PRODUCTS AND OPERATIONS
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

The benefits of a Validated Zero Trust Solution

Herb Kelsey

Federal CTO

Copyright © 2023 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.

Table of Contents

Copyright © 2023 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.

Introduction

Ransomware attack encrypts critical systems, causes widespread disruption, and exposes sensitive data.

This headline could have been about the City of Atlanta,[1] the Colonial Pipeline,[2] or Toyota[3]. On November 28, 2022, it was about Suffolk County in the U.S. state of New York[4]. Governments and global businesses—large and small—are desperately seeking to secure their systems, applications, and data with a Zero Trust solution, given these ever-evolving threats. In a previous paper, we described the benefits of a Zero Trust solution and the need to embark on the journey with a definite end in mind. However, many organizations, including technology vendors, are following a self-defined approach using an assortment of single-purpose solutions. This self-styled approach has its limitations as it is not scalable across the whole enterprise and often gives rise to additional security vulnerabilities.

A practical alternative would be to set validated Zero Trust as your destination and deploy a solution that:

- Implements the U.S. Department of Defense's (DoD) latest Zero Trust reference architecture
- Meets the appropriate National Institute of Standards and Technology (NIST) controls
- Passes the stringent requirements of a DOD security assessment
- Integrates across all seven pillars of Zero Trust
- Emphasizes data and workload migration for rapid adoption

Dell Technologies is building an ecosystem and assembling a validated Zero Trust solution that meets all these requirements and delivers end-to-end security while taking the integration burden off the enterprise.

The self-defined approach to Zero Trust is not working

NIST defines Zero Trust as an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.[5] Zero Trust as a concept has been around for a while. Since its inception, it has expanded in scope and is now subject to validation against definitive requirements. However, there has hardly been any clarity on how to build a validated Zero Trust enterprise network. Most companies and vendors have been pursuing an ad hoc approach toward its implementation. They would typically embark on a journey that only targets one of the seven essential Zero Trust pillars depicted in Figure 1.

These seven pillars practically describe any network at a high level in the context of Zero Trust. Organizations usually start with the user pillar. They enable federated user identity to allow authorized users access to multiple applications and domains using a single set of credentials. While this may seem like a logical starting point, it is a dangerous approach. Starting by federating the user identity—before protecting the data and automating the threat response—just makes it convenient for hackers to attack the entire enterprise.

This scenario is an example of an enterprise self-defining their Zero Trust approach and leveraging a set of single-purpose products to address the symptoms while ignoring the underlying problem. This tactic may improve security in specific areas but may create vulnerabilities in others. Most importantly though, it will not

[1] Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare, Lily Hay Newman, WIRED, April 23, 2018, https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[2] Hackers Breached Colonial Pipeline Using Compromised Password, William Turton and Kartikay Mehrotra, June 4, 2021 https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[3] Toyota Halts Production Across Japan After Ransomware Attack, Phil Muncaster, Infosecurity Magazine, March 1, 2022, https://www.infosecurity-magazine.com/news/toyota-production-japan-ransomware/

[4] How a Cyberattack Plunged a Long Island County Into the 1990s, Sarah Maslin Nir, The New York Times, November 28, 2022, https://www.nytimes.com/2022/11/28/nyregion/suffolk-county-cyber-attack.html

[5] Zero Trust Architecture, NIST Special Publication 800-207, August 2020, https://doi.org/10.6028/NIST.SP.800-207

Copyright © 2023 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.

