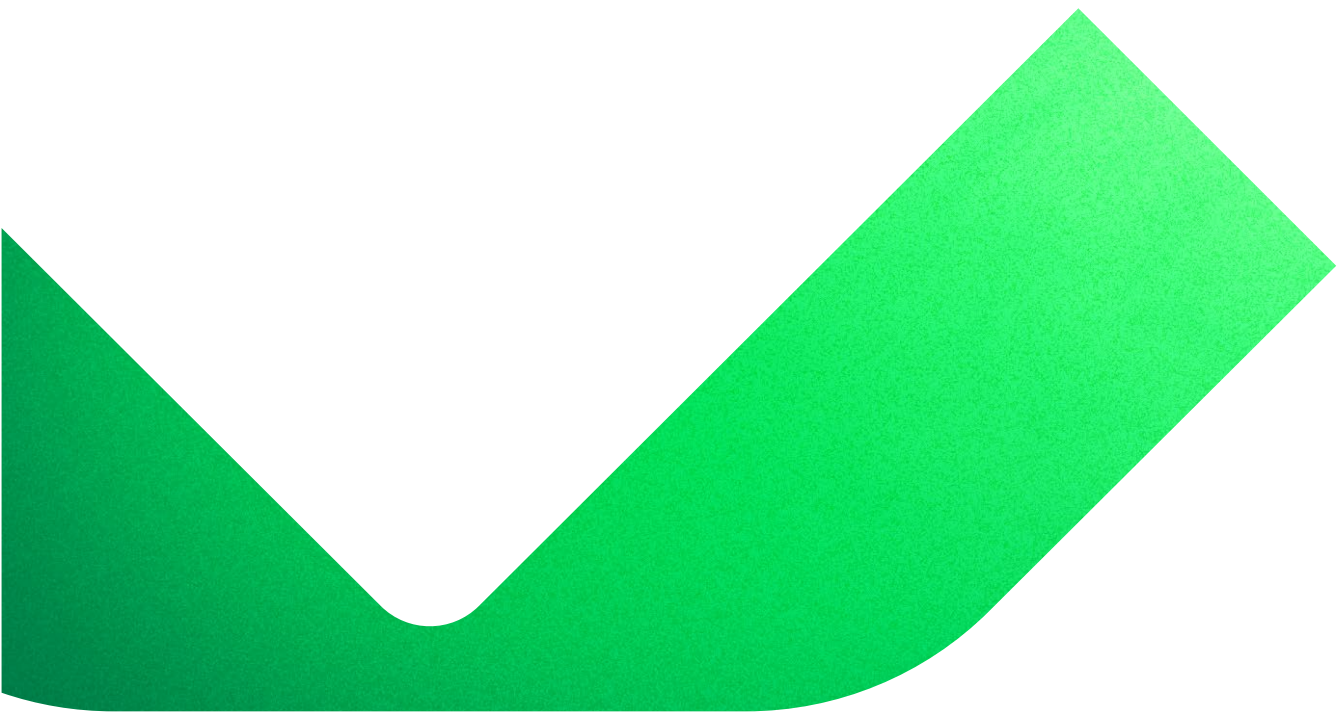
Zero Trust Data Resilience (ZTDR)

Secure Data Backup and Recovery Architecture

A Pragmatic Approach to Implementing Zero Trust



Overview

Organizations of all sizes across all industries understand the importance of Zero Trust in ensuring their data and business is secure. However, the current Zero Trust model has yet to be applied to data backup and recovery in a substantive way. The concept of extending Zero Trust principles to data backup and recovery aligns with the holistic nature of cybersecurity, and protecting sensitive information involves more than just perimeter security.

To address this challenge, Veeam collaborated with Zero Trust expert, Jason Garbis of Numberline Security, on the Zero Trust Data Resilience Framework that is designed to minimize risk, fortify data protection, and revolutionize an organization's security posture. This framework builds on the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM) and extends the main principles of ZTMM to a backup and recovery scenario. The Zero Trust Data Resilience Framework implies that trust is never assumed and security measures are consistently applied throughout the data lifecycle including backup and recovery process; it is a practical model that will help both IT and Security teams significantly reduce risk, enhance data protection, and dramatically improve any organization's security posture.

