



# An Iterative Approach to Zero Trust Pursuits

*July 2024*

**DELL**Technologies

## Abstract

---

Zero Trust implementation can follow either a Greenfield approach, where the system is built from scratch incorporating Zero Trust architectures, or a Brownfield approach, which involves retrofitting and building upon existing systems. This whitepaper focuses on the Brownfield, or Iterative, approach for its applicability in the federal context and how Dell is positioned to assist federal customers.

## Revisions

| Date      | Description     |
|-----------|-----------------|
| June 2024 | Initial release |
|           |                 |

## Acknowledgements

Author: Dirk Wiker

Support:

Other:

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Copyright © 2024 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [7/31/2024]  
[[Category]] [[Manager]]

## Table of Contents

---

|  |           |
|--|-----------|
| <b>Abstract .....</b>                                  | <b>2</b>  |
| <b>Revisions.....</b>                                  | <b>1</b>  |
| <b>Executive Summary .....</b>                         | <b>1</b>  |
| <b>The Zero Trust Security Model.....</b>              | <b>2</b>  |
| Zero Trust and the Federal Government .....            | 2         |
| Federal Requirements.....                              | 4         |
| Challenges of Zero Trust.....                          | 6         |
| <b>Brownfield versus Greenfield Environments .....</b> | <b>7</b>  |
| Greenfield Approach .....                              | 7         |
| Brownfield Approach .....                              | 7         |
| <b>Secure-by-Design in Dell Hardware.....</b>          | <b>8</b>  |
| Supply Chain Security .....                            | 8         |
| Supplier Selection and Vetting .....                   | 8         |
| Secure Manufacturing.....                              | 8         |
| Secure Component Validation .....                      | 8         |
| Transportation and Delivery .....                      | 9         |
| Continuous Improvement and Risk Management .....       | 9         |
| Collaboration with Industry and Standards Bodies.....  | 9         |
| Built-in Security .....                                | 10        |
| Secure Design and Development.....                     | 10        |
| Secure Boot.....                                       | 10        |
| Physical Security .....                                | 11        |
| Recovery Mechanisms .....                              | 11        |
| Built-in Security and Zero Trust.....                  | 11        |
| Comprehensive Zero Trust Solutions .....               | 12        |
| Dell Validated Designs.....                            | 13        |
| OEM Engineered Solutions .....                         | 13        |
| Third-Party Software.....                              | 13        |
| <b>Select Solutions for Government.....</b>            | <b>14</b> |
| User Pillar.....                                       | 14        |

---

|   |           |
|---|-----------|
| Identity, Credentialing, and Access Management .....      | 14        |
| Device & Endpoint Pillar.....                             | 15        |
| Comply-to-Connect.....                                    | 15        |
| Endpoint Detection and Response .....                     | 15        |
| Hardware Inventory .....                                  | 15        |
| Network & Environment Pillar .....                        | 16        |
| Secure Access Service Edge .....                          | 16        |
| Application & Workload Pillar .....                       | 16        |
| Application Programming Interface Security .....          | 16        |
| DevSecOps.....  | 17        |
| Data Pillar .....   | 17        |
| Enterprise Log Management .....                           | 17        |
| Visibility & Analytics Pillar .....                       | 17        |
| AI and Machine Learning for Visibility and Analysis ..... | 18        |
| Automation & Orchestration Pillar .....                   | 18        |
| Security Orchestration, Automation, and Reporting .....   | 18        |
| <b>Best Practices for the Federal Government.....</b>     | <b>20</b> |
| Guidance for Federal Civilian Agencies .....              | 20        |
| NIST SP 800-207.....                                      | 20        |
| NIST SP 1800-35.....                                      | 21        |
| The CISA Zero Trust Maturity Model .....                  | 21        |
| Guidance for the Department of Defense .....              | 21        |
| DoD Zero Trust Reference Architecture .....               | 21        |
| NSA Cybersecurity Information Sheets .....                | 22        |
| DoD Zero Trust Capability Execution Roadmap .....         | 22        |
| DoD Zero Trust Overlays.....                              | 22        |
| <b>Conclusion .....</b>                                   | <b>23</b> |
| <b>References .....</b>                                   | <b>24</b> |

## Executive Summary

---

In today's digital age, cybersecurity is more important than ever, especially within federal government agencies where the protection of sensitive data is crucial. Zero Trust principles are essential to enhancing cybersecurity across the federal landscape. Dell Technologies' approach to security in its products is intrinsic in nature, and Dell hardware provides a secure foundation for Zero Trust Architectures. However, Zero Trust capabilities span multiple pillars and there is not a single security vendor that can offer just one product (or suite of products) that covers every aspect of Zero Trust. Dell Technologies, as a leading industry integrator, has leveraged its extensive partnerships with leading security companies, to provide comprehensive solutions for implementing Zero Trust principles.

While Dell is building an end-to-end Zero Trust Architecture for a Greenfield approach to Zero Trust, many agencies are opting towards the Brownfield, or iterative, approach to implementing Zero Trust to comply with several government mandates. Federal agencies and departments have significant investments in infrastructure and security platforms that can already be effectively utilized for Zero Trust. However, recent executive orders and subsequent Zero Trust mandates did not have funding attached for a "start from scratch" approach and federal entities will require certain technologies to fill capabilities gaps. Dell is committed to providing comprehensive, integrated Zero Trust solutions for this iterative approach that addresses the complex challenges faced by the federal government in modernizing its cybersecurity posture.

Dell is helping federal customers that are focused on progressively integrating Zero Trust principles into existing federal IT systems, thereby minimizing disruption and optimizing resource allocation. By tailoring solutions that fit within the operational constraints of government systems, Dell ensures that each phase of implementation enhances security postures effectively, without the need for complete system overhauls.

## The Zero Trust Security Model

The term “Zero Trust” was devised in 2010 but is really an extension of the long-accepted cybersecurity principle of least privilege access extended to all IT resources. In this model, implicit trust is minimized or eliminated all completely.

The perimeter-based security model that was relied on for years “trusted” all resource access within a perimeter – typically residing on a network controlled by the organization. However, malicious adversaries took advantage of this implicit trust through attacks such as social engineering. Further complicating the perimeter-based security model is the increasing difficulty in identifying a clear perimeter surrounding the entirety of an organization’s data. Data resides in the cloud, Software-as-a-Service (SaaS) providers, at the edge, and traditional data centers. This data is on networks no longer controlled by the organization.

Zero Trust aims to overcome these challenges by ensuring access to every resource is continually authorized, no matter where that resource resides. Adopting Zero Trust principles requires a change in organizational culture, reconfiguring security platforms, and most likely implementing new technologies.

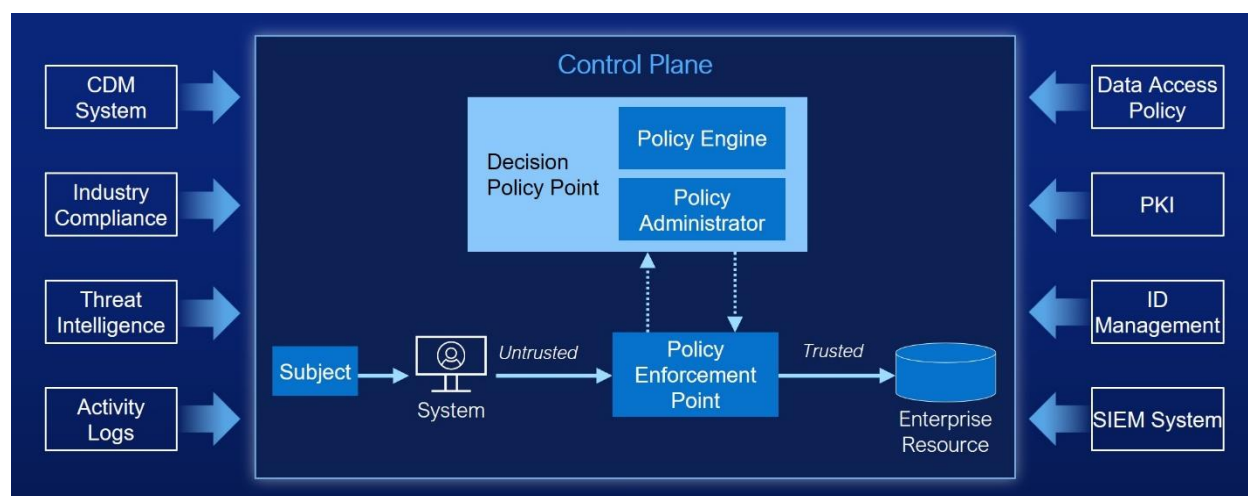
## Zero Trust and the Federal Government

The foundational documentation for Zero Trust within the federal government is the National Institute of Standards and Technology’s (NIST) Special Publication (SP) 800-207. SP 800-207 defines Zero Trust according to the federal government:

- **Zero Trust** provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.
- **Zero Trust architecture** is an enterprise’s cybersecurity plan that utilizes Zero Trust concepts and encompasses component relationships, workflow planning, and access policies. A Zero Trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place as a product of a zero trust architecture plan.

SP 800-207 describes Zero Trust and different approaches for implementing these principles in an organization’s IT environments. Zero Trust is not a single product or architecture but a set of guiding principles for workflow, system design, and operations. The key element of Zero Trust principles is verification of assets within the enterprise prior to providing access and continued verification prior to execution of processes or lateral movement within the network.

Figure 1: Logical Zero Trust Architecture according to NIST.



