DELL Technologies

Technical Whitepaper

Zero-Trust

A key framework in Dell Technologies overall Data Protection Strategy

How PowerProtect Cyber Recovery increases resilience by aligning to the Zero Trust framework

Abstract

A good cyber resilience posture starts with knowing who or what has access to your company's vital assets. Deploying a Zero Trust architecture within your infrastructure gives you peace of mind that the integrity of your devices, applications and data are secure. Dell PowerProtect Cyber Recovery solution helps increase the resilience of your infrastructure and can be a key component to helping you on your journey in building out a Zero Trust architecture.

Table of contents

Introduction

Using guidance from the Cybersecurity and Infrastructure Security Agency's (CISA) "Shields Up" campaign, the U.S. government has recommended "all organizations--regardless of size--adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets."[1] One key component to strengthening cybersecurity is Zero Trust, a framework for verifying, assuring, and protecting data. The security model is not a new concept. What has changed is the landscape.

Today's enterprise environments consist of many interconnected segments: corporate networks, on-prem infrastructure and applications, cloud-based infrastructure and applications, remote and mobile workforce environments, and an increasing number of sensors and devices at the edge. This infrastructure evolution has created more opportunity for threats to access critical data, forcing organizations to reevaluate traditional data protection methodology. Perimeter-based defenses are no longer adequate.

Organizations need a comprehensive approach to cyber risk mitigation that goes beyond mere threat detection. Lax security on internal networks has enabled intruders to launch full-scale cyberattacks on strategic assets in the data center. Insider attacks—intentional or otherwise—have also been rising annually; they now constitute a significant percentage of enterprise breaches. A newly remote workforce, precipitated by the global pandemic, further exacerbated security concerns by extending networks beyond traditional boundaries. The introduction of Bring Your Own Device (BYOD) policies and the extension of data centers to public clouds have also introduced increased risk. Enterprise vulnerability is due to a combination of factors, creating the need for a more effective and resilient approach to cybersecurity.

This white paper is intended to show how a Zero Trust architecture is a key framework followed across Dell Technologies' overall data protection strategy, and in particular, how the Dell PowerProtect Cyber Recovery solution fits into this framework.

[1] https://zerotrust.cyber.gov/

What is Zero Trust

Zero Trust principles are not new, but the concept is experiencing a renaissance because it addresses many of the cybersecurity challenges, we face today. The Zero Trust concept was introduced in 1994, when Dr. Stephen Paul Marsh wrote his doctoral thesis on "Formalising Trust as a Computation Concept." He posited that trust was an inherently human concept, a "social phenomenon" that could be codified and understood by artificial intelligence. But it wasn't until 2010 that John Kindervag, an analyst at Forrester Research, realized the potential of the idea. Kindervag challenged the prevailing wisdom--that creating a strong perimeter was enough to keep an organization secure. He suggested not trusting anything inside the perimeter either. Zero Trust describes the process and technologies of implementing trust on a transactional basis. The framework focuses on authentication and authorization of all users on a network while still maintaining the pace and availability of services.

As defined by National Institute of Standards and Technology (NIST) Special Publication 800-207, "Zero Trust is a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least-privileged per-request access decisions in information systems and services" under the assumption that the network is compromised. A Zero Trust architecture (ZTA) uses Zero Trust principles to plan industrial and enterprise infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established.[2] A Zero Trust architecture is an enterprise's cybersecurity plan that utilizes Zero Trust concepts and encompasses component relationships, workflow planning, and access policies. Zero Trust Security, also known as perimeter-less security, describes a comprehensive approach to the design and implementation of IT systems. The main concept behind Zero Trust security is "never trust, always verify."

The Cybersecurity & Infrastructure Security Agency's (CISA's) Zero Trust Maturity Model is one of many roadmaps, specific to the federal government, for agencies to reference as they transition towards a Zero Trust architecture. The goal of the maturity model is to assist agencies in developing trust strategies and implementation plans and present ways in which various CISA services can support Zero Trust solutions across agencies.

