Zero Trust Cybersecurity
Current Trends

April 18, 2019

American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology (ACT) is a non-profit educational organization established to create a more effective and innovative government. ACT-IAC provides a unique, objective, and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communication between government and industry, collaborative and innovative problem solving, and a more professional and qualified workforce.

The information, conclusions, and recommendations contained in this publication were produced by volunteers from government and industry who share the ACT-IAC vision of a more effective and innovative government. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over thirty years of experience, to produce outcomes that are consensus-based. The findings and recommendations contained in this report are based on consensus and do not represent the views of any particular individual or organization.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC does not accept government funding.

ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of technology. For additional information, visit the ACT-IAC website at www.actiac.org

Disclaimer

This document has been prepared to contribute to a more effective, efficient, and innovative government. The information contained in this report is the result of a collaborative process in which a number of individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product, or vendor.

Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.

Copyright

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or www.actiac.org.

Table of Contents

Executive Summary

Recent advances in technology create many opportunities to significantly modernize government services to catch up with private sector capabilities and citizens' expectations. The proliferation and continuation of serious cybersecurity incidents demonstrate that current approaches to protecting government systems and data are inadequate. Today's systems are expanding and evolving into mobile and cloud-enabled environments that stretch traditional perimeter-based cybersecurity approaches to the breaking point. Unless these deficiencies and challenges are addressed effectively and expeditiously, the government will be unable to properly protect our national assets and realize the potential benefits technology advances offer. Clearly, new and more effective approaches to cybersecurity are required. One new approach, known as "Zero Trust (ZT)", has the potential to substantially change and improve agencies' abilities to protect their systems and data. ZT is a security concept anchored on the principle that organizations need to proactively control all interactions between people, data, and information systems to reduce security risks to acceptable levels.

Despite increasing budget challenges, an overtaxed workforce, and difficulties recruiting and retaining qualified talent; agencies are still expected to modernize their aging cybersecurity architectures to address new threats and service requirements. ACT-IAC was asked by the Federal CIO Council to assess the maturity of ZT technologies, their readiness and suitability for use in government, and the issues agencies would face if they chose to pursue ZT. This report provides the results of that assessment.

Modern IT security solutions need to incorporate several minimum characteristics:

1. Segregate users, devices, data, and services, within a trust framework, to ensure every access request is validated and deliberately permitted or disapproved;
2. Be resistant and resilient to attack without a large administrative burden; and
3. Be able to easily and rapidly (if not automatically) adjust to an ever-changing service environment also without a large administrative burden.

ZT satisfies these characteristics by treating all users, devices, data, and service requests the same. It shifts from the traditional security policy of all assets in an organization being open and accessible to requiring continuous authentication and authorization for any asset to be accessible. This fundamental change is the essence of ZT. ZT is not a thing you buy, it is a security concept, strategy, and architectural design approach.

During the course of our work, we found that ZT solutions are widely available and currently in use in the private sector. Many companies are developing new capabilities and solutions to support ZT and there is healthy competition in the marketplace. We observed that no single, holistic ZT solution is currently available from a single vendor. Acquiring a comprehensive solution would require integration of multiple vendors' products and services. Many companies have established strategic partnerships and agreements with other companies to offer more

comprehensive, integrated, and interoperable solutions. We also found that several different ZT architecture approaches are available for agencies to choose from.

Implementing ZT does not require a wholesale replacement of existing networks or a massive acquisition of new technologies. ZT should augment other existing cybersecurity practices and tools. Many federal agencies already have elements of ZT in their infrastructure and follow practices that support it in their day-to-day operations. Elements such as identity credential and access management (ICAM), access standards based on trust algorithms, automated policy decisions, and continuous monitoring are critical complements to a successful ZT. ZT lends itself to an incremental approach. It affords agencies a lot of latitude on their scale, pace, risk appetite, and ultimate extent of implementation. However, it is important for organizations to have a firm grasp of their users and their roles, their data, and their technology assets before beginning to implement ZT.

Implementing ZT requires a "whole-of-agency" effort. Because ZT can affect mission program systems' security, risks, and performance, it is imperative for agency heads and affected program leaders to work together with IT staff on the design and implementation of ZT. Absent this engagement, there can be a high rate of perceived failure in information technology (IT) projects even when the project is 100% compliant with its requirements[1]. ZT needs to be mission-driven, not an IT-driven effort for its own sake.

Project Background

In May, 2017, the President established the American Technology Council (ATC) to promote the secure and efficient use of IT across the federal government and directed it to produce a report on modernizing federal IT. The IT Modernization Report[2], published later in 2017, and associated Executive Order 2, will enable agencies "…to move from protection of their network perimeters and managing legacy physical deployments toward protection of Federal data and cloud-optimized deployments." It acknowledges that success in this effort requires new approaches and strategies; not only in applied technology, but also in legal, policy, resource allocation, acquisition, and workforce areas.

In May 2018, the Federal CIO Council Services, Strategy, and Infrastructure Committee asked ACT-IAC to undertake a project related to zero trust (ZT) and potential federal agency adoption. Concurrently, federal agencies initiated a transition of network services from the current General Services Administration (GSA) Networx contract to the new Enterprise Infrastructure Solutions (EIS) contract by March 2023. The federal government has a unique opportunity to capitalize

[1] Doherty, N. F., Ashurst, C., & Peppard, J. (2012). Factors affecting the successful realisation of benefits from systems development projects: Findings from three case studies. Journal of Information Technology, 27(1), 1-16. doi: http://dx.doi.org.library.capella.edu/10.1057/jit.2011.8

[2] https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

on the confluence of IT modernization and EIS transition to profoundly transform agencies' network service delivery and data protection.

ACT-IAC established a project team of government and industry volunteers primarily from its Networks and Telecommunication and Cybersecurity Communities of Interest. Their work was designed to assess the technical maturity and availability for procurement of ZT technologies and services and identify and address other important issues related to potential federal agency adoption.

The project focused on two work-streams. The first work-stream assessed what practical tools are available in the marketplace to support ZT and identified notional capabilities that are not yet procurable. Market research focused on assessing technology maturity and readiness, fitness for use, scalability, and affordability based on actual implementations. This included presentations and demonstrations by six companies (Cisco, Duo, Palo Alto, Zscaler, Fortinet, and Cyxtera) that already provide elements of ZT in their products and services to the commercial and public sectors. The second work-stream focused on trust algorithms. These dynamic algorithms are used to generate trust scores that are essential to comprehensive ZT solutions. Trust scores are used to grant, limit, or deny access based on defined criteria. The project team developed an understanding of the existing body of work on trust algorithms to advise federal agencies on this topic.

Other potential areas of study identified in early discussions, including implementation and policy issues and pilot projects, are outside the scope of this report. ACT-IAC may undertake additional work to address those issues in the future if requested.

What Is Zero Trust?

Zero Trust was introduced in 2004 as a security design concept by the Jericho Forum, a UK based group of Chief Information Security Officers (CISOs), after they saw the way access and authorization was changing due to the accelerated use of cloud and mobile computing This visionary group posited a security model that was right for a world where the traditional perimeter was dissolving, or becoming less relevant, workflows were moving to the cloud and mobile endpoints were becoming the norm for application access. In recent years, we have seen this accelerate as the move toward robust, fast 5G networks[3] has some organizations questioning whether they should provide network services at all. In 2010 John Kindervag, while doing research at Forrester, coined the term "Zero Trust" or "Zero Trust Networks" as a way to solve the de-perimeterization problem posed by the Jericho Forum. Since then, interest has increased in zero trust as a potential security approach to address the dissolving or constantly moving perimeter.

Most existing corporate networks are flat – i.e. there is little or no separation of data and user networks. That weakness of the traditional hub-and-spoke network model lies in its

[3]Fifth-generation (5G) is the latest iteration of cellular technology engineered to greatly increase the speed and responsiveness of wireless networks.https://searchnetworking.techtarget.com/definition/5G

architecture. Crossing the chasm from trust to distrust via a firewall is inherently risky. Instead, Zero Trust no longer distinguishes between “inside” and “outside” the network perimeter.

In general, Zero Trust:

- provides a consistent security strategy of users accessing data that resides anywhere, from anywhere in any way;
- assumes a “‘never trust and always verify” stance when accessing services and/or data;
- requires continuous authorization no matter what the originating request location; and
- increases visibility and analytics across the network.