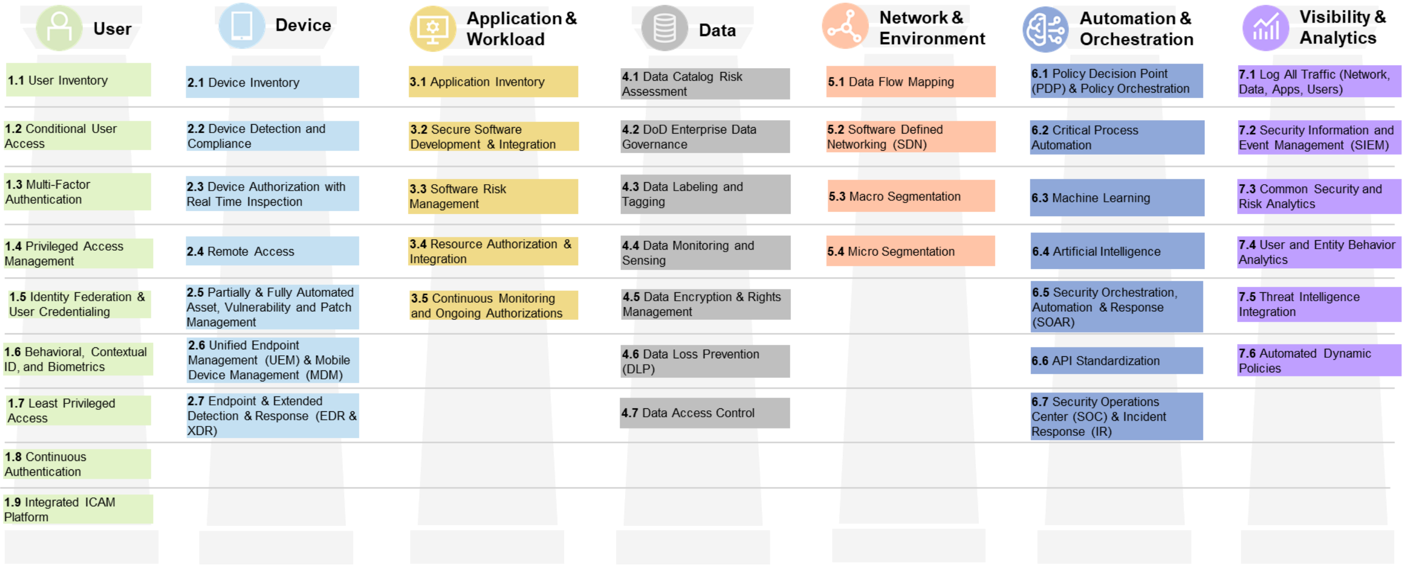
stop an adversary from exploiting the enterprise's data and systems once they get in. If an organization does not prioritize all seven pillars equally and modernize them simultaneously, attackers will target and use the weak points in the neglected pillars. Hackers thrive in an environment where they can exploit the functionalities meant to make things convenient for the users.

There is a better way: choose a validated Zero Trust solution

The U.S. DoD followed up on its seven-pillar Zero Trust reference architecture[6] with its Zero Trust Strategy in November 2022.[7] In that document, the DoD laid out its vision and established a path for all DoD components to achieve Zero Trust. This approach not only impacts the federal government but also those enterprises classified as critical infrastructure players[8] and entities that receive funding from the government. Dell Technologies believes the DoD strategy sets the gold standard and default baseline for Zero Trust.

As depicted in Figure 1, the DoD has developed an implementation road map by breaking down the **seven pillars** of the Zero Trust reference architecture into **45 capabilities**. Each capability is further divided and organized into **152 Zero Trust activities**.[9] These activities will enable the DoD to regulate compliance with the Zero Trust Strategy at two levels of maturity—**Target and Advanced**.

Target Level Zero Trust includes the minimum set of **91 activities** to help secure and protect the enterprise while managing risks from currently known threats. Once they reach the Target Level, organizations can move to Advanced Level Zero Trust as current risks are mitigated. Advanced capabilities include the complete set of **152 activities** that enable adaptive responses to cybersecurity risks and threats while offering the highest level of protection.



User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Figure 1 The seven pillars of Zero Trust broken down into 45 capabilities

[6] DoD Zero Trust Reference Architecture, Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, September 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[7] DoD Zero Trust Strategy, DoD CIO Zero Trust Portfolio Management Office (PfMO), November 15, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[8] Critical Infrastructure Sectors, Cybersecurity & Infrastructure Security Agency (CISA), https://www.cisa.gov/critical-infrastructure-sectors

