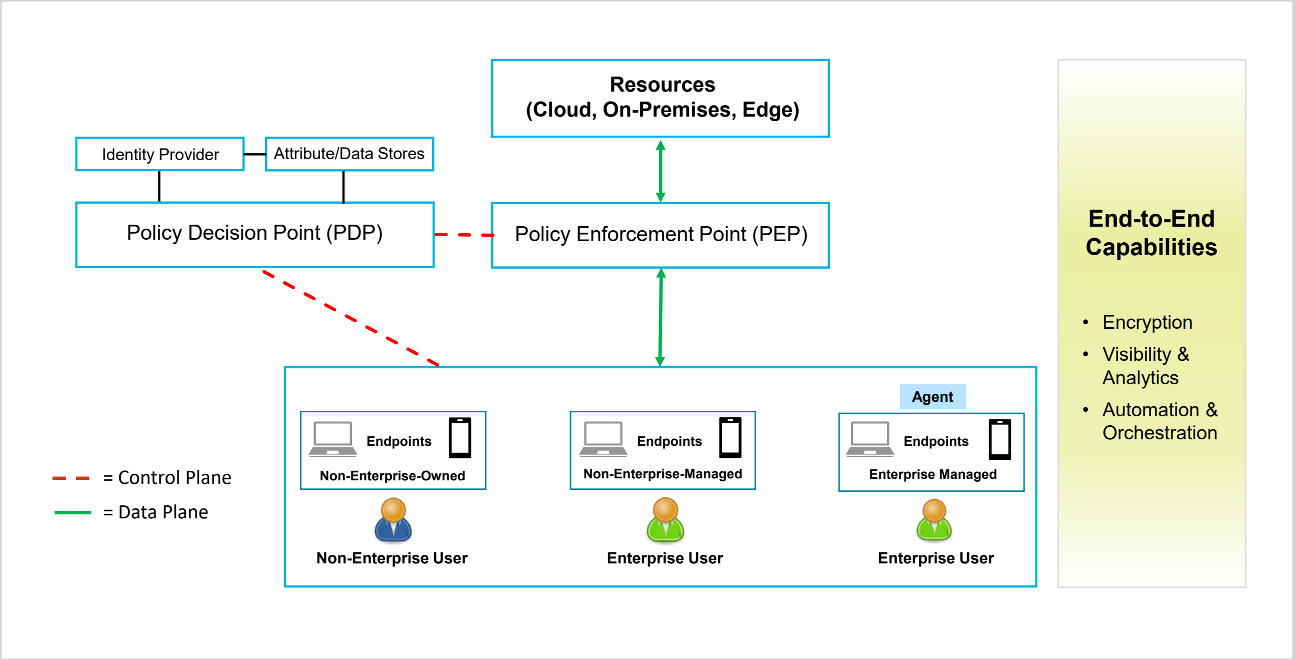


FIGURE 2: EXAMPLE ZTA REFERENCE ARCHITECTURE

resource over the data plane is based on continuous authentication and dynamic evaluation of attributes. The PEP enforces network and application access policies.

ZTA makes use of end-to-end capabilities for a secure and integrated architecture. It uses encryption to ensure the end-to-end communications (path) is protected against unauthorized disclosure and modification. Visibility and Analytics enhance security operations by detecting anomalous behavior and implementing dynamic changes to security policies based on evolving threat conditions. Automation and Orchestration, such as SOAR, improve cybersecurity posture by automating response actions in a more efficient manner across the enterprise.

Zero Trust Use Cases

ZTA use cases define the context needed to understand the application of Zero Trust implementation for end-to-end transactions and data flows. Use cases for a specific organization should be created based on the following:

- Resources that support critical mission/ business processes
- Organizational policies
- Data type and sensitivity
- Location of resources
- User types, attributes, and credentials
- User locations and connectivity options
- Device types and credentials.

Common use cases illustrate where the application of ZTA would provide benefits. Use case examples for a typical enterprise are depicted in Figure 3. The figure identifies enterprise and non-enterprise users with different device types, each of which needs to be supported by access policies.

