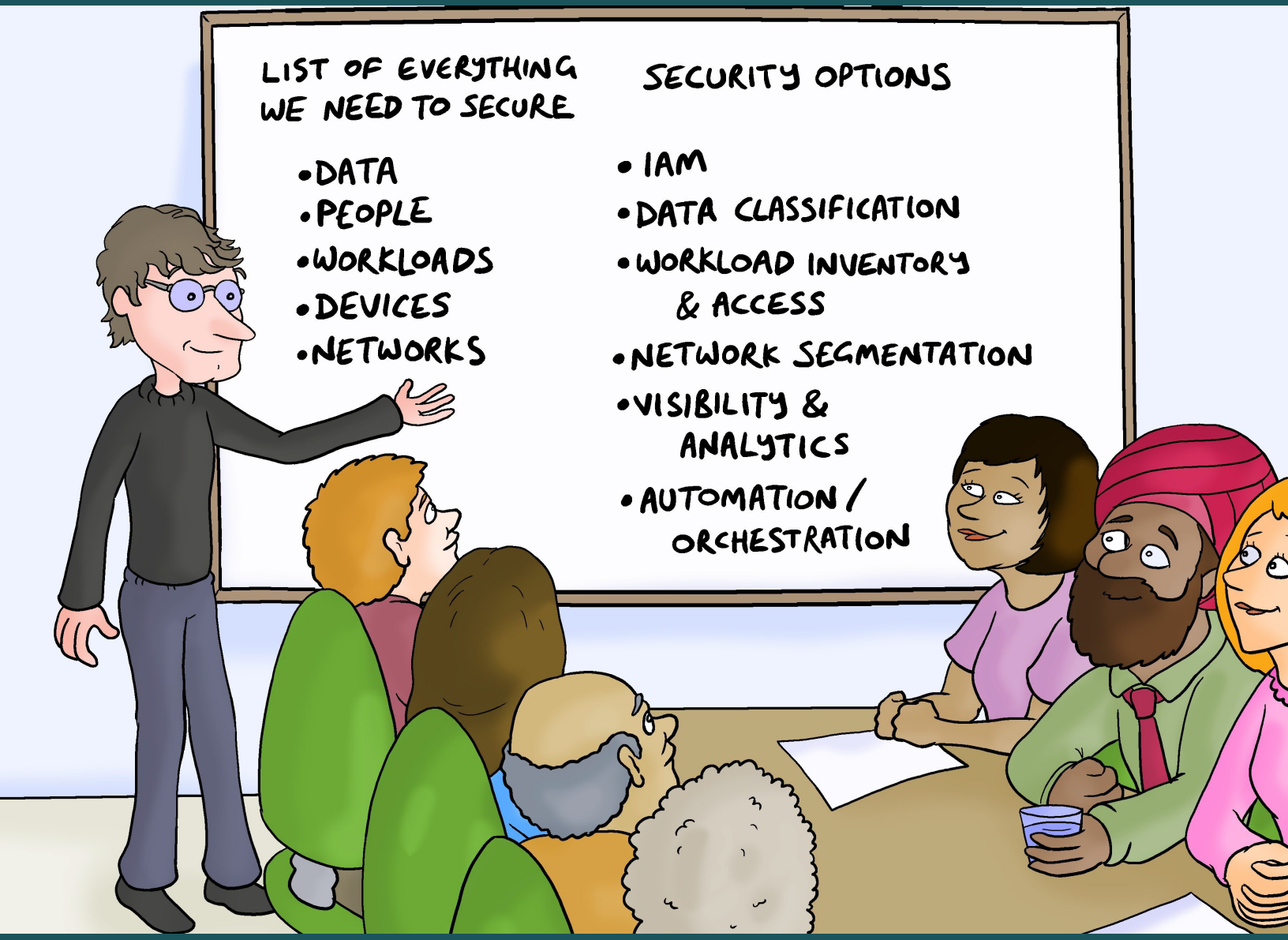
ConversationalGeek®

Zero Trust
Buyer's Guide



Sponsored by Forcepoint

Zero Trust Buyer's Guide

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Choosing the Right Zero Trust Solution

