OBJECT FIRST

White Paper

Zero Trust and Enterprise Data Backup

Extending Zero Trust to Data Resilience

Cyberattacks and Ransomware Target Backup Data in

93%

of Attacks.

Backup data is often the primary target of ransomware and data exfiltration attacks, but existing Zero Trust frameworks do not include the security of data backup and recovery systems.

Source

Zero Trust and Data Backup and Recovery

The Zero Trust model represents the current best practice for organizations seeking to protect and secure their data and business. However, this model has not been substantively applied to data backup and recovery. Zero Trust advisory firm Numberline Security and Veeam recently collaborated on research to fill this gap and reduce risk for organizations seeking to evolve beyond perimeter security. Their research resulted in the new model - Zero Trust Data Resilience (ZTDR).

Zero Trust Data Resilience builds on the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM) as a foundation, extending its principles to enterprise data backup and recovery.

The Zero Trust Data Resilience framework is a practical guide for IT and Security teams to improve data protection, reduce security risk, and enhance an organization's cyber resilience.

The original research: "Zero Trust Data Resilience — A Secure Data Backup and Recovery Model" is available at:
https://go.veeam.com/zero-trust-data-resilience

Zero Trust Principles

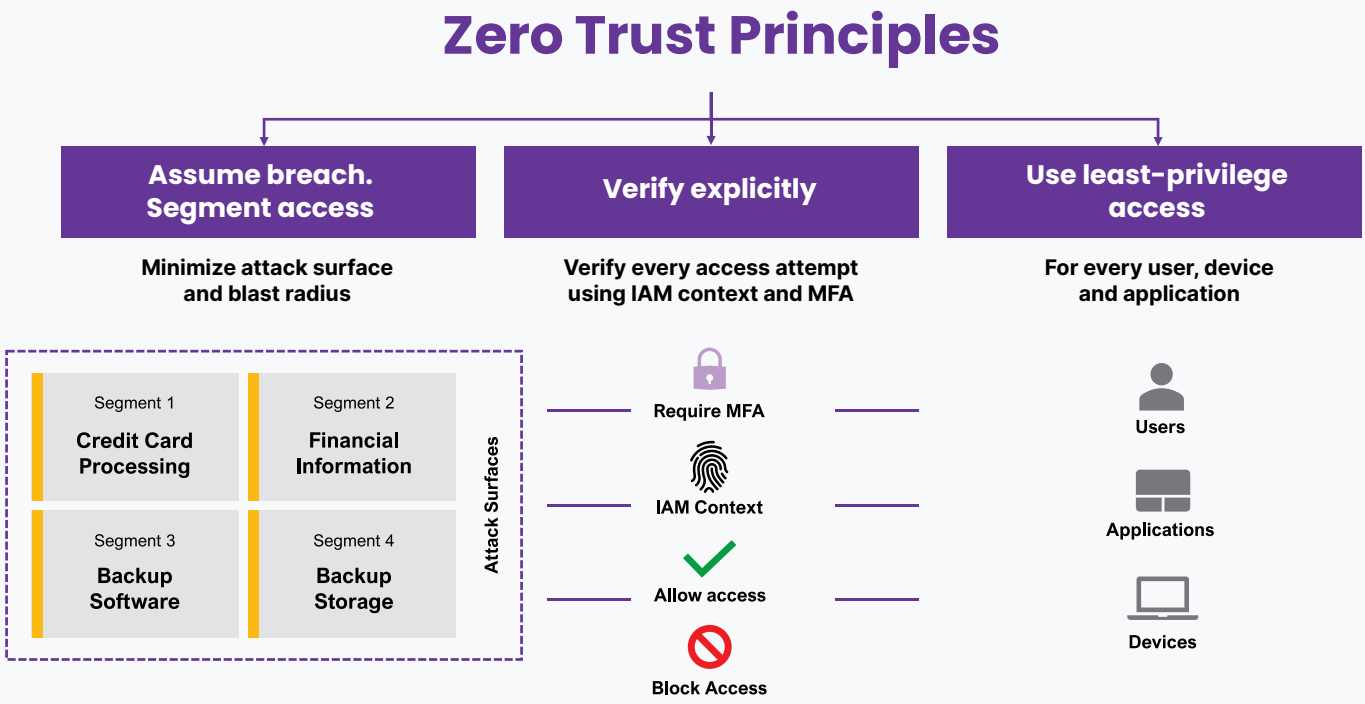
Zero Trust is a security paradigm replacing the more traditional and increasingly ineffective perimeter-based security approach. Zero Trust is being adopted as the best-in-class IT security standard by the US government and enterprises worldwide.