A primary use case illustrated in Figure 3 is Enterprise Application access for enterprise

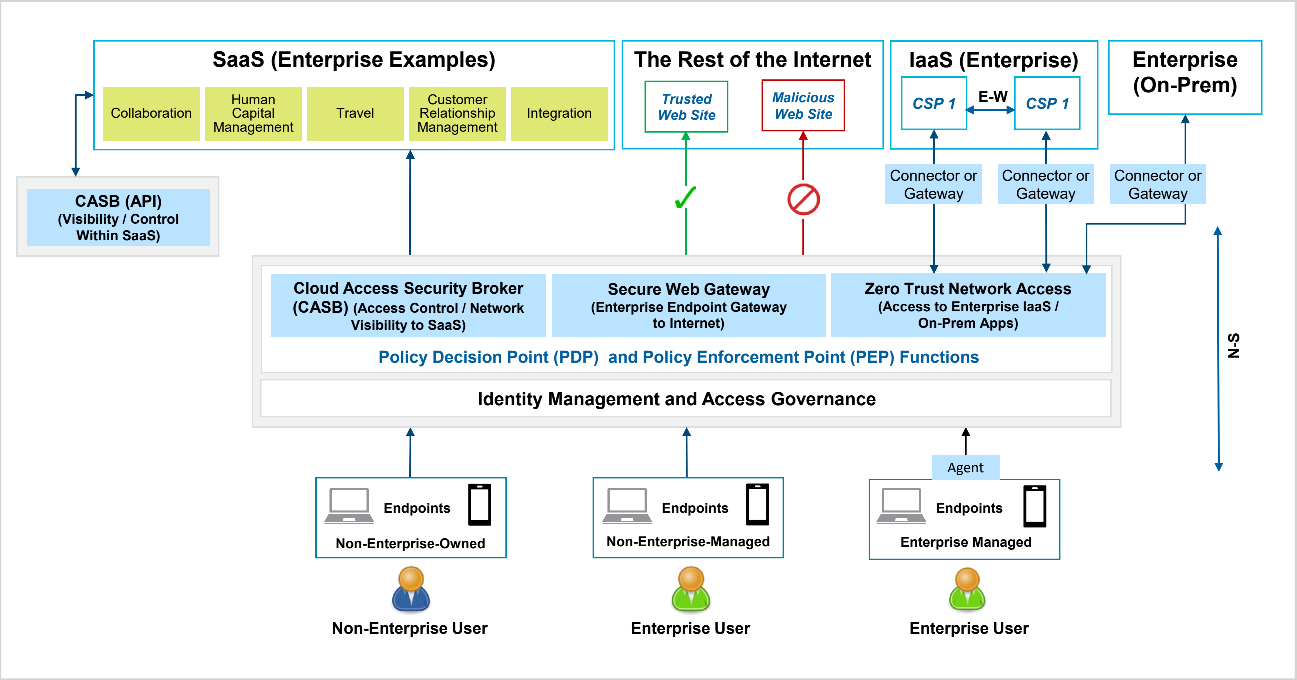

SaaS (Enterprise Examples)
Collaboration
Human Capital Management
Travel
Customer Relationship Management
Integration
The Rest of the Internet
Trusted Web Site
Malicious Web Site
IaaS (Enterprise)
CSP 1
E-W
CSP 1
Enterprise (On-Prem)
Connector or Gateway
Connector or Gateway
Connector or Gateway
CASB (API) (Visibility / Control Within SaaS)
✓
Cloud Access Security Broker (CASB) (Access Control / Network Visibility to SaaS)
Secure Web Gateway (Enterprise Endpoint Gateway to Internet)
Zero Trust Network Access (Access to Enterprise IaaS / On-Prem Apps)
Policy Decision Point (PDP) and Policy Enforcement Point (PEP) Functions
Identity Management and Access Governance
N-S
Agent
Endpoints
Non-Enterprise-Owned
Endpoints
Non-Enterprise-Managed
Endpoints
Enterprise Managed
Non-Enterprise User
Enterprise User
Enterprise User

FIGURE 3: COMMON USE CASES

users. In this case, a user commonly has devices known to and managed by the organization and is connecting from an internal network or remotely over the internet. The user is requesting access to an application owned and managed by the enterprise either on-premises or as Infrastructure as a Service (IaaS). Zero Trust Network Access [16] enables access to resources hosted by a Cloud Service Provider (CSP) or on-premises. The resources are protected via a Connector or Gateway to enforce authorized connections and application segmentation.

Another common use case is Software as a Service (SaaS) Application Access for enterprise users. In this case the enterprise has limited control of applications' security configuration and posture. A Cloud Access Security Broker (CASB) [17] may be used to monitor and potentially control the flow of traffic and user access to the SaaS application. Although not depicted, a CASB can also be used for IaaS monitoring.

Internet Connections for Enterprise Users is also common. A Secure Web Gateway (SWG) function [18] is used to determine which sites can be accessed, supports permit/deny rules for types of network traffic, and captures logs for monitoring. The primary purpose of the SWG is to prevent malicious network traffic either entering or leaving the enterprise.