Additionally, Zero Trust depends on five fundamental assertions:

- the network is always assumed to be hostile;
- external and internal threats exist on the network at all times;
- network locality is not sufficient for deciding trust in a network;
- every device, user, and network flow is authenticated and authorized; and
- policies must be dynamic and calculated from as many sources of data as possible.

Fundamental Pillars of Zero Trust

Zero Trust can be thought of as a strategic initiative that, together with an organizing framework, enables decision makers and security leaders to achieve pragmatic and effective security implementations. ZT efforts need to incorporate, coordinate, and integrate a challenging combination of policies, practices, and technologies to succeed. A conceptual security model can be helpful to understand and organize those components (see Figure 1 for an example of a zero trust security model).

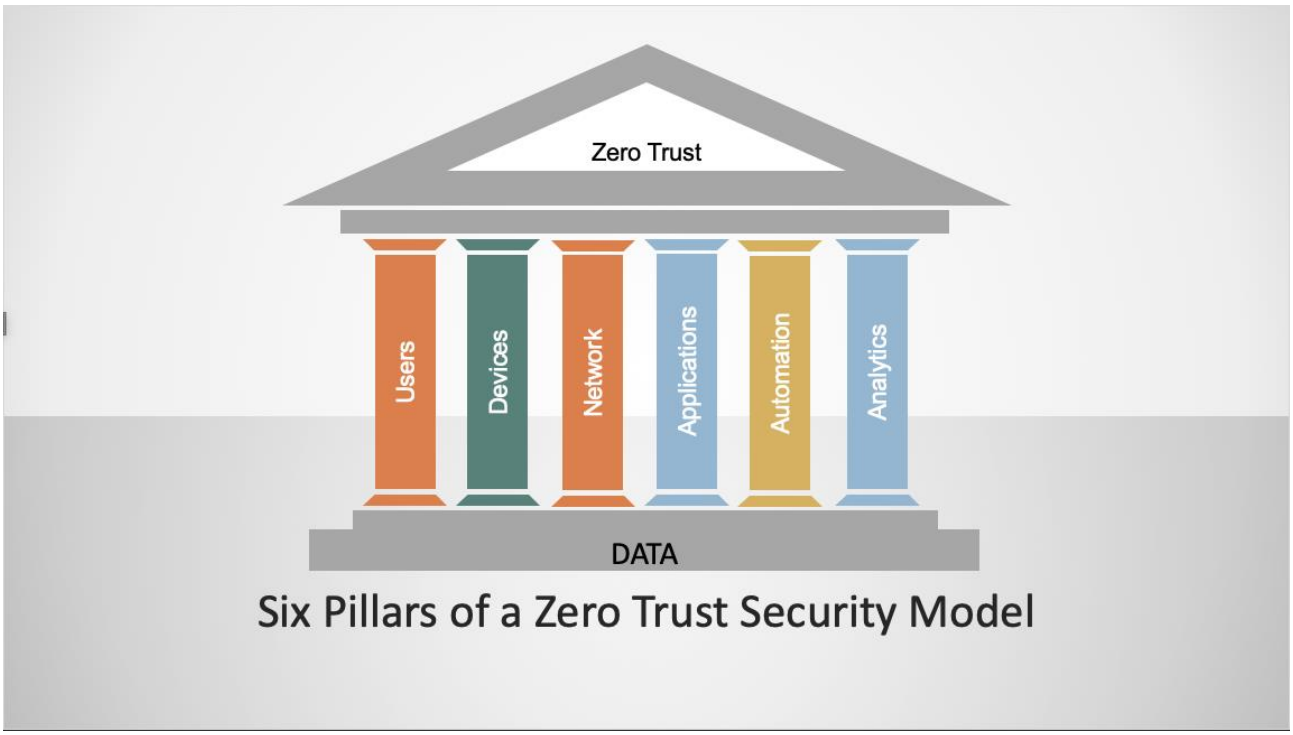


Figure 1 - Six Pillars of a Zero Trust Security Model

Mission Focus

Ensuring that mission program and executive leaders understand the need for and support Zero Trust capabilities will help ensure a successful implementation. IT capabilities exist within the organization to enable the mission and do not exist for their own sake. This logic extends to Zero Trust. The need for information protection should be driven by the mission with fulfillment by the IT organization. IT organizations should work with the mission and senior leadership to garner support and champions to create an organizational requirement for Zero Trust.

Data Foundation

The purpose for a Zero Trust architecture is to protect data. A clear understanding of an organization's data assets is critical for a successful implementation of a zero-trust architecture. Organizations need to categorize their data assets in terms of mission criticality and use this information to develop a data management strategy as part of their overall ZT approach.

Pillar #1 - Users
People/Identity Security

Ongoing authentication of trusted users is paramount to ZT. This encompasses the use of technologies like Identity, Credential, and Access Management (ICAM) and multi-factor authentication and continuously monitoring and validating user trustworthiness to govern their access and privileges. Technologies for securing and protecting users' interactions, such as traditional web gateway solutions, are also important.

Pillar #2 - Devices
Device Security

Real-time cybersecurity posture and trustworthiness of devices is a foundational attribute of a ZT approach. Some "system of record" solutions such as Mobile Device Managers provide data that can be useful for device-trust assessments. In addition, other assessments should be conducted for every access request (e.g. examinations of compromise state, software versions, protection status, encryption enablement, etc.).

Pillar #3 - Network
Network Security

Some argue that perimeter protections are becoming less important for networks, workflows, tools and operations. This is not due to a single technology or use-case, but rather a culmination of many new technologies and services that allow users to work and communicate in new ways. Zero Trust Networks are sometimes described as "perimeterless", however this is a bit of a misnomer. Zero Trust Networks actually attempt to move perimeters in from the network edge and segment and isolate critical data from other data. The perimeter is still a reality, albeit in much more granular ways. The traditional infrastructure firewall perimeter "castle and moat" approach is not sufficient. The perimeter must move closer to the data in concert with micro-segmentation to strengthen protections and controls.

Network security is expanding as agencies grow their networks to partially or fully transition to Software Defined Networks, Software Defined Wide Area Networks and internet-based technologies. It is critical to (a) control privileged network access, (b) manage internal and external data flows, (c) prevent lateral movement in the network, and (d) have visibility to make dynamic policy and trust decision on network and data traffic. The ability to segment, isolate, and control the network continues to be a pivotal point of security and essential for a Zero Trust Network.

Pillar #4 - Applications
Application and Workload Security

Securing and properly managing the application layer as well as compute containers and virtual machines is central to ZT adoption. Having the ability to identify and control the technology stack facilitates more granular and accurate access decisions. Unsurprisingly, multi-factor authentication is an increasingly critical part of providing proper access control to applications in ZT environments.

Pillar #5 - Automation
Security Automation and Orchestration

Harmonious, cost effective ZT makes full use of security automation response tools that automate tasks across products through workflows while allowing for end-user oversight and interaction. Security Operation Centers commonly make use of other automated tools for security information and event management and user and entity behavior analysis. Security orchestration connects these security tools and assists in managing disparate security systems. Working in an integrated manner, these tools can greatly reduce manual effort and event reaction times and reduce costs.

Pillar #6 - Analytics
Security Visibility and Analytics

You can't combat a threat you can't see or understand. ZT leverages tools like security information management, advanced security analytics platforms, security user behavior analytics, and other analytics systems to enable security experts to observe in real time what is happening and orient defenses more intelligently. The focus on the analysis of cyber-related event data can help develop proactive security measures before an actual incident occurs.

Other Zero Trust Security Models

Several other models are available to help organizations understand the concepts and guide their efforts to introduce zero trust into their environments. One model is the Zero Trust eXtended (ZTX) Ecosystem framework[4] developed by Forrester. The framework is described as a security architecture and operations playbook. Another model is the Continuous Adaptive Risk and Trust Assessment (CARTA)[5] model from Gartner. CARTA is described as an approach to support digital business transformation in an environment of advanced threats that requires a new approach for all facets of security. Zero Trust can be a subcomponent of the overall CARTA security approach.