The maturity model, which includes five pillars and three cross-cutting capabilities, is based on the foundations of Zero Trust. Within each pillar, the maturity model provides agencies with specific examples of a traditional, advanced, and optimal zero trust architecture. CISA drafted the Zero Trust Maturity Model in June of 2021 to assist agencies in complying with Executive Order 14028 "Improving the Nation's Cybersecurity."[3]

The National Counterintelligence and Security Center (NCSC), a part of the Office of the Director for National Intelligence, provides an alternate but consistent approach in identifying key principles behind Zero Trust architectures. The NCSC calls out the essential need for a single, strong source of user identity, user authentication, machine authentication, additional context, such as policy compliance and device health, authorization policies to access an application and access control policies within an application.

It should be noted that employees may view a "never-trust" system as cumbersome because they must constantly prove their legitimacy to an individual system. While the challenges of a Zero Trust environment make it more difficult to maneuver, it is still, by far, the most effective and secure. A Zero Trust infrastructure is the most effective tool against unauthorized lateral movement.

[2] https://doi.org/10.6028/NIST.SP.800-207
[3] https://www.federalregister.gov/executive-order/14028

The Tenets of Zero Trust

NIST Special Publication 800-207 Zero Trust Architecture states that a zero trust architecture is designed and deployed with adherence to the following tenets:

- All Data Sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per session basis
- 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.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed
- The enterprise collects as much information as possible related to the current state of assets, network infrastructure and communications and uses it to improve its security posture

Zero Trust is not a single architecture, it is a set of guiding principles for workflow, operations, and systems design. The importance of a strong Identity, Credentialing, and Access Management practice cannot be overstated. It is a key component. Without it, all underlying security practices are at risk. An effective ICAM solution must include tools and controls that can capture and store user login details, facilitate the assignment and revocation of user access credentials, and conduct oversite of a central database of user roles, levels, and access privileges.

Logical Components of Zero Trust

Access is granted to a resource via a Policy Decision Point (PDP) and a corresponding Policy Enforcement Point (PEP). The basic tenets of authentication and authorization ensure that the subject is authentic and is granted access to a resource.

The implicit zone represents an area where all entities are trusted to at least the level of the last PDP/PEP gateway and applies a set of controls to all traffic beyond the PDP/PEP checkpoint. Zero trust provides a framework to move the PDP/PEP checkpoints closer to the resource with the goal of explicitly authenticating and authorizing all subjects, assets, and workflows within an enterprise. The PDP is broken down into two logical components: the policy engine and the policy administrator. **It is important to note that a critical component of a ZTA is the separation of the control plane and the data plane**. Enterprise assets can reach the PEP component, but the PEP is the only component that accesses the policy administrator.