The enterprise may also need to support incoming connections from external users on the internet, including employees with permission to use their personal device. These must be filtered and inspected by the SWG. Public-facing websites must be protected against malicious actors seeking to disrupt services, plant malware, or deface the website. Many organizations have commercial business partners or research institutions with which they share data or sensitive intellectual property via trusted websites. The SWG enables access to trusted websites and may include the ability to perform inbound/outbound Transport Layer Security inspection.

Machine-to-Machine interactions, also commonly referred to as "east-west" communications, also need to be protected. Some applications have a distributed architecture where various system components may reside in different data centers or commercial clouds, or a hybrid of the two. In addition, data backup and disaster recovery often depend on synchronization of data across locations. The majority of ZTA solutions focus on user-to-machine interactions, and machine-to-machine solutions are not as mature.

ZTA Implementation Considerations

As discussed earlier, ZTA is an architecture approach and strategy requiring the integration of multiple capabilities. Transitioning to ZTA requires a mature state of readiness and a phased rollout, and there are several known implementation challenges to developing a complete and integrated solution.

To assist with ZTA transition planning, a published example of a transition plan is Google's BeyondCorp [19, 20]. In this section, we will examine these recommendations and supplement them with knowledge of our customer environments.

We will also discuss the known challenges to implementation, lessons learned, potential mitigations, and further research needs.

Phased Transition Plans

Due to the broad impact of ZTA on business operations and the interdependencies of the technical capabilities, most organizations will need a multi-year transition. In terms of readiness, Google emphasizes the importance of commitment and buy-in at all levels and across all stakeholders, and constant communication throughout the transition. As with any project of this magnitude, effective program management and understanding of costs and benefits to the core mission are essential. It is also important to communicate the plans and train the user community on the policies and any changes to the interfaces and workflows. To ensure adequate visibility and control, the operational processes and tools need to be in place.

TRANSITIONING TO ZTA REQUIRES A MATURE STATE OF READINESS AND A PHASED ROLLOUT, AND THERE ARE SEVERAL KNOWN IMPLEMENTATION CHALLENGES TO DEVELOPING A COMPLETE AND INTEGRATED SOLUTION.

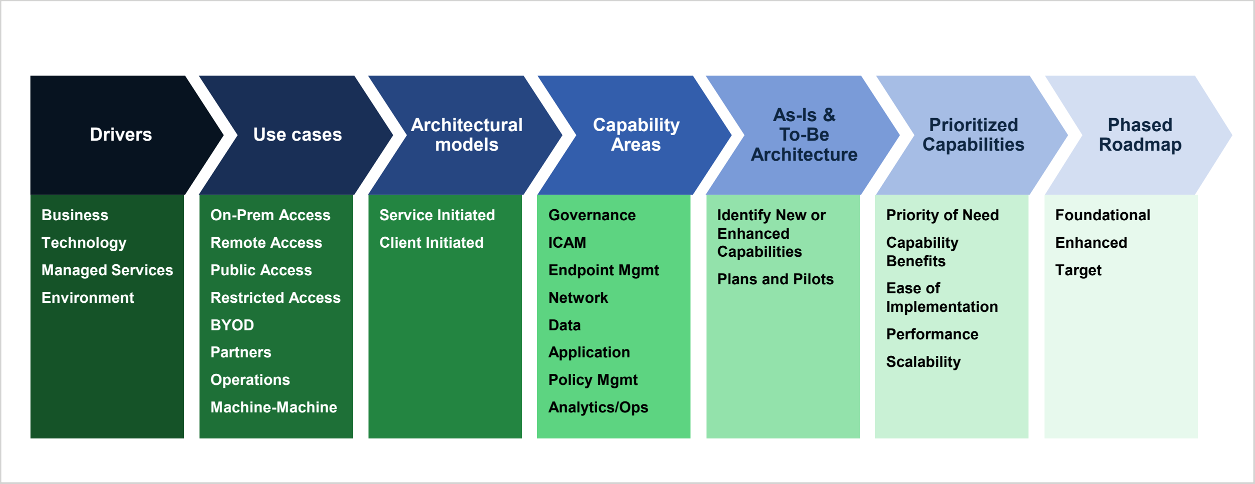
The transition from perimeter-based architectures and implied trust of internal networks to ZTA will require careful planning to ensure functionality and availability of enterprise services (e.g., network management) [5, 6]. Some current applications and services use the organization's source Internet Protocol (IP) address space for access control. When a remote user accesses cloud resources, they will no longer have a "trusted network" IP address and would be denied access unless the service policies are changed. Initially, a layered series of defenses must be maintained until confidence is gained in the new system. A gradual piloting and phased transition approach with careful monitoring will be required. The transition plan should include gradual decommissioning of redundant capabilities. In some cases, it may make sense to leave existing systems in place to provide added layers of security against advanced cyber adversaries.