NIST SP 800-207 describes logical components of a Zero Trust Architecture. These include:

- **Policy Decision Point (PDP)** – The PDP is a component of a Zero Trust Architecture that evaluates access requests against established security policies to make a decision. It determines whether a

given request by a user or system to access resources should be allowed or denied based on the policy rules, the attributes of the requestor, and the state or context of the environment. It is the central authority in the decision-making process regarding access control. There will most likely be several PDPs in an environment. The PDP is composed of the following sub-components:

- **Policy Engine** – This sub-component uses a trust algorithm to make decisions to either allow, deny, or revoke access to resources.
- **Policy Administrator** – This sub-component is responsible for communicating with the Policy Enforcement Point (PEP) to allow or deny access based on the decision of the Policy Engine.
- **Policy Enforcement Point (PEP)** – This logical component directly enforces access control decisions as provided by the Policy Decision Point. It is responsible for intercepting a user or device's access request to resources and then enforcing the decision to allow or deny the request based on the guidance received from the PDP. Essentially, the PEP acts at the gateway through which requests for accessing network resources are allowed or blocked.
- **Policy Information Point (PIP)** – This component is not explicitly mentioned in SP 800-207 but the concept is documented. PIPs act as the sources of information for the Policy Decision Point(s). Examples from NIST include Continuous Diagnostic and Monitoring (CDM) systems, threat intelligence feeds, and network/system logs. PIPs are represented by the boxes on the left and right of *Figure 1*.

NIST SP 800-207 further defines seven tenets of Zero Trust:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

In February 2021, the Department of Defense (DoD) released the Zero Trust Reference Architecture (ZTRA) v1.0, which provided a framework for cybersecurity architectures. These architectures are to be data-centric and founded on Zero Trust principles. Seven pillars were defined based on the seven tenets from NIST and the pillars described in the Forrester Zero Trust eXtended (ZTX) Ecosystem from 2018.

- User
- Device
- Network/Environment
- Application & Workload
- Data
- Visibility & Analytics
- Automation & Orchestration

In the fall of 2021, the Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA) published their draft Zero Trust Maturity Model that focused on the first five pillars while recognizing the importance of the cross-cutting Visibility/Analytics and Automation/Orchestration functions. Because of this evolution, the DoD identifies seven pillars of zero trust, while Federal Civilian agencies focus on five.

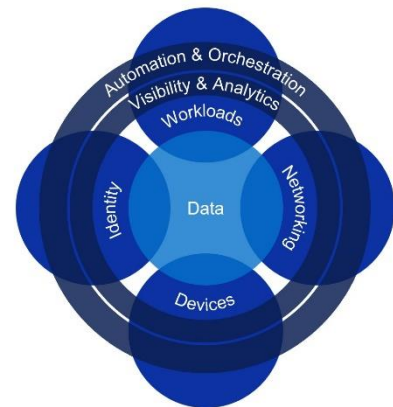


Figure 2: The Seven Pillars with Data being central to Zero Trust.

## Federal Requirements

On May 12, 2021, the President of the United States released an Executive Order regarding Improving the Nation's Cybersecurity.






The order detailed the persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, private sector, and the American people.

The primary goals of the Executive Order as detailed in the document:

- Removing Barriers to Sharing Threat Information
- Modernizing Federal Government Cybersecurity
- Enhancing Software Supply Chain Security
- Establishing a Cyber Safety Review Board
- Standardizing the Federal Government's Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks
- Improving the Federal Government's Investigative and Remediation Capabilities

Following the release of the Executive Order, the Office of Management and Budget released Memorandums to support the Executive Order with more specificity in action and direction. Of particular interest is OMB Memorandum M-22-09, which is the Federal Civilian Zero Trust Strategy. This strategy mandates federal agencies adopt a Zero Trust cybersecurity architecture to strengthen their security postures and protect against evolving cyber threats. There are 19 requirements across the five pillars that each federal civilian agency must implement before September 30, 2024 (**Figure 3**).

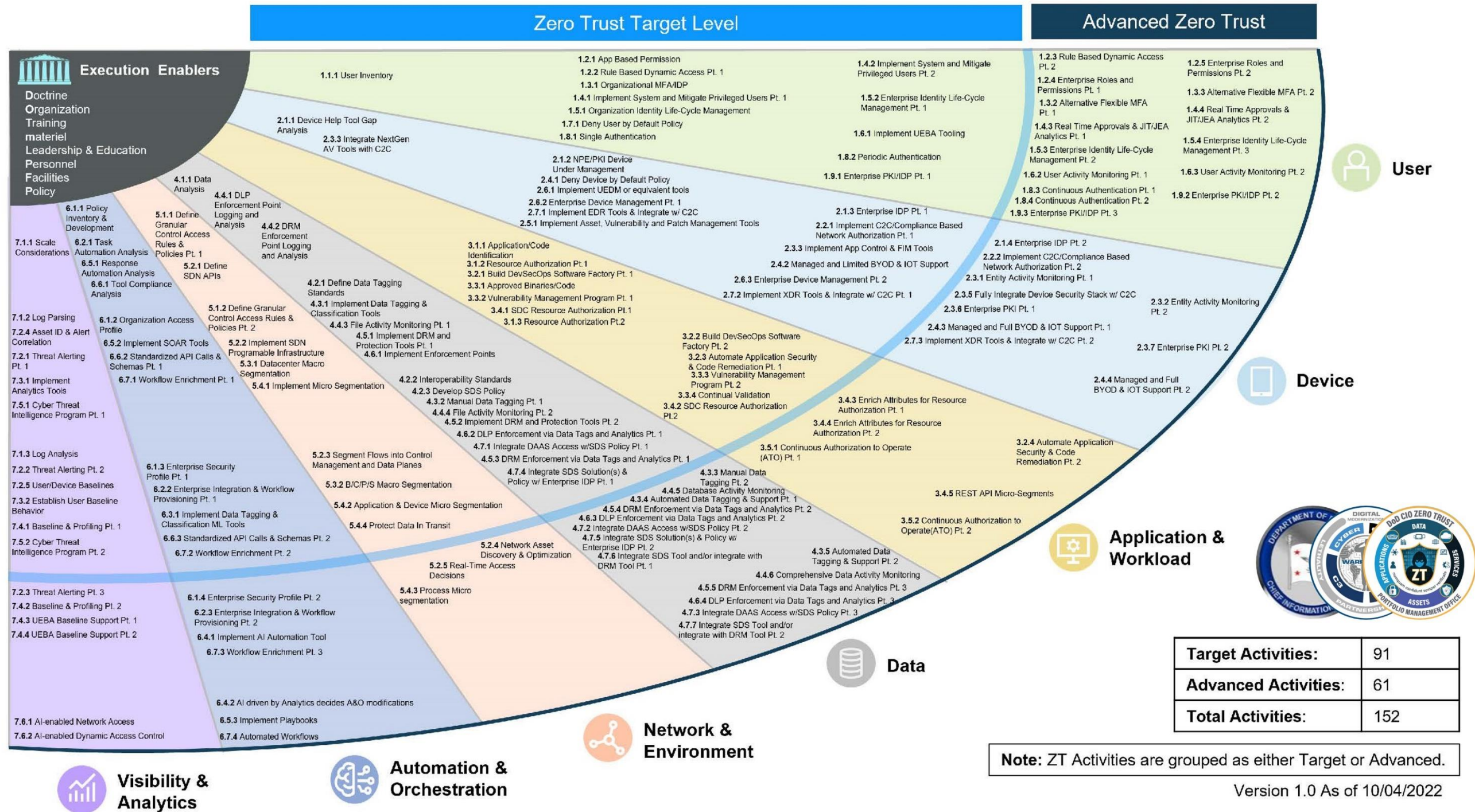
Figure 3: The 19 Zero Trust Requirements for Federal Civilian

|                                   |  |                        |    |   |
|---|--|--|--|---|
| Identity  | Devices  | Networks   | Applications & Workloads   | Data  |
| Identity Management<br><br>Multi-Factor Authentication<br><br>Role and Attribute Based Access Control (RBAC / ABAC) | Device Inventory (CDM)<br><br>Endpoint Detection and Response (OMB M-22-01)        | Encrypted DNS<br><br>Encrypt All HTTP Traffic (HTTPS)<br><br>Encrypted Email<br><br>Network Segmentation | Application Security Testing<br><br>3 <sup>rd</sup> Part Testing and Validation<br><br>Vulnerability Disclosure Program<br><br>Internet Accessible Web Applications<br><br>Internet Application Discovery<br><br>Immutable Workloads | Data Security Strategy<br><br>Security Orchestration, Automation, and Reporting (SOAR)<br><br>Data Access Auditing<br><br>Enterprise Log Management (OMB M-21-31) |

The Department of Defense published their Zero Trust Strategy in October 2022 with 152 activities across the seven pillars (**Figure 4**).

Each DoD component has until September 30, 2027 to implement the 91 target activities and if applicable, the 61 advanced activities will need to be finished by 2032.