Want to learn more about Zero Trust Data Resilience?
Download the whitepaper

The Veeam Approach to Zero Trust: Zero Trust Data Resilience (ZTDR)

Zero Trust is foundational to an organization's security strategy and key tenants like segmentation across the most critical data assets, least privileged access, and continuous authentication and authorization with Identity and Access Management (IAM) best practices are particularly relevant when it comes to safeguarding backup environments. By incorporating a Zero Trust Data Resilience function, organizations can address the unique challenges posed by data protection solutions and ensure a comprehensive security strategy for organizations regardless of if they are on-premises, in the cloud, or in hybrid environments.

A critical concept of Zero Trust is to always assume a breach, regardless of the security of a given environment. In the ZTDR methodology a critical technique to combat this risk is via the separation of backup management software and backup storage into separate resilience zones or security domains, isolating the backup data from any threats to backup management software, whether those threats are internal or external. Veeam supports multiple technologies to create resilience zones with highly secure, immutable storage (See Figure 1).

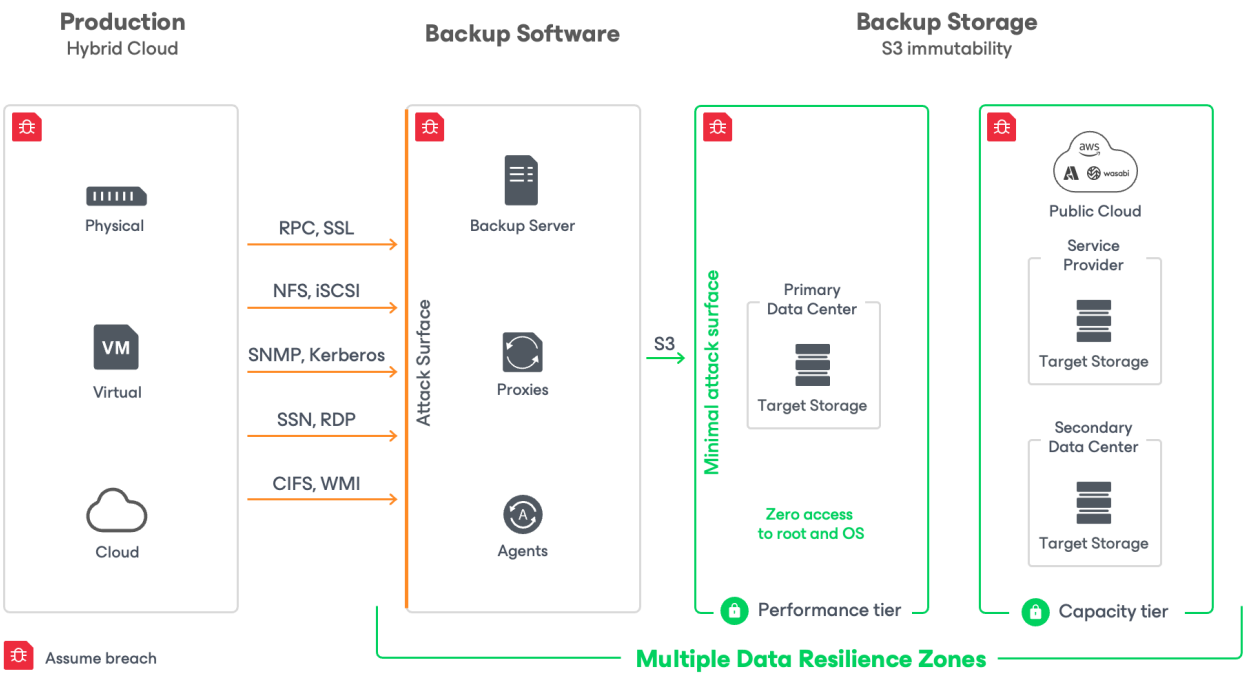


Figure 1

Because data protection solutions have some of the highest levels of read and write access to production data across the organization, and often to the most critical data, it's imperative for an organizations' backup environment to be secure and protected thru Zero Trust best practices.