As the transition plan is being developed, it is critical to gain buy-in from stakeholders along the way. For a successful implementation, a phased transition should migrate user groups gradually, with lower-risk groups going earlier. A governance structure to communicate with, train, and support users, including a help desk, should be put in place. Last, the deprecation of obsolete or redundant capabilities over time will provide financial and administration benefits and potentially improve performance and security operations.

A planning roadmap is recommended to capture these transition issues. The steps in developing a high-level transition plan are shown in Figure 4. The first step is to determine business drivers and stakeholders key to decision-making. This team should assess and prioritize candidate use cases. This will involve the identification of critical assets and development of access policies. This can often be a time-consuming task and is key to the successful implementation of ZTA.

Once the use cases are understood, the various target architecture models should be assessed for which is most appropriate given the current architecture and use cases. Then the technical readiness of key capabilities must be evaluated to identify new or enhanced capabilities required. Small-scale pilots and perhaps simulations are recommended to evaluate various possible solutions and their impact on current business processes and users before proceeding.

Since there are many moving parts are interdependent, it will be necessary to prioritize and sequence the rollout of capabilities. The transition plan should be documented and agreed to by stakeholders. The user community must also be informed and trained in any changes to workflows. A help desk for support must be available. Finally, a plan to decommission legacy capabilities when appropriate will potentially save cost and improve performance.



Drivers	Use cases	Architectural models	Capability Areas	As-Is & To-Be Architecture	Prioritized Capabilities	Phased Roadmap
Business Technology Managed Services Environment	On-Prem Access Remote Access Public Access Restricted Access BYOD Partners Operations Machine-Machine	Service Initiated Client Initiated	Governance ICAM Endpoint Mgmt Network Data Application Policy Mgmt Analytics/Ops	Identify New or Enhanced Capabilities Plans and Pilots	Priority of Need Capability Benefits Ease of Implementation Performance Scalability	Foundational Enhanced Target

FIGURE 4: TRANSITION PLANNING

Technical Readiness

The technical readiness of the capabilities is a crucial step. Several organizations provide advice for organizations to perform a self-assessment on the prerequisites for a successful ZTA deployment, including the American Council for Technology-Industry Advisory Council, Forrester, and Microsoft [7, 21, 22]. Based on these sources and our own experience, to determine technical readiness and perform the migration, the maturity of the major components of the architecture needs to be assessed, including:

- Development of least privileged access policies that support desired workflows
- Data/asset inventory and critical asset identification
- Device management and security
- Network segmentation strategy at a sufficiently granular level
- Existing network traffic flows
- Application security, including APIs, containers, and virtual machines
- Operations impact, including security automation and analytics capability.

Not all the major components need to be fully mature to start migration to ZTA. For example, a ZTA approach focused on ICAM and micro-segmentation might be a logical first step. This decision will be determined by the unique needs and status of the organization. Moving from pilots to implementation must be done carefully to minimize disruptions. The following section addresses some important considerations that will impact the transition.

Implementation Challenges

ZTA is still emerging, and product lines are incomplete. As with any new technological approach, potential vulnerabilities, start-up costs, and transition hurdles must be addressed. Organizations need a sufficient level of process and policy maturity and an understanding of user access policies in order to use ZTA effectively. Many organizations may lack the policies, processes, and skill levels needed. The following sections discuss common and significant ZTA-related challenges.

Policy Management

Correct implementation of ZTA relies heavily on definition and enforcement of appropriate policies such as least privilege, and on accurate knowledge of the user and device attributes such as identity, location, and behavior. Appropriate policies are unique to each organization and require buy-in from multiple stakeholders. This must be done carefully, as an ill-considered security policy will result in an organization denying access and preventing users from accomplishing their work. Consensus on policy development may take considerable time and effort to move from broad network access policies to more granular access to specific resources based on a richer set of attributes for user, device, and environment.

ZTA may impose more granular, differentiated, and restrictive security policies that will be more complex to implement and administer. Automation of policy management and distribution will be key to handling the complex and dynamic nature of a ZTA. The data sources required to implement the policy must be identified and either aggregated or ingested to help inform policy decisions. In addition, dynamic policy approaches must be considered within the software development continuous integration/continuous deployment pipeline to ensure that policies keep up with rapid deployments.