Privacy Concerns

It is very important to integrate privacy into ZT architecture designs and lifecycle processes. Privacy concerns around IT investments are increasing as we push computing to "the edge" resulting in an increasingly complex world of interconnected information systems and devices. The full integration of privacy controls into the security control catalog is a primary objective of the next generation of the NIST SP 800-53 (rev 5) security and privacy control standards. ZT implementations will likely have new and different approaches to monitor user behavior and/or track user identity. ZT practitioners need to ensure they comply with applicable privacy laws,

[4] https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210
[5] https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/

regulations, standards, and policies. Success in this area can be best achieved by closely coordinating design and development efforts with agency privacy officers. It is especially important to make sure that all ZT implementations have appropriate disclosures in agency privacy impact assessments (PIAs) as required by section 208 of the E-Government Act of 2002[6]. For additional information on managing privacy risk, please refer to NISTIR 8062, "*An Introduction to Privacy Engineering and Risk Management in Federal Systems"*.[7]

BeyondCorp – An Example of Zero Trust

The most talked-about and documented early example of a Zero Trust implementation is the Google "BeyondCorp" model[8] (see Figure 2). BeyondCorp is offered as an example of an actual Zero Trust implementation. While Google is a commercial enterprise, many of their internal components should be familiar to any enterprise. This example is provided for illustrative purposes only and does not imply endorsement or recommendation for adoption by any other organization.

BeyondCorp is based on the original Zero Trust premise that traditional perimeter-based security is not sufficient to protect internal networks and data. Also, Google recognizes and promotes the growth of cloud technologies and moving applications from on-premise data centers to cloud-provided applications and services. Several principles are essential to BeyondCorp's Zero Trust approach:

- Connecting from a particular network must not determine which services you can access.
- Access to services is granted based on what we know about you and your device.
- All access to services must be authenticated, authorized and encrypted.

Additionally, Google BeyondCorp identifies the following components that can be mapped to the Zero Trust pillars listed above:

- Single sign-on
- Access proxy
- Access control engine
- User inventory
- Device inventory
- Security policy
- Trust repository

---

[6] https://www.govinfo.gov/app/details/PLAW-107publ347

[7] https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[8] https://cloud.google.com/beyondcorp/

- User inventory
- Device inventory
- Security policy
- Trust repository

The components are delivered as part of the Google Cloud Platform with many being delivered by Google Integrated Access Proxy. Since this is a cloud-only delivery strategy, the use of virtual software based solutions to compliment the use of a Software Defined Perimeter is necessary. Applications are migrated to the cloud where granular access controls can be delivered. This eliminates the need to grant applications access into the Google intranet.

Google uses a proxy-based approach which acts as the enforcement point to control access to hosted applications that are delivered on the Google Cloud Platform. This proxy approach has been refined and is being delivered as the Cloud Identity-Aware Proxy offering that controls the essential pillars of Zero Trust.

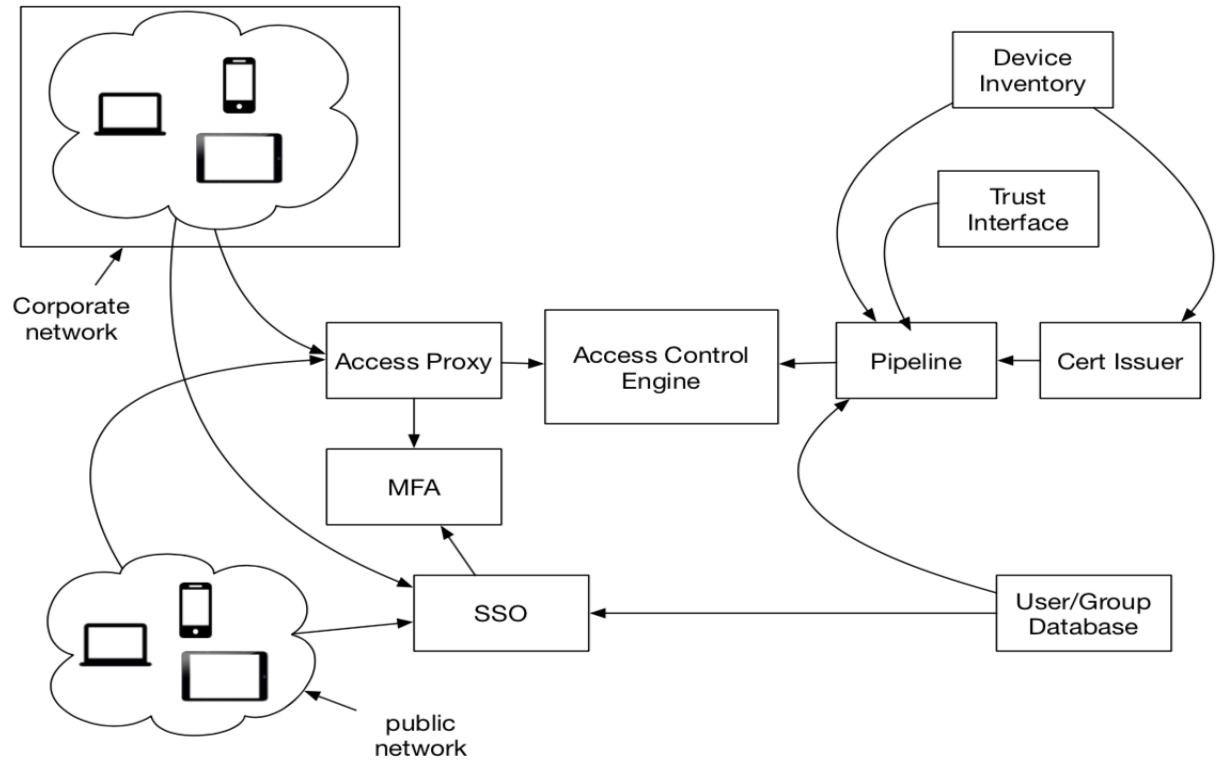


Figure 2 - Google BeyondCorp Model

Establishing Trust is Foundational

As a framework, Zero Trust implies innate distrust ("default deny") requiring an adaptive deployment model that emphasizes continuous monitoring and assessment. Dynamic, context-sensitive trust extension limits access based on whatever threshold credentialing policies assign. One of the first questions in this trust-centric shift is "How do we determine how trustworthy something is?" Many security organizations struggle to answer this question. Traditional programs assume all data and transactions are trusted and that compromises, loss of data, malicious actors, etc. would degrade that trust. Zero Trust flips the trust calculation by assuming all data and transactions are untrusted from the outset. The new question is "How do we gain sufficient trust?" While some key concepts and components can be applied to all deployments, there is no set formula that can be applied across every organization. Trust will change depending on the organizations' needs and focus. Zero Trust environments integrate controls for data, users, devices and apps to manage the trustworthiness of all transactions (refer to Figure 3).