Zero Trust (ZT) methodology and associated architectures have gained prominence as governments face a growing number of Advanced Persistent Threats (APT) from peer, near-peer, and quasi proxy government/criminal groups. The transition from small groups of tinkerers and opportunists to nation-states and technologically advanced criminal groups, we need to change how we design, monitor, andtake actions. Zero Trust Architecture (ZTA) is much more than a hypothetical paradigm. It is a real security architecture mandated at the highest level of the United States Government. President Biden's May 12, 2021 Cybersecurity Executive Order requires federal agencies to develop an implementation plan for Zero Trust. Defense Information Systems Agency (DISA) just made public Department of Defense (DoD) Zero Trust reference architecture. NIST recently published their version in Special Publication 800-207. ***Bottom line, Zero Trust is here to stay, and your organization has a mandate to implement it.***

ZTNA is a suite of capabilities that brings together identity, devices, network, applications, data, and behavior analytics to make a decision on whether a user is authorized to access a given resource and if the user behavior is deemed risky removals of permission. The good news is that Zero Trust does not require you rip out all existing security controls and start fresh. You can begin implementing Zero Trust right away by augmenting your current infrastructure with capabilities we outline in this Buyer's Guide. We will cover foundational capabilities you must implement to start building a Zero Trust Architecture, as well as some advanced capabilities to get you thinking about the future. Zero Trust is a journey. Our goal is to provide you with foundational building blocks to get started.

- Andrey Zhuk, Cyber Solutions Architect

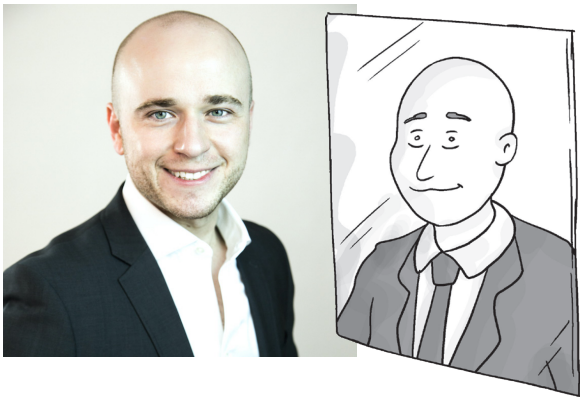


Table of Contents

Zero Trust Model

Zero Trust Model

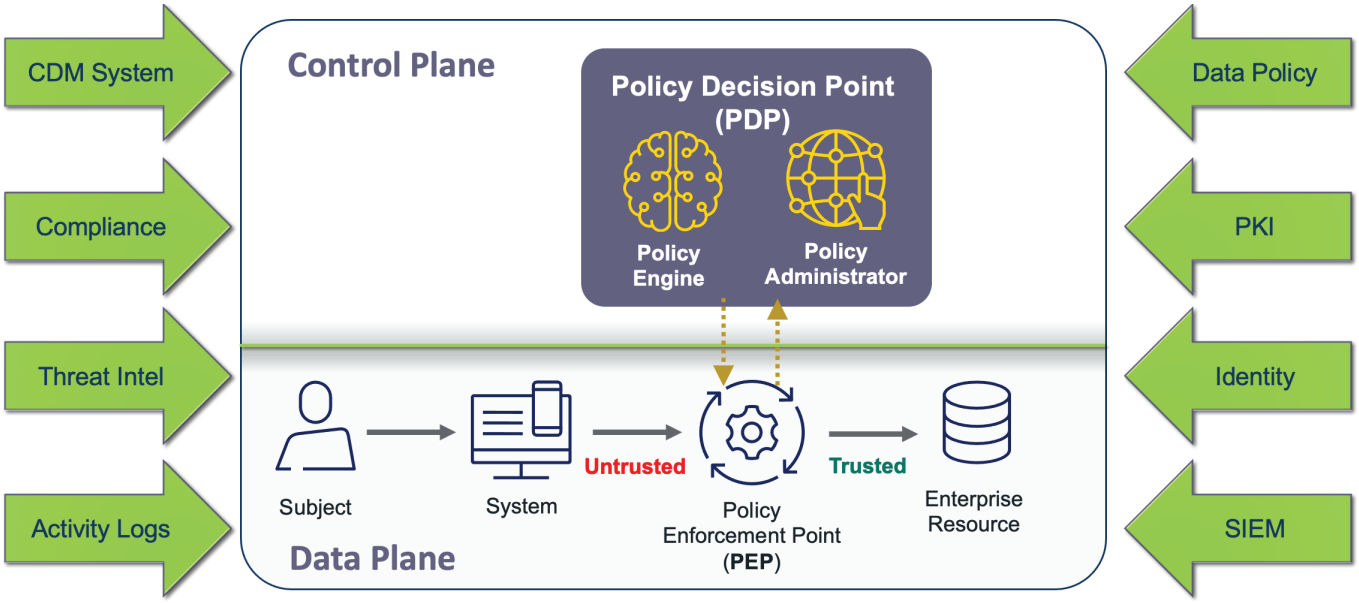
A widely accepted conceptual model for Zero Trust is Forrester's Zero Trust eXtended (ZTX). ZTX places data in the center, as shown in Figure 1. This reflects Forrester's belief that the data explosion in both on-prem and cloud environments is at the center of what must be protected. The surrounding elements – people, workloads, devices, networks – are conduits to data and therefore need protection as well. Let's briefly discuss each of these elements.