The access decision may be based on either criteria or score-based trust algorithms, or a combination of the two [6]. Criteria-based access uses Boolean "if-then-else" testing of conditions, while score-

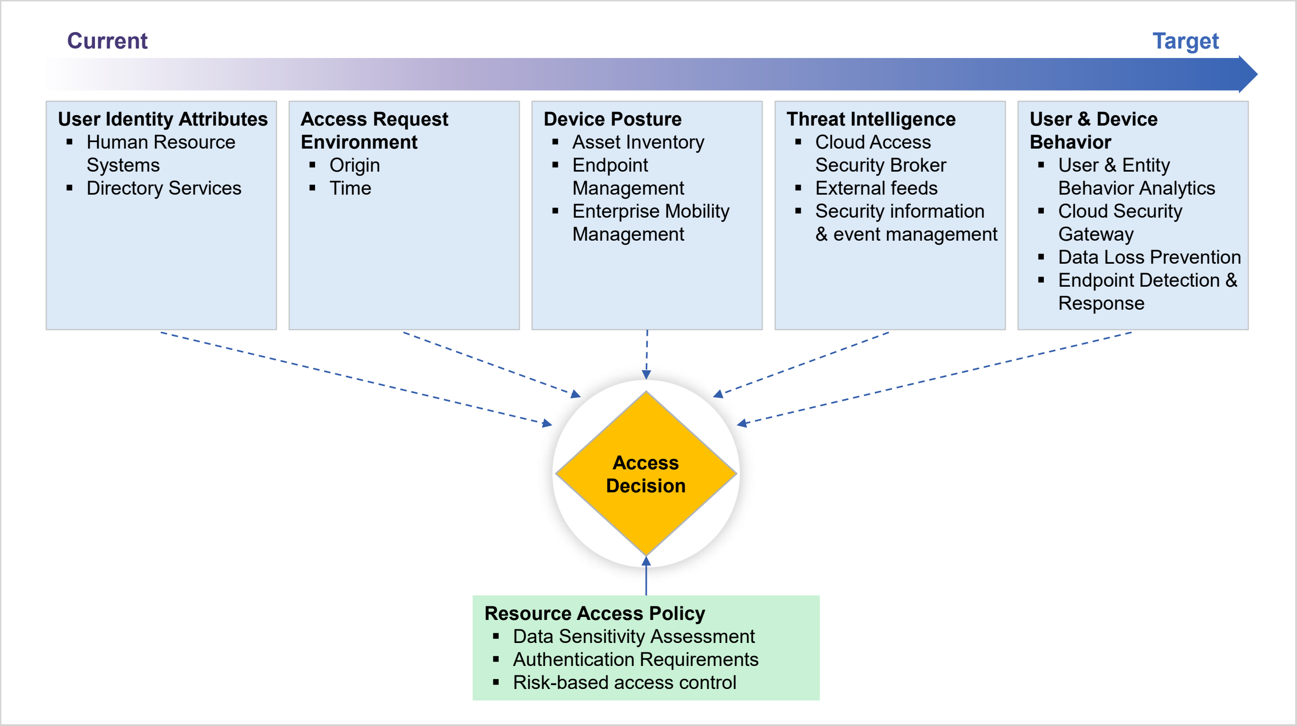


FIGURE 5: FINE-GRAINED ACCESS CONTROL AND DATA SOURCES PHASING

based algorithms seek to calculate a risk level of the access request and compare it to the sensitivity of the resource. Score-based algorithms and implementation are in an early stage of maturity and introduce questions about interoperability across vendors and federated enterprises.

A phased introduction of fine-grained policies may be appropriate, and an example phasing with associated data sources is provided in Figure 5. In this example, additional data sources are added gradually, and the associated resource access policies, based on the sensitivity of the resource, must be evolved in concert. Such a phased approach is recommended to minimize disruptions while learning what policies will ensure that users have the necessary access to perform their work while moving toward least privilege [6, 19, 20]. Also, the availability of necessary data feeds will be phased in over time, with advanced user behavioral analytics and threat intelligence coming later.

Interoperability and Integration

Commercial vendors entering the ZTA arena are marketing ZTA solutions often consisting of adaptation of their current products, combined with new capabilities, partnerships, and acquisitions. This has led to somewhat disparate interpretations of the approach and lack of interoperability between implementations. Careful interoperability testing will be required, particularly in federated organizations where different business units or operating divisions may implement different solutions.

A ZTA will not likely exist in isolation; it will interact with commercial clouds, with non-Zero Trust enclaves and networks, and with other security components. Enterprise systems have been built over the past 10 years using architectural patterns that emphasize strong perimeter security and centralized monitoring and control points, and ZTA will have to interact with these systems for the foreseeable future.

With the rollout of 5G and proliferation of connected devices, the continuous integration of more distributed device types and data sources will require flexible and agile processes. Several areas exist where ZTA would benefit from the development of industry standards, such as a common ontology for ZTA access control attributes (e.g., user and device) to enable consistent access enforcement, promote interoperability of ZTA products, and allow federation across organizations with varying policies. A flexible policy framework must be identified to drive the attribute ontology.