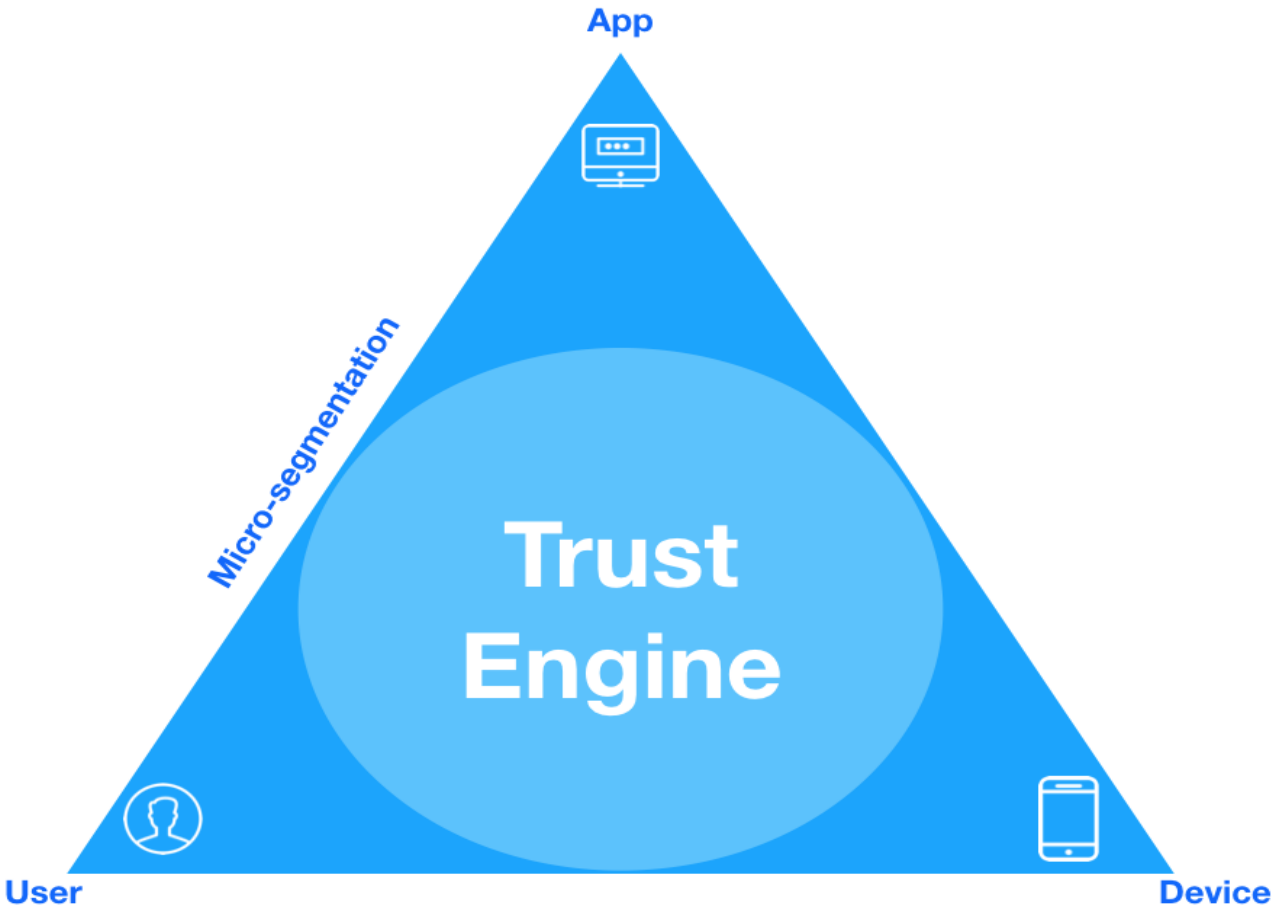


Figure 3 - Zero Trust Triangle

Trust Engine is a technology used to dynamically evaluate the overall trust of a user, device, or application in the network by giving it a trust score. The trust engine uses the calculated trust score to make policy-based authorization decisions for each transaction request.

Trust Score is a value calculated from factors and conditions, either pre-defined or selected by the organization, used to determine the trustworthiness of a given user, device, or application. Information like location, time of day, length of access, and action taken are examples of potential factors for determining the trust score.

Micro-segmentation is a security technique that enables fine-grained security policies to be assigned to data center applications, down to the workload level as well as devices. This means that security policies can be synchronized with a virtual network, virtual machine, operating system or other virtual security targets.

Within the Zero Trust Triangle, the Trust Engine evaluates the trustworthiness of any agent that enters the network via the use of a trust score. Agent, or "Network Agent", is the term given to the combination of data known about the actors in a network request, typically containing a user, application, and device. This combination of data is queried on demand in real-time to provide situational context to make the best authorization decisions possible. After the trust score is computed, the user, application, device, and score are bonded to form an agent. Policy can then be applied against the agent in order to authorize the request.

Zero Trust architecture is based on the Control Plane/Data Plane model (see Figure 4). The control plane is made up of components that receive and process requests from data plane devices that wish to access (or grant access to) network resources[9]. Almost everything else within the Zero Trust architecture is referred to as the data plane, which the control plane coordinates and configures. The data plane contains all of the applications, firewalls, proxies, and routers that directly process all traffic on the network.[10]

The architecture illustrated in Figure 4 supports requests for access to protected resources that are first made through the control plane, where both the device and user must be authenticated and authorized. Fine-grained policy can be applied at this layer, perhaps based on role in the organization, time of day, or type of device. Access to more secure resources can additionally mandate stronger authentication. Once the control plane has decided that the request will be allowed, it dynamically configures the data plane to accept traffic from that client (and that client only). In addition, it can coordinate the details of an encrypted tunnel between the requester and the resource. This can include temporary one-time-use credentials, keys, and ephemeral port numbers. While some compromises can be made on the strength of these measures, the basic idea is that an authoritative source, or trusted third party, is granted the ability to authenticate, authorize, and coordinate access in real time, based on a variety of inputs.[11]

[9] Sourced from :*Zero Trust Networks*, Evan Gilman & Doug Barth, ISBN: 978-1-491-96219-0

[10] Sourced from: *Zero Trust Networks*, Evan Gilman & Doug Barth, ISBN: 978-1-491-96219-0

[11] Sourced from: *Zero Trust Networks*, Evan Gilman & Doug Barth, ISBN: 978-1-491-96219-0

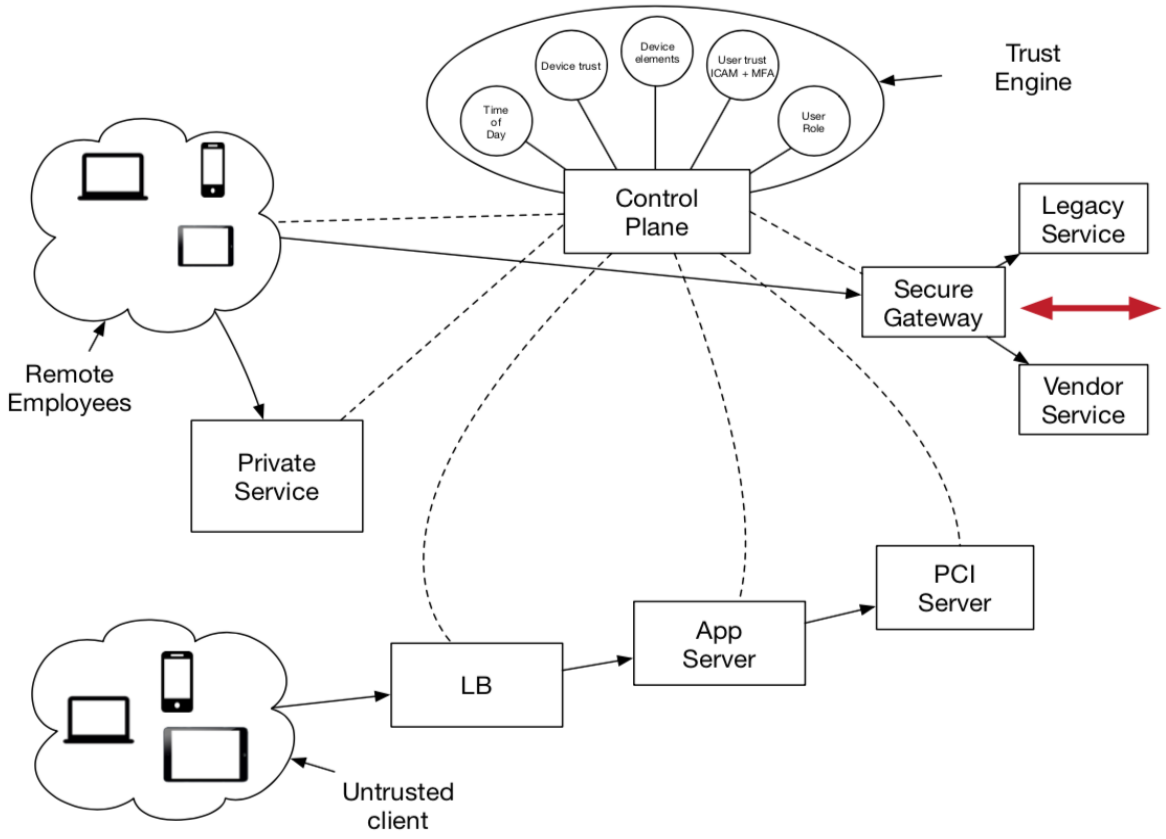


Figure 4 - Control and Data Plane Functionality Within the Zero Trust Architecture

The richness of information contained within the agent allows very flexible yet fine-grained access control, which can adapt to varying conditions by including the score component in policies. If the request is authorized, the control plane signals the data plane to accept the incoming request. This action can configure encryption details as well. Encryption can be applied to data at rest and data in motion at the device level, application level, or both. At least one is required for confidentiality.