- **Data:** Data is at the center of the ZTX model and is the unit of value that a ZT system must protect. Agencies should develop Data Classification and Protection policies that will ultimately be enforced by the ZT system when authorizing access.
- **People:** Identity and Access Management (IAM) is the foundational capability of a ZT system. ZT shifts from coarse identity attributes of legacy IAM systems (username + password) to fine-grained Role- and Attribute-Based Access Control (RBAC and ABAC).
- **Workloads:** Physical servers, virtual machines (VMs), containers, and the applications they run. ZT requires RBAC and ABAC for workload access, enforced consistently across hybrid environments.

- **Devices:** These include Government Furnished Equipment (GFE), BYOD and Internet of Things (IoT) devices. ZT requires identity, inventory, isolation, security, and control of all devices.
- **Network:** The focus here is primarily on network segmentation – both from a user and a server perspective – to provide better security based on identity-centric attributes.
- **Security:** In a modern enterprise, it is usually the security products that provide "Visibility and Analytics" and "Automation and Orchestration" functionality. These allow for informed security decisions based on contextual information, enforced in an automated fashion. Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools are key components.

Zero Trust Reference Architecture

In talking about Zero Trust, we need to have a Reference Architecture that we can "point to" in explaining the different components of the solution. For a Reference Architecture, we will use the NIST SP 800-207 because it's currently the most comprehensive and accessible guide to Zero Trust that stays vendor agnostic and domain neutral (as in NOT specific to Public Sector, Defense, or Commercial environments). Note that this is an idealized model showing logical components and their interactions (Figure 2). The ZTA logical components use a separate Control Plane to communicate, while application data is transmitted over the Data Plane.



The two core logical components of ZTA are the Policy Decision Point (PDP) and Policy Enforcement Point (PEP):

- **PDP:** This is the "brain" of ZTA. Whenever a user (aka subject) wants to access a resource, the PDP evaluates the Kipling Questions about the user, makes an access decision, and continuously evaluates the session for unwanted behavior. Currently there is no single PDP vendor on the market. In a real-world implementation of ZTA, PDP will consist of an amalgam of network controllers, device management solutions, SIEM and SOAR tools, all tied together with IAM.
- **PEP:** These are the devices and applications that enforce access controls and security policy. These include firewalls, endpoint agents, web gateways, network access controls, a web single sign on (SSO) portal that acts as a gatekeeper to a resource. What's the difference between traditional security controls (like a firewall) and a Zero Trust PEP? A PEP must be able to receive ongoing updates from the PDP and automatically adjust the policies it's enforcing in near-real time. So, for example, a firewall can become a Zero Trust PEP if it receives dynamic policy updates in response to security events via a SOAR tool.

The external elements (e.g., Threat Intel, PKI, ID Management) provide important inputs to the Zero Trust system. These elements provide context and influence dynamic security decisions of the PDP. We will discuss each of these in the sections that follow.