Zero Trust Data Resilience Principles

Building on CISA Zero Trust Maturity Model (see Figure 2), there are additional considerations an organization should apply specifically to the Data pillar.

CISO Zero Trust Maturity Model

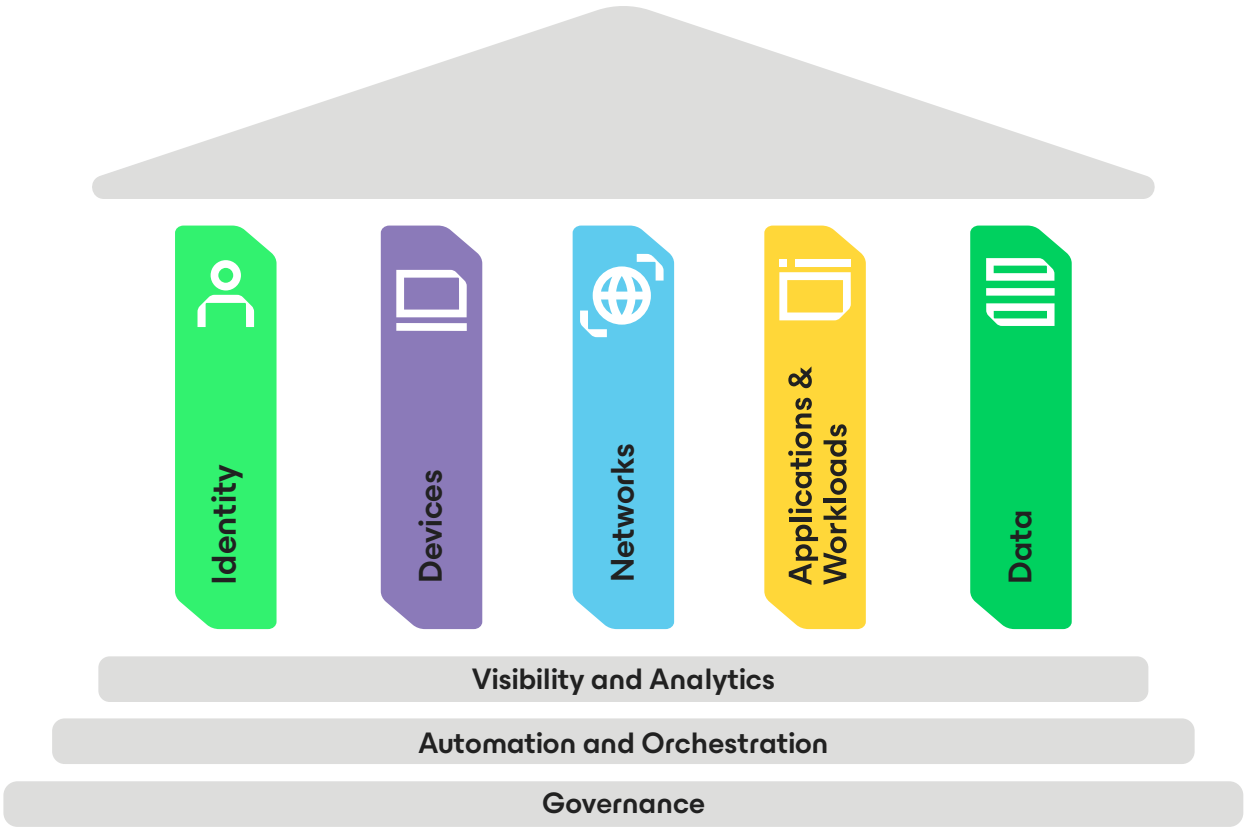


Figure 2

The Zero Trust Data Resilience research paper highlights 5 core principles of Zero Trust Data Resilience (ZTDR) to help organization's overall cyber resilience strategy, ensuring the protection of critical data assets in the face of evolving cyber threats.