With these authentication and authorization components, and the aid of the control plane in coordinating encrypted channels, the zero trust model can assert that every single flow on the network is authenticated and expected. Hosts and network devices can drop traffic that has not had all of these components applied, significantly reducing the likelihood of sensitive data leaks. Additionally, by logging each of the control plane events and actions, network traffic can be easily audited on a flow-by-flow or request-by-request basis.

Benefits Of Zero Trust

When evaluating the move to a Zero Trust architecture, both technical and business leaders within an organization must see the potential benefits. Core ZT outcomes should be focused on creating more secure networks, making data safer, reducing negative impacts from breaches, improving compliance and visibility, achieving lower cybersecurity costs, and improving the overall risk posture of the organization. The benefits realized depend on the degree to which ZT principles are deployed and on the operational model used. Lost or stolen data, exfiltrated intellectual property, and other types of breaches cost organizations money and reputations. Avoiding such occurrences is key to a successful ZT adoption.

A More Secure Network

Implementing a “never trust, always verify” approach should strengthen visibility into what is happening across the network. New tools can provide increased visibility into the user, device, location, and reputation of anyone requesting access. It is difficult for operators to prevent or repair what they cannot see, so visibility is key. If a user, device, or behavior is not recognized or is out-of-bounds of a user’s baseline risk score, they will be dropped. ZT also segments the internal architecture to limit user “roaming” often associated with system penetration breaches.

Traditionally, enterprises have deployed “internal firewalls” as a method of segmenting, but today enhanced approaches are available to enable micro-perimeters. With ZT, users can no longer log in and have the ”run of the network”. Instead, they are authorized to use only the specific micro-perimeters linked to pre-determined trust levels and access.

There are, however, challenges associated with implementing ZT’s stringent network, application, and data access rules. First, strong identity management and authentication tools must be properly configured and re-examined on a continual basis. User profiles must be kept current and trust algorithms carefully designed to facilitate proper access and usage rights. Second, users may find that access to critical data and systems is put under strict scrutiny and may be more time consuming than what they were accustomed to.

A Focus on Safer Data

Protecting data traversing and stored in a network is a major part of any network’s value. Protecting all data, whether at rest or in motion, is a major pillar of a ZT architecture. Key technologies aiding with this protection include encryption, virtual private networks (VPNs), and data loss prevention capabilities. Network operators can choose individual tools for each type of protection or they can choose a consolidated tool that offers multiple capabilities.

Recent trends associated with the move to cloud computing and the increase of “Internet-of-Things” devices have broadened the edge of the network. This can create opportunities for data to be manipulated, so extending protection for data as it moves around interconnected networks is important. ZT approaches stress identifying high value data and prioritizing protections for it. Protecting data with network segmentation can help avoid “brick” attacks

(deleted data), and in turn, can keep the data integrity high and reduce the likelihood of costly remediation lawsuits.

A key challenge associated with new data architectures that create encrypted data vaults is that they spread data around hybrid cloud environments requiring varying levels of authentication. These approaches may produce unacceptably long wait times for users to access their data. This requires careful data architecture planning and data categorization decisions that are grounded in solid risk management decisions.

Improved Protection Against Existing and Evolving Threats

Traditionally, threats evolve as quickly as security researchers release patches for vulnerabilities they find. Over time, leading edge companies learned that offering payment for vulnerability research, in the form of "bug bounties" is a very effective (and lucrative) way to identify vulnerable systems before they are exploited. This, in effect, pits legitimate security researchers against hostile "hackers": The competition between them continues to evolve the threat landscape. However, while the vulnerability marketplace benefits organizations, state-based hostile actors have also evolved.

State-funded hackers are well trained and resourced and persistent. There is sufficient evidence that many nation states have offensive cyber capabilities which are full-time jobs. The use of new tactics, techniques, and procedures, like artificial intelligence and machine learning combined with state-level exploit code (e.g., Eternal Blue), is growing exponentially. This can overwhelm a vulnerable organization's security operations team with more incidents than they can possibly address. It can also enable attackers to move laterally within a compromised organization with previously unseen speed and accuracy. Any new security capability must be resilient to the new reality and effectively lower both the external (Internet-discoverable) and internal (insider threat) attack surfaces.

Zero Trust addresses both of these issues in a similar, unbending manner: deny access to any service or data without sufficient authentication. In a standard current network design, a network agent is commonly granted access after working through a two-factor process of producing a memorized password and a token code or hardware authenticator. Adding ZT components, associated with a behavioral trust score, location ID, and micro-segmentation, would strengthen the decision of whether to allow an agent onto the network. Once on the network, it would prevent the ability to roam to unauthorized areas. Combining ZT capabilities with traditional tools like next-generation firewalls, data-loss prevention, and behavior heuristics can further strengthen the network.

Challenges associated with strong authentication include user convenience, process complexity, timeliness of access, and known vulnerabilities to "beat" the authentication process. For example, the answers to many common security questions used for authentication purposes can be found in public records (e.g. your father's middle name) or socially engineered (e.g. phishing emails or phone calls). Likewise, if someone's biometric data is stolen, it is compromised for life.

Reduced Impact from Breaches

Implementing a ZT architecture will reduce the impact of breaches due to the segmentation of the network and the fact that users are given limited access. Smaller impacts from a breach will reduce business disruption and keep remediation costs low. A smaller impact from a breach can help maintain an organization's reputation and trust by its customers and stakeholders. Segmentation is the key technology to limit the area impacted from a breach. Limiting access to only areas of the network where individual users need to go helps reduce the impact of breaches.

The challenge is to do provide adequate network segmentation to improve security layer while avoiding detrimental impacts to network performance, application performance, and business workflow needs. Access controls remain essential, but they must be reinforced with strong identification and authentication management practices, policies, and tools.

Improved Compliance and Visibility

There is no shortage of existing or pending compliance requirements for federal agency networks including the Federal Information Security Management Act, Federal Risk and Authorization Management Program (FedRAMP), Trusted Internet Connections (TIC) 3.0, and National Institute of Standards and Technology (NIST) publications. Applying these requirements across an entire network can be challenging; however, through a segmented approach, compliance can often be addressed in smaller, more relevant audits allowing agencies to meet compliance requirements more quickly. A reusable template approach can be used for network segments that have similar characteristics. The key benefit is speed to compliance. There are also benefits from improved visibility within a ZT architecture. Improved visibility of who, what, and where enables network operators to more closely log behavior and activities. Analytics processed from the improved visibility further benefit the network operators.

There are certainly challenges in implementing strong network segmentation practices and getting CISOs to accept re-use of common templates for similar network segmentations. In addition, audit entities (internal and external) need to be on-board with smaller, targeted audits of segment networks and understand the interdependencies that exist.

Potential Cost Reduction

Lower costs can result from better integrated tools, reduced VPN usage, simpler operational models, and avoidance of lost data, lawsuits, and damaged reputations. Each of these potential cost savings can become an added benefit of the ZT architecture. Government organizations may seek to refresh infrastructure using low cost commodity circuits made feasible (with respect to risks) when coupled with ZT architecture. These lower cost, direct Internet access circuits also promote the added benefit of more secure Software-Defined Wide Area Network (SD-WAN) connections.

As with all technology changes, the challenge associated with demonstrating higher return-on-investment and reduced overall cybersecurity costs is the time required to deliver results. Some

costs can be reduced relatively quickly while others require more time. Organizations should consider the following:

- Assess what components/elements an agency already has deployed (or soon to be deployed) that address the various pillars of Zero Trust. These are sunk costs that may not need to be included in new ROI calculations or discussions. Moreover, integration with existing tools can dramatically lower investments needed to operate ZT.
- ROI is not easy to justify without factoring in the "costs" or impact associated with risk levels and occurrences.
- Bottom line - Zero Trust must simplify, not complicate, your security strategy to save money.