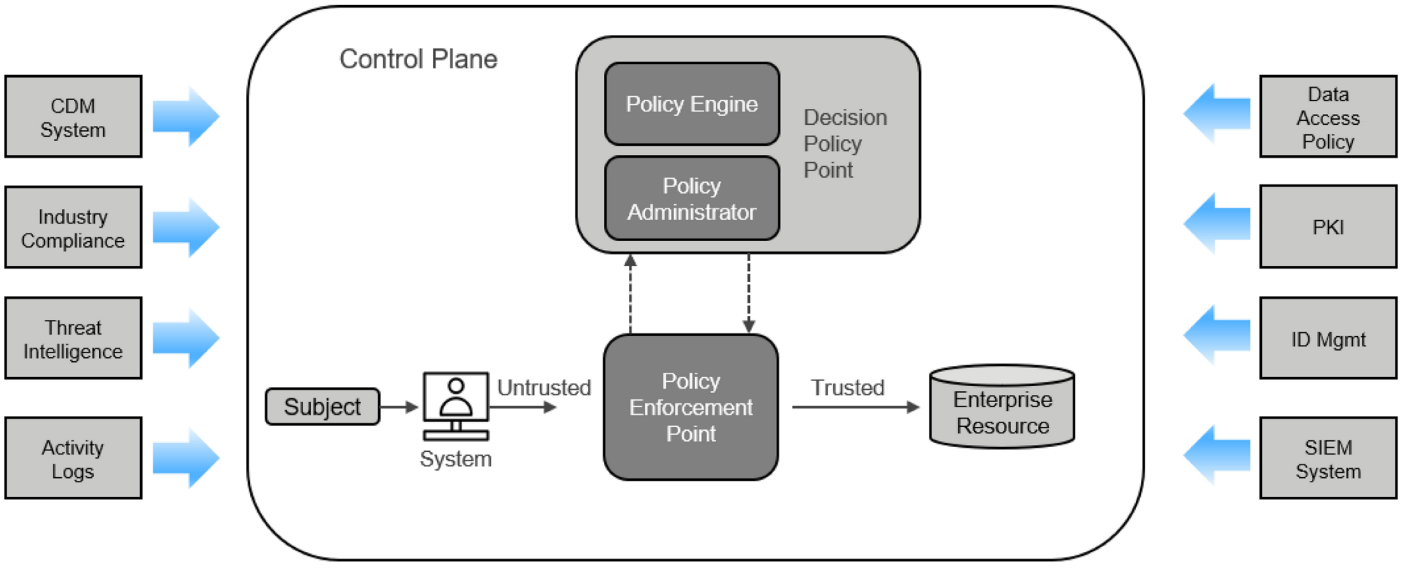

Figure 1: Zero Trust Logical Components NIST SP (Special Publication) 800-207

The Dell Technologies Pillars of Zero Trust

Dell Technologies is following the government architecture model and guidelines from the NIST SP 800-207 Zero Trust and information security model. It consists of five pillars and two cross-cutting capabilities. The goal of this model is to make it easier for cybersecurity leaders to assess their current cybersecurity maturity level. It also provides a way to discuss Dell Technologies solutions and how they fit into the Zero Trust principles and architecture.

