A PRACTICAL GUIDE
FOR IT & SECURITY PROFESSIONALS

Extending Zero Trust to Data Backup and Recovery

Executive Summary

Zero Trust is a modern and highly effective strategy for better securing our enterprise IT infrastructure against ransomware and other threats. Data backup and recovery systems are critical to our enterprises, and must be included in any Zero Trust initiative.

However, Zero Trust can be complicated to architect and implement, and until now, there has been no consensus on how to best apply it to data backup and recovery systems.

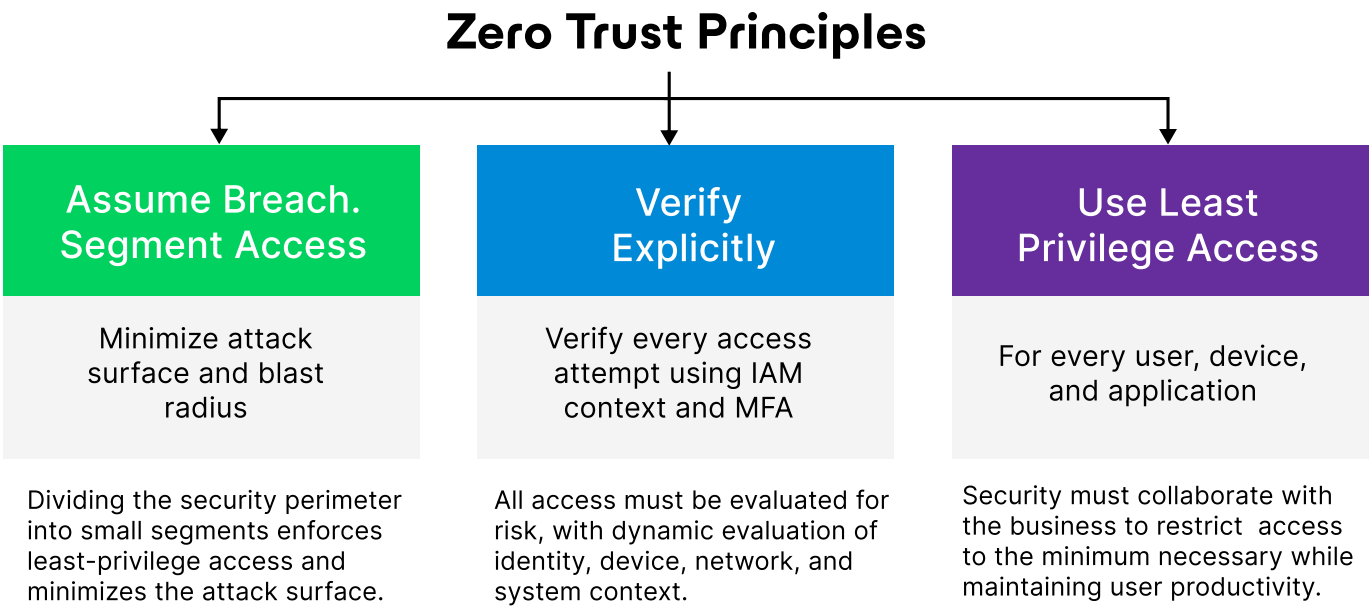
Zero Trust Data Resilience (ZTDR) – a new model introduced by Veeam and Numberline Security – builds on the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model. ZTDR extends the principles of Zero Trust to backup and recovery, ensuring enterprises can reduce risk and meet their security and resilience goals.

By following the Zero Trust Data Resilience approach explained in this guide, you'll learn what to look for in a data backup and recovery platform and architecture, and be able to get started quickly and effectively in your environment.

Zero Trust: A Brief Introduction

Zero Trust is a modern security strategy based on the idea that no user, device, or network packet should be implicitly trusted. To ensure data security, access to critical data assets should be segmented and all communications must be authenticated, evaluated, and authorized before any access is granted. This must be applied to each segment and its data, applications, assets, or services.

This is a significant shift from traditional information security architectures, which were based on static, network-based perimeters — and which have clearly failed to keep our enterprises safe from ransomware and malicious actors.



Introducing Zero Trust Data Resilience (ZTDR)

Data backup and recovery systems are critical elements of enterprise IT, as well as frequent targets for attack. They must be properly and holistically secured.