Summary

Zero Trust is not a single architecture but a set of guiding principles for workflow, system design, and operations that can be used to improve security posture of your organization. Transitioning to a Zero Trust Architecture is a journey and cannot be accomplished with a point product or wholesale replacement of technology. In fact, many organizations already have elements of ZTA in their infrastructure today. Organizations should take a phased approach to implementing Zero Trust with a two- to three-year horizon as a typical time frame. We recommend you create a Zero Trust program roadmap that tackles the various technology areas found in the following Zero Trust pillars:

- **Identity and Access Management:** Identity is at the core of Zero Trust and should be the first and primary focus.
- **Workloads:** Applications and workloads are generally well known and under an organization's control; they are the "low hanging fruit" compared to securing end-user devices.
- **Devices:** Devices encompass GFE laptops, BYOD and IoT devices; the greatest challenge here is developing a strategy for BYOD and IoT devices like cameras, printers, badge readers, etc.
- **Network:** Perimeter is now "the edge" of your network; you need to redraw logical segmentation boundaries around network assets and create isolation between segments using software-defined perimeter.
- **Data:** Despite being at the center of the Zero Trust model, this is a challenging area due to the sheer volume of data within a typical agency; initially focus on securing access to the data (Phases 1-4).

At the core of these pillars is the Zero Trust position of never trusting access requests without verifying. In addition, mature implementations of Zero Trust rely on continual continuous and adaptive authentication and authorization where some or all of these pillars are monitored for changes in behavior, condition, etc. and can dynamically revoke or reduce access as is deemed necessary based on policy.

Your implementation plan should cover all of these Zero Trust pillars, first assessing what you can do relatively easily with existing architecture and policies. You should define where your biggest gaps are in terms of in-place technologies and the ability for new Zero Trust-centric solutions to integrae with existing architectures. By understanding both where you are today with Zero Trust and where your gaps are, you'll have an appropriate understanding of where to get started.

How to Use This Guide

How to Use This Buyer's Guide

Conversational Geek Buyer's Guides help you assess and choose the right solution for your organization. *We do this by breaking the guide into two parts.*

Selection Criteria

We first provide you with a number of important buying criteria to consider. Each criteria section focuses on a particular set of features and capabilities available by solutions today. Those capabilities are then broken down into two distinct categories:

- **Required:** The capabilities listed in this criteria category are those that are fundamental for purchase consideration`. Any solution you consider on your shortlist should have the capabilities listed at a minimum.
- **Optional:** The capabilities listed in this criteria category are features that will enhance your use of the solution but aren't part of the core required capabilities. An optional capability might be considered innovative in nature or simply be of value but only to organizations with specific needs.

Start by reading the Selection Criteria portion of the Buyer's Guide, taking note of which capabilities are important to you, regardless of whether they are listed as *Required* or *Optional*.

Evaluation Worksheets

We then provide you with a set of worksheets that you can print and use to evaluate each solution you are considering. Print out one copy of the worksheets for each solution being considered. Each criteria set and associated capabilities is represented in the worksheets, split up between *Required* or *Optional* capabilities.

Mousepads

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Ergonomic Design		Available in multiple color			
Memory Foam Wrist Rest		Available in multiple sizes			
Non-Slip Base					
				Total Optional Score	

For *Required* capabilities, assess whether these capabilities are available for each solution. For *Optional* capabilities, assign a value in the **Importance** column representing how important each capability listed is to your organization on a scale of 1-10 (with 10 being very important). Then in the **Score** column, assign the solution a subjective score, again on a scale of 1-10, with 10 being the highest. Multiply each **Importance** value with the corresponding **Score** value to get the **Calculated** value. Add the **Calculated** values to get the **Total Optional Score**.

Your worksheets should look something like this when completed:

Mousepads

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Ergonomic Design	✔	Available in multiple color	1	1	1
Memory Foam Wrist Rest	✔	Available in multiple sizes	5	10	50
Non-Slip Base	✔				
				Total Optional Score	51

Lastly, compare the availability of *Required* capabilities, and each of the Total Optional Scores for each solution being considered to determine which solution is right for your organization.

Buying Criteria Detail

Identity and Access Management

Workloads and Applications

Devices

Network

Data

Security

Identity and Access Management

Identity is at the heart of a Zero Trust implementation. IAM systems are responsible for creating, storing and managing enterprise user accounts and identity records. These systems contain necessary subject information (e.g., name, email address, certificates) and other enterprise characteristics such as role, access attributes, and assigned assets.