Least Privilege Access

This principle emphasizes granting access to a person, process, device, or workload that is essential to perform it's intended function.

Controlled Access for Backup Infrastructure:

- Implementing Zero Trust policies for controlling access to backup infrastructure ensures that only validated users can establish connections to the backup solution. This is a crucial step in preventing unauthorized access and potential data breaches.

Granular Self-Service Roles and Restricted Backup Admin Roles:

- Providing granular self-service roles and restricted backup admin roles within Veeam demonstrates a commitment to the principle of least privilege. This ensures that users have access only to the specific functions necessary for their tasks, reducing the likelihood of inadvertent or intentional misuse.

Identity and Access Management (IAM) Best Practices

- Enforcing IAM best practices, like the use of Multi-Factor Authentication (MFA), adds an extra layer of security to the backup environment. This is a critical measure to prevent unauthorized access, especially given the high levels of privilege associated with backup solutions.

"Four-Eyes" Principle for Critical Operational Decisions:

- Incorporating the "four-eyes" principle for critical operational decisions ensures that key actions require the approval or verification of at least two authorized individuals. This adds an additional layer of oversight and reduces the risk of malicious or erroneous activities.

Immutability

Even with a secure network perimeter, a critical concept of Zero Trust is to assume breach. Immutability of backups is a powerful defense mechanism, as it ensures that an internal or external threat actor cannot modify or delete critical backup data.

Segmentation for Minimizing the Attack Surface and Blast Radius:

- Segmenting backup software and backup storage into separate resilience zones is the key concept of ZTDR. This minimizes the potential impact of internal or external threats by isolating critical components. Ensuring that backup software has no OS/management level permissions on the backup storage adds an extra layer of protection.

Multiple Resilience Zones and 3-2-1-1 Backup Rule:

- Multiple data resilience zones or security domains provide multi-layered security. In addition, the 3-2-1-1 backup rule is a best practice for backup strategy and aligns well with the principles of data resilience. Having at least three copies of data, on two different media types, and with at least one offsite copy and at least one air-gapped or immutable provides multi-layered security, reducing the risk of data loss.

Resilience Zones

A core Zero Trust concept for networking is micro-segmentation to break up security perimeters into smaller zones, thus reducing the attack surface, the blast radius of any compromised zone and the lateral movement of an attacker. For ZTDR, this concept can be applied by using data resilience zones. Resilience zones separate backup storage and isolate the storage control plane from the backup software and its control plane. This provides a critical line of demarcation that ensures backup data survivability even in the event of compromised backup software. This can happen for a multitude of reasons, including internal threat actors. A backup system must ensure that backup data can be simply and quickly recovered from a clean install of the backup software.

Production infrastructure

Veeam infrastructure

Autonomous backup data

Immutable | Encrypted | 3-2-1-1-0

Data Integrity and Enhanced Security:

- Configuring a compatible backup repository and setting a retention period for immutable backups is a proactive measure to ensure data integrity and enhanced security. Immutable backups act as a safeguard against ransomware attacks and other forms of data manipulation.

System Resilience

A holistic approach to IT Security encompasses resilience across the entire ecosystem, including platforms, tools, technology, and processes. Veeam's diverse resilience options demonstrate a commitment to providing organizations with tools to withstand various types of disruptions, including a full system loss.

Time Shift Detection for Immutable Backups:

- The implementation of time shift detection is a proactive measure to prevent the deletion of immutable backups, even in the face of compromised NTP (Network Time Protocol). This feature enhances the security and reliability of backup repositories, ensuring the integrity of critical backup data.