By following ZTDR principles, and choosing backup and storage vendors based on ZTDR guidance, your enterprise will obtain stronger defenses, more efficient operations, and faster and more reliable recovery.

ZTDR Extends Core Zero Trust Principles

Separation of Backup Software and Backup Storage	Multiple Resilience Zones	Immutable Backup Storage
Minimize attack surface and blast radius	3-2-1 Backup Rule	Protect backup data from modification or deletion
SOLUTION REQUIREMENTS		
Look for data backup and recovery solutions that are architected with separation between backup software and storage, and which ideally prevent root or OS access to backup storage. These capabilities will allow you to strictly enforce access controls via Zero Trust policies.	Look for data backup and recovery solutions that support multiple resilience zones, meaning that your organization can survive the loss or compromise of any single backup system or storage environment. This will enable you to easily meet 3-2-1 backup guidelines.	Look for data backup and recovery solutions that easily and efficiently support robust and reliable immutable backup storage. This will give you full confidence that your backed up data is protected from deletion or modification, even in the presence of a malicious actor.

The 3-2-1 Rule for Backup Best Practices:

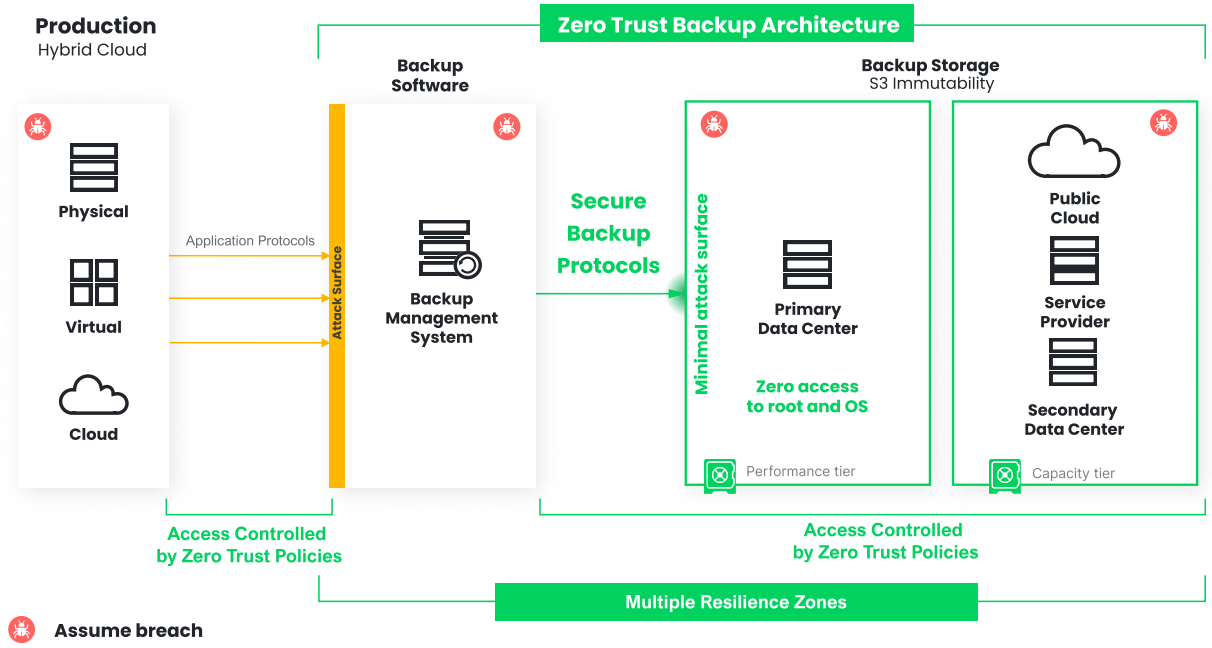
3 3 copies of data, including production data.

2 2 copies of backup data on immutable storage in separate resilience zones.

1 1 copy off-site.

ZTDR Reference Architecture

This ZTDR Reference Architecture shows you how a Zero Trust platform should be deployed in conjunction with your backup management and storage systems.



Getting Started with ZTDR

While Zero Trust is a journey, there are immediate and impactful steps you can take to improve the security resilience of your data backup and recovery infrastructure

This Week:

Explore how well your backup and recovery systems meet ZTDR requirements

Task	Questions to Ask
Talk to your network and IT infrastructure teams about your network segmentation	• How is our network segmented? • Is backup software and backup storage segmented into separate security zones? • How is access to and from each segment of backup infrastructure controlled?
Evaluate whether your backup data storage is organized into multiple resilience zones	• Are we following industry guidance around 3-2-1? • What happens to our backup and recovery processes if one of our backup zones is unavailable? • What happens to our backup and recovery processes if two of our backup zones are unavailable?