As ZTA gets deployed across IT environments and use cases, an added area for interoperability and integration is interaction with Internet of Things (IoT) and Industrial Control Systems. This includes integration of Zero Trust principles within Operational Technology (OT) systems used to monitor and manage control systems and at the boundaries between IT and OT systems.

Research and modeling are required to determine workable frameworks and determine the effectiveness of trust scoring algorithms in enhancing security. Industry groups and/or standards should be leveraged to move to interoperable systems.

Security Operations Center Integration and Analytics

ZTA implementations provide several new components to an enterprise infrastructure, which can provide additional, dynamic, and more detailed sensor data. ZTA places more reliance on sensors at the endpoints, which will need more sophisticated capabilities. Without a defined network perimeter to monitor and control the flow of traffic, the monitoring must be distributed at user and application endpoints and policy enforcement points, in addition to or instead of existing network sensors. Security response and incident management processes will need to be updated to reflect added sensors and Zero Trust components (e.g., PDP/PEP).

AS WE MOVE TOWARD A FUTURE WITH IOT AND CONNECTIVITY USING 5G WIRELESS, THE VOLUME, VARIETY, AND VELOCITY OF SECURITY POLICIES AND OPERATIONS FOR SOFTWARE-DEFINED RESOURCES WILL INCREASE SIGNIFICANTLY.

As we move toward a future with IoT and connectivity using 5G wireless, the volume, variety, and velocity of security policies and operations for software-defined resources will increase significantly. This includes challenges with high-speed streaming analytics for access control; aggregating, correlating, and analyzing data for situational awareness; acting on security incidents with policy changes at various control points; and the ability to perform post-incident forensics, among other things. The operational architecture for ZTA must address these challenges to provide integrated and enhanced situational awareness to Security Operations Center (SOC) analysts. The methods and capabilities for this new environment are a crucial area for further research.

Security Vulnerabilities

While ZTA holds promise for improving security, potential vulnerabilities also exist with this new approach, which must be studied and considered before migration and on an ongoing basis.

Perhaps the most serious potential vulnerability is a compromised ZTA control plane. This would provide an adversary free reign to allow external connections to critical resources and could cause large-scale service disruptions. The attack surface of the control plane must be thoroughly assessed, and vulnerabilities identified and mitigated. This includes redundancy of components and periodic testing to validate failover scenarios.

The ZTA PDP is only as effective as the data stores that interface with the PDP. Near-real-time update processes of Human Resource (HR) data input from HR systems that supply changes in employee status and roles, and a trusted certificate authority and revocation source, are required to enforce dynamic access policies and minimize the attack window.

The monolithic perimeter boundary currently serves as a centralized point to detect and mitigate Denial of Service (DoS) attacks before they can affect the internal network resources. By avoiding traditional access points, the distributed nature of ZTA increases cyber-resiliency, but it can make these attacks harder to detect and respond to using conventional approaches. Detection and mitigation techniques need to be studied further for effectiveness.

Organizations need a mature process for creating and maintaining an accurate inventory of all devices allowed to access resources. This inventory should be built as devices are acquired, not by asset discovery. Devices will need a viable mechanism for protecting keys and certificates. This requires mature processes for purchasing and for provisioning certificates for the devices.

Access control decisions may be based on user and device attributes. This requires mature and timely processes for managing patching and device configurations to avoid a self-inflicted denial of service for valid users with an unpatched device.

Endpoint Security is a critical concern in ZTA, because end-to-end encryption requires more monitoring at the endpoints. Device identification and authentication can often be achieved using public key certificates. However, BYOD introduces potential vulnerabilities into the system because the organization has limited to no control over what other software or hardware may be on the user’s device. In addition, the Internet of Things integrates many simple devices that may have limited security capabilities. To enforce ZTA policies for BYOD and IoT, the enterprise should either establish a set of requirements mandating security software be present on the device that can provide an acceptable level of security, integrate mitigating controls within the network, or establish policies that limit access to resources.

To hunt for attacks, defensive cyber operations often depend on centralized inspection points having visibility into traffic flowing across the network. ZTA principles suggest that all traffic be encrypted as it moves across the network, which can restrict the inspection to the endpoints of the traffic path. Device management and monitoring capabilities (including analysis of encrypted network traffic) should be given careful attention.

Security protocols, such as those employed for a software-defined perimeter and host-based micro-segmentation, should be analyzed and carefully implemented to ensure they are used properly in a ZTA context.

The security vulnerabilities in ZTA described above should be explored thoroughly via modeling and simulation, threat-based assessments, penetration testing, and red team exercises.