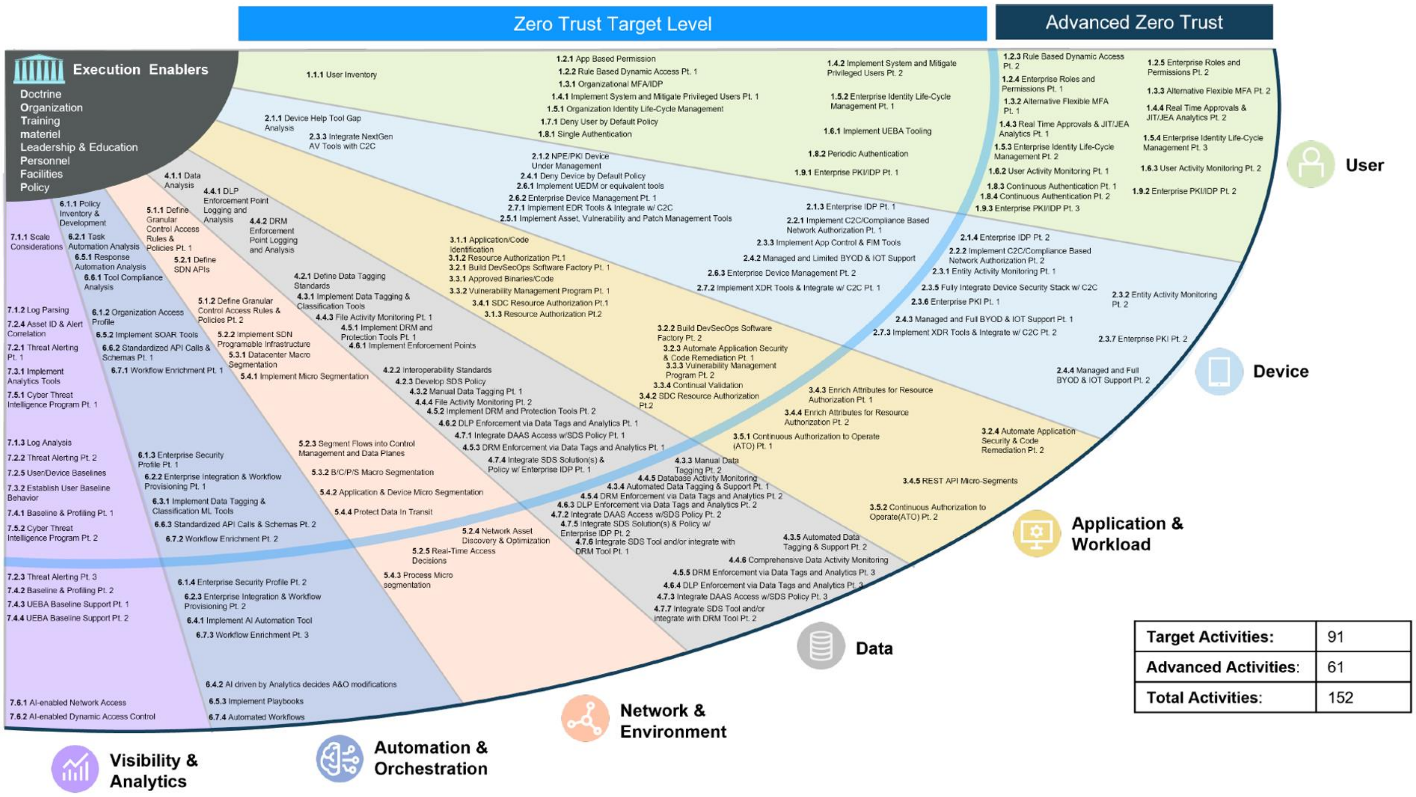
[9] DoD Zero Trust Capability Execution Roadmap, DoD CIO PfMO, November 15, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTExecutionRoadmap.pdf

Copyright © 2023 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.

The 152 activities are realized by mapping them to over 1000 NIST security controls[10]. These controls are cross-referenced to over 200 vendor products and capabilities. A government assessment team will use this requirements matrix to validate the solution's implementation and certify its compliance. Only a system that complies with all applicable NIST 800-53 controls mapped to their respective activities can be considered a **validated Zero Trust solution**.

The validated Zero Trust approach stresses integration **across all seven pillars**. The goal is to establish multiple policy checkpoints and automatically approve or deny requests based on the user's behavior patterns. Such a solution is not architected for convenience. It minimizes the impact on users while allowing the system to downgrade access or even shut out users and equipment that do not show good behavior. For example, an employee in the marketing department trying to access sensitive customer information from an unfamiliar device or location would immediately trigger an automated response to stop suspicious activity.