Task	Questions to Ask
Determine whether your backup storage systems are properly immutable	• How does your storage vendor document and guarantee immutability? • Can a malicious admin change immutability or retention settings using root or OS access to storage? • What happens if system time is maliciously advanced?
Validate Your Recovery Processes	• What is our DR Response Plan? When did we last test it? • How many people from the IT or storage team can successfully recover a system by following the documented steps? • What happens if (important person X) is unavailable during an incident?

Next Week:

Validate your processes and tools, and then plan and build consensus for short and medium term changes to your backup and recovery infrastructure and processes

Task	Questions to Ask
Evaluate your confidence, and the repeatability of your recovery processes by performing regular (weekly / monthly) tests	• How often do we do our recovery tests? • What did we learn about documentation or process gaps? • When can we remediate these?
Begin planning for network configuration, segmentation, or firewall rule changes	• Who on the IT or Security team can I collaborate with to scope out potential changes? • Who in the security team is leading our Zero Trust initiative, and how can I support it? • What network segmentation or infrastructure changes do we have in progress?
Plan for any storage configuration changes or new vendor evaluations, in order to close any immutability gaps	• What is our process for evaluating and procuring additional backup storage? • What sort of financial, efficiency, or risk justification would we need to make? • How should I go about getting approval to initiate a vendor evaluation process?
Assign responsible owners for any process and documentation improvements	• Who would be involved in approving and implementing changes to (process X)? • How can we set a mutually agreeable deadline for implementation?

Next Month:

Begin implementing short-term changes, and begin to identify any needed longer-term changes

Task	Questions to Ask
Deploy your improved disaster recovery processes, and test again	• How much did our DR processes improve? • Did we address all the process and documentation gaps?
Validate and iterate on network segmentation	• What areas of the network still grant broad network access to and from our backup systems? • How can we tighten this up to improve our resilience against ransomware?
Execute on storage capacity, locations, and immutability improvements	• How comfortable are we with our backup storage capacity? • How confident are we that our backup storage systems are immutable? • How well are we following the 3-2-1 best practices guidance? • How are we utilizing multiple resilience zones?

What Else Should You Look For?

In addition to the three core ZTDR principles, there are two other requirements you should be looking for when you're evaluating a data backup and recovery vendor solution.

Proactive Disaster Recovery Validation

Incidents which require recovery of backed-up data are going to occur at unexpected times, and likely under high-stress circumstances. It's important that your organization has well-understood, well-documented, and well-rehearsed Disaster Recovery plans and processes. Also ensure that you have a high degree of confidence in the integrity and validity of the backed-up data.

Operational Simplicity

Make sure that you select a system that's simple enough for your organization to easily and confidently operate, while still providing enough capability, scalability, and sophistication to fully meet your enterprise's needs. Work to clearly understand your staff's capacity and skills, so that operations aren't dependent on any single individual or "superhero."

Frequently Asked Questions

Is Zero Trust something you can buy from a vendor?

No - Zero Trust is something you **do** - it's a security strategy, which changes and improves IT, security, and business outcomes.

Is Zero Trust just about restricting access, and reducing user productivity?

No – Zero trust is about eliminating all **unnecessary** access, while keeping users productive. Many enterprises actually **improve** user productivity and user experience with Zero Trust.

Why does zero trust matter?

Zero Trust is the most effective way to defend our enterprises against risks like ransomware, malicious actors and other risks. Given the current threat landscape, we have a responsibility to utilize it.

Can you use your current security infrastructure for Zero Trust?

Most likely, yes! When used properly, modern firewall, identity, and infrastructure systems can support you as you begin your Zero Trust journey. Achieving optimal levels of Zero Trust maturity may require additional investments, which can be guided by tools like the ZTDR reference architecture.

ADDITIONAL RESOURCES

Want to find out more about Zero Trust and ZTDR?

Visit the Veeam website to read the full ZTDR research and to see Veeam's approach to data security, and cyber resilience.

To read the full ZTDR research whitepaper and to get Numberline Security's perspective on this, visit the Numberline website.