Zero Trust is universally applicable to organizations that operate on-premises, in the cloud and hybrid environments, as well as to enterprises of different sizes and across industries.

The primary principles of Zero Trust include:

- **Assume a breach. Segment access** to the most critical data assets to minimize the attack surface and blast radius for each segment.
- **Verify explicitly.** Always authenticate and authorize by leveraging Identity and Access Management (IAM) context (location, time, etc.) and strong MFA-based authentication.
- **Use least-privilege access** for every user, device, and application.

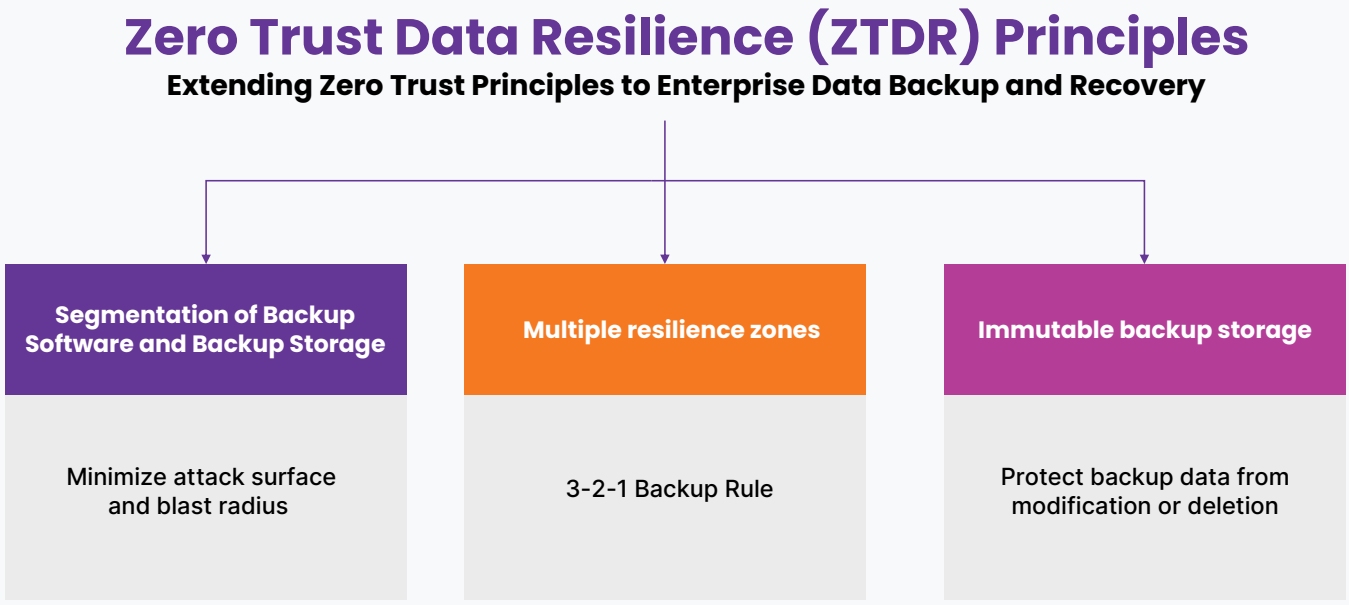
In addition, Zero Trust mandates continuous security visibility and analytics, automation and orchestration, and governance for data lifecycle management.



Zero Trust Data Resilience (ZTDR) Principles

Zero Trust Data Resilience research introduces the following ZTDR principles extending Zero Trust to Enterprise Data Backup and Recovery:

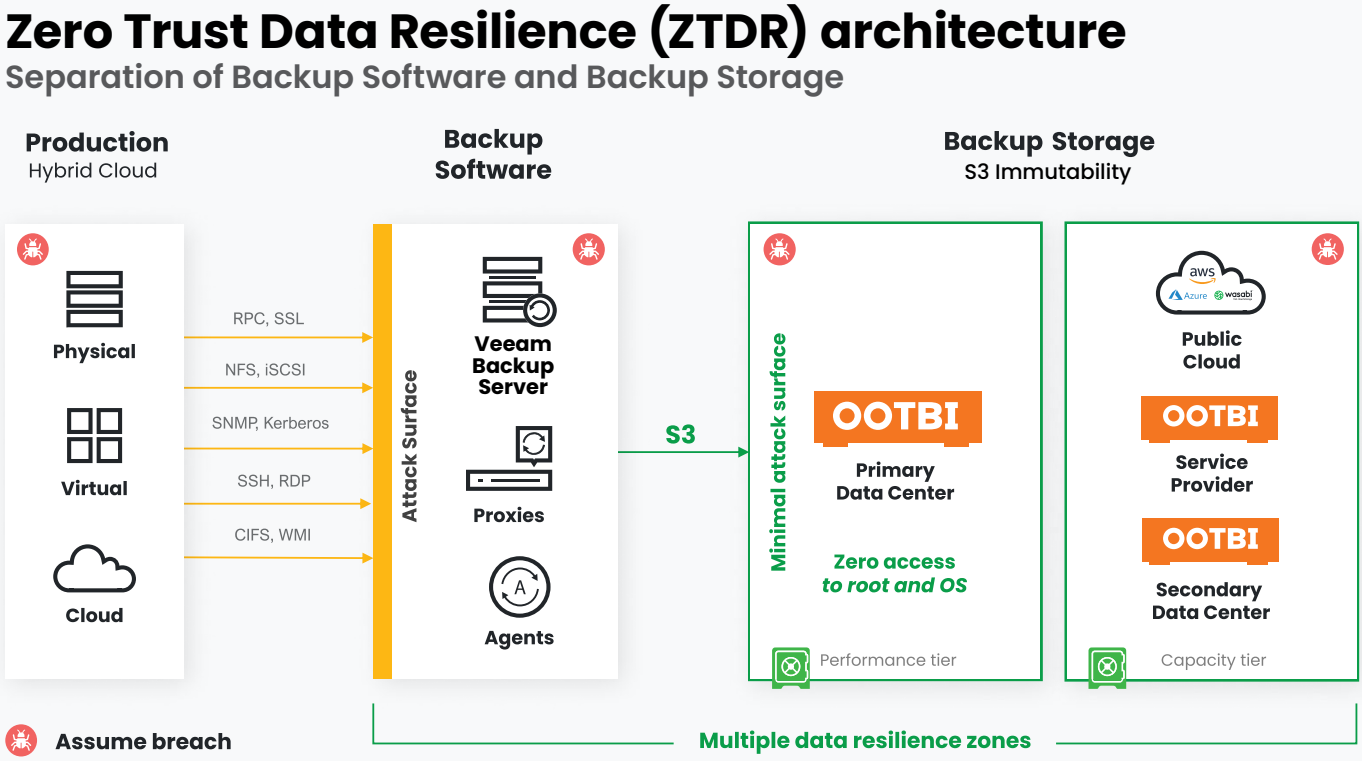
- **Segmentation — Separation of Backup Software and Backup Storage** to enforce least-privilege access, as well as to minimize the attack surface and blast radius.
- **Multiple data resilience zones or security domains** to comply with **3-2-1 Backup Rule** and to ensure multi-layered security.
- **Immutable backup storage** to protect backup data from modifications and deletions. **Zero access to root and OS,** protecting against external attackers and compromised administrators is a must-have as part of **true immutability.**



Separation of Backup Software and Backup Storage

Backup infrastructure inherently has a large attack surface, requiring read and write access to production systems across all enterprise applications and data sources for both on-premises and hybrid cloud environments. To mitigate this risk, Zero Trust Data Resilience requires that backup infrastructure is segmented into multiple resilience zones or security domains — such as Backup Software, Primary Backup Storage, and Secondary Backup Storage — each with its least-privileged access, reduced attack surface and minimal blast radius. In this case, the Backup Software may still have an exposed attack surface, but the Backup Storage will have a minimal attack surface. This is achieved by using Zero Trust access control and a secure communication protocol such as S3 over HTTPS to minimize the risk of penetration to the Backup Storage component (See Figure 1).

Figure 1



Multiple Data Resilience Zones

A core Zero Trust concept for networking is microsegmentation to break up security perimeters into smaller zones, to enforce least-privilege access, as well as reduce 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 bad actors. A backup system must ensure that backup data can be simply and quickly recovered from a clean install of the backup software. Multiple data resilience zones ensure the efficacy of the multi- layered security strategy and your compliance with the 3-2-1 Backup Rule.