The key to **validated Zero Trust** is verified security by design and automation of policy. It assumes that the adversary is already in the system or able to gain access. The only recourse is to protect the broader enterprise by limiting what any user can do at a given time, using incremental policy decisions and policy enforcement points. A single user—authorized or unauthorized—can no longer have continual and complete access to an enterprise without incremental validation and attribution.[11] A detailed example illustrating the hacker's journey through a validated Zero Trust environment is in the appendix.


Zero Trust Target Level
Advanced Zero Trust
Execution Enablers
Doctrine
Organization
Training
materiel
Leadership & Education
Personnel
Facilities
Policy
1.1.1 User Inventory
1.2.1 App Based Permission
1.2.2 Rule Based Dynamic Access Pt. 1
1.3.1 Organizational MFA/IDP
1.4.1 Implement System and Mitigate Privileged Users Pt. 1
1.5.1 Organization Identity Life-Cycle Management
1.7.1 Deny User by Default Policy
1.8.1 Single Authentication
1.4.2 Implement System and Mitigate Privileged Users Pt. 2
1.5.2 Enterprise Identity Life-Cycle Management Pt. 1
1.6.1 Implement UEBA Tooling
1.8.2 Periodic Authentication
1.9.1 Enterprise PKI/IDP Pt. 1
1.2.3 Rule Based Dynamic Access Pt. 2
1.2.4 Enterprise Roles and Permissions Pt. 1
1.3.2 Alternative Flexible MFA Pt. 1
1.4.3 Real Time Approvals & JIT/JEA Analytics Pt. 1
1.5.3 Enterprise Identity Life-Cycle Management Pt. 2
1.6.2 User Activity Monitoring Pt. 1
1.8.3 Continuous Authentication Pt. 1
1.8.4 Continuous Authentication Pt. 2
1.9.3 Enterprise PKI/IDP Pt. 3
1.2.5 Enterprise Roles and Permissions Pt. 2
1.3.3 Alternative Flexible MFA Pt. 2
1.4.4 Real Time Approvals & JIT/JEA Analytics Pt. 2
1.5.4 Enterprise Identity Life-Cycle Management Pt. 3
1.6.3 User Activity Monitoring Pt. 2
1.9.2 Enterprise PKI/IDP Pt. 2
User
2.1.1 Device Help Tool Gap Analysis
2.3.3 Integrate NextGen AV Tools with C2C
2.1.2 NPE/PKI Device Under Management
2.4.1 Deny Device by Default Policy
2.6.1 Implement UEDM or equivalent tools
2.6.2 Enterprise Device Management Pt. 1
2.7.1 Implement EDR Tools & Integrate w/ C2C
2.5.1 Implement Asset, Vulnerability and Patch Management Tools
2.1.3 Enterprise IDP Pt. 1
2.2.1 Implement C2C/Compliance Based Network Authorization Pt. 1
2.3.3 Implement App Control & FIM Tools
2.4.2 Managed and Limited BYOD & IOT Support
2.6.3 Enterprise Device Management Pt. 2
2.7.2 Implement XDR Tools & Integrate w/ C2C Pt. 1
2.1.4 Enterprise IDP Pt. 2
2.2.2 Implement C2C/Compliance Based Network Authorization Pt. 2
2.3.1 Entity Activity Monitoring Pt. 1
2.3.5 Fully Integrate Device Security Stack w/ C2C
2.3.6 Enterprise PKI Pt. 1
2.4.3 Managed and Full BYOD & IOT Support Pt. 1
2.7.3 Implement XDR Tools & Integrate w/ C2C Pt. 2
2.3.2 Entity Activity Monitoring Pt. 2
2.3.7 Enterprise PKI Pt. 2
2.4.4 Managed and Full BYOD & IOT Support Pt. 2
Device
3.1.1 Application/Code Identification
3.1.2 Resource Authorization Pt.1
3.2.1 Build DevSecOps Software Factory Pt. 1
3.3.1 Approved Binaries/Code
3.3.2 Vulnerability Management Program Pt. 1
3.4.1 SDC Resource Authorization Pt.1
3.1.3 Resource Authorization Pt.2
3.2.2 Build DevSecOps Software Factory Pt. 2
3.2.3 Automate Application Security & Code Remediation Pt. 1
3.3.3 Vulnerability Management Program Pt. 2
3.3.4 Continual Validation
3.4.2 SDC Resource Authorization Pt.2
3.4.3 Enrich Attributes for Resource Authorization Pt. 1
3.4.4 Enrich Attributes for Resource Authorization Pt. 2
3.5.1 Continuous Authorization to Operate (ATO) Pt. 1
