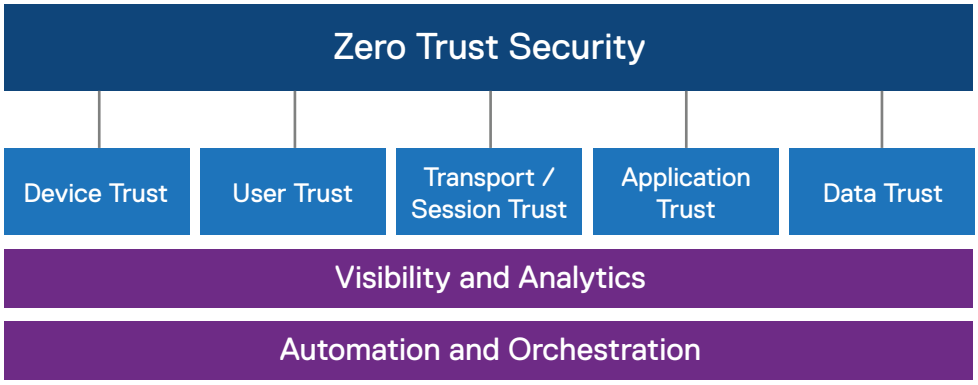
DELL Technologies

Cybersecurity Whitepaper

The Pathway to a Zero-Trust Workspace

The Five Pillars of Zero-Trust Architecture

The Zero Trust architecture consists of five pillars. Trust must be established in each pillar to decide whether to grant or deny access. By establishing trust across the five pillars, visibility is expanded which supports end-to-end analytics. Visibility and analytics are a critical part of the Zero Trust architecture, and they help to establish a deeper and broader footprint in each pillar.



Dell Zero-Trust Workspace

VMware is uniquely positioned to help you on your Zero Trust journey, with the broadest portfolio of solutions covering all five pillars of trust.

vmware	Device	User	Transport	Applications	Data
VMware Workspace ONE	✓	✓		✓	✓
VMware Unified Access Gateway	✓		✓		
VMware Carbon Black	✓				
VMware NSX-T Data Center			✓		✓
VMware Horizon 7			✓	✓	✓

Component Path to a Zero-Trust Workspace

The Zero Trust Imperative

As the Department of Defense continues large-scale telework, it's working to build a zero-trust security architecture into its networks — particularly as the department battles an increase in phishing attacks. John Sherman, the DOD's principal deputy chief information officer, said the challenges of the pandemic have pushed the conversion toward action. But the move hasn't been without resistance, Sherman said, hinting there has been dissent among some agencies in DOD over how to make zero trust a reality.

"This crisis has forced us to think differently," – John Sherman, DoD's Principal Deputy CIO

fedscoop

The Zero-Trust Imperative

https://www.fedscoop.com/teleworking-zero-trust-in-dod-phishing-attacks-increase/

Assembling the Blocks

Device Trust

Parameters

- Management
- Inventory
- Compliance
- Authentication

Solution Blocks

VVMware Workspace ONE – Device Trust

VMware Unified Access Gateway – Device Authentication

VMware Carbon Black – Endpoint Security

User

Parameters

- Password Authentication
- Multi-factor Authentication
- Conditional Access Dynamic Risk Scoring

Solution Blocks

VMware Workspace ONE Access & Intelligence – Provides strong authentication and dynamic conditional access

Transport

Parameters

- Micro-Segmentation
- Transport Encryption
- Session Protection

Solution Blocks

VMware Unified Access Gateway & Horizon 7 – Provides secure session transport

VMware NSX-T Data Center – Provides resource segmentation to apply least privileged network access

Applications

Parameters

- Single Sin-On
- Isolation
- Any Device Access

Solution Blocks

VMware Workspace ONE UEM & Horizon 7 – Provides application trust

VMware Workspace ONE Access – Provides single sign-on with strong user authentication

Data

Parameters

- Protecting Data-at-Rest
- Integrity
- Data Loss Prevention (DLP)
- Classification

Solution Blocks

VMware Workspace ONE UEM & Horizon 7 & NSX-T data Center– Provides data integrity and data control

Unifying the Five Pillars

Analytics and Automation

Establishing trust across the five pillars of Zero Trust architecture provides visibility and analytics. Implementation of a system that provides visibility through logging all traffic is critical to perform effective analytics. The resulting analytics should be leveraged to make effective dynamic policy and trust decisions.

With visibility and analytics, automation and orchestration can be established. Workspace ONE and Horizon platform services allow for the collection of contextual information from across the entire environment. This contextual awareness feeds intelligence, allowing for just-in-time decisions, and use automation for threat remediation.