3-2-1 Backup Rule

3

At least three (3) copies of data including production data.

2

At least two (2) copies of backup data on immutable storage in separate resilience zones.

1

At least one (1) copy off-site.

Immutable Backup Storage

According to ZTDR, backed up data must also be immutable so that even in the event of a ransomware attack, backed up data cannot be modified or deleted. Data resilience can be maximized by providing customers with a hardened, immutable storage target set to compliance mode with **zero access to the operating system or root account.** This storage can include vendor-specific solutions and protocols or industry-standard protocols like S3.

S3-native Immutability and Security

S3 provides the most trusted industry-standard storage immutability, security, IAM and secure communication protocol.

Open Design and Architecture

Open Design and Architecture is one of the fundamental principles of IT security in general. Using industry-standard S3 protocol as opposed to a proprietary protocol aligns best with this principle.

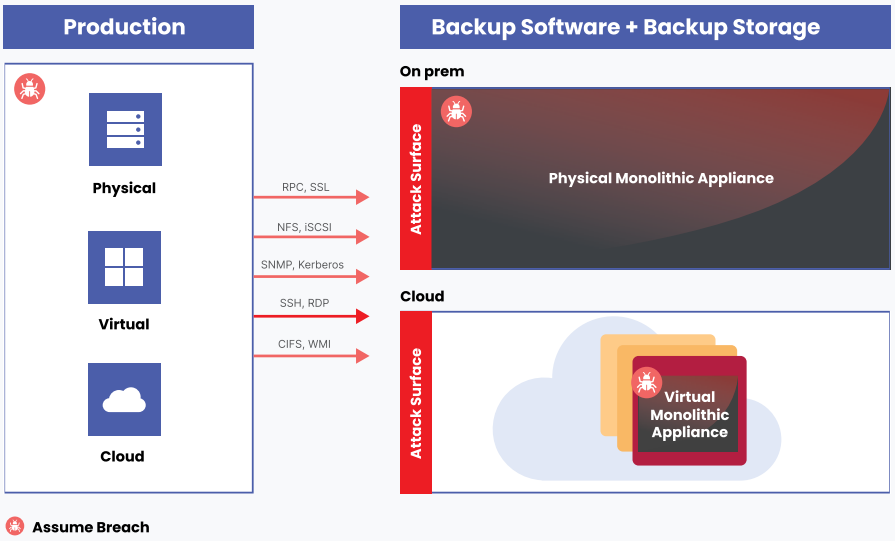
A well-architected enterprise data backup and recovery system will include segmentation between the Backup Management Software and Backup Storage layers. This segmentation is critical to maintain the resilience, immutability, and flexibility enterprises need. This reduces the attack surface and ensures multi-layered security, dramatically reducing the data breach risk.

Monolithic Appliance: Not Zero Trust

An alternative architecture such as Monolithic Appliance does not meet the requirements of Zero Trust Data Resilience as there is no separation of Backup Software and Backup Storage. This architecture does not provide true immutability because, upon breach, an attacker will have full access to the Backup Software and Storage. The attacker may now be able to modify, delete, or render backup data inaccessible. In other words, the blast radius of an attack would include the full backup and recovery system (see Figure 2). Also, this approach places a large amount of trust in the vendor's proprietary file system immutability.