Scalability and Performance

Many organizations have very large, complex, and distributed networks with tens or even hundreds of thousands of endpoints. The scalability of ZTA to these levels must be demonstrated, including its impact on operational processes. Encrypting all transactions, micro-segmentation, and software-defined networking require additional processing and may impact performance. Modeling and simulation, testing, and pilot programs can provide insights into these impacts before full deployment. One should consider the elastic properties of a Zero Trust solution to support scaling and performance.

Administrative Issues

Workflow management is creating, maintaining, and optimizing the paths that data follows through a system to complete tasks in a given process. Because of techniques like conditional access, micro-segmentation, and traffic encryption, traditional workflows might work differently as an enterprise migrates to ZTA. Previously allowed data flows might be blocked, and encrypting all traffic in the system might inadvertently make it harder to share data among multiple applications or users. The enterprise and supporting organizations will need to analyze current workflows and data paths carefully when migrating to ZTA, to ensure business processes are not unintentionally blocked.

ZTA techniques such as segmentation and stricter trust controls often eliminate the capabilities of an "all-powerful" administrator with access to everything in an enterprise system. This is good from a security standpoint, as it mitigates against insider threats and limits the potential damage from a successful attack against a system administrator. However, it can make day-to-day system management more difficult, as fixing problems that cross segmentation boundaries can require coordination among multiple administrators.

Summary and Future Work

While ZTA holds great promise, we have identified several areas that require more investigation and research to move into large-scale implementation. This early in the implementation cycle, many unknowns remain.

In general, evaluation of ZTA will include the following parallel activities: (1) determining the organization's drivers and use cases and documenting select business case scenarios and policies based on ZTA; (2) developing general implementation guidance on ZTA; (3) conducting hands-on technology assessment and gap analysis of emerging commercial offerings and industry standards; (4) and supporting investigations and research into the key areas identified in the previous sections, which can include modeling and simulation, prototyping, piloting products, red teaming, penetration testing, and gathering lessons learned from early adopters.

A phased implementation of ZTA may begin for organizations sufficiently mature in at least some of the required capabilities. Executive support, careful planning with constant monitoring, and communication with staff are required to minimize disruption and maintain buy-in.

Interoperability between products in a ZTA, between federated enterprises deploying ZTA with heterogenous solutions, and with existing security capabilities should be understood to avoid unintended interactions. Industry groups could facilitate consensus on technical issues.

Different ZTA products determine trust scores and enforce access decisions differently, even if similar types of attributes are employed. Inconsistent access decisions and interpretation by PEPs in federated enterprises are possible without a common view of attribute definitions and values.

The security vulnerabilities in ZTA should be explored thoroughly via modeling and simulation, vulnerability assessments, penetration testing, and red team exercises. Appropriate mitigations should be identified or developed. This includes assessing the attack surface of the control plane, the ability to detect and mitigate DDoS attacks, BYOD and IoT device integration, traffic visibility at endpoints, and gaps in authentication protocols.

Various authentication scenarios, including identity federation, MFA, privileged access management, tiered data access, and delegation to third-party authentication services should be modeled with ZTA to ensure correct operations.

Experimentation and piloting of the various use cases, including machine-machine interactions, should be performed to ensure correct operation before implementation. Current solutions primarily focus on “north-south” user-to-resource access control. “East-west” communications between non-person entities in an efficient manner across multi-cloud and hybrid-cloud implementations must be evaluated.

ZTA presents numerous operational challenges, including high-speed streaming analytics for access control; aggregating, correlating, and analyzing data for situational awareness; automating and orchestrating policy distribution; acting on security incidents with policy changes at various control points; and the ability to perform post-incident forensics. Methods and tools are needed to support a scalable operations architecture that is efficient and meets the needs of SOC analysts.

The scalability of ZTA to accommodate the needs of large, diverse, and loosely federated enterprises must be evaluated. The performance of ZTA across large, distributed enterprises with heavy traffic loads, encryption, monitoring, and blocking should also be verified.

The implementation of 5G network slicing introduces further questions on how ZTA can be used both to protect a network slice and to protect the 5G core itself.

The proliferation of devices with less processing capability in the IoT space may require new capabilities in the architecture. This includes integration of Zero Trust principles within OT environments (e.g., control systems).

Enterprise security modernization is an on-going process that must evolve with changes in threats, use cases and technology. Future work will be needed on extending and adapting Zero Trust principles.

In conclusion, ZTA is a promising new enterprise security architecture that is gaining momentum worldwide. Existing capabilities can be leveraged and integrated to support Zero Trust principles, but the transition to a mature ZTA will require additional capabilities over time. We recommend proceeding in this direction but with executive support, careful planning, piloting, employee feedback, and phased implementation to avoid disruption to operations. In addition, investment into the above research areas will greatly benefit users, network operators, and equipment vendors alike.