Required Capabilities

- **Authentication and Authorization for All Users and NPEs:** IAM solution must be able to verify the identity of a subject and enforce access control for all end points, devices, apps, services, and APIs. Access control must be driven by identity-centric and contextual policies.
- **Continuous and Adaptive Authentication and Authorization:** Capability to dynamically adjust privilege level or revoke access for a given user based on change in user behavior.
- **Multi-Factor Authentication (MFA):** Ensure the MFA product uses an app or security token (e.g., CAC card) as the secondary authentication method. Email and text message verification should only be used as a last resort.
- **Support for Modern Identity Protocols:** In addition to supporting LDAP, IAM system must support modern protocols like SAML, OAuth2, SCIM and OpenID Connect (OIDC).
- **Identity Federation:** Most large organizations have multiple identity sources because of mergers, acquisitions, restructuring, unfinished cloud migrations. Ability to federate identities is crucial.
- **Public Key Infrastructure (PKI) Support:** PKI is responsible for generating and logging certificates issued by organization's resources, subjects, services and applications. Look for an IAM solution that integrates with global certificate authorities like DigiCert and VeriSign, as well as U.S. Federal PKI systems built upon X.509 certificates.

Why Start With Identity?

Before you can establish what workloads and resources are accessible, enforce policies, identify suspicious behavior, and more, Zero Trust needs to first know what identity is requesting the access and whether the user of that identity is actually its' owner.

Optional Capabilities

- **Transparent Authentication to All Services:** Having to repeatedly re-enter one's credentials can be painful. Having a solution that can automatically check users' credentials "behind the scenes" allows for a better Quality of Experience (QoE).
- **Privileged Access Management (PAM):** A PAM solution provides "password vaulting" capabilities for privileged admin accounts. For example, a cloud service has a single admin root account, but multiple administrators need to have access to it. A PAM solution enables this workflow.

Workloads and Applications

The rapid adoption of cloud and the new rapid application development compute models have made workload security an urgent area of focus. In developing a ZTA roadmap, we encourage your organization to establish a robust cloud governance process that keeps track of workload inventory and continuously monitors workload configurations.

Required Capabilities

- **Software-Defined Compute (SDC):** Ability for software to provision and manage compute configurations on programmable infrastructure such as physical and virtual servers.
- **Workload Inventory:** Cloud environments make it trivial to stand up a new server without going through due security process. Look for tools that can automatically discover and inventory your workloads, whether on-premises or in the cloud.
- **Configuration Management:** Ability to maintain computer systems, servers and software in a desired, consistent state. Maintaining configuration baselines for organization's IT inventory.
- **Automated Compliance:** Ensures that an organization remains compliant with applicable regulations (e.g., FISMA, ISO, CIS, HIPAA, SOC2). If configuration drift is detected, the solution should be able to bring workloads into compliance.
- **Containers and Kubernetes Support:** Management and security monitoring for VMware Tanzu, Kubernetes Grid, OpenShift, Kubernetes on Amazon EC2, Azure, Google VMS, and others.
- **ITSM Integration:** IT Service Management (ITSM) refers to tools and processes used by IT teams to operate organization's IT infrastructure. Look for products that offer integration capabilities with ITSM platforms like ServiceNow and BMC.

Why Worry About Workloads and Applications?

You can't secure what you aren't aware of. Keeping and inventory and monitoring the configurations of workloads and applications facilitates an ability to continuously ensure the environment – and the provided access to it – is up to date.

- **Mutual TLS (mTLS):** When visiting a secure site, like a bank, we authenticate the bank's server. With mTLS, the client authenticates the server, and the server authenticates the client.

Optional Capabilites

- **Cloaked Applications:** This is usually achieved through Single Packet Authorization (SPA). SPA refers to a series of cryptographic techniques to make internet-facing servers invisible to unauthorized users. Only devices that have been seeded with the cryptographic secret will be able to generate a valid SPA packet and, subsequently, establish a network connection. This approach reduces the attack surface and becomes invisible to adversarial reconnaissance.
- **DevSecOps:** This is not a "feature" per se, but rather a paradigm to be followed. Look for solutions that offer broad integration with Continuous Integration / Continuous Delivery (CI/CD) ecosystem tools.
- **Software Supply Chain:** Ability to validate the security of a binary, library or source code used to build an application. For example, prevent threat actor from compromising a vendor's software update package to gain entry into organization's IT environment.