3.2.4 Automate Application Security & Code Remediation Pt. 2
3.4.5 REST API Micro-Segments
3.5.2 Continuous Authorization to Operate(ATO) Pt. 2
Application & Workload
4.1.1 Data Analysis
4.4.1 DLP Enforcement Point Logging and Analysis
4.4.2 DRM Enforcement Point Logging and Analysis
4.2.1 Define Data Tagging Standards
4.3.1 Implement Data Tagging & Classification Tools
4.4.3 File Activity Monitoring Pt. 1
4.5.1 Implement DRM and Protection Tools Pt. 1
4.6.1 Implement Enforcement Points
4.2.2 Interoperability Standards
4.2.3 Develop SDS Policy
4.3.2 Manual Data Tagging Pt. 1
4.4.4 File Activity Monitoring Pt. 2
4.5.2 Implement DRM and Protection Tools Pt. 2
4.6.2 DLP Enforcement via Data Tags and Analytics Pt. 1
4.7.1 Integrate DAAS Access w/SDS Policy Pt. 1
4.5.3 DRM Enforcement via Data Tags and Analytics Pt. 1
4.7.4 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 1
4.3.3 Manual Data Tagging Pt. 2
4.4.5 Database Activity Monitoring
4.3.4 Automated Data Tagging & Support Pt. 1
4.5.4 DRM Enforcement via Data Tags and Analytics Pt. 2
4.6.3 DLP Enforcement via Data Tags and Analytics Pt. 2
4.7.2 Integrate DAAS Access w/SDS Policy Pt. 2
4.7.5 Integrate SDS Solution(s) & Policy w/ Enterprise IDP Pt. 2
4.7.6 Integrate SDS Tool and/or integrate with DRM Tool Pt. 1
4.3.5 Automated Data Tagging & Support Pt. 2
4.4.6 Comprehensive Data Activity Monitoring
4.5.5 DRM Enforcement via Data Tags and Analytics Pt. 3
4.6.4 DLP Enforcement via Data Tags and Analytics Pt. 3
4.7.3 Integrate DAAS Access w/SDS Policy Pt. 3
4.7.7 Integrate SDS Tool and/or integrate with DRM Tool Pt. 2
Data
5.1.1 Define Granular Control Access Rules & Policies Pt. 1
5.2.1 Define SDN APIs
5.1.2 Define Granular Control Access Rules & Policies Pt. 2
5.2.2 Implement SDN Programable Infrastructure
5.3.1 Datacenter Macro Segmentation
5.4.1 Implement Micro Segmentation
5.2.3 Segment Flows into Control Management and Data Planes
5.3.2 B/C/P/S Macro Segmentation
5.4.2 Application & Device Micro Segmentation
5.4.4 Protect Data In Transit
5.2.4 Network Asset Discovery & Optimization
5.2.5 Real-Time Access Decisions
5.4.3 Process Micro segmentation
Network & Environment
6.1.1 Policy Inventory & Development
6.2.1 Task Automation Analysis
6.5.1 Response Automation Analysis
6.6.1 Tool Compliance Analysis
6.1.2 Organization Access Profile
6.5.2 Implement SOAR Tools
6.6.2 Standardized API Calls & Schemas Pt. 1
6.7.1 Workflow Enrichment Pt. 1
6.1.3 Enterprise Security Profile Pt. 1
6.2.2 Enterprise Integration & Workflow Provisioning Pt. 1
6.3.1 Implement Data Tagging & Classification ML Tools
6.6.3 Standardized API Calls & Schemas Pt. 2
6.7.2 Workflow Enrichment Pt. 2
6.1.4 Enterprise Security Profile Pt. 2
6.2.3 Enterprise Integration & Workflow Provisioning Pt. 2
6.4.1 Implement AI Automation Tool
6.7.3 Workflow Enrichment Pt. 3
6.4.2 AI driven by Analytics decides A&O modifications
6.5.3 Implement Playbooks
6.7.4 Automated Workflows
Automation & Orchestration
7.1.1 Scale Considerations
7.1.2 Log Parsing
7.2.4 Asset ID & Alert Correlation
7.2.1 Threat Alerting Pt. 1
7.3.1 Implement Analytics Tools
7.5.1 Cyber Threat Intelligence Program Pt. 1
7.1.3 Log Analysis
7.2.2 Threat Alerting Pt. 2
7.2.5 User/Device Baselines
7.3.2 Establish User Baseline Behavior
7.4.1 Baseline & Profiling Pt. 1
7.5.2 Cyber Threat Intelligence Program Pt. 2
7.2.3 Threat Alerting Pt. 3
7.4.2 Baseline & Profiling Pt. 2
7.4.3 UEBA Baseline Support Pt. 1
7.4.4 UEBA Baseline Support Pt. 2
7.6.1 AI-enabled Network Access
7.6.2 AI-enabled Dynamic Access Control
Visibility & Analytics