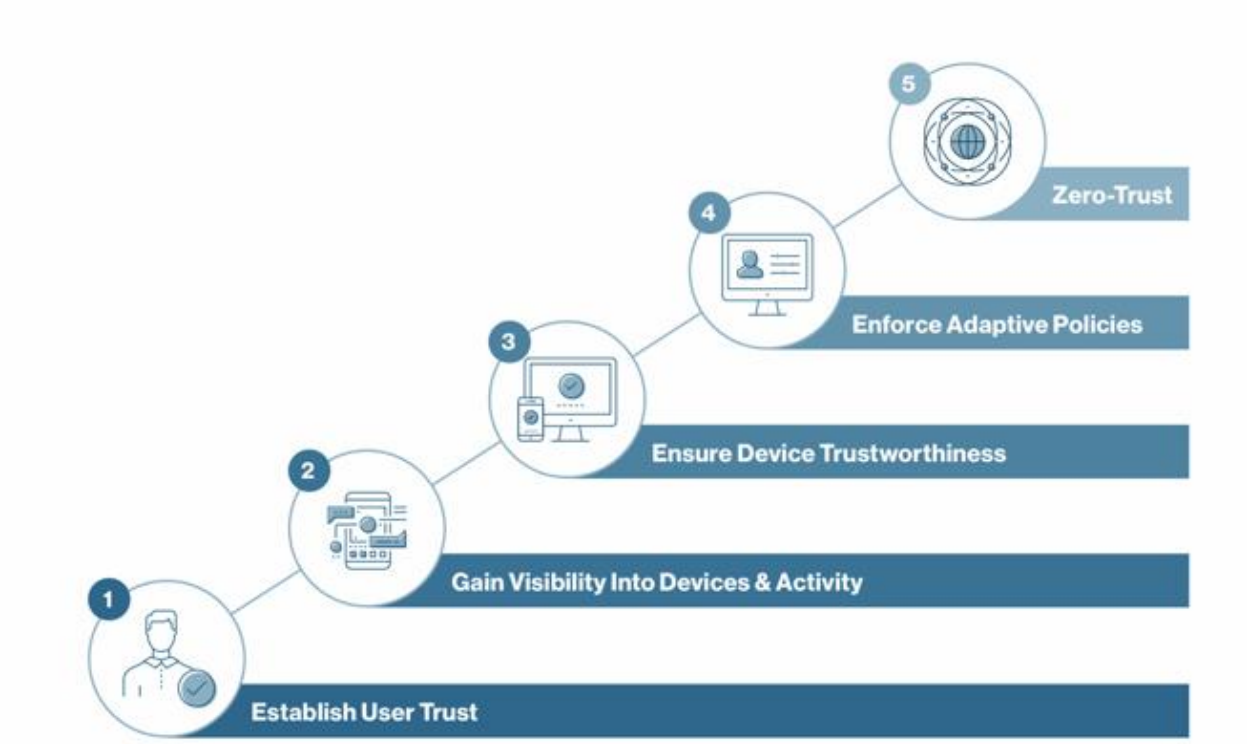
Suggested Steps to Deploy Zero Trust

If you are planning to include Zero Trust in your security strategy, your current environment may already include ZT tools and components that can be leveraged. For example, an agency that already has a strong ICAM implementation, with multi-factor authentication, can leverage it to support the Zero Trust "user pillar" capability. Similarly, if an agency has Mobile Device Management or system inventory tools, they could be leveraged for the "device pillar" component. In any changes to security architecture, it is important to consider what existing spending can be leveraged and how and where the new model can be implemented quickly.

None of the companies ACT-IAC invited to participate in this project identified a single, comprehensive Zero Trust solution. They work with other companies that offer complementary capabilities to provide complete solutions. It is important to ensure the right approach is chosen early in the planning stage. In choosing a specific ZT solution, decisions must balance security and costs and be able to solve both today's and tomorrow's challenges. Zero Trust can provide a mature solution today that does not need to add operational complexity or require major architecture changes. In fact, it can simplify operations while increasing security and protecting critical, high value assets.

The abilities to see and verify who has access to applications and data and ensure that trusted traffic has not been compromised is critical. Solutions should be able to analyze allowed traffic for active threats, malware, viruses, compromised credentials and restricted sensitive data. Behavioral analytics and automation can be applied to consolidated logging to stop hidden bad actors from appearing to be trusted. Zero Trust is about using the pillars for granular, limited, and validated access control. A common framework will allow these pillars to work in unison while reducing complexity through integration and strategic partnerships.

Zero Trust Networking transitions don't have to happen all at once. A ZT maturity model can help guide organizations embarking on a Zero Trust journey. The model can help organize, track, and communicate the work being done. These models can be customized to account for where the effort begins and track progress across the major milestones. Figure 5 contains an example of a maturity model:



Stage 1		Stage 2		Stage 3		Stage 4		Stage 5	
Establish User Trust		Device and Activity visibility		Trustworthy Device		Adaptive Policies		Zero Trust	
	Rate		Rate		Rate		Rate		Rate
Does your organisation have a clear ICAM strategy aligned with its business needs that has resulted in a full implementation and integration of an MFA solution supported by risk based policies?	2	Does your organisation have an up to date asset inventory that distinguishes between managed and unmanaged devices providing a hygienic check on them as part of an integrated IT and security function	3	Does your organisation have a trusted device policy that prompts users to update their devices against measured vulnerabilities within a managed process and reports on out of policy devices?	2	Does your organisation control user access through a centrally managed policy that identifies and acts upon exceptions	3	Does your organisation have a business aligned zero trust strategy supported by an architecture and set of processes that enables users to seamless access both in premise and cloud applications	1

Acme Corporation Current Status

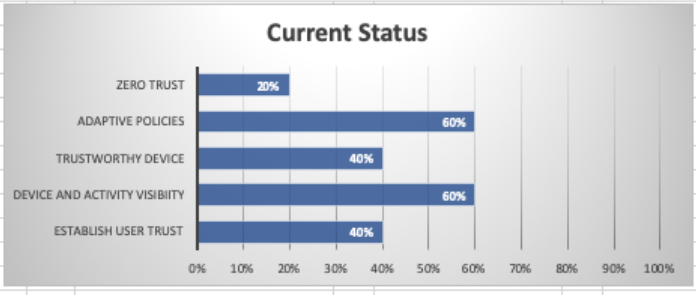


Figure 5 - Example of Zero Trust Maturity Model

As Gartner Research's Neil McDonald writes in his December 2018 report "Zero Trust Is an Initial Step on the Roadmap to CARTA[12]","…most enterprise data centers are isolated from public networks and separated from end-user hardware. As with end-user access to the public internet, access to a data center is granted based on trust...trust typically established by validation of an IP address. In a data center, proprietary enterprise information and applications are stored laterally. That flat hierarchy means that if a bad actor infiltrates the data center, all information is at risk." As McDonald notes, "An attacker that gains a foothold on one server can easily spread laterally (east/west) to other systems." That kind of lateral movement is a common vector for threats to spread – consider the recent Cryptolocker and Petya malware infections.

Microsegmentation can help defend against lateral movements Microsegmentation is a network-management approach that – as its name implies – segments user traffic into contextual lanes. As Network World's Ann Bednarz notes[13], microsegmentation allows enterprises to isolate workloads, and secure them from one another. Policy definition is logical, meaning that network traffic can be narrowed to isolated user channels. Think of it as a secure tunnel between an authorized user, an application, and their device. More importantly, microsegmentation dissociates segmentation security policy by IP address, and instead associates defined-access policy by that authorized user and app. It also (generally) mandates segment-monitoring, baseline flow assessment, and anomaly detection.

Common microsegmentation steps include:

1. Perform an audit. Map all forms of network connectivity (including LAN, WAN/SD-WAN, remote, even internet local breakouts) between users, applications, data stores, etc.
2. Identify risks.
3. Define a "default-deny" segmentation approach: What will you secure? What will you isolate? Will you use containers or even APIs to segment traffic?
4. Define policy by segment: Ensure policy is tied to logical attributes not IP addresses.
5. Assess the technology gap, including (according to Gartner's McDonald) network overlays, encryption, SD-WAN integration, security appliances (both physical and virtual), etc.

Another option is the use of a Software-Defined Perimeter (SDP) to enable access without sacrificing security. With SDP, users, regardless of whether they are inside or outside the network, connect directly to resources, whether they reside in the cloud, in the data center, or on the internet; all without connecting to the corporate network. SDP security software establishes a secure perimeter around each user's network traffic – creating a network of one, so to speak. As an example, Google employs its own SDP for employees called BeyondCorp.

