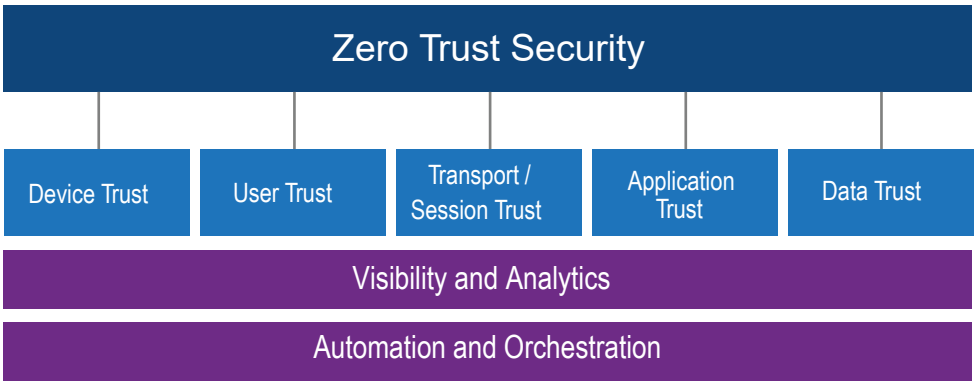
DELL Technologies

# The Pathway to a Zero Trust Security Model

## 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 (FedRAMP Authorized) | ✓ | ✓ | | ✓ | ✓ |
| VMware Unified Access Gateway | ✓ | | ✓ | | |
| VMware Carbon Black | ✓ | | | | |
| VMware NSX-T Data Center | | | ✓ | | ✓ |
| VMware Horizon 7 | | | ✓ | ✓ | ✓ |

Component Path to a Zero-Trust Workspace

### Zero Trust Networks: The Future of Security

The evolution of networks organizations have undergone remarkable change. Today the network boundaries have become opaque and modern IT involves containers, serverless and cloud computing, mobile users, mobile applications, and mobile storage. These are all major disruptors of traditional security architectures.

The ever-growing challenge to protect critical data, especially with the development of continued disruptors, is leading organizations toward a zero-trust security model that addresses their needs in today's digitally robust world.

Zero trust offers more than a line of defense; the model's security benefits deliver considerable business value. At Dell Technologies and VMware, we believe that a zero-trust approach to security will facilitate greater control over access, authorization to applications and sensitive data, and reduced IT complexity while delivering a superior user experience.

"Zero trust, if it's done correctly, is disruptive—it should disrupt the activities of the bad guys."
*- Kathleen Moriarty, Security Innovations Principal, Dell Technologies*

# Assembling the Blocks

## Device Trust

Parameters
- Management
- Inventory
- Compliance
- Authentication

VMware Solution
- ✓ VMware 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

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

## Transport

Parameters
- Micro-Segmentation
- Transport Encryption
- Session Protection

VMware Solution
- ✓ 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

VMware Solution
- ✓ 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

VMware Solution
- ✓ 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

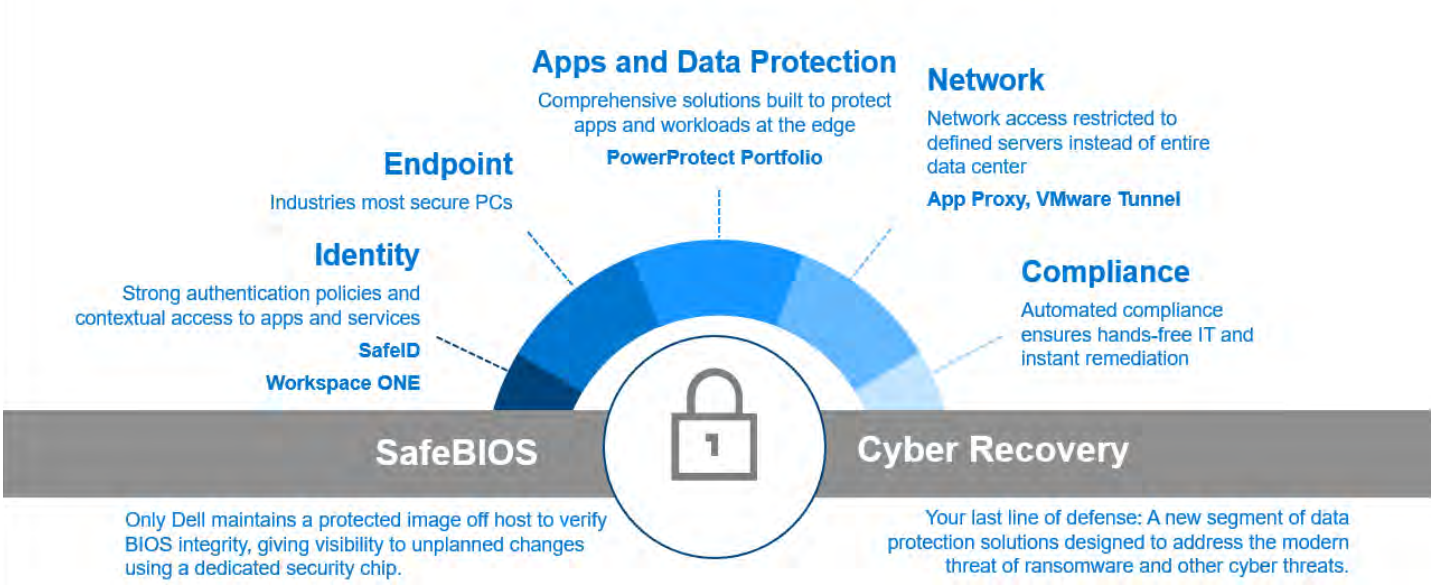
VMware
- Workspace ONE UEM
- Workspace ONE Intelligence