Figure 4: 152 Activities in the DoD ZT Strategy



## Challenges of Zero Trust

While Zero Trust offers significant security advantages, federal agencies face considerable challenges in its implementation. These challenges largely stem from the model's stringent access controls and the comprehensive monitoring it requires, demanding a significant transformation of existing IT infrastructure and policies. Integrating Zero Trust involves not just technological upgrades but also a cultural shift within the organization to embrace new operational paradigms. Additionally, retrofitting legacy systems with new protocols can be resource-intensive and disruptive. However, despite these hurdles, the benefits of enhanced security, reduced insider threats, and improved data management capabilities make the pursuit of Zero Trust a worthwhile journey. Some of the challenges include:

- **Complexity:** Implementing Zero Trust can be complex and challenging, as it requires integrating various security technologies, policies, and processes. It can be difficult to get all these components to work together seamlessly, and to ensure that they are properly configured and maintained.
- **Cost:** Implementing Zero Trust can be costly, as it requires investment in new security technologies, policies, and processes. It may also require additional staff to manage and maintain these technologies, which can increase costs even further. The federal mandates requiring implementation of Zero Trust principles did not come with additional funding for agencies.
- **Legacy systems:** Legacy systems can be a significant challenge when implementing Zero Trust, as they may not be compatible with modern security technologies and policies. There are still several legacy systems in use throughout the government, such as mainframes, Internet of Things (IoT), and Operational Technology (OT) platforms. These systems cannot be easily replaced, and unique solutions will need to be deployed to integrate them into a Zero Trust environment.
- **Lack of standardization:** Zero Trust introduces some new logical components like PDPs, PEPs, and PIPs. There are no stand-alone systems that fully fulfil these roles rather it is often a combination of security platforms. Further, there are no standards for communication between these logical components (e.g. APIs). Each security vendor is creating their own methods for communications.
- **User experience:** Zero Trust can sometimes create a poor user experience, as it may require users to authenticate multiple times or restrict their access to resources. This can lead to frustration and reduced productivity.
- **Organizational culture:** Zero Trust requires a shift in organizational culture, as it assumes that *no user or device can be trusted*, even if they are inside the organization's network perimeter. This can be a difficult mindset for some organizations to adopt and may require significant change management efforts.

## Brownfield versus Greenfield Environments

---

When developing and implementing new systems, projects, or policies in the realm of information technology and cybersecurity, the terms Greenfield and Brownfield are used to describe the underlying environment conditions. These terms take on particular significance when adopting Zero Trust architectures. The Greenfield approach involves starting from scratch, building a new Zero Trust infrastructure without the constraints of existing systems. In contrast, the Brownfield approach entails integrating Zero Trust principles into an organization's current infrastructure, working within the confines of legacy systems and existing security platforms.

### Greenfield Approach

Adopting a Greenfield approach means starting anew, constructing systems or comprehensively revamping existing ones without the need to accommodate legacy technologies or previous designs. It is like working with a blank canvas. This method offers the freedom to design the system leveraging cutting-edge technologies and adhering to best practices, unencumbered by constraints. It facilitates the seamless integration of state-of-the-art security measures from the ground up, ensuring that all elements of the Zero Trust model are fully optimized and cohesively implemented. However, the primary challenge lies in the potentially substantial costs and significant resource investments required. Furthermore, there is a risk of disruption during the transition to the new system, which can be substantial and impactful.

The DoD Zero Trust Strategy identified three Courses of Action (COAs). COA2 and COA3 are greenfield approaches for implementing the Zero Trust activities. COA2 is a full end-to-end implementation within the Joint Warfighter Cloud Capability cloud environments. Hyper-scaler providers (Oracle, Microsoft, Amazon, and Google) are working on implementing the 91 target-level activities within the DoD strategy.

COA3 is a private cloud Greenfield implementation that covers all 152 activities, including the advanced ones. Dell has done considerable work following this approach with Project Fort Zero. This project aims to industrialize the end-to-end Zero Trust architecture the DoD had previously built based on the DoD Zero Trust Reference Architecture. Project Fort Zero allows customers to migrate critical workloads to a complete Zero Trust environment.

### Brownfield Approach

The Brownfield approach entails modifying and enhancing current systems to incorporate new technologies and policies. This approach operates within the confines of existing infrastructure and legacy systems. Typically, the Brownfield route is more cost-effective and less disruptive in the short term. It enables organizations to capitalize on their existing technological investments and gradually integrate new solutions, a process that can be more manageable and carry less risk. However, integrating new technologies with outdated ones can lead to compatibility issues and may limit the functionality of the newer systems. This approach also necessitates more intricate management and careful planning to ensure that all components of the system adhere to Zero Trust principles without impacting an agency's mission.

While the DoD Zero Trust strategy identified COA2 and COA3, both Greenfield options the primary focus was COA1, the Brownfield approach. The Capability Execution Roadmap released with the strategy focused solely on COA1 with recommended timelines for implementation. Every federal civilian agency is also following the Brownfield approach.

## Secure-by-Design in Dell Hardware

---

Dell Technologies has embraced the Zero Trust security model and declared it as the “north star” guiding security principle. As organizations increasingly rely on digital infrastructure, the security of IT hardware and the underlying supply chain processes and technology are more important than ever. Dell's comprehensive security strategy integrates Zero Trust principles across the entire product lifecycle, from initial design to final delivery and beyond. Dell is committed to providing federal customers products that can be trusted.

This commitment to security starts with Dell's supply chain security strategy, which exemplifies Zero Trust principles by enforcing rigorous controls at every stage. The multi-layered approach employed by Dell safeguards data, personnel, and physical assets, mitigating risks associated with tampering and counterfeit components. Each element, from component procurement to final product assembly, undergoes stringent security protocols to prevent unauthorized access and ensure compliance with our exacting standards. Dell actively collaborates with federal organizations such as NIST to continuously refine supply chain security practices. The commitment to these types of collaborations helps set industry benchmarks for security, ensuring Dell's practices not only comply with, but help define standards for supply chain security.

At Dell Technologies, security is embedded within the hardware design from inception. Products are engineered with built-in security features, aligning with Zero Trust principles. These intrinsic security concepts extend throughout the manufacturing processes, where components undergo rigorous validation against their original specifications to verify integrity and authenticity without presuming trust. Dell integrates additional security capabilities that align with Zero Trust tenets, such as firmware digital signing, BIOS recovery, and chassis intrusion detection. These features collectively ensure that security is maintained continuously, detecting and responding to threats in real-time and maintaining the integrity of our products throughout their lifecycle.

Zero Trust Architectures start with a secure infrastructure and Dell's compute, storage, and networking hardware provide for this critical foundation.

## Supply Chain Security

Dell's commitment to delivering reliable and secure products is underpinned by a robust supply chain security strategy that encompasses rigorous processes and advanced technologies to safeguard every step from supplier selection to product delivery.

### Supplier Selection and Vetting

Dell's supplier selection process is highly structured to ensure that only secure and reliable suppliers enter its supply chain network. This includes thorough security assessments to evaluate potential suppliers' security postures, encompassing cyber defenses, physical security measures, and employee background checks. Dell also conducts in-depth Quality Process Audits at supplier facilities to ensure compliance with its exacting standards for security, quality, and operational integrity.

### Secure Manufacturing

At the manufacturing stage, Dell ensures the security of the manufacturing environment and the integrity of the process. Facilities are secured with controlled access systems to prevent unauthorized entry and are continuously monitored by surveillance systems. High-risk components are tagged with unique identifiers, such as serial numbers or Dell-prescribed Piece-Part Identification (PPID) labels, maintaining traceability and preventing counterfeit components from entering the supply chain.

### Secure Component Validation

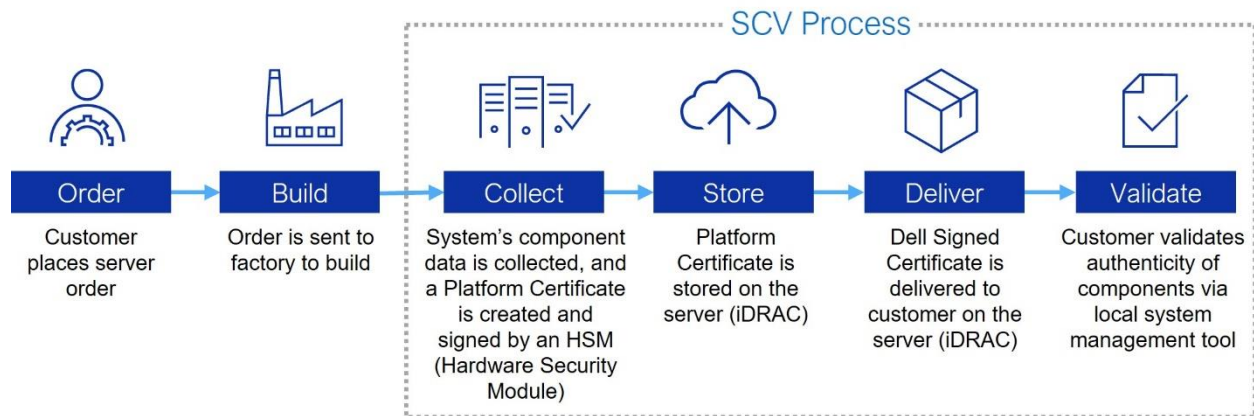
Secure Component Validation (SCV) is a pivotal technology employed by Dell to enhance the security and integrity of its supply chain. SCV works by uniquely identifying and validating the critical components used in Dell's products. Each component, such as motherboards or hard drives, is affixed with a unique

---

identifier, typically a Dell-prescribed PPID label or an electronic identifier captured during the manufacturing process. These identifiers contain detailed information about the component, including the supplier, part number, and manufacturing details.