With agencies aggressively moving to more evolving network models, it is no longer efficient to backhaul traffic through central locations just to access increasingly mobile data from

[12] https://www.gartner.com/doc/3895267/zero-trust-initial-step-roadmap
[13] https://www.networkworld.com/article/3247672/virtualization/what-is-microsegmentation-how-getting-granular-improves-network-security.html

increasingly mobile locations. With the evolving and expanding structure of government networks, the Internet, a network not controlled by agencies, has become the new network that is used to access data. New technologies need to be used to help agencies maintain control and visibility over the increasing number of connections and transports for data, e.g. technologies such as SDP. Users (or an SDP host) cannot initiate or accept communication with another SDP host until after connecting to an SDP Controller that authorizes the transaction. A key concept in SDP approaches is the SDP Controller instructions to SDP hosts removes the need for DNS information and port visibility to the "outside" effectively "cloaking" or creating an invisible "dark" network to outsiders.

SDP represents an approach to cybersecurity that creates a protective barrier around high value enterprise applications and data access. This technology, and others like it, can protect application infrastructure against existing and newly emerging cyber threats. For example, existing attacks such as credential theft and server exploitation are blocked dynamically as these technologies only allow access from devices registered to authenticated users which is a key Zero Trust element.

SDP capabilities can be successfully delivered in different ways, e.g. via an agent, in-line software, as a cloud service, and in some cases, even on-premise. SDP comports with Zero Trust by maintaining a default-deny posture for every transaction. Policy is defined by user and context (typically including behavioral analytics), reducing risk below that of micro-segmentation alone. The risk of unauthorized lateral movement is eliminated because all transactions are assessed the same way they occur inside or outside the enterprise firewall.

Commitment to moving to a software-based security model is key to SDP success. Government agencies evaluating SDP options must consider:

- Distributed security model (e.g. how many data centers serve cloud-based security access?)
- To what extent can network security hardware be sunsetted?
- Supported app platforms – running in a federal data center? Or a government cloud?
- Treatment of unmanaged devices – can users employ mobile devices (including tablets and smartphones) to get their work done?

SDP enables authenticated users to access authorized applications and data running in any environment without placing the users on the network or exposing private applications to the internet. Any technology being explored for Zero Trust networks should support the following essential principles:

- maintaining authentication
- dynamic authorization and trust, and
- constant visibility.

Challenges to Zero Trust in the Federal Government

As noted, Zero Trust is a security strategy that is comprised of elements that are very much in use today in the federal space. Nevertheless, there are challenges in deploying and operating any new technology. There are also challenges which are unique to specific operating environments. The challenges in the federal government are due in part to a combination of its size, maturity, and dependencies. How they affect deploying and operating a ZT solution is addressed below.

Wide Variances in Cybersecurity Maturity

The largest operational challenge to deploying successful ZT solutions across the federal government is the general lack of cybersecurity maturity. Most federal agencies lack the fundamentals (e.g. agency policies, processes, and tools) requisite to undertaking a ZT deployment. This is evidenced by the Federal Cybersecurity Risk Determination Report[14] (May 18, 2018) which identified, among other things, a general lack of standardized IT capabilities and network visibility. These factors alone create an operational challenge which can delay a successful ZT implementation by months or even years as agencies struggle to work through basics like application and server inventory. Adopting a ZT maturity model approach to implementation can help address critical capabilities needed to successfully and more rapidly address roadblocks and move agencies into increasingly mature cybersecurity postures.

There are over one hundred small federal agencies that face another operational challenge. Zero Trust can augment an organization's existing suite of cybersecurity tools but it will not replace them. Most small agencies lack the budget and IT security expertise necessary to achieve compliance with the myriad cybersecurity and risk management requirements. Even if they have a solid grasp on policies, processes, and tools, unless an external organization (e.g. DHS, GSA's Centers of Excellence, etc.) provides assistance and support, Zero Trust is unlikely to be implemented in many small agencies. Complicating the issue, centrally-provided security services are often too expensive for small agencies to afford.

Shared System and Network Connections

Another challenging aspect of a successful Zero Trust deployment is the widespread system interdependencies in federal IT. Nearly every federal agency receives or provides, services (e.g., billing, time and attendance, travel, human resources, etc.) from/to other federal agencies. Ensuring a successful ZT deployment will require detailed provider and customer coordination and interaction at a technical level, which in turn may require a service provider to divulge

[14]https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf

information which may not have been previously required. Agencies unfamiliar or unprepared to support a partner agency ZT deployment may add unforeseen delays.

Centralized service providers who are prepared can quickly and easily transfer required information, but ZT deployments may also experience complications where there are multiple dependencies. This can be especially impactful with large-scale extra-agency dependencies which are highly regulated (e.g., financial and health sectors). Lastly, these dependencies are a two-way street: as private-sector partners move to ZT solutions, federal agencies can expect to support requirements. In all cases, communicating early and often with service providers, partners, and customers will go a long way in overcoming these challenges.

Moving Away from Compliance Focus

While the challenges listed above are difficult, they're only part of the picture. Cybersecurity requirements increase at a greater pace than the budgets to address them. This creates a culture of "chasing green" (i.e., the red, yellow, green performance scoring model): focusing less on managing risk and more on the reportable elements which are seen up the chain. For instance, Continuous Monitoring is a critical aspect of any effective cybersecurity program, but so is Threat Intelligence and Red Teaming exercises: but only one is reported up. Therefore, it's unlikely to see widespread adoption of Zero Trust unless it is designated as a government-wide priority–All relevant activities associated with Zero Trust need to be a key focus for agencies to achieve the desired outcomes. Designating Zero Trust a government-wide priority could also promote wider and faster adoption.

Incorporating TIC 3.0 Requirements

Another challenge with ZT and how it works with or supports the new Trusted Internet Connection (TIC) 3.0 guidance. The following list of TIC Use Cases were released in concert with the TIC 3.0 memorandum. DHS intends that this effort will result in the continuous improvement and development of updated TIC Use Cases that account for emerging technologies and evolving cyber threats. DHS has defined four different use cases to cover areas such as cloud applications (Use Case #1), agency branch offices located outside of the agency defined security perimeter (Use Case #2), remote users located outside of the agency defined security perimeter (Use Case #3) and traditional TIC security approached not covered in the other DHS TIC Use Cases (Use Case #4). The following DHS-defined TIC Use Cases best fit a ZT solution approach:

Use Case #1 - Cloud: These sets of (growing) TIC Use Cases cover some of the most prevalent cloud models used by agencies today. These include:

a. Infrastructure as a Service (IaaS)

b. Software as a Service (SaaS)

c. Email as a Service (EaaS)

d. Platform as a Service (PaaS)

The use of ZT can fit into either the Software as a Service (SaaS) or within an established Platform as a Service (PaaS) categories of cloud services. Any ZT cloud based functionality that is FedRAMP certified can be developed for an approved TIC 3.0 use case #1 application.

Use Case #2 - Agency Branch Office: This use case assumes that there is a branch office of an agency, separate from the agency headquarters (HQ), which utilizes HQ for the majority of their services (including generic web traffic). This case supports agencies that want to enable SD-WAN technologies. An SD-WAN connection to a ZT FedRAMP approved SaaS Cloud application is a good fit for this defined TIC 3.0 use case.

Use Case #3 - Remote Users: This use case is an evolution of the original FedRAMP TIC Overlay (FTO) activities. The use case demonstrates how a remote user connects to the agency's traditional network, cloud, and the Internet using government furnished equipment (GFE). A FedRAMPed ZT solution is a good fit for this DHS defined TIC 3.0 case

Ability to Procure Zero Trust Networks in the Federal Marketplace

If federal agencies are looking for a specific Zero Trust procurement vehicle in the marketplace, they won't find it today. However, now that there is an understanding that ZT is a "framework and architecture", there are plenty of options to procure the enabling technology product and service components. It is likely that a ZT undertaking would involve both services and products, so it is recommended that agencies pursue contract vehicles that can accommodate both. Additionally, agencies should look for flexibility in the service offerings to allow them to customize their statements of work to meet the exact needs of their projects to include the potential for a complete managed service arrangement. The following are examples of how ZT can fit into some of the most widely used federal contract vehicles

GSA SCHEDULE 70

This long running contract has been a solid option for years and has served the government well. Agencies can procure a wide array of ZT components through Schedule 70 to include a focused listing of cyber offerings under "Highly Adaptive Cybersecurity Services" SIN 132-45. There seems to be enough flexibility with Schedule 70 to buy products, services, or any combination. Of course, it is recommended that agencies verify any procurement approach with their internal, expert contract and procurement teams before proceeding.