References

1. N. Evans, *The Importance of Zero-Trust and an Adaptive Perimeter in Cyber Fortifications*, IDG Contributor Network, May 2014.
2. Microsoft Corporation, *Enable a Remote Workforce by Embracing Zero Trust Security*, 2021. Accessed: https://www.microsoft.com/en-us/security/business/zero-trust
3. J. Kindervag, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, Forrester Research, Inc., September 2016.
4. R. Ward and B. Beyer, *BeyondCorp: A New Approach to Enterprise Security,* USENIX Security Conference, December 2014.
5. National Security Agency, *Embracing a Zero Trust Model*, February 2021. Accessed: https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.pdf
6. National Institute of Standards and Technology (NIST), *Zero Trust Architecture*, NIST Special Publication 800-207, August 2020. Accessed: https://www.nist.gov/publications/zero-trust-architecture
7. The American Council for Technology-Industry Advisory Council (ACT-IAC), *Zero Trust Cybersecurity Current Trends,* April 2019. Accessed: https://www.actiac.org/zero-trust-cybersecurity-current-trends
8. E. Gilman and D. Barth, Zero Trust Networks: *Building Secure Systems in Untrusted Networks,* Sebastopol, CA: O'Reilly Media, Inc., 2017.
9. *Report to the President on Federal IT Modernization,* 2017. Accessed: https://itmodernization.cio.gov/
10. National Institute of Standards and Technology (NIST), *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*, NIST Special Publication 800-160 Vol. 2, November 2019. Accessed: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf
11. TechTarget Network, *SOAR (security orchestration, automation and response)*, March 2021. Accessed: What is SOAR (Security Orchestration, Automation and Response)? A definition from WhatIs.com (techtarget.com)
12. Exabeam, User and Entity Behavior Analytics, April 2021. Accessed: https://www.exabeam.com/siem-guide/ueba/
13. NIST, *Identity, Credential, and Access Management (ICAM)*, 2021. Accessed: Identity, Credential, and Access Management (ICAM) - Glossary I CSRC (nist.gov)
14. NIST, *Data Loss Prevention*, 2021. Accessed: data loss prevention - Glossary I CSRC (nist.gov)
15. NIST, *Multi-Factor Authentication (MFA)*, 2021. Accessed: Multi-Factor Authentication (MFA) - Glossary I CSRC (nist.gov)
16. Gartner Glossary, *Zero Trust Network Access (ZTNA)*, 2021. Accessed: Definition of Zero Trust Network Access (ZTNA) - Gartner Information Technology Glossary
17. TechTarget Network, cloud access security broker (CASB), March 2021. Accessed: What is a CASB? Cloud Access Security Brokers Explained (techtarget.com)
18. Gartner Glossary, *Secure Web Gateway*, 2021. Accessed: Definition of Secure Web Gateway - IT Glossary I Gartner

19. Google Online Security Blog, *How Google Adopted BeyondCorp,* June 27, 2019. Accessed: https://security.googleblog.com/2019/06/how-google-adopted-beyondcorp.html
20. B. Osborn, J. McWilliams, B. Beyer, and M. Saltonstall, *BeyondCorp: Design to Deployment at Google,* USENIX Security Conference, Spring 2016.
21. Forrester Research, Inc., *The Zero Trust Security Playbook for 2021*, 2021. Licensed for Distribution.
22. Microsoft Corporation, *Zero Trust Maturity Model*. March 19, 2021. Accessed: https://www.microsoft.com/en-us/itshowcase/implementing-a-zero-trust-security-model-at-microsoft

Appendix A: Abbreviations and Acronyms

API	Application Programming Interface
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
CSP	Cloud Service Provider
DDoS	Distributed DoS
DoS	Denial of Service
HR	Human Resources
IaaS	Infrastructure as a Service
ICAM	Identity, Credential, and Access Management
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
MFA	Multi-Factor Authentication
OT	Operational Technology
PDP	Policy Decision Point
PEP	Policy Enforcement Point
SaaS	Software as a Service
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SWG	Secure Web Gateway
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
ZTA	Zero Trust Architectures

ABOUT THE AUTHORS

Deirdre Doherty is a Department Manager and Senior Principal Cybersecurity Architect in MITRE Labs' Cyber Solutions Innovation Center. She provides consulting on enterprise-wide and cloud-based security architectures, seeking to advance the state of cybersecurity while leveraging the functionality and cost efficiencies of advanced technologies.

Brian McKenney is a Senior Principal Cybersecurity Architect in MITRE Labs' Cyber Solutions Innovation Center. As Enterprise Security Architecture Capability Area Lead, he provides consulting on the integration of cybersecurity capabilities within evolving enterprise, cloud, and network security architectures.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™