When a Dell product is assembled, a manifest of installed components is generated, cryptographically signed by a Dell Certificate Authority, and stored securely within the system. This manifest serves as a baseline for future validation checks. When the product reaches the customer, Dell provides a validation tool that compares the current state of the components against the manifest. If the validation tool detects any discrepancies, it indicates potential tampering or unauthorized modifications, prompting further investigation. This process not only ensures the authenticity and integrity of the components used in Dell products but also provides customers with assurance that their systems are secure from the factory to delivery.

Figure 5. Secure Component Validation



## Transportation and Delivery

Dell employs advanced technologies to secure and monitor products during shipment. Products are secured with tamper-evident packaging to detect and deter unauthorized access during transit. Additionally, GPS tracking and IoT devices are utilized to monitor the location and condition of shipments in real-time, providing alerts for any deviations or tampering attempts.

## Continuous Improvement and Risk Management

Dell's approach to supply chain security is dynamic, characterized by continuous monitoring and improvement. Regular audits of suppliers and manufacturing facilities ensure ongoing compliance with Dell's security standards. The company adapts its security measures based on emerging threats and vulnerabilities, incorporating new technologies and processes as needed.

## Collaboration with Industry and Standards Bodies

Dell's approach to supply chain security is significantly enhanced through its extensive collaboration with various industry partners and standards bodies. This proactive engagement not only helps Dell refine its security measures but also contributes to shaping industry-wide best practices and standards.

Dell actively participates with key standards organizations that influence global security protocols and practices. This includes involvement with NIST, where Dell contributes to developing new guidelines for technology and cybersecurity, especially pertaining to supply chain risks. Dell's participation ensures its practices align with current standards while influencing the evolution of future security benchmarks.

Dell takes a leadership role in various industry consortiums and forums dedicated to advancing technology security. As a founding member of the Trusted Computing Group (TCG), Dell helps develop standards that ensure the security of computing environments, thereby enhancing the security of its supply chain. As a co-founder and active participant in SAFECode, a non-profit group promoting software

development and security best practices, Dell shares insights, learns from peers, and adopts cutting-edge secure software development practices crucial for maintaining supply chain software component security.

Partnering with academic institutions and research organizations, Dell advances cybersecurity research and development. These collaborations foster security technology and practice innovations applicable within Dell's supply chain while keeping the company at the forefront of cybersecurity advancements.

## Built-in Security

Dell's approach to intrinsic security in its hardware is a fundamental foundation of the company's overarching cybersecurity strategy. This security is deeply embedded from the foundational design level, ensuring strong protections are an integral part of the device's operation, rather than an afterthought.

Secure-by-design tenets include:

- **Protect:** Protect server during every aspect of lifecycle, including BMC, BIOS, firmware, data, and physical hardware.
- **Detect:** Detect malicious cyberattacks and unapproved changes; engage IT administrators proactively.
- **Recover:** Recover BIOS, firmware, and operating system to a known good state; securely retire or repurpose servers.

## Secure Design and Development

At the outset of the hardware design process, Dell employs a Secure Development Lifecycle (SDL) that seamlessly weaves security considerations throughout the development cycle. This includes thorough risk assessments to identify potential security vulnerabilities and comprehensive design reviews to ensure all security requirements are effectively met.

## Secure Boot

Dell's Secure Boot process plays a crucial role in ensuring that each device starts up securely and operates as intended, free from malicious software interference. This process is carefully engineered to protect the integrity of the operating system from the moment the device is powered on.

Dell utilizes the Unified Extensible Firmware Interface (UEFI), a modern firmware architecture, to replace the older BIOS firmware. UEFI provides more robust security features compared to its predecessor, notably the Secure Boot feature that ensures only signed, trusted software can load during the device's startup. This capability is crucial for preventing rootkits and other low-level malware threats from embedding themselves within the operating system.

The Secure Boot process involves verifying the digital signatures of the operating system and other startup software. Dell ensures that each piece of executable code has been signed by a trusted certificate authority before it is allowed to run. This step is vital in preventing unauthorized software from being loaded during the boot process, thereby protecting the system against potential security threats.

Dell enhances the Secure Boot process with the integration of Trusted Platform Module (TPM) technology. TPM is a hardware-based security device that provides a secure crypto-processor, which can securely store artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. During the boot process, TPM works in conjunction with Secure Boot to ensure a tamper-free environment, facilitating a secure and trusted boot pathway from firmware initialization to operating system load.

Dell establishes a hardware root of trust, which is a set of cryptographic keys securely embedded in hardware at the manufacturing stage. This root of trust is used during the Secure Boot process to verify the integrity and authenticity of the firmware and software loading on the device. It ensures that only firmware and software that have been verified as secure and trustworthy are executed during boot, offering a strong defense against firmware tampering and unauthorized changes.

Dell provides options for administrators to manage Secure Boot settings via the UEFI firmware settings menu. This flexibility allows IT professionals to add custom security measures or modify existing ones

according to specific organizational security policies. It also facilitates the management of keys and certificates that control what software is trusted during the boot process.

## Physical Security

Dell incorporates several sophisticated physical security measures to protect its hardware from unauthorized access and tampering. These measures are designed to ensure the integrity and confidentiality of data stored on Dell devices, safeguarding them from physical threats and breaches.

One of the most direct forms of physical security Dell employs is chassis intrusion detection. This feature is integrated into many Dell systems. It involves sensors that detect when the case of the device has been opened or tampered with, even when there is no power. Any unauthorized access triggers an alert that can be logged by the system and reported to administrators through management software. This allows IT support personnel to quickly respond to potential security breaches and investigate any unauthorized physical access.

For enhanced security, it is possible to fully disable USB ports. USB ports can be disabled just on the front of a server as well. This flexibility allows USB ports to be deactivated during regular production operations, with the option to temporarily reactivate them when needed, such as providing access to a crash cart for debugging purposes.

## Recovery Mechanisms

Dell hardware is equipped with sophisticated recovery mechanisms designed to ensure resilience and restore functionality rapidly in the event of hardware or software failures.

One key feature is the BIOS Recovery capability, which allows servers to automatically revert to a previous, safe BIOS version if corruption occurs due to a failed update or malware intrusion. Similarly, Dell servers can recover an operating system from a recovery partition or external media, which is crucial for quickly resuming operations after software-related disruptions.

The Secure Restore functionality further enhances Dell's cyber-resilient infrastructure by enabling servers to reset the firmware to factory settings, eliminating any malicious modifications. This reversion to a known-good state is essential for mitigating firmware-level security breaches.

Remote management is facilitated through the Integrated Dell Remote Access Controller (iDRAC), which allows IT administrators to conduct recovery operations remotely. This includes capabilities like system resets and power cycling, significantly reducing downtime by eliminating the need for physical access to the hardware.

Dell also emphasizes redundancy and failover by incorporating redundant components such as power supplies, hard drives in RAID configurations, and network interfaces. This redundancy allows the system to continue operating even if one component fails and supports seamless failover to maintain continuous service availability.

## Built-in Security and Zero Trust

There are several requirements described in the federal civilian and DoD Zero Trust strategies. Most of these mandates are for enterprise-wide capabilities, but Dell's hardware incorporates many Zero Trust features directly. Dell hardware also allows seamless integration with enterprise Zero Trust environments. See table below.

| Zero Trust Pillar | NIST Description   | PowerEdge Highlights  |
|-------------------|--|---|
| <b>User</b>       | <ul style="list-style-type: none"> <li>User identification, authentication, and access control</li> <li>Only validated and authorized users can access data and resources.</li> <li>The principle of least privilege is applied where users are granted the minimum level of access required to perform their specific tasks.</li> </ul> | <ul style="list-style-type: none"> <li>Identity and Access Management</li> <li>Multi-Factor Authentication —RSA Secure ID, PIV/CAC</li> <li>Active Directory or LDAP integration with single sign-on (SSO) support</li> <li>Role-based access control and auditing</li> </ul> |

|                                     |  |  |
|-------------------------------------|--|--|
| <b>Device</b>                       | <ul style="list-style-type: none"> <li>Monitoring and enforcement of device health, compliance, and device posture assessment:</li> <li>Monitoring - looking for anomalies and suspicious read/write activity.</li> <li>Health – confirming the latest version of the firmware.</li> <li>All devices are identified, inventoried, authorized, authenticated, and updated.</li> </ul> | <ul style="list-style-type: none"> <li>Silicon Root-of-Trust (ROT) with complementary Intel Boot Guard and AMD Platform Secure Boot (AMD PSB)</li> <li>Secure supply chain with Secured Component Verification (SCV)</li> <li>Chassis locks and intrusion detection</li> <li>Dynamic USB port enable/disable</li> <li>Trusted Platform Module</li> <li>Peripheral device attestation with SPDM (Security Protocol Data Model from DMTF)</li> <li>802.1X/802.1AR based attestation</li> </ul> |
| <b>Data</b>                         | Ensure data transparency and visibility by using enterprise infrastructure, applications, standards, solid end-to-end encryption, and data tagging.  | <ul style="list-style-type: none"> <li>Data-at-rest protection:</li> <li>Drive encryption with local (LKM) or Secure Enterprise Key Management (SEKM) with RAID controller as well as direct-attached NVMe drive support</li> <li>Confidential compute—Intel SGX, Intel MKTME, Intel Trust Domain Extensions (TDX), AMD Secure Memory Encryption (SME), AMD Secure Encrypted Virtualization (SEV) and SEV-SNP</li> </ul>   |
| <b>Application and Workload</b>     | Secure applications and workloads and protect containers and virtual machines.   | <ul style="list-style-type: none"> <li>Secure Development Lifecycle</li> <li>Cryptographically signed BIOS and firmware updates</li> <li>Secure end-to-end boot and Unified Extensible Firmware Interface (UEFI) boot capabilities</li> <li>Compliance drift detection</li> <li>Rapid Response and mitigations for CVEs</li> </ul>   |
| <b>Network and Environment</b>      | <ul style="list-style-type: none"> <li>Encrypt, monitor, and analyze network.</li> <li>Logically and physically segment, isolate, and control the network and the environment (on-premises and off-premises) using granular access and policy restrictions.</li> </ul>   | <ul style="list-style-type: none"> <li>Dedicated BMC network module</li> <li>SSH/TLS communication options</li> <li>TLS 1.3 support</li> <li>DPU/SmartNIC support</li> </ul>   |
| <b>Visibility and Analytics</b>     | Monitor activities and behaviors across the infrastructure (user, device, data, network, and application) to identify patterns and anomalies. Use analytics to detect and respond to security threats.   | <ul style="list-style-type: none"> <li>Persistent event logging and auditing</li> <li>Real-time and boot time firmware scanning</li> <li>Security alerts</li> <li>Event management and remediation</li> </ul>  |
| <b>Automation and Orchestration</b> | Automate manual security and other applicable processes to take policy-based actions across the enterprise with speed and at scale.  | <ul style="list-style-type: none"> <li>Policy based drift detection</li> <li>Firmware rollback</li> <li>Automatic BIOS and operating system recovery</li> <li>Centralized firmware and software updates</li> <li>Automatic SSL certificate renewal</li> </ul>  |