GSA ENTERPRISE INFRASTRUCTURE SOLUTIONS (EIS)

Some agencies may choose to deploy components of ZT as part of their transformation and modernization efforts via the GSA Enterprise Infrastructure Solutions (EIS) vehicle. Although no

specific or named ZT services appear to be listed on EIS, GSA was forward-thinking with the offering of three contract line item number (CLIN) types to accommodate agency-specific requirements: Individual Case Basis (ICB) CLINs, Task Order Unique CLINs (TUCs), and Catalog CLINs. These CLIN types offer the flexibility to customize Agency needs and bundle standalone components together into more of a “solution”.

DHS CONTINUOUS DIAGNOSTICS & MITIGATION (CDM) AND OTHERS

Agencies seeking even more options could consider other potential contract vehicles including DHS Continuous Diagnostics & Mitigation (CDM), NASA SEWP 5, STARS II, and Alliant II (expiring soon!). Whichever contract vehicle an agency selects, consideration should be made for availability of products, services, preferred primes, cost, and flexibility. The bottom line is that agencies should expect to see more “ZT” specific language in upcoming contract releases and modifications, but there appears to be enough current and flexible contract options in the federal marketplace to get agencies started on the road toward ZT.

Concluding Observations

Zero Trust is an evolutionary framework, not a revolutionary approach. It builds on existing security concepts and does not introduce a radical new approach to cybersecurity. Like most security concepts, Zero Trust relies on a fundamental understanding of an organization’s services, data, users, and endpoints to be effective. There is no “free lunch” regarding up-front resource investment. Policy definitions, concepts of deployment, trust determination (and decay), enforcement mechanisms, logging aggregation, etc., all need to be considered prior to deploying a solution. That said, many large-scale organizations (such as Google, Akamai, and Purdue) that have made the investment show real return on security investment. The critical question becomes whether ZT is mature enough to be a compelling choice for government today.

ZT is not a technology in and of itself but a shift in the design approach for cybersecurity. The current field of solutions show very mature and proven solutions when the network design uses the integration of multiple vendor offerings into a comprehensive solution. However, there are currently no vendors in the market offering a complete and comprehensive ZT/SDN solution. Depending on what they seek, agencies may need to plan for a coordinated acquisition of products and services from multiple vendors to meet their requirements. Although there don’t appear to be specific and named “ ZT” contract vehicles available in the Federal space, opportunities do exist to procure the enabling cyber product and service components of ZT via existing vehicles.

No matter the solutions decided on for pursuing a Zero Trust Network, elements such as Software Defined Networking and Identity, Credential, and Access Management (ICAM) are essential components for a successful long term ZT strategy. ZT can augment and compliment other cybersecurity tools and practices rather than replacing them. Threat intelligence,

continuous monitoring, and Red Teaming exercises remain important components to Zero Trust Networking environments and a comprehensive security approach.

There is little doubt that an effective Zero Trust Networking deployment can significantly improve an organization's cybersecurity posture. However, many federal agencies have a myriad of challenges including complex data and service interdependencies with other organizations. These dependencies must be carefully considered prior to extending ZT to mission-critical, multi-organizational workflows. ZT is a mature strategy that can provide a positive cybersecurity return on investment but it may require up-front investments depending on what agencies already have in place.

Credits

ACT-IAC would like to recognize the following organizations and people for their contributions to this report:

Project Volunteers

ACT-IAC Project Leader

Dave McClure	Accenture Federal Services

Project Leadership Team

Darren Death	ASRC Federal
JD Henley	Verizon
Jeff Flick	National Oceanic and Atmospheric Administration
Steve Hernandez	Department of Education

Project Team Major Contributors

Dan Jacobs	General Services Administration
Dave Harris	Department of the Interior
Emell McKelvey	Mackkell Technologies LLC
Jeff Lamoureaux	Palo Alto Networks
Jim Harrison	Fortinet
Sean Frazier	Duo Security
Stephen Kovac	Zscaler
Theodore Gates	Cisco

ACT-IAC Staff Support

Mike Howell

Mark Karkenny

Companies That Provided Demonstrations and Presentations

Cisco

Cyxtera

Duo

Fortinet

Palo Alto Networks

Zscaler

Companies that Provided Professional Expertise and Advice

Forrester

Gartner

Glossary

CAC - Common Access Card. Department of Defense identity credential

CDM - Continuous Diagnostics and Mitigation – federal program overseen by the Department of Homeland Security to fortifying the cybersecurity of government networks and systems by providing capabilities and tools and identifying and prioritizing cybersecurity risks on an ongoing basis

Control Plane - components of Zero Trust Networks that receive and process requests from data plane devices that wish to access (or grant access to) network resources.

Data Plane Definition – component of Zero Trust Networks that contains the applications, firewalls, proxies, and routers that directly process all traffic on the network.

Deperimeterization – a strategy for protecting data on multiple levels by using encryption and dynamic data-level authentication.[15]

EIS - Enterprise Infrastructure Solutions – federal government-wide telecommunications and networking solutions contract

ICAM – Identity, Credential, and Access Management - the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources.

ITSM - Information Technology Service Management – the activities involved in designing, creating, delivering, supporting and managing the lifecycle of IT services.

MFA - Multi-Factor Authentication - authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) for authentication.

Network Agent - the combination of data known about the actors in a network request, typically containing a user, application, and device, that is queried to make authorization decisions.

PIV - Personal Identity Verification – a process used to verify the identity of an individual in order to grant them access to information systems and facilities.

PIV Card - Personal Identity Verification Card– a United States Federal smart card that contains the necessary data for the cardholder to be granted access to Federal facilities and information systems and assure appropriate levels of security for all applicable Federal applications.

PIV-D - NIST Special Publication 800-157 standard for the adoption of identity certificates for mobile devices to replace physical PIV cards, which are hard to implement with mobile devices.

[15] https://searchsecurity.techtarget.com/definition/deperimeterization

SDN - Software Defined Networking - an approach to cloud computing that facilitates network management and enables programmatically efficient network configuration in order to improve network performance and monitoring

SDP – Software Defined Perimeter - a security framework to microsegment network access by dynamically creating one-to-one network connections between the user and the resources they access.

TIC - Trusted Internet Connection - program mandated by the Office of Management and Budget to optimize federal network connections and improve incident response capability through centralized gateway monitoring at a select group of TIC Access Providers. By reducing the number of access points, the government could more easily monitor and identify potentially malicious traffic.

Zero Trust - ZT - a security concept centered on the belief that organizations should not automatically trust anything *inside* or *outside* their perimeters and instead must verify anything and everything trying to connect to their systems before granting access[16].

[16] https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html

References

1. Report to the President on Federal IT Modernization, https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf

2. Presidential Executive Order on Strengthening Cybersecurity, https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

3. BeyondCorp, https://cloud.google.com/beyondcorp/

4. Zero Trust Networks, Evan Gilman & Doug Barth, ISBN: 978-1-491-96219-0

5. Doherty, N. F., Ashurst, C., & Peppard, J. (2012). Factors affecting the successful realization of benefits from systems development projects: Findings from three case studies. Journal of Information Technology, 27(1), 1-16.

6. Karanja, E. (2017). The role of the chief information security officer in the management of IT security. Information and Computer Security, 25(3), 300-329.

7. The Zero Trust eXtended (ZTX) Ecosystem**,** *Extending Zero Trust Security Across Your Digital Business, https://www.forrester.com/report/The+Zero+Trust+eXtended+ZTX+Ecosystem/-/E-RES137210*

8. Seven Imperatives to Adopt a CARTA Strategic Approach, https://www.gartner.com/doc/3871363/seven-imperatives-adopt-carta-strategic

9. Zero Trust is an Initial Step on the Roadmap to CARTA, https://www.gartner.com/doc/3895267/zero-trust-initial-step-roadmap