Devices

As part of the ZTA roadmap, organizations must be able to identify, authenticate, authorize, monitor, secure, control, and isolate every device that connects to the network at any time. Internet of Things (IoT) will make this exponentially more difficult. The DHS CDM program has initiated several efforts to build the capabilities needed within federal agencies to move to ZTA. For example, DHS Hardware Asset Management (HWAM) program under CDM is an effort to help agencies identify devices on their network infrastructure and to deploy secure configurations to them.

Required Capabilities

- **Device Authentication and Authorization:** Ability to verify identity of a device and, upon authentication, grant or deny access to data, assets, applications or services.
- **Agent-Based Architecture:** An agent is installed on a user's machine or a server. This is the most effective way to implement SDP and provides a great degree of control and backwards compatibility with legacy applications.

- **Software-Defined Perimeter (SDP):** A network security "bubble" around a device. Device cannot communicate on the network without authorization from the ZT control plane. This is also referred to as host-based micro-segmentation.
- **Device Discovery and Baselining:** Ability to discover devices on the network and bring them into compliance with an approved configuration baseline.
- **Hardware and Software Inventory:** A ZT system must maintain an up-to-date inventory of all assets as well as any guest devices connecting to organization's network.
- **Device Compliance:** Capability to evaluate security posture (e.g., operating system and patch level) and enforce compliance on mobile devices, laptops, servers, data center components, etc.
- **Endpoint Detection and Response (EDR):** An extension of endpoint antivirus capability, EDR provides real-time monitoring and detection of malicious events on endpoint. EDR creates an attack timeline to aid in incident response.
- **Works On-Premises and Off-Premises:** With the rise of remote work, it is essential for ZT solutions to have parity in capabilities both on-premises and off-premises, as well as in the cloud.

Optional Capabilities

- **Browser-Based Architecture:** "Clientless" or browser-based approach where the user connects to a web application via a secure web portal. This approach is not a viable solution for a full ZTA deployment but is an effective method for accommodating BYOD use cases.
- **Unified Endpoint Management (UEM):** Ability to centrally manage an organization's devices and deploy baseline software configurations in a systemic fashion for mobile devices and personal computers.
- **In-Session Monitoring:** Ability to monitor users' behavior within an authenticated session. You may want to monitor for privilege escalation or excessive data movement.
- **IoT Segmentation:** Ability to isolate IoT devices from the main network and maintain visibility.

Devices are on Par with Identity

Zero Trust isn't just concerned about users that connect to the network; it also concerns itself with any and every device that exists on the network at any point in time. Whether it's to isolate devices, modify their security configurations, or monitor them for potential threats, devices need to be a part of your strategy.

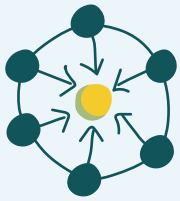
Network

The network piece of a Zero Trust deployment is probably the most difficult one. This is because despite the increase in speeds and feeds, fundamental networking has largely remained the same since the late 1990s. Even in 2021, most networks are still configured on a device-by-device basis. The Cloud Era brought about the concept of network automation, which is now starting to trickle into the enterprise campus and data center networks. As such, we are now seeing a big push for Software Defined Networking (SDN), whereby a network controller configures underlying devices and creates a logical overlay of networks on top of physical infrastructure. All SDN products on the market are built on the philosophy of Zero Trust. So, buying a solution from the likes of Cisco, VMware, or Arista can be an easy button.

Unfortunately, most organizations won't have the resources, manpower, or appetite to lift and shift to a purely SDN environment. The good news is that there are many solutions on the market that can play with your existing infrastructure and allow you to move closer towards Zero Trust Architecture. Below we present critical capabilities to look for.

Required Capabilities

- **Macro-segmentation:** Ability to segment traffic on the network using broad categories, such as location, network type, branch or organization. In the new world of SDN, the concept of a rigid physical VLAN is disappearing and we now use the term "macro-segmentation."
- **Micro-segmentation:** Method of creating zones to isolate workloads and users from one another and secure them individually. Provides highly granular visibility and control over data flows.
- **Encrypted Data Plane:** Data plane communications must be encrypted. Any exceptions must be deliberate (e.g., DNS).
- **Application Bindings:** capability of a network security device (e.g., a firewall) to attach user identity to a particular application session. The user is only allowed to access the application they are authenticated to.
- **Centralized Management and Control:** ZT is all about having a centralized control plane that can dynamically and continuously respond to user and device behaviors.
- **API Programmability:** The future of networking is in programmability, automation, and Infrastructure as Code (IaC). Look for network devices that offer rich API programmability.