## Comprehensive Zero Trust Solutions

Dell has evolved from primarily an OEM hardware provider to a holistic solutions provider in the federal space, particularly in advancing Zero Trust architectures that align with federal mandates. Achieving comprehensive enterprise-level Zero Trust capabilities extends beyond the hardware layer. As federal agencies confront increasingly sophisticated cybersecurity threats, Dell not only supplies secure hardware but is building outcome-based solutions that strengthen agencies' missions through enhanced data protection and system integrity.

Dell's approach to Zero Trust centers on offering comprehensive solutions that integrate seamlessly with existing agency frameworks, supporting the distinct needs of federal operations. These solutions are engineered to meet stringent requirements set forth by federal cybersecurity mandates, which emphasize verifying and securing all endpoints, rigorously managing identities, and controlling access across

networks. No vendor can provide a single product or suite of products that span all capabilities across the Zero Trust pillars, including Dell Technologies. As an industry leading integrator, Dell is leveraging its own advanced technology and an extensive partner ecosystem to provide these solutions. With Dell hardware and best-in-class security partners, Dell delivers Zero Trust solutions for capabilities such as identity verification, micro-segmentation, least privilege access control, real-time threat detection and response, anomaly detection, and multi-factor authentication (MFA).

These comprehensive solutions consist of Dell Validated Designs (DVDs), OEM Engineered Solutions, and third-party software.

## Dell Validated Designs

Dell Technologies Validated Designs are meticulously tested and proven configurations, specifically designed from the outset to meet the unique requirements of government agencies implementing Zero Trust architectures. Each solution is developed to dynamically align with specific use cases prevalent in the government sector. These solutions undergo rigorous testing and are thoroughly documented to expedite and streamline the deployment of new secure systems.

- **Reliable:** Dell offers proven and documented solutions, supported by design guides and white papers, that significantly reduce deployment risks and enhance operational efficiency—key factors for government applications where security and reliability are of utmost importance.
- **Efficient:** The pre-tested and validated integrated designs, developed by Dell Technologies engineers along with their partners, ensure that government customers spend less time on the planning, deployment, and testing phases. This efficiency is crucial for quick adaptation to evolving security threats and compliance requirements.
- **Flexible:** Dell Technologies provides a variety of consumption models that are designed to align seamlessly with the specific applications, IT strategies, and mission objectives of government agencies. This flexibility supports the diverse needs of different government departments, facilitating the adoption of Zero Trust principles across all levels of the organization.

## OEM Engineered Solutions

Dell's OEM Engineered Solutions are comprehensive solutions for various technology capabilities, many of which are cybersecurity focused. These are specifically developed to support Zero Trust capabilities required by the DoD and Federal Civilian Executive Branch (FCEB) agencies. These solutions are crafted through strategic collaborations with OEM technology partners, utilizing Intellectual Property (IP) from Dell's comprehensive partner ecosystem and Dell's advanced technology platforms. The aim is to deliver highly specialized solutions tailored to meet the rigorous security demands of the federal sector.

To ensure adherence to Zero Trust security frameworks, these solutions are configured into specific solution SKUs that integrate seamlessly with the Dell Technologies fulfillment process. This meticulous configuration guarantees that each solution is turnkey, fully integrated, and validated by our OEM partners, thus ensuring they meet the stringent security requirements necessary for federal applications.

## Third-Party Software

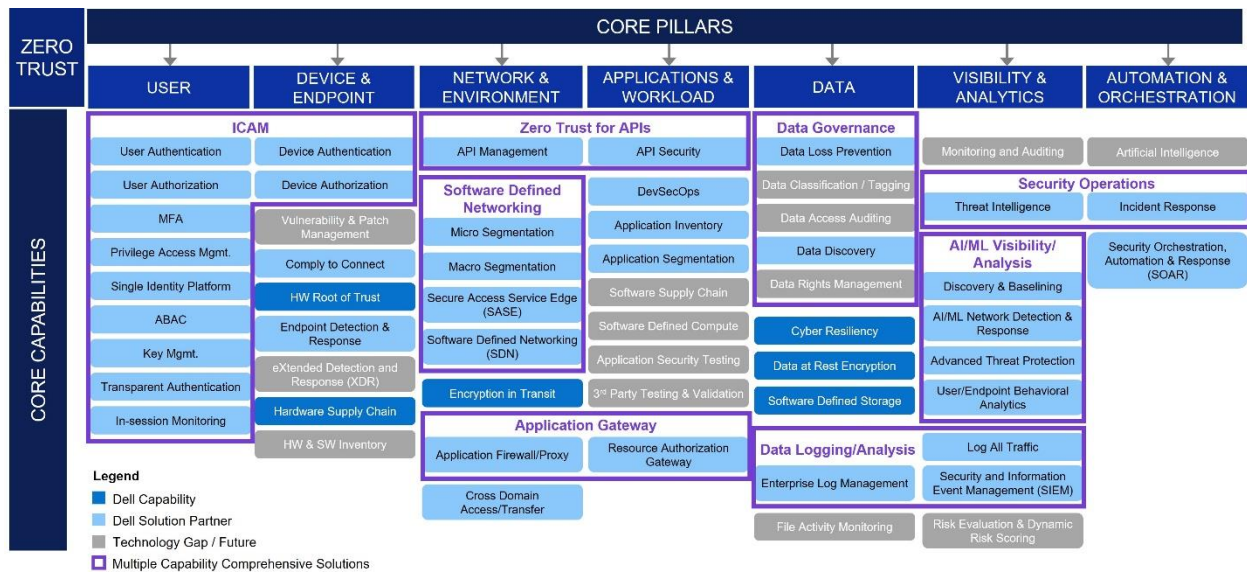
Federal customers often require capabilities that can be effectively met through standalone software or product licenses without needing a fully architected solution. Dell Technologies offers a comprehensive portfolio of such solutions, including various security software and licenses that enhance operational efficiency. These solutions can be directly purchased and are designed to complement Dell's hardware products, such as an Endpoint Detection and Response (EDR) client installed on a Dell laptop. This allows for immediate security enhancements without extensive system overhauls.

The Cloud Software & Security team at Dell manages an extensive network of security software partnerships, ensuring federal customers have access to leading-edge tools from top vendors. These vetted and optimized solutions enable rapid deployment of critical security capabilities, aligning with Zero Trust architecture strategies. Dell's offerings are scalable and flexible, providing immediate value and facilitating long-term resilience against emerging threats. This positions Dell as a key enabler for federal customers striving to achieve comprehensive Zero Trust security.

# Select Solutions for Government

Dell Technologies offers a suite of comprehensive solutions tailored specifically for the federal agencies that are adopting the iterative approach to Zero Trust. By integrating advanced technologies and strategic partnerships, Dell's solutions provide robust protections that meet or exceed stringent federal standards, support compliance requirements, and safeguard critical infrastructures against evolving cyber threats. The select Dell Federal Zero Trust solutions below are organized according to pillar.

Figure 6. Dell Zero Trust Capability Model.



## User Pillar

The user pillar forms a cornerstone of Zero Trust security, particularly critical in federal government settings where safeguarding sensitive information and critical systems is paramount. Central to Zero Trust is the principle that trust is never assumed, regardless of the user's location—inside or outside the network. This approach requires rigorous identity verification and access controls, such as MFA, to ensure that resource access is securely controlled and monitored. By implementing least privilege access, the user pillar minimizes the potential impact of compromised credentials and reduces the overall attack surface. Continuous monitoring of user behavior allows for the detection of anomalies that may indicate security threats, which enhances federal agencies' abilities to protect national security interests and comply with the two Zero Trust strategies.

## Identity, Credentialing, and Access Management

Dell Technologies has developed a comprehensive Identity, Credential, and Access Management (ICAM) solution tailored for the federal government, in collaboration with industry-leading partners. This solution has been effectively deployed to support critical missions in the federal government. Dell's ICAM solution is designed with a modular approach, supporting component-level onboarding that allows federal agencies the flexibility to initiate deployments within their data centers and progressively incorporate edge and cloud elements as their needs evolve. This modular approach not only offers scalability but also accommodates the unique operational and budgetary requirements of federal agencies.