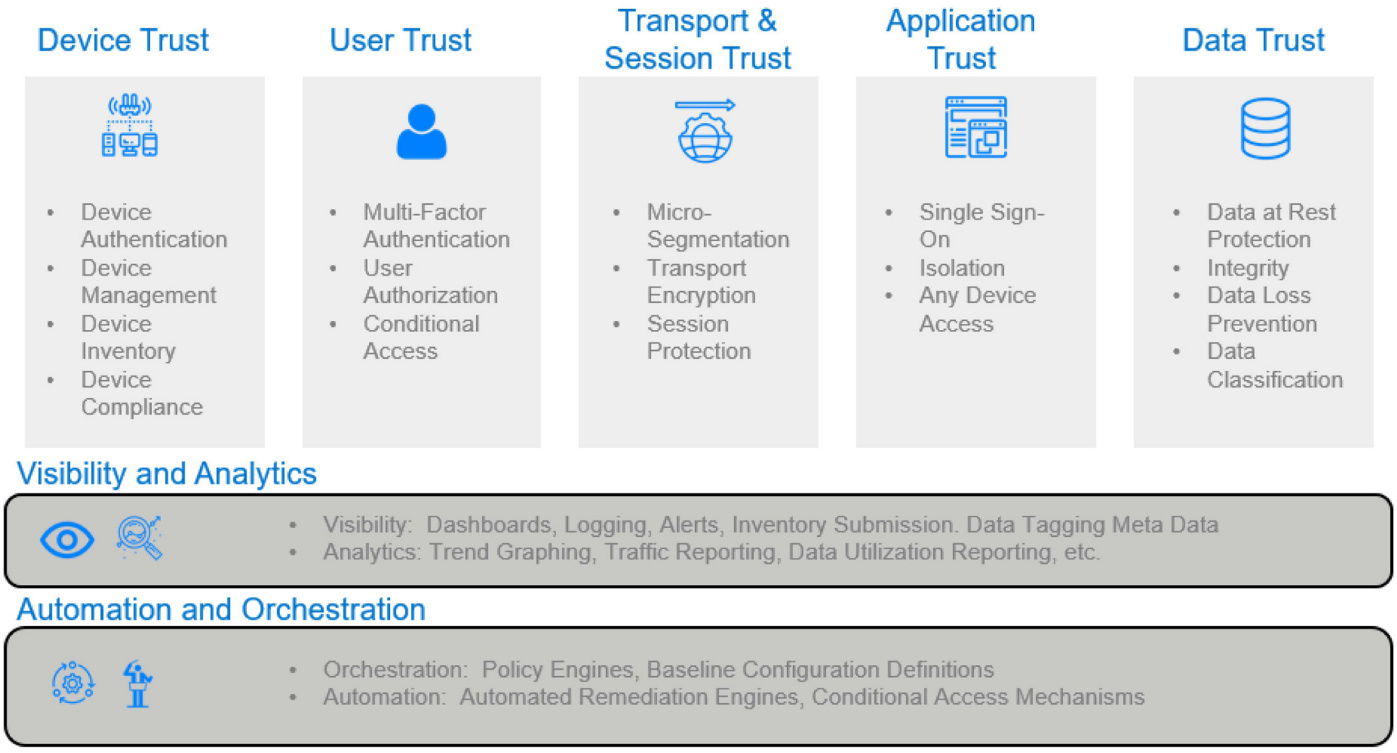

Figure 2: Seven Pillars of Zero Trust

1. Device Trust: Defined as any physical device within an enterprise.
2. User Trust: Defined as a user, administrator, and service level accounts.
3. Transport/Session Trust: Defined as the communication path utilized to move into, across, and out of an enterprise network.
4. Application Trust: Defined as both local and cloud applications that enter, work within, or leave the network for data access.
5. Data Trust: Defined by the organization as key assets used to execute the function and mission of the organization that can be held within the enterprise and extended into cloud services.
6. Visibility and Analytics: Defined by the resources from the 5 pillars that should be enabled, to the fullest extent, to allow for analysis of the secure state and function of the pillar definition.
7. Automation and Orchestration: Defined using the visibility and analytics output to perform policy enforcement, baseline configuration definitions, automated remediation, and conditional access models.

When cybersecurity risk is countered by strong policies, guidance, identity and access management, monitoring and good cyber hygiene, it is possible to reduce overall risk and protect against major threats.

A properly architected Zero Trust infrastructure is far less susceptible to malware in general, and ransomware specifically, for a variety of reasons. Zero Trust provides better protection:

- against Zero Day attacks,
- from runaway processes crossing “authentication boundaries,” due to macro and micro segmentation,
- and from privilege escalation, which is often used for successful ransomware attacks due to Zero Trust’s Privilege Access Management controls and continuous authentication.

Secure backups shouldn’t be excluded from the Zero Trust process. Air-gapped or otherwise, all backups are at risk of insider hacks, which is what a Zero Trust infrastructure is designed to mitigate.

Dell PowerProtect Cyber Recovery Vault

The PowerProtect Cyber Recovery vault provides the last line of defense against cyber-attacks. It offers multiple layers of protection to provide resilience against cyber-attacks, even from an insider threat. It moves critical data away from the attack surface, physically isolating it within a protected part of the data center and requires separate security credentials and multifactor authentication for access. Additional safeguards include an automated operational air gap to provide network isolation and eliminate management interfaces which could be compromised. PowerProtect Cyber Recovery automates the synchronization of data between production systems and the vault creating immutable copies with locked retention policies. If a cyber-attack occurs you can quickly identify a clean copy of data, recover your critical infrastructure and data, and get your business back up and running.