The Network Plays a Big Role

Organizations can both use their network design to help proactively implement Zero Trust principles, as well as leverage any ability to limit, segment, or otherwise isolate communications dynamically to quickly and effectively respond to potential threats, stopping them in their tracks.

Optional Capabilities

- **SD-WAN:** Software-Defined Wide Area Networks (SD-WAN) create logical, encrypted overlay networks over a public infrastructure, like the Internet. SD-WAN allows for micro-segmentation of WAN traffic and remote office connectivity, all while providing centralized management.
- **SDN:** Ability to provision and manage network configurations on programmable infrastructure via a network controller and APIs. SDN enables the network to dynamically respond to threats, enhancing your organization's cyber resiliency.
- **Fully Encrypted Traffic:** In traditional networks, there is still control plane communication that is unencrypted (e.g., STP, LLDP, ICMP, etc.). To encrypt all traffic, both control and data plane, you need to move to a SDN architecture where the underlying physical network is cryptographically separated from the logical network where data plane traffic flows.

Data

Data is at the center of Zero Trust. Data is the ultimate target for a cyber adversary, whether their goal is to steal it (cyber espionage), destroy it (offensive capabilities), or hold your organization hostage (ransomware). A clear understanding of an organization's data is critical for successful implementation of ZTA. Organizations need to categorize their data in terms of mission criticality and use this information to develop a comprehensive data management strategy as part of their ZTA roadmap.

Required Capabilities

- **Role Based Access Control (RBAC):** Organizations can create "roles" and associate them with a set of allowed data operations. Each user within an organization can then be
- **Software-Defined Storage (SDS):** Ability for software to provision and manage storage configurations on programmable infrastructure such as physical and virtual Network Attached Storage (NAS), Storage Area Networks (SAN), and Hyperconverged Infrastructure (HCI).
- **Data Discovery:** Ability to discover data based on key words, RegEx, hashes, or fuzzy matches.
- **Data Tagging:** Ability to assign metadata, or tag, to a file either manually or in semi-automatic fashion. ZT system can then enforce granular access control based on the assigned data tags.

Know Where Your Data Exists

Every aspect of Zero Trust is working in concert to make sure only the right individuals have the right access to your organization's valuable data. By understanding where it exists within the environment, it's possible to implement more effective Zero Trust strategies that find the right balance between productivity and security.

- **Data Loss Prevention (DLP):** DLP is the policy enforcement extension of data discovery and data tagging capabilities. DLP can be implemented as an endpoint agent, a network tap or as storage crawler to actively prevent exfiltration of organization's sensitive data.
- **Immutable Backups:** These are data backups that cannot be modified by a malicious administrator or ransomware agent.
- **Data Encryption and Key Management:** Needless to say, in the ZT model, all data needs to be encrypted with strong ciphers, whether data is at rest or in motion. A Key Management System (KMS) is required to regularly update the encryption keys. Look for a KMS system that is FIPS 140-2, Level 1 and 3 validated.

Optional Capabilities

- **Attribute Based Access Control (ABAC):** ABAC takes RBAC and makes it more granular. Allowed data operations are now based not only on roles but also user attributes, such as geography, time of day, security risk, type of device, etc. (The Kipling Questions)
- **Fully Automatic Data Tagging:** Ability to leverage Artificial Intelligence (AI) and Machine Learning (ML) to intelligently tag data without human intervention.
- **Data Rights Management (DRM):** DRM uses cryptographic techniques to prevent unauthorized users or devices from modifying, accessing, or distributing data beyond an allowed boundary.
- **Runtime Encryption:** Ability to protect application data in memory, at runtime.

Security

Why did we leave security till last? The reason is that in previous sections we already outlined security capabilities for Identity, Workload, Device, and Data pillars of the Zero Trust model. However, we didn't touch on the "*Visibility and Analytics*" and "*Automation and Orchestration*" pillars. These are the capabilities we would like to cover here.