Target Activities:	91
Advanced Activities:	61
Total Activities:	152

Figure 2 The 152 activities involved in a Validated Zero Trust Approach

The DoD framework also recognizes that Zero Trust is not just about technology but will require changes across the entire organization. It provides the foundation to help align ongoing and future efforts, investments, and initiatives across nontechnical capabilities and activities that address culture, governance, and elements of Doctrine, Organization, Training, material, Leadership and Education, Personnel, Facilities, and Policy

[10] Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Rev. 5, December 10, 2020 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[11] Principle of Least Privilege Security Principle, Charlie Miller, Shared Assessments, October 01, 2020, https://sharedassessments.org/blog/principle-of-least-privilege-the-basics-a-security-principle-to-live-by/

Copyright © 2023 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.

(DOTmLPF-P).[12]

The **seven pillars** from the Zero Trust reference architecture are broken down into **45 capabilities**. Each capability is further divided and organized into **152 Zero Trust activities**.

Complying with these activities will validate the Zero Trust Strategy at two levels of maturity—**Target (91 activities)** and **Advanced (all 152 activities)**.

Why trust the U.S. DoD's Zero Trust Strategy?

The U.S. DoD is one of the world's leading experts in data security. It is responsible for securing some of the most sensitive secrets under the most hostile conditions created by nation-states. They work with NIST, through the National Security Agency (NSA),[13] to create globally recognized standards for security measures, such as AES-256,[14] the most widely known data encryption standard, while deprecating standards like MD5[15] when they find vulnerabilities.

The U.S. DoD is a global enterprise. Its standards impact all its partner nations, from the Five Eyes (FVEY) to the North Atlantic Treaty Organization (NATO), the Asia-Pacific region, and beyond. Domestically, the U.S. government is under a mandate to implement Zero Trust. Many enterprises fall within the 16 critical infrastructure sectors, including the Defense Industrial Base (DIB).[16] The U.S. government encourages using small and medium businesses; this mandate implies that more than 250,000 corporations will need to operate under similar security requirements for the DoD alone.

Moreover, the DoD is ahead of the curve in Zero Trust, not just in strategy but also in implementation, which will start in 2023. Dell has chosen to follow DoD guidance for their proven expertise and help them implement this plan.

There is a clear path to validated Zero Trust

The DoD has defined three courses of action (COA) for implementing the Zero Trust Strategy: **COA-1 tackles the brownfield environment** by upgrading existing systems; **COA-2 uses public clouds**; and **COA-3 builds a private cloud**, either on-premises or as a Service (aaS), using managed co-location. Based on their analysis, COA-3 is quicker than COA-1 and will be directly certified at the Advanced Level.[17] It also offers the most flexible deployment options and supports distinct scenarios in addition to the core enterprise network, such as edge and other tactical scale Zero Trust deployments.