Flexible Recovery Options:

- Veeam enables flexible recovery options, even to dissimilar environments, and supports physical and virtual deployments, as well as hybrid environments, to align with the diverse IT infrastructures that organizations may operate. This flexibility enables organizations to fast recovery: for example on-premises VMware to AWS or Azure, or AWS to Azure incase the original environment is not available.

Granular Data Restoration Options:

- The flexibility in restoring data to different environments and at different granularities enhances overall data resilience. This adaptability allows organizations to tailor their recovery processes based on the specific needs of different scenarios.

Proactive Validation

Constant validation of functional aspects and processes is key to ensuring that data remains protected and that any anomalies are detected and addressed promptly.

Continuous Monitoring and validation:

- The emphasis on monitoring systems 365/24/7 reflects the understanding that cybersecurity threats can emerge at any time. By having real-time insights into the state of the environment, administrators can detect any anomalies early on and allows organizations to investigate and respond before a potential cyberattack or data loss occurs.

- Leveraging tools like Veeam ONE for monitoring is a proactive approach to maintaining the health and security of backup and recovery environments. Veeam ONE's ability to monitor various parameters, including CPU usage, datastore write rate, network transmit rate, and incremental backup size, provides organizations with valuable insights into potential issues.

End-to-End Visibility:

- The concept of end-to-end visibility across the data protection infrastructure is essential. It ensures that organizations have a comprehensive understanding of the health and status of their backup and recovery systems, enabling them to make informed decisions and take swift action when needed.
- As a part of Veeam's recent 12.1 release, Veeam's new Threat Center aggregates insights from the entire platform and infrastructure, combining this into a single pane of glass highlighting threats, identifying risks, and providing organizations with a simple and powerful security scorecard for their entire data protection environment.

Operational Simplicity

The importance of operational simplicity during disasters or cybersecurity events is a recognition of the critical role that simplicity plays in effective recovery. The longer the downtime, the greater the impact on an organization's operations and bottom line.

Average Downtime in Ransomware Attacks:

- As reported in Veeam's 2023 Ransomware Trends Report, the average downtime from a ransomware attack is three weeks. This underscores the urgency and significance of rapid recovery especially critical during high-pressure situations where every moment counts.

Balancing Tools, People, and Processes:

- Striking the right balance between tools, people, and processes is a key challenge, particularly when organizations are dealing with a disaster or cyberattack. Operational simplicity involves streamlining workflows, optimizing processes, and ensuring that the right tools are in place for efficient recovery.

Investment in Simplifying Restore Capabilities:

- Industry leaders like Veeam, proactively invest in providing restore capabilities by addressing the complexities of recovery. The ability to restore data from one platform to another and leverage tools like Veeam's Recovery Orchestrator showcases a dedication to simplifying complex restore scenarios and keeps failover plans updated, automated, and fully tested, ensuring readiness during high-pressure scenarios.

Learn about the latest security capabilities in Version 12.1

Conclusion

As our digital landscape evolves and expands, so do cyberattacks and threat actor capabilities. As a result, we have a pressing need to unify and strengthen IT and security collaboration and effectiveness to better protect and defend our organizations' data, devices, and people. This journey toward maturity won't happen overnight, but it is imperative that this starts to happen sooner rather than later. The first step is Zero Trust. CISA's Zero Trust Maturity Model (ZTMM) provides core principles that are critical to securing and protecting an organization but does not cover everything. The introduction of Zero Trust Data Resilience (ZTDR) as an extension of CISA's Zero Trust Maturity Model (ZTMM) is a strategic and forward-thinking approach to addressing the evolving landscape of cyber threats.

The incorporation of ZTDR principles, including least privileged access, immutability, system resilience, proactive validation, and operational simplicity, showcases a comprehensive strategy for securing and protecting organizational data. By embracing ZTDR, organizations will have a clear and concrete pathway to strengthening their security posture. This means more efficient operations and alignment between IT and security teams that will ultimately lead to a faster and safer recovery.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data freedom, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 74% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.