Figure 2

Monolithic Appliance. On-premises and in the Cloud. Not Zero Trust



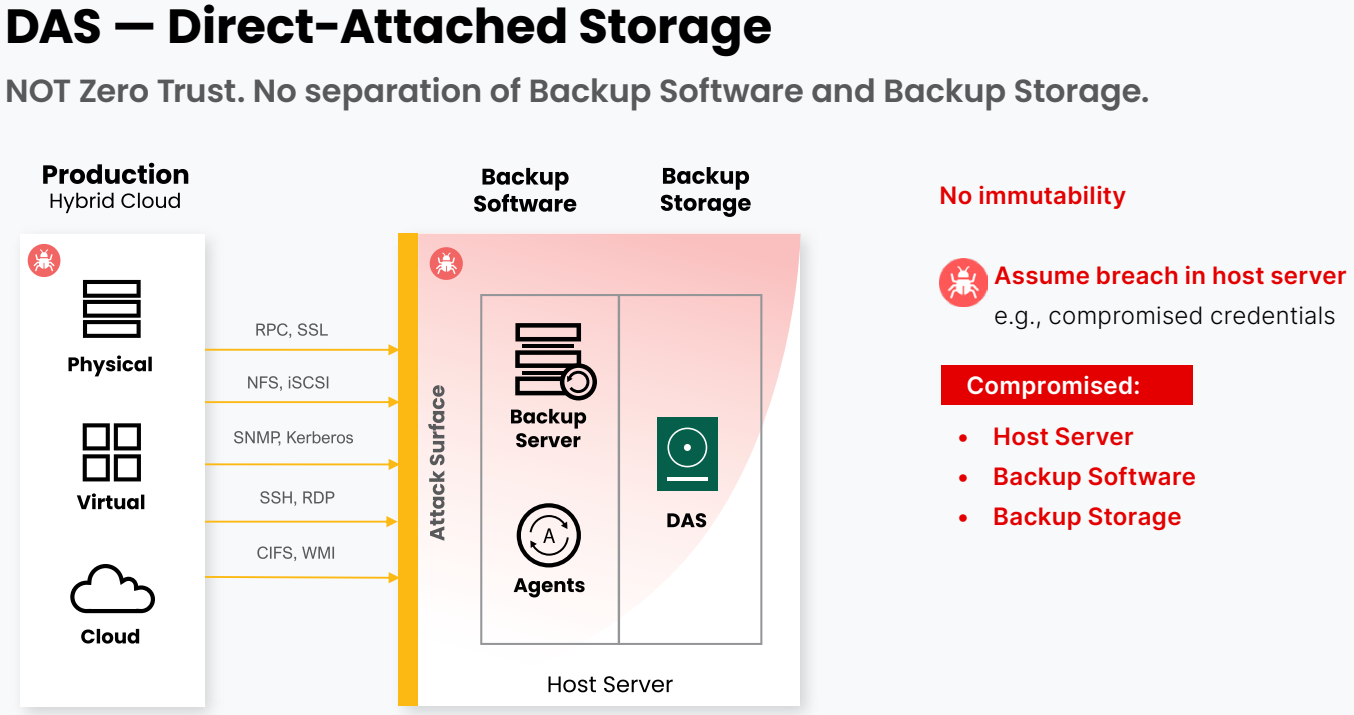
- **Assume breach** in physical appliance or Cloud instance
- **No true immutability** in case of a breach
- **No separation** of Backup Software and Backup Storage
- **Blast radius takes the full appliance**

In addition, it's important to recognize that deploying a monolithic virtual appliance into a cloud instance falls short of ensuring true immutability in a hybrid cloud scenario. In the event of a breach, where OS, instance, or account-level credentials are compromised, the entire virtual appliance becomes susceptible, expanding the blast radius. The security vulnerability stems from performing data backup into the proprietary storage housed within the cloud-based virtual appliance. This weakness — caused by architectural misalignment with ZTDR — could be solved by backing up data directly into immutable cloud object storage external to the instance.

Direct-Attached Storage (DAS): Not Zero Trust

Direct-Attached Storage (DAS) does not offer immutability, and is attached directly to the Veeam Backup & Replication server with no separation of Backup Software and Backup Storage. An attacker who gains access to the host by exploiting an OS or application vulnerability can access all data on that system (see Figure 3).

Figure 3



Conclusion

As cyber threats escalate, it's evident that relying solely on traditional security measures is no longer sufficient. Embracing the Zero Trust approach becomes crucial for enhancing cyber resilience. While organizations are increasingly adopting the principles of Zero Trust to bolster data protection and mitigate downtime, the conventional Zero Trust Maturity Model (ZTMM) falls short in offering specific guidance for enterprise data backup and recovery.

Zero Trust Data Resilience (ZTDR) is a new model that extends the principles of Zero Trust to the backup and recovery use case. The foundational principles of ZTDR are segmentation of Backup Software and Backup Storage, multiple data resilience zones to comply with the 3-2-1 Backup Rule, and immutable backup storage to protect data from modifications and deletions. Object First aligns with these best practices to deliver optimal storage solutions to achieve true Zero Trust Data Resilience.

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, ultimately leading to a faster and safer recovery.

Best Storage for Veeam