The ICAM framework includes several critical capabilities essential for robust identity and access management in government settings: Identity Management, Directory Virtualization, Identity Access Management, Attribute-Based Access Control, and Privileged Access Management. Each component plays a vital role in enhancing security and operational efficiency by ensuring that only authorized individuals have access to sensitive systems and information. The solution's flexibility and comprehensive

features make it ideal for starting with a proof-of-concept that can be expanded to a full network implementation, spanning from edge devices through data centers and into cloud environments. Currently utilized within the federal government, this ICAM solution represents a strategic approach to secure digital identity and access management, ensuring alignment with Zero Trust strategies.

## Device & Endpoint Pillar

The device pillar is crucial in a Zero Trust environment as it ensures that every device accessing the network is authenticated and continuously validated for security compliance before being granted access to resources. This is particularly vital in environments with a diverse array of endpoints, as it prevents compromised or unauthorized devices from becoming a gateway for security breaches. By implementing strict controls such as device profiling, health checks, and adherence to security policies, organizations can ensure that only secure, compliant devices operate within their networks. This meticulous verification process not only fortifies the network against external threats but also supports secure mobility and remote work, which are increasingly prevalent in today's government workplace.

## Comply-to-Connect

Comply-to-Connect, commonly notated as C2C, represents the Department of Defense's significant advancement in network security across all networks within the Department of Defense Information Network (DoDIN), encompassing both non-classified and classified levels. This technology is also sometimes referred to as Network Access Control (NAC) and is very relevant for FCEB agencies as well.

Dell, in partnership with Forescout's NAC, offers federal agencies an advanced solution for securing endpoints across their digital landscape. By implementing real-time visibility and automated access controls, this joint solution ensures only compliant devices connect to federal networks, aligning with stringent cybersecurity policies. The Dell and Forescout integration strengthens endpoint security, necessary for protecting national data and maintaining operational integrity within the federal space.

## Endpoint Detection and Response

CrowdStrike Falcon Endpoint Detection and Response (EDR) offers government agencies a powerful layer of defense against sophisticated cyber threats. By leveraging advanced AI and machine learning technologies, CrowdStrike EDR provides real-time threat detection, automated response capabilities, and continuous monitoring across all endpoints. This state-of-the-art solution is designed to identify and mitigate threats before they can compromise sensitive data, ensuring that government operations remain secure and uninterrupted.

When CrowdStrike, Intel, and Dell unite, federal customers gain unparalleled security advantages. This partnership not only streamlines and strengthens PC security but also aligns with the Department of Defense's Zero Trust requirements for EDR. Furthermore, it meets and exceeds the mandates of OMB M-22-01 and OMB M-22-09 for federal civilian agencies, ensuring comprehensive protection on Dell's Intel vPro-enabled devices through the integration of CrowdStrike Falcon. This collaboration delivers a secure, seamless experience, providing deep security layers essential for federal operations.

## Hardware Inventory

Partnering with Eracent and ServiceNow, Dell can offer government customers a comprehensive IT Asset Management solution that streamlines asset management processes, reduces software spend, and minimizes audit and security risks. This collaboration leverages Eracent's automated Software Asset Management/ITAM solutions and ServiceNow's IT service management capabilities, providing a unified platform for tracking, managing, and optimizing IT assets across their lifecycle. This synergy ensures enhanced visibility, improved compliance, and optimized usage of IT assets, delivering significant cost savings and operational efficiencies for customers. ITAM ensures every asset is identified, monitored, and managed, which is a foundational principal to zero trust – knowing exactly what exists within an enterprise environment.

## Network & Environment Pillar

The network pillar is essential for Zero Trust because it secures and controls the flow of information across federal organizations. This pillar focuses on segmenting the network into smaller, manageable zones to limit lateral movement by potential intruders and reduce the attack surface. By enforcing strict access controls and inspecting and logging all network traffic, the network pillar helps ensure that users and devices can only access network segments and resources that are necessary for their specific roles. This not only enhances security by minimizing the impact of breaches but also aligns with the Zero Trust principle of "never trust, always verify," ensuring continuous evaluation of all network connections for suspicious activity or anomalies.

### Secure Access Service Edge

Dell Technologies and Versa Networks have partnered to deliver a Secure Access Service Edge (SASE) solution, which converges network and security functions with SD-WAN capabilities to support the dynamic, secure access needs of federal organizations. Versa Network's SASE technology simplifies traditional network architecture, reduces point product complexity, and delivers optimized and automated traffic management across data planes. This enables federal agencies to not only automate and streamline traffic through a central control plane but also to achieve an unprecedented level of agility and protection in their network operations. By leveraging this solution, federal agencies can ensure their infrastructure is resilient, responsive, and ready to meet the current and future demands of secure, software-defined networking. This solution is currently being used in DoD programs such as the DISA Thunderdome project.

Dell also has strategic partnerships with other leading network security companies such as Palo Alto, Fortinet, and ForcePoint/EverFox.

## Application & Workload Pillar

The application and workload pillar is crucial for implementing Zero Trust security as it directly addresses the security of software environments, from traditional applications to dynamic cloud-based workloads. By focusing on securing these elements, organizations ensure that applications, regardless of their hosting location, operate under strict access controls and are continuously monitored for threats. This pillar facilitates the application of fine-grained permissions and secure coding practices, effectively reducing vulnerabilities and preventing unauthorized access. Moreover, by isolating applications and workloads, organizations can prevent breach propagation, ensuring that an attack on one application does not compromise the entire system. This approach supports the overarching Zero Trust mandate of minimizing trust zones and verifying everything, thereby safeguarding critical business processes and data.

### Application Programming Interface Security

Dell Technologies' robust infrastructure, Corsha's innovative MFA technology, and Red Hat 3scale's API management capabilities create a secure, scalable, and efficient API gateway solution. Federal agencies often handle sensitive information and require the highest levels of security to protect against unauthorized access and cyber threats. This approach adds a critical layer of security by requiring multiple forms of verification before granting access to sensitive data and services through APIs, effectively mitigating the risk of data breaches and cyber-attacks.

This solution addresses the unique security needs of the federal government by offering a solution that is both easy to integrate and capable of scaling to meet the demands of large, complex government systems. Corsha's MFA technology introduces a dynamic security model that adapts to each access attempt, making unauthorized access significantly more difficult. Meanwhile, Red Hat 3scale's API management platform provides the tools necessary for federal agencies to deploy, manage, and scale their APIs across internal and external environments securely. This not only enhances the overall security posture but also improves operational efficiency and facilitates compliance with federal regulations. This partner solution ensures that agencies can leverage the power of APIs for digital transformation while maintaining the utmost security and compliance.

## DevSecOps

Scalable container platforms like Red Hat OpenShift work best when paired with a fast, scalable infrastructure platform, making OpenShift and Dell Technologies the perfect team. With our hardware and Red Hat OpenShift, agencies and departments can have a robust, secure platform for all their workloads, from bare metal, to virtualized, to containerized.

Red Hat and Dell Technologies deliver tested, validated, and documented design and deployment guidance to help customers rapidly implement the Red Hat OpenShift Container Platform on Dell Technologies infrastructure and minimize time to production.

The Red Hat OpenShift Container Platform provides a self-service platform to create and deploy applications on demand, enabling faster development and release lifecycles. The Dell Technologies and Red Hat deployment guides describe the infrastructure required to deploy and operate the platform and provides the information needed to facilitate readiness for day two operations.

Dell Technologies also partners with SUSE and VMware to broaden its ecosystem, enhancing its ability to support diverse government infrastructure needs. With SUSE Rancher, Dell delivers scalable and reliable solutions that leverages an enterprise-level container management platform, ideal for managing complex workloads and ensuring security. Meanwhile, the partnership with VMware Tanzu enhances Dell's offerings in Kubernetes management and modern application development, providing customers with integrated solutions that streamline operations from infrastructure to application layer, facilitating a smooth transition to cloud-native environments. These partnerships underscore Dell's commitment to providing comprehensive, multi-platform support and enhancing operational efficiency across all types of workloads.

## Data Pillar

The idea of protecting data is central to Zero Trust. Applying Zero Trust principles ensures that data security is maintained at its core, regardless of where the data resides—whether on-premises, in the cloud, or in hybrid environments. The capabilities within this pillar focus on classifying, encrypting, and continuously monitoring data to control who can access it and under what conditions. By implementing rigorous access controls and encryption, organizations can protect sensitive data from unauthorized access and breaches. Additionally, real-time data monitoring and analytics help detect and respond to anomalies quickly, preventing potential data leaks or compromises. This proactive approach to data security reduces the risk of insider threats and external attacks and makes technologies in the data pillar critical in overall Zero Trust strategies for federal agencies.

## Enterprise Log Management

Integrated with Dell's advanced storage and compute solutions, the Elastic suite (Elasticsearch, Logstash, and Kibana) offers a comprehensive suite of tools tailored to meet the stringent requirements of government agencies, particularly in compliance with logging mandates like OMB M-21-31 and SIEM (Security Information and Event Management) requirements in the DoD Zero Trust Strategy.

The powerful combination of Elastic, Logstash, and Kibana's scalable search capabilities and real-time analytics can sift through vast amounts of data efficiently, allowing for quick retrieval of relevant information. At the same time, Dell's robust storage systems ensure the integrity and availability of data, which is critical for government operations.