Visibility and Analytics

Parameters

- Log Collection
- Centralized Log Repository
- Monitoring Dashboards
- Troubleshooting Consoles

Solution Blocks

VMware

- Horizon 7
- Unified Access Gateway
- Workspace ONE Access
- Workspace ONE UEM
- Workspace ONE Intelligence
- Workspace ONE Trust Network

Visibility and Analytics

Parameters

- Compliance Engine on Device
- APIs for External Program Integration
- Contextual Workflows for Automation Remediation

Solution Blocks

VMware

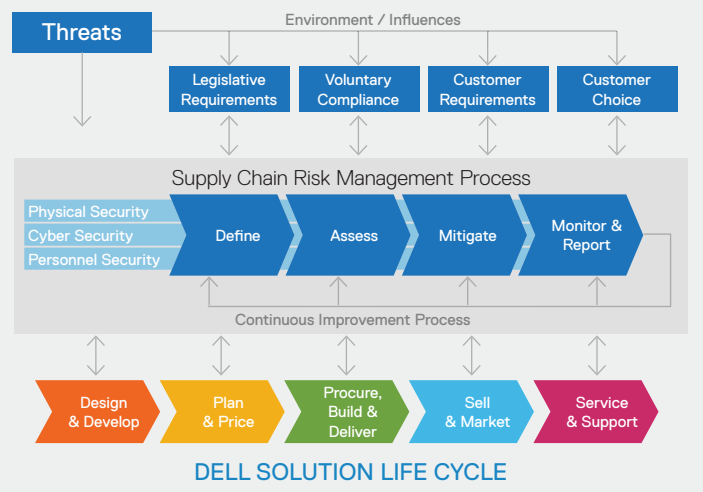
- Workspace ONE UEM
- Workspace ONE Intelligence

Cybersecurity Architecture & Zero Trust

Dell Hardware to Support Zero Trust Pursuit

The underlying architecture of any solution should leverage hardware and software products that provide industry leading cybersecurity features provided by a company that pursues the best principles in providing a secure supply chain.

Secure Supply Chain



Dell's Supply Chain Risk Management framework mirrors that of the comprehensive risk management framework of the National Infrastructure Protection Plan (NIPP), which outlines how government and the private sector can work together to mitigate risks and meet security objectives. Dell's framework incorporates an open feedback loop that allows for continuous improvement. Risk mitigation plans are prioritized and implemented as appropriate throughout the entire solution life cycle.

Dell Trusted Client BIOS

Dell has been involved in contributing to, and building devices that adhere to, recommendations from NIST around firmware security and resilience. NIST Special Publication SP800-193 has outlined overall resilience guidelines for device firmware (including BIOS) and has been helpful in confirming the value in Dell's below the OS security investments and direction.

	Dell Unique	Industry Standard
Respond	Dell BIOS Recovery Dell SafeBIOS Image Capture	
Detect	Discrete TMP Dell SafeBIOS Verification Dell SafeBIOS IoA	Runtime BIOS Resilience TCG Measured Boot Downgrade
Prevent	Fused Root of Trust Dell UEFI Secure Boot BIOS Passwords	Intel BIOS Guard Intel Boot Guard Authenticated Updates BIOS Public Keys

Leveraging the PowerEdge Custom UEFI Security Advantage

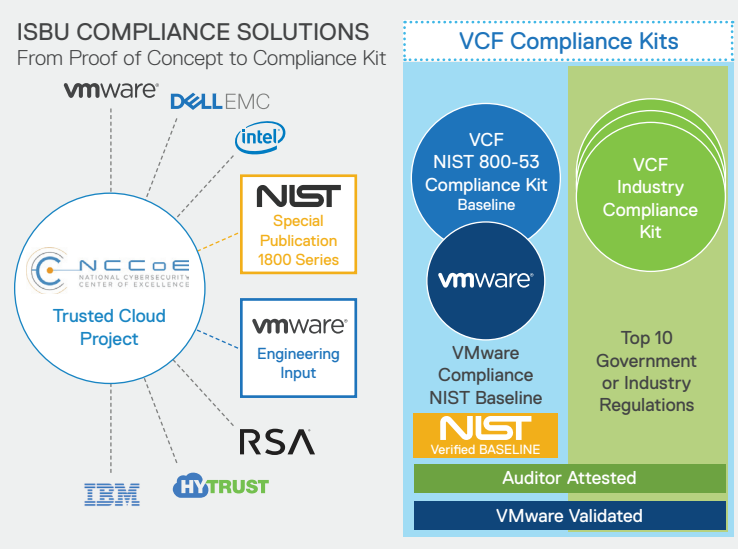
Exclusive support for the principles and requirements outlined in the NSA's UEFI Secure Boot Customization technical report.

What customer's should ask from their solution provider

- Does your solution provide a custom UEFI secure boot capable of removing the cert risk exposed by Boothole?
- Does your solution provide an immutable silicon-based chain of trust
- Signed firmware updates using SHA-256 hashing with 2048-bit RSA encryption for signature for all key server components
- Options for TPM 2.0

NSA: UEFI Secure Boot Customization Paper

Dell Technologies Trusted Hybrid Cloud – For Compliance Drive Customers



A hardware/software hyperconverged hybrid cloud solution that is delivered to help customers meet industry and government cybersecurity compliancy goals.

DELL Technologies

References

Additional Resources

To learn more about the Zero Trust model, follow the Zero Trust Activity Path, which contains a curated list of assets to help you master the VMware Zero Trust architecture. This activity path and more resources are available on Digital Workspace Tech Zone. You can also explore the following resources:

- Activity Path: Understanding Zero Trust
- Video: VMware Zero Trust: Technical Overview
- Product page: Zero Trust Security for the Digital Workspace
- Blog post: Brian Madden: What is zero trust, and how real is it today?
- Guide: Zero Trust Secure Access to Traditional Applications with Vmware

Contact your Dell Sales Representative with additional questions on this topic.