True to the maxim, "the smallest of implementations is worth more than the grandest of intentions," in October

[12] Strategic Leaders: How's Your DOTMLPF-P?, Col. John Boggs, Fortitude Consult, 2015, https://www.fortitudeconsult.com/resources/articles/strategic-leaders-hows-your-dot-ml-pf-p/#:~:text=DOTMLPF%2DP%20is%20an%20acronym,supports%20effectively%20operationalizing%20the%20strategy
[13] Center for Cybersecurity Standards, National Security Agency, https://www.nsa.gov/Cybersecurity/Partnership/Standards/
[14] Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms, Bryan Weeks, Mark Bean, Tom Rozylowicz, Chris Ficke, National Security Agency, May 2000, https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/aes-development/NSA-AESfinalreport.pdf
[15] Definition of MD5, Mary E. Shacklett, TechTarget, https://www.techtarget.com/searchsecurity/definition/MD5
[16] Defense Industrial Base Sector, CISA, https://www.cisa.gov/defense-industrial-base-sector
[17] DoD Zero Trust Capability Execution Roadmap, DoD CIO PfMO, November 15, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilityExecutionRoadmap.pdf

Copyright © 2023 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.

2022, Dell Technologies announced that it would power the Zero Trust Center of Excellence at DreamPort,[18] where it will provide organizations with a secure data center to validate Zero Trust use cases. The company's participation and leadership in this initiative form the foundation of COA-3. This Center of Excellence will use the DoD Zero Trust Reference Architecture as its foundation for organizations to test configurations before deploying in their environments.

This approach will allow Dell to understand the operational impacts, validate the customer workloads in that environment, and industrialize the architecture into a repeatable build. We can optimize application and data placement in this multicloud multi-tier environment and implement all 152 activities. By orchestrating across an extensive partner ecosystem, Dell will deliver a repeatable build of a validated Zero Trust cloud, providing a quicker path to adoption and easing the integration and orchestration burden for customers.

Once a Zero Trust private cloud is installed on-premises or accessed as a service, organizations will need to migrate their workloads, data, and known users and devices to it. It will also have some operational impacts, including the need for new ways of administering the solution and modernizing their approach to the security operation center (SOC). Dell Technologies has identified seven service offerings that support adopting a validated Zero Trust solution, including assessment, preparation, installation, policy management, administration, SOC management, and workload migration. We will discuss these offerings in detail in a separate paper.

Conclusion

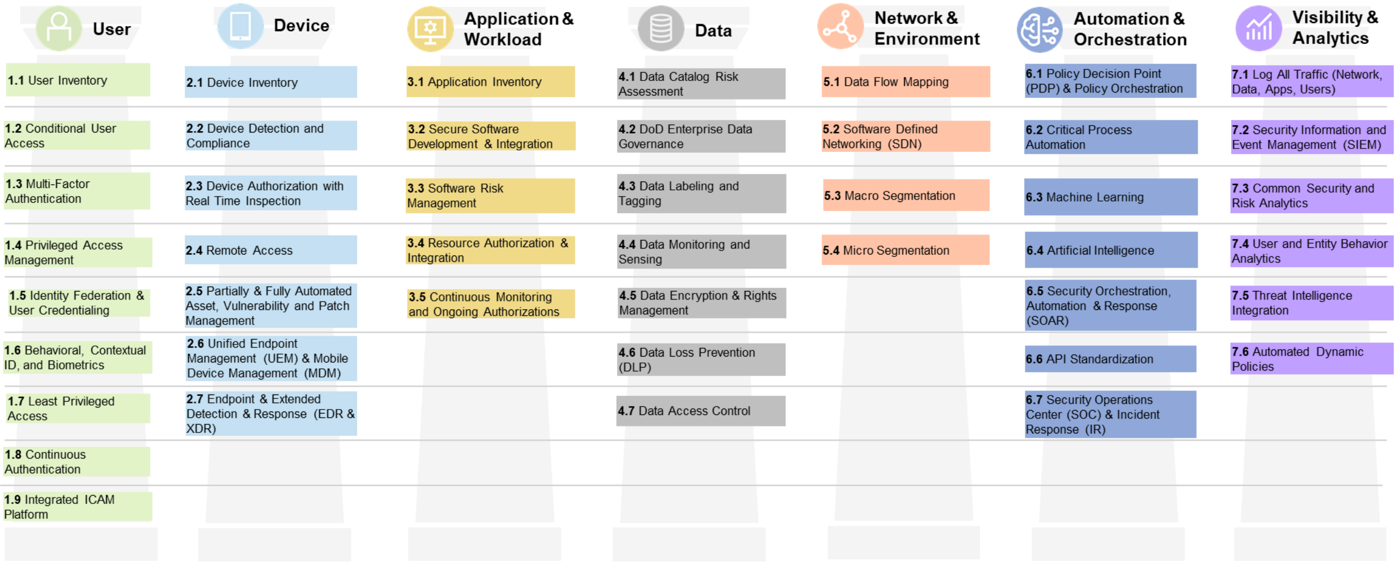
While the overwhelming evidence suggesting the need and demand for a Zero Trust solution is irrefutable, attempting an ad hoc and piecemeal approach to its implementation is futile. Dell has committed to and invested in developing a validated Zero Trust solution. The company will use its deep vendor relationships to keep the integrated solution up to date and undergo periodic government validation to help ease the integration burden for organizations across the globe.