# Cybersecurity Architecture and 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.

### Above and Below the OS Protection




### End-to-End Security

With Dell BIOS, Dell maintains a protected image off host to verify BIOS integrity, giving visibility to unplanned changes, using a dedicated security chip. Should the BIOS get corrupted or tampered with, we give customers flexible reimage options as opposed to simply pushing a refresh without prior approval.

But not all threats are malware. Protecting the endpoint is a good start, but you also need to secure your data center too. Because of this, we deliver security built-in to our industry-leading servers, storage, HCI, and data protection appliances to help protect data wherever it is stored, managed or used – in on-premises data centers and cloud environments. For maximum efficiency and peace of mind, we also offer a cyber recovery, designed to address the modern threat of ransomware and other cyber threats.

### 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.

### Leveraging the PowerEdge Custom UEFI Security Advantage

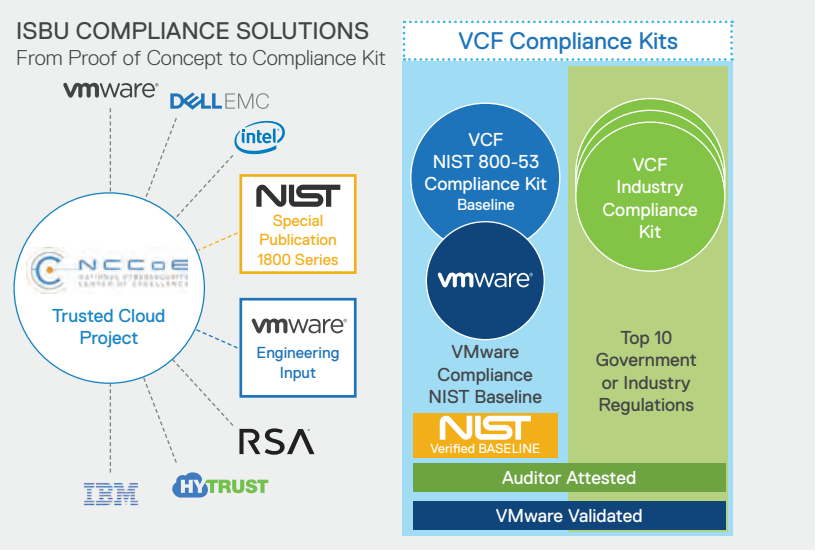
Exclusive support for the principles and requirements outlined in the NSA's UEFI Secure Boot Customization technical report.

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 Hybrid Cloud for Governance & Compliance




Dell Technologies and VMware provide a hardware/ software hyper-converged hybrid cloud solution with advanced features to improve your capabilities before, during, and after a security incident.

Provide maximum control of data and infrastructure with ISBU compliant solutions, including endorsements for meeting all of the data vaulting requirements of the Sheltered Harbor standard, protecting U.S. financial institutions from cyber threats like ransomware.

# 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
- Forrester whitepaper: How to Get From Here to Zero Trust
- Tool: Cyber Resiliency Assessment
- Solution Guide: Dell EMC Cyber Recovery with Unysis Stealth

Contact your Dell Sales Representative with any additional questions.



DELL Technologies