Required Capabilities

- **SIEM:** SIEM collects, aggregates, normalizes, and correlates log data for detection and evaluation of security events. SIEM provides real-time feedback on the security posture of enterprise information systems. In context of ZTA today, an SIEM can be viewed as a quasi-PDP. With time, as dedicated PDP products come on the market, an SIEM will serve as another input to the PDP to make a policy enforcement decision.
- **SOAR:** SOAR capability is a natural extension of a SIEM and provides structured, event-driven, automated responses to security events. SOAR can make your existing security controls "Zero Trust capable." For example, a traditional firewall has static rules. SOAR can use APIs to instruct the firewall to dynamically adjust its rule set in response to security events generated by tthe SIEM, thus transforming the firewall into a Zero Trust PEP.

Optional Capabilities

- **Threat Intelligence:** These provide information about newly discovered attacks and vulnerabilities from internal or external sources that help Zero Trust PDP make access decisions.
- **User Activity Monitoring (UAM):** Capability to monitor all types of user activity, including system, data, application, and network actions that users take (even web browsing habits), whether users are accessing unauthorized or sensitive files. This capability is raditionally implemented in an SIEM, but can also be implemented within the identity, workload, device, or network components of ZTA.
- **Continuous Diagnostics and Mitigation (CDM) System:** We already called out inventorying, security posture management, compliance and configuration baselining capabilities for workloads and devices. Currently these are disparate products. With time, they will be consolidated and unified under a single platform that NIST and DHS call CDM.

Beyond Basic Security

The use of security solutions designed to improve visibility and response are key to the success of Zero Trust as threat actors change their focus, tactics, and execution, seeking to increase their ability to remain working undetected.

Evaluation Worksheets

Please feel free to print out the following evaluation worksheet pages, filling in a copy for each of the shortlisted vendors your organization is considering.

The online version of this worksheet can be found at:
goto.cg/3w4hiBV

Identity and Access Management

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Authentication/Authorization for All Users & NPEs		Transparent Auth. to All Svcs			
Continuous/Adaptive Authentication & Authorization		Privileged Access Mgmt (PAM)			
Multi-Factor Authentication (MFA)					
Support for Modern Identity Protocols					
Identity Federation					
Public Key Infrastructure (PKI) Support					
				Total Optional Score	

Workloads and Applications

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Software-Defined Compute (SDC)		Cloaked Applications			
Workload Inventory		DevSecOps			
Automated Compliance		Software Supply Chain			
Containers and Kubernetes Support					
ITSM Integration					
Mutual TLS (mTLS)					
				Total Optional Score	

Devices

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Device Authentication and Authorization		Browser-Based Architecture			
Agent-Based Architecture		Unified Endpoint Mgmt (UEM)			
Software-Defined Perimeter (SDP)		In-Session Monitoring			
Device Discovery and Baselining		IoT Segmentation			
Hardware and Software Inventory					
Device Compliance					
Endpoint Detection and Response (EDR)					
Works On-Premises and Off-Premises					
				Total Optional Score	

Network

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Macro-segmentation		SD-WAN			
Micro-segmentation		SDN			
Encrypted Data Plane		Fully Encrypted Traffic			
Application Bindings					
Centralized Management and Control					
API Programmability					
				Total Optional Score	

Data

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
Role Based Access Control (RBAC)		Attribute Based Acc Ctr (ABAC)			
Software-Defined Storage (SDS)		Fully Automatic Data Tagging			
Data Discovery		Data Rights Management (DRM)			
Data Tagging		Runtime Encryption			
Data Loss Prevention (DLP)					
Immutable Backups					
Data Encryption and Key Management					
				Total Optional Score	

Security

Required Features		Optional Features			
Capability	Avail.	Capability	Imp.	Score	Calc.
SIEM		Threat Intelligence			
SOAR		User Activity Monitoring (UAM)			
		Cont Diag & Mitig (CDM) System			
				Total Optional Score	

Forcepoint

About the Sponsor

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

To learn more, visit ***www.forcepoint.com***

About the Author

Andrey Zhuk is a Cloud Security Architect at CTG Federal, where he helps US Government Agencies adopt new cloud services and secure agency assets in the cloud. Andrey is an experienced cloud, cyber and network architect with over 13 years of experience in US Federal Government space.