[18] Dell Technologies Delivers Zero Trust, Cybersecurity Solutions to Protect Multicloud and Edge Environments, October 4, 2022, https://investors.delltechnologies.com/news-releases/news-release-details/dell-technologies-delivers-zero-trust-cybersecurity-solutions

Copyright © 2023 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.

Appendix

A hacker's Zero Trust experience



User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

Figure 3 Zero Trust Capabilities

Referencing Figure 3, here are the capabilities (Cap.) that an attacker would encounter in a validated Zero Trust environment. First, the hacker would face multifactor authentication (Cap. 1.3) and behavioral, contextual, and biometric identification. This would include verifying the time and location they were trying to access the system (Cap. 1.6). There will also be steps to identify the device and ensure it complies with company policy before granting access (Cap. 2.2). This could mean checking for specific software patches or system versions on the device (Cap. 2.5). The user and the device would be evaluated by the AI and Machine learning models to determine if this user is behaving consistently with their normal behavior. The hacker would need to mimic the authorized user's behavior to gain access. Good and bad results are gathered and logged (Cap. 7.1) to inform threat intelligence (Cap. 7.5) and to build models to improve the system's security (Cap. 7.6). Although this decision process is the user's first encounter with automated policy orchestration (Cap. 6.1), it would not be their last. Many hackers would fail here. Let us assume they gain access.

Once the user is logged into the Zero Trust system, they will face continuous authentication (Cap. 1.8). They are also subject to least privileged access at the start of their session (Cap. 1.7). They may choose to elevate their privileges on the system to install specific malware, or gain access to more sensitive areas of the system. To do so, they would have to complete the privileged access procedures (Cap. 1.4). The software-defined network they are using (Cap. 5.2) for their session would be microsegmented (Cap. 5.3) to ensure they could only access the bare minimum of enterprise data.

Once they request access to data (Cap. 4.5) or applications (Cap. 3.3), their rights would be reviewed and processed by policy orchestration (Cap. 6.1). Part of the assessment to grant access to the requested data and application would again include a behavior assessment (Cap. 7.4). Let us say the hacker gains access to the chosen application and data. Now they unleash their ransomware malware which encrypts everything on the network. Due to microsegmentation (Cap. 5.3), the network would only connect to the requested application and data. The impact of the attack would be limited to the scope of the microsegmented network for this user's request. This is a vast improvement over the ransomware reaching out over the entire enterprise network. Let us call that attack a failure.

Not wanting to waste stolen credentials and access, the hacker regroups and tries to steal data instead. They leave behind malware that will transmit corporate data later. The type and amount of data must be within this hacked user's access. This is verified by the policy orchestration (Cap. 6.1). Without the privileged access, the hacker was unable to obtain (Cap. 1.4), if the data extraction is out of the norm, high data access at an

Copyright © 2023 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.

uncommon time of day would trigger data loss prevention (Cap. 4.6). If the data extraction was low volume and slow, it would still be restricted to the microsegmented network. Since the system is continuously monitored (Cap. 4.4), and threat intelligence is continuously updated (Cap. 7.5), known malware could also be detected within this user's microsegmented network.

This is a high-level description of the challenge a hacker would have to launch a successful ransomware attack against a validated Zero Trust system. You can see how users are subject to capabilities across multiple pillars to perform a work activity. The detailed data flows are shown in the Zero Trust 2.0 Reference Architecture[19].

[19] DoD Zero Trust Reference Architecture, Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, September 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Copyright © 2023 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.