## Visibility & Analytics Pillar

Capabilities in the visibility and analytics pillar are indispensable in a Zero Trust environment because they provide the critical insights needed to enforce strict security policies effectively. Technologies in this pillar ensure government agencies have holistic visibility into all network traffic, user activities, and device interactions, which is necessary for detecting and responding to potential threats in real time. By integrating advanced analytics and machine learning, the visibility and analytics pillar can identify abnormal behavior patterns and potential security breaches before they cause significant harm. This

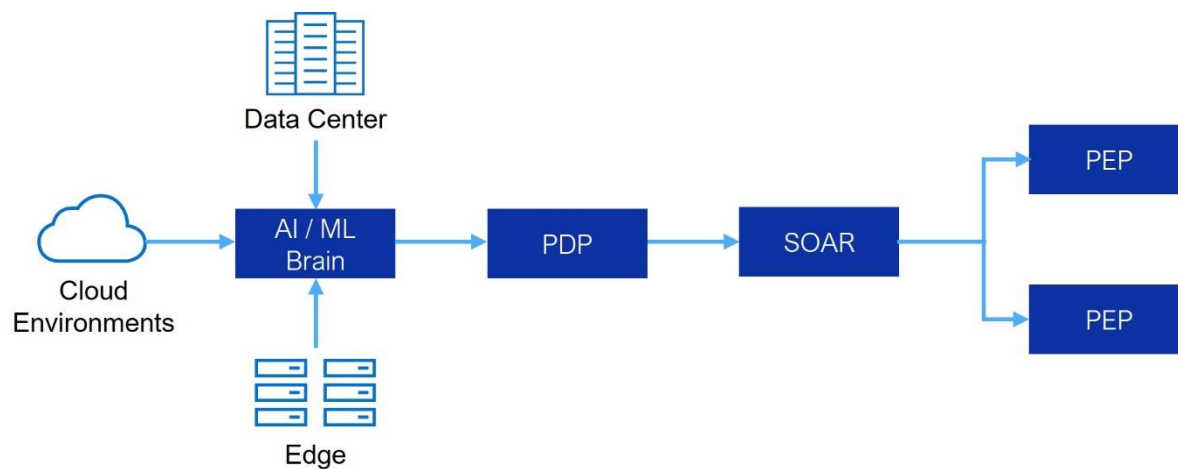
continuous monitoring and analysis of data across the IT environment enables the DoD and FCEB agencies to dynamically adapt their security measures, ensuring the Zero Trust principles of continuous verification and least privilege access are effectively applied.

## AI and Machine Learning for Visibility and Analysis

Many threats can be detected through the use of signatures, but many unknown threats, such as zero-days and new adversarial techniques, can go unnoticed for long periods of time. Real-time detection of both known and unknown cyber risks are critical within a Zero Trust environment. AI and Machine Learning network analytics will play a crucial role in implementing and maintaining a zero-trust security environment.

The Visibility and Analytics technology used in this bundled solution utilizes advanced analytics and machine learning to identify and prioritize threats, providing security teams with actionable insights to quickly respond to incidents. This platform integrates directly with Policy Decision Points; Policy Enforcement Points; or Security Orchestration, Automation, and Reporting platforms to automate security incident response in near real-time. By combining partner solutions with Dell hardware, organizations can deploy a reliable and performant NDR solution that is capable of scaling to meet the needs of even the largest and most complex networks.

Figure 7. Title.



## Automation & Orchestration Pillar

The automation and orchestration pillar is important because it enhances the ability to respond in near real-time to security incidents and manage complex environments at scale. By automating the enforcement of security policies and orchestrating responses to security events, technologies in this pillar reduce the reliance on manual processes, which are often slow and prone to error. Automation ensures that security controls are consistently applied across all assets, while orchestration helps coordinate defenses across various layers of the infrastructure, improving overall security posture. This integration of automated processes and coordinated responses is necessary for maintaining effective defenses in dynamic and complex government IT environments. It enables government agencies to adapt security measures in real-time and mitigate threats before they can exploit vulnerabilities.

## Security Orchestration, Automation, and Reporting

Enabling Zero Trust is a difficult task and cannot be accomplished by a single vendor alone. That's why Dell has partnered with the best security companies in the world to deliver comprehensive outcome-based solutions. A key security partner for Zero Trust is Palo Alto Networks.

Palo Alto Networks' Cortex XSOAR platform offers a comprehensive solution that can significantly assist government agencies in meeting Zero Trust requirements. By providing a robust Security Orchestration,

Automation, and Response (SOAR) framework, Cortex XSOAR enables agencies to automate and orchestrate their security operations, thereby enhancing their ability to detect, respond to, and remediate threats more efficiently and effectively. The platform's ability to integrate multiple threat intelligence feeds enhances the security decision-making process by offering enriched data and improved alert triage. This integration facilitates a more dynamic and informed response mechanism, allowing agencies to adapt quickly to new and emerging threats. The efficiencies gained through automation, such as a reduction in remediation time and a decrease in the number of incidents requiring manual interaction, ensure that government agencies can maintain a proactive and resilient security posture essential for achieving Zero Trust.

# Best Practices for the Federal Government

---

In the federal sector, implementing Zero Trust architectures is a difficult task that has unique challenges stemming from the government's Zero Trust mandates and the critical nature of its operations. The stakes are exceptionally high, with potential breaches threatening not just data but possibly national security as well. Luckily, federal organizations do not have to fully recreate the wheel because the government has offered tools and guidance for applying this security framework in existing federal environments. Although some of these resources are tailored for DoD or federal civilian agencies specifically, they can be applicable for any organization wishing to adopt the Zero Trust security model.

The guidance and best practices for implementing Zero Trust Architectures below are based on the iterative/brownfield approach to Zero Trust. The comprehensive Dell solutions mentioned in the previous section can be used by agencies employing these practices.

## Guidance for Federal Civilian Agencies

### NIST SP 800-207

The foundational document for Zero Trust in the federal government is NIST Special Publication 800-207. This document provides a framework for implementing Zero Trust architectures. It outlines the principles, concepts, and definitions related to Zero Trust, providing agencies with a starting point for transitioning from traditional perimeter-based security models to a Zero Trust model where security is dynamic and based on not trusting anyone by default, regardless of their location inside or outside the network.

There are three approaches for agencies to consider outlined in SP 800-207:

- **Enhanced Identity Governance**
  - Implement strong identity and access management (IAM) policies and technologies, such as MFA, to ensure that only authorized users have access to resources.
  - Implement role-based access controls (RBAC) to ensure that users have access to only the resources that they need to perform their jobs.
  - Implement continuous monitoring of user activity to detect and respond to anomalous behavior.
  - Implement real-time risk assessments to ensure that access is granted based on the context of the user and the resource being accessed.
- **Micro-segmentation**
  - Identify the network segments that need to be isolated, such as those containing sensitive data or critical assets.
  - Implement segmentation policies to limit network traffic between segments and prevent lateral movement of attackers.
  - Use a network access control (NAC) solution to enforce access policies and control connected devices.
  - Implement a network traffic analysis (NTA) solution to monitor network traffic and detect anomalous behavior.
- **Software Defined Perimeters**
  - Implement SDN controllers to manage network traffic and enforce policies.
  - Use SDN to segment the network and limit network traffic between segments.
  - Implement flow-based access controls to enforce policy-based network segmentation.
  - Use SDN to dynamically isolate compromised devices and quarantine them from the rest of the network.
  - Implement real-time risk assessments to ensure that access is granted based on the context of the user and the resource being accessed.

## NIST SP 1800-35

The NIST Cybersecurity Practice Guides (Special Publication 1800 series) are designed to address specific cybersecurity challenges faced in both public and private sectors. These documents are practical, user-friendly guides that help in adopting standards-based approaches to cybersecurity. They provide detailed demonstrations on how to implement solutions that align with established standards and best practices, complete with materials lists, configuration files, and other necessary details for users to replicate similar cybersecurity measures.

SP 1800-35 focuses specifically on Zero Trust Architectures. These guides emphasize securing data and resources through strictly controlled access. Zero Trust architectures are designed to facilitate secure and authorized access to enterprise resources distributed across various environments, supporting a hybrid workforce and external partners. Every access request is evaluated by verifying available contextual information such as the identity and role of the requester, the health and credentials of the device, resource sensitivity, user location, and behavior consistency. If the request meets the enterprise's access policy, a secure session is established to safeguard all data exchanges. SP 1800-35 details using commercially available technologies to create interoperable, open, standards-based Zero Trust implementations in line with the principles set forth in NIST SP 800-207, Zero Trust Architecture. This NIST Cybersecurity Practice Guide demonstrates how these technologies can be integrated to develop various Zero Trust architecture configurations effectively.

## The CISA Zero Trust Maturity Model

Federal civilian agencies might want to utilize the CISA Zero Trust Maturity Model for helping to implement Zero Trust architectures. This model serves as a valuable framework for systematically assessing current security practices against Zero Trust principles and identifying areas for improvement. Federal agencies can use the CISA Maturity Model effectively for these areas:

- **Assessment of Current Posture:** The CISA Maturity Model provides an approach to evaluate existing cybersecurity measures against the ideal state of Zero Trust security. Agencies can use this model to conduct an audit of their networks, systems, and data management practices to understand where they stand in the Zero Trust maturity spectrum.
- **Roadmap Development:** Based on the assessment results, agencies can develop a tailored roadmap that outlines incremental steps towards achieving Zero Trust. The model's tiered maturity levels guide agencies in progressing through more sophisticated stages of security practices, ensuring a structured and manageable approach to enhancing their cybersecurity posture.
- **Prioritization of Resources:** With its emphasis on gradual progression, the model helps agencies prioritize their resources and focus on high-impact areas that require immediate attention.
- **Benchmarking and Metrics:** Using the maturity model, agencies can establish benchmarks and metrics to measure their progress in implementing Zero Trust principles. This quantitative approach not only helps in tracking the Zero Trust journey of agencies but also in justifying cybersecurity investments and strategies to stakeholders.