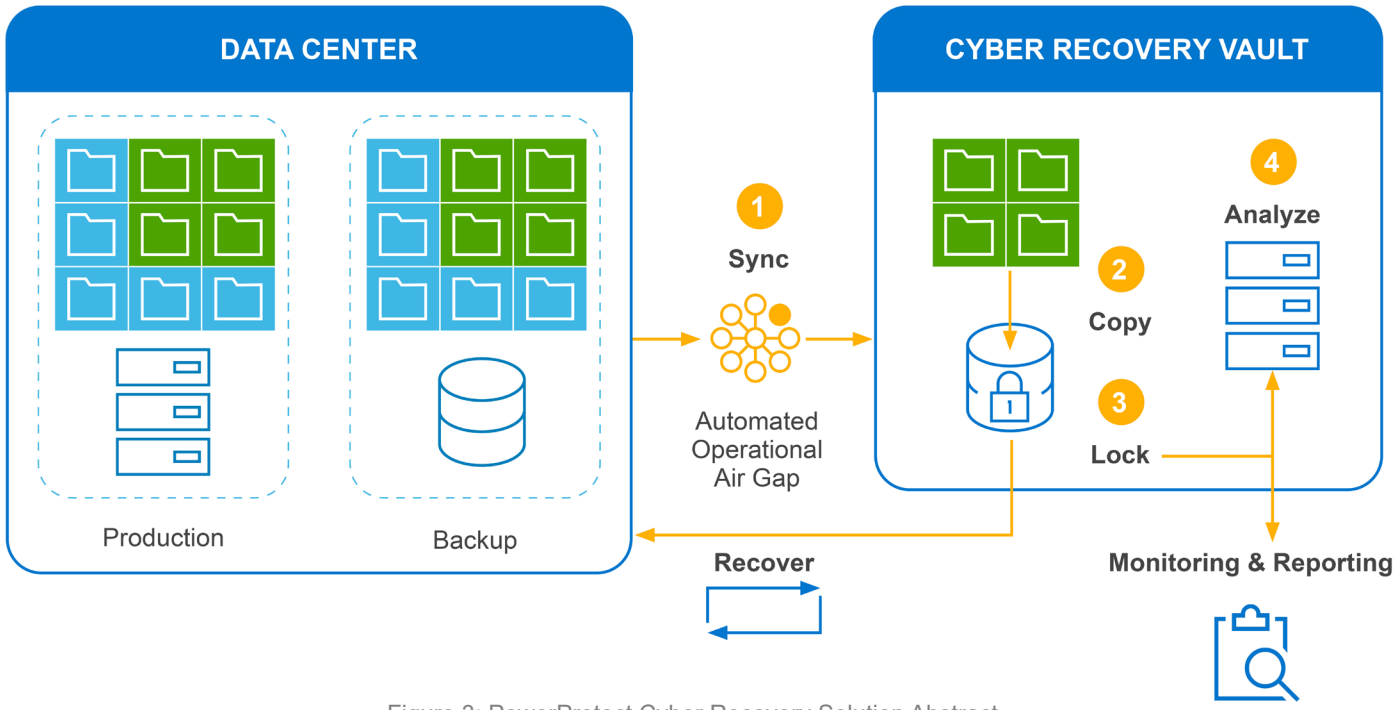

Figure 3: PowerProtect Cyber Recovery Solution Abstract

The vault operates in 4 basic steps:

1. The PowerProtect Cyber Recovery Software and PowerProtect DD devices separate the untrusted zone from the implicit Trust Zone by establishing a policy decision point and a policy enforcement point. Data representing critical applications is synced through the logical air gap, which is unlocked by the management server inside the vault and replicated into the vault target storage. The air gap is then re-established. This makes access control enforcement as granular as possible making the vault invisible to unauthorized resources (human, software, hardware, networking, etc.). The replication plane, control plane and data plane are separated in the vault. At this point Isolation is established.

2. A copy of that data is made. Vault retention is configurable, with most customers keeping copies for 2 weeks and for as long as 1 month. This provides several effective tools in responding to a cyber-attack. Unlike a natural disaster event you must determine the last known good copy of your data prior to recovery or restoration. Being able to roll back to the last known good copy is essential given the average adversarial dwell time.
3. The data is then retention locked to further protect it from accidental or intentional deletion. It is important to understand that immutability does not equal invulnerability. In simple terms, immutable storage alone is best used to prevent data alteration through "normal" means. Therefore, immutability in a production setting adds a layer of defense and should absolutely continue to be used in an overall data protection model. It, however, cannot be viewed as or used as the last line of defense in the event of a catastrophic attack. Immutability must be tied to isolation to ensure that your critical data is safe and available to recover from an attack. Without isolation, immutable storage is not enough, it may be enough to survive a run of the mill, unsophisticated attack but it will certainly not stand up to a targeted and sophisticated attack. Immutability alone offers no protection against system overrides, clock-based attacks, system factory reset, altering or eliminating retention policies, kernel access, firmware corruption, boot lock, snap corruption, or physical access.
4. The data is then presented to our analytics engine, CyberSense performs a full content scan of the data (file metadata, document header and documents content) replicated into the vault. This includes the scanning of unstructured files, databases, and core infrastructure. CyberSense is an important component in enabling speedy recovery after an attack, by determining whether a data set is valid and usable for recovery to a 99.5% confidence in finding corruption.

CyberSense uses the following steps to make this determination; CyberSense analyzes the data in its native backup software format so there is no need for the original backup software in the vault because the analysis is done without rehydrating the backup image. This capability is critically important in defending against sleeperware or zero-day exploits. The vault is essentially a "zero oxygen environment" so any dormant malware will never be able to execute. CyberSense analytics makes over 200 observations per file. Analysis is performed by machine learning algorithms on the analytics to determine if an attack on the data has occurred by looking for indicators of compromise. This process is typically performed after each new replication. This creates observation points which can be compared to previous observations to see how data has changed.

Forensic reporting and analysis tools are available to assist with the investigative process. At this point it is critically important to understand that disaster recovery is very different than cyber recovery. In a cyber recovery scenario confidence in the integrity of the data is paramount. In other words, am I able to recover clean data? Where is my last known clean copy of data? Just as important is quickly determining the "blast" radius of the attack. What was affected? Whose credentials were used. What files were corrupted? What malware/ransomware/attack vector was used? When did the attack begin? The answers to all these questions are quickly determined using CyberSense in the vault.

After the declaration of an event, the incident response team can quickly begin mitigation and remediation measures because CyberSense has already performed the prerequisite identification and detection tasks. Remember that cyber restore and cyber recovery are not the same. A cyber restore does not rebuild a service, it simply restores data to an existing infrastructure. Cyber Recovery includes the rebuilding of a service and all the required components and dependencies invoking the correct people, process and technology.

PowerProtect Cyber Recovery Solution Alignment to the Zero Trust Pillars

Device Trust	User Trust	Transport & Session Trust	Application Trust	Data Trust
• Key Exchange Authentication between source and target datadomains • Data Encryption in Flight • Replication Context only accepted for data synchronization • Vault is not accessible from production or disaster recovery environments • Physical and Logical Isolation of Vault • Vault environment is invisible to production and disaster recovery-based credentials and applications	• Multifactor Authentication • Role Based Access Control • Dual Authentication within the Vault • Least Privilege Access • Conditional Access (physical and logical isolation) • User re-authentication for data destructive commands	• Data in flight encryption • Replication initiated from within the vault- data is pulled into vault • Data Containerization • Uses certificate based mutually authenticated TLS connection • Separation of management plane, replication plane, and data plane. • Data remains in native backup format during transport • Secure protocol access	• Physical and Logical Isolation of Vault • Single Sign On • Invisible to production and disaster recovery environments • Vault environment cannot be pinged	• Data at rest encryption • NTP Security for Vault machine clocks • Advanced Immutability via data isolation and dual authentication requirement • Full content analysis of vault data and trained to identify thousands of variants • Post Attack Forensic Tools • Data Integrity Checks • 99.5% confidence level that the recoverable data is clean and without persistence • Hardened to prevent time drift without NTP

Visibility & Analytics: CyberSense analyzes the backup data without restoring from the backup image and creates statistics that are fed to the machine learning algorithms for early identification of a cyberattack. Once an attack is detected, CyberSense reports on the activity, identifies which files were involved in the attack, and enables rapid recovery of the attacked data. The addition of a machine learning layer analyzes all the collected statistics and makes a yes/no determination of a successful attack. It also identifies the type of attack vector with a greater than 99% recall, with many of the false results being false positives, and can detect invalid logins

Automation & Orchestration: Power Protect Cyber Recovery automates the synchronization of data between production systems and the vault creating immutable copies with locked retention policies. If a cyber attack occurs you can quickly identify a clean copy of data, recover your critical systems and get your business back up and running.

Figure 4: PowerProtect Cyber Recovery Product Feature Mapping

For further reading and expansion of details concerning the Dell PowerProtect Cyber Recovery vault implementations please refer to PowerProtect Cyber Recovery

Learn more about Dell PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

View more Security resources

Join the conversation with #PowerProtect

DELL Technologies