## Guidance for the Department of Defense

### DoD Zero Trust Reference Architecture

The DoD Zero Trust Reference Architecture (ZT RA), prepared by the Defense Information Systems Agency (DISA) and the National Security Agency (NSA), provides a strategic framework and detailed guidance for DoD entities aiming to implement Zero Trust principles within their cybersecurity ecosystems. This architecture is not merely prescriptive but serves as a dynamic blueprint that identifies the core principles, pillars, and capabilities essential for securing DoD networks against sophisticated threats in an increasingly complex cybersecurity landscape.

For DoD customers, this document is particularly valuable as it delineates a path from traditional security models to a comprehensive Zero Trust approach, emphasizing the importance of treating all users, devices, and network flows as potentially hostile, regardless of their location. By adopting the framework outlined in the ZT RA, DoD agencies can systematically enhance their cybersecurity defenses to address

both external and insider threats more effectively. The architecture supports a phased implementation, allowing DoD components to gradually integrate Zero Trust strategies and technologies in alignment with their operational needs and security objectives. Additionally, it provides use cases and transition planning strategies to guide entities through the practical aspects of deploying Zero Trust architectures, ensuring that every step contributes towards creating a resilient, agile, and secure IT environment capable of supporting mission-critical operations under a constant cyber threat.

## NSA Cybersecurity Information Sheets

Customers within DoD can enhance their Zero Trust implementation by integrating guidance from the NSA's Cybersecurity Information Sheets (CSIs), which cover the pillars of Zero Trust. Utilizing these guidelines ensures that security solutions are aligned with the latest and most authoritative practices in cybersecurity.

Adopting NSA recommendations across the Zero Trust pillars allows agencies to improve network visibility and analytics, strengthen identity verification, improve endpoint security, and secure data environments. The concepts introduced in these cybersecurity information sheet provide guidance on enhancing existing security controls across the Zero Trust pillars to limit the potential impact of a compromise.

## DoD Zero Trust Capability Execution Roadmap

The DoD Zero Trust Capability Execution Roadmap outlines a comprehensive strategy for implementing Zero Trust capabilities across the DoD by the end of Fiscal Year 2027. This document presents a well-defined timeline starting in FY23, emphasizing a systematic approach through COA1 (Brownfield Approach) that spans various phases and critical activities required for a successful transition to a Zero Trust architecture.

DoD customers can utilize this roadmap as a strategic guide to plan and prioritize their Zero Trust initiatives effectively. It provides a structured timeline for implementing key capabilities such as user authentication, device security, and data protection. The roadmap details how activities are sequenced and interdependent, offering DoD entities a clear progression path towards achieving Target and Advanced Zero Trust levels. This methodical approach ensures that stakeholders can align their security enhancements with overarching DoD timelines and objectives, facilitating a coordinated and efficient transition to a robust Zero Trust environment.

## DoD Zero Trust Overlays

The DoD Zero Trust Overlays document serves as a pivotal resource for DoD customers working towards implementing Zero Trust security architectures. Its purpose is to assist DoD components by providing a detailed alignment of security controls with the specific requirements and strategies of Zero Trust. This alignment is helpful for adapting existing systems and protocols to Zero Trust principles, which include minimizing access, scrutinizing all cybersecurity activities, and continuously authenticating and validating security postures. The overlays outlined in the document apply to various pillars of Zero Trust architecture, such as user, device, network, and data environments, ensuring comprehensive coverage and actionable insights.

For DoD customers, utilizing this document means they can systematically approach the implementation of Zero Trust by following a structured guide that lays out necessary activities, expected outcomes, and the integration of security controls across their IT environments. This is instrumental in not just meeting the Zero Trust Strategy requirements but also in fostering a secure, resilient organizational culture capable of defending against sophisticated threats in a no-perimeter world.

## Conclusion

---

Dell Technologies is not just a hardware provider, but a strategic cybersecurity partner. Leveraging its advanced technological solutions, robust industry partnerships, and deep understanding of federal needs, Dell is uniquely positioned to navigate the complex terrain of Zero Trust. Dell's approach goes beyond off-the-shelf solutions, offering rigorously tested, government-tailored Validated Designs that align precisely with federal Zero Trust mandates.

Dell's holistic strategy encompasses every facet of Zero Trust—from secure supply chains and intrinsically secure hardware to comprehensive user and application security. By integrating cutting-edge technologies with established federal frameworks, Dell ensures that agencies can fill gaps in their Zero Trust capabilities without compromising operational integrity. This approach not only fortifies defenses against increasingly sophisticated cyber threats but also enhances operational efficiency, enabling agencies to focus on their core missions.

In an era where cyber warfare is a daily reality, Dell's expertise in Zero Trust implementation is more than a technological advantage—it's a critical asset in safeguarding America's digital frontiers. By providing federal agencies with state-of-the-art, compliant security solutions, Dell is helping to protect the nation's most sensitive information and critical infrastructure.

## References

---

NIST SP 800-53, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

NIST SP 800-207, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

NIST SP 1800-35: <https://csrc.nist.gov/pubs/sp/1800/35/2prd>

DoD Zero Trust Reference Architecture v1.0,  
[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT\\_RA\\_v1.1\(U\)\\_Mar21.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf)

DoD Zero Trust Reference Architecture v2.0,  
[https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT\\_RA\\_v2.0\(U\)\\_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)

CISA Zero Trust Maturity Model, [https://www.cisa.gov/sites/default/files/2023-04/zero\\_trust\\_maturity\\_model\\_v2\\_508.pdf](https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf)

NSA: Embracing a Zero Trust Security Model, [https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI\\_EMBRACING\\_ZT\\_SECURITY\\_MODEL\\_UOO115131-21.PDF](https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF)

NSA: Advancing Zero Trust Maturity Throughout the User Pillar:  
[https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI\\_Zero\\_Trust\\_User\\_Pillar\\_v1.1.PDF](https://media.defense.gov/2023/Mar/14/2003178390/-1/-1/0/CSI_Zero_Trust_User_Pillar_v1.1.PDF)

NSA: Advancing Zero Trust Maturity Throughout the Device Pillar:  
<https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/0/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF>

NSA: Advancing Zero Trust Maturity Throughout the Data Pillar:  
[https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI\\_DATA\\_PILLAR\\_ZT.PDF](https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF)

NSA: Advancing Zero Trust Maturity Throughout the Network and Environment Pillar:  
<https://media.defense.gov/2024/Mar/05/2003405462/-1/-1/0/CSI-ZERO-TRUST-NETWORK-ENVIRONMENT-PILLAR.PDF>

NSA: Advancing Zero Trust Maturity Throughout the Application and Workload Pillar:  
<https://media.defense.gov/2024/May/22/2003470825/-1/-1/0/CSI-APPLICATION-AND-WORKLOAD-PILLAR.PDF>

NSA: Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar:  
<https://media.defense.gov/2024/May/30/2003475230/-1/-1/0/CSI-VISIBILITY-AND-ANALYTICS-PILLAR.PDF>

NSA: Advancing Zero Trust Through the Automation and Orchestration Pillar:  
<https://media.defense.gov/2024/Jul/10/2003500250/-1/-1/0/CSI-ZT-AUTOMATION-ORCHESTRATION-PILLAR.PDF>

Executive Order 14028, <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>

National Security Memo 8, <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/>

OMB M-22-09, <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

OMB M-23-31, <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf>

OMB M-22-01, <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf>

NSM-10: National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems | The White House

OMB M-22-18, <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>

OMB M-23-02, <https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf>

DoD Zero Trust Strategy: <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>

DoD Zero Trust Capabilities Execution Roadmap:

<https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTExecutionRoadmap.pdf>

DoD Zero Trust Overlays: <https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays-2024Feb.pdf>

Dell Technologies Supply Chain Assurance,

[https://i.dell.com/sites/csdocuments/CorpComm\\_Docs/en/supply-chain-assurance.pdf?newtab=true](https://i.dell.com/sites/csdocuments/CorpComm_Docs/en/supply-chain-assurance.pdf?newtab=true)

Dell Trusted Devices, <https://www.delltechnologies.com/en-us/collaterals/unauth/white-papers/products/security/dell-trusted-device-below-the-os-whitepaper.pdf>

Cyber Resilient Security with PowerEdge™, <https://dl.dell.com/manuals/common/dell-emc-poweredge-cyber-resilient-security.pdf>

Dell EMC OpenManage Enterprise, <https://www.dell.com/en-us/dt/solutions/openmanage/enterprise.htm>

Introduction to VMware Zero Trust, <https://techzone.vmware.com/resource/introduction-vmware-zero-trust#section1>

Dell Product Security Configuration Guides, <https://support.emc.com/kb/209687>

Dell Vulnerability Response Policy, <https://www.dell.com/support/contents/en-us/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy>  
NCCoE: Trusted Cloud: VMware Hybrid Cloud IaaS Environments

NCCoE: Trusted Cloud: VMware Hybrid Cloud IaaS Environments,  
<https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments>