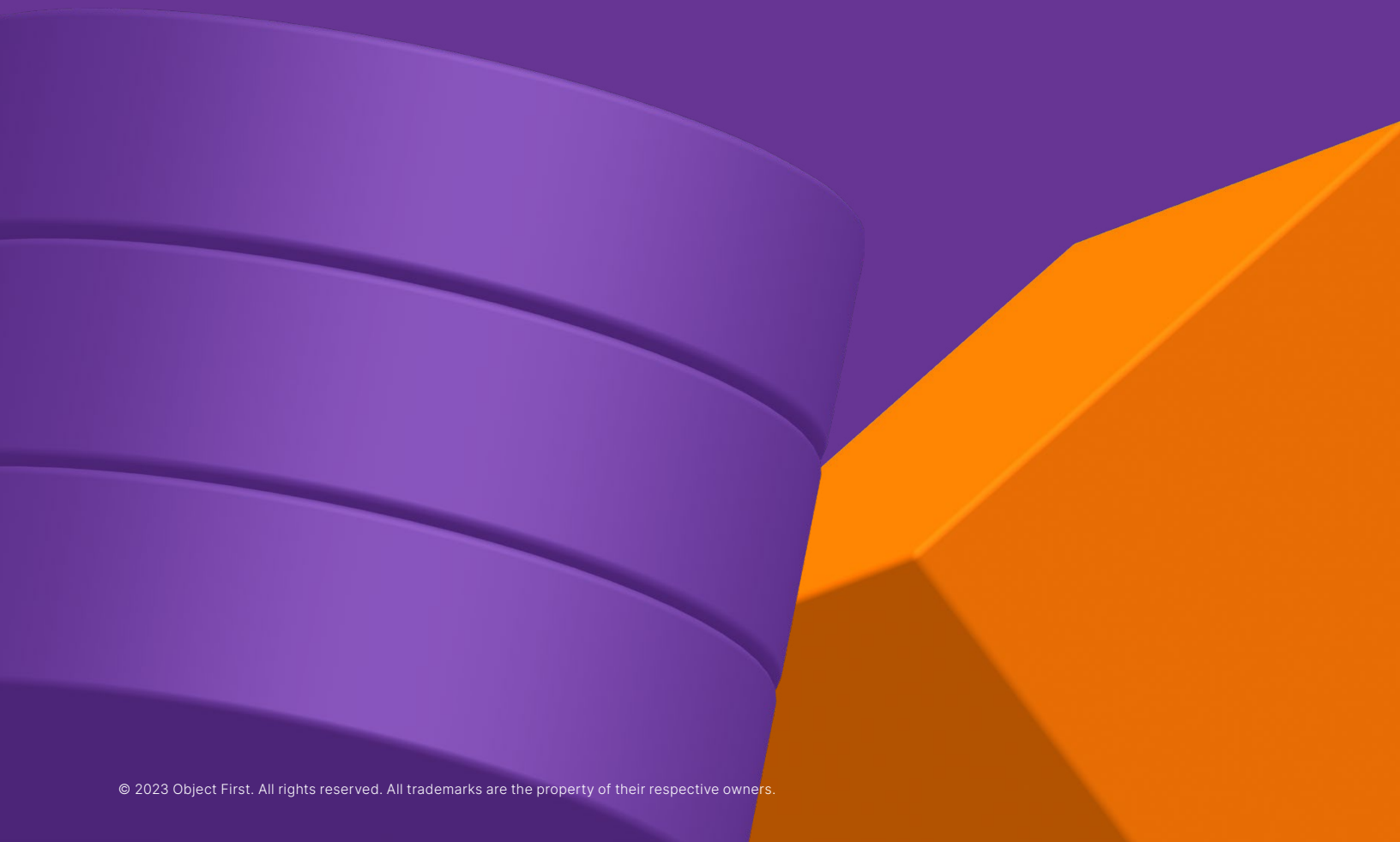
OBJECT FIRST

White Paper

Zero Trust and Secure Backup Storage

Implementing Zero Trust Data Resilience (ZTDR) for Secure Backup Data Storage



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 Data Resilience (ZTDR) Principles

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.

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 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 Zero Trust Data Resilience research highlights 5 core principles of Zero Trust Data Resilience (ZTDR):

- **Least Privilege Access.** Controlled and limited access to backup infrastructure including backup storage using IAM best practices and strong MFA.
- **Immutability** to ensure backup data cannot be modified or deleted. Segmentation of backup software and backup storage to minimize the attack surface and blast radius.
- **System Resilience.** Backup infrastructure including backup software and backup storage must be resilient to failure and attack.
- **Proactive Validation** with orchestrated recovery testing as well as end-to-end visibility and integrated threat detection using advanced AI/ML-based analysis, anti-virus and YARA scanning.
- **Operational Simplicity** reducing an average downtime from a cybersecurity event by keeping recovery plans updated, automated, and fully tested.

The original research and Veeam's white paper: "Zero Trust Data Resilience — A Pragmatic Approach to Implementing Zero Trust" is available at: https://go.veeam.com/zero-trust-data-resilience

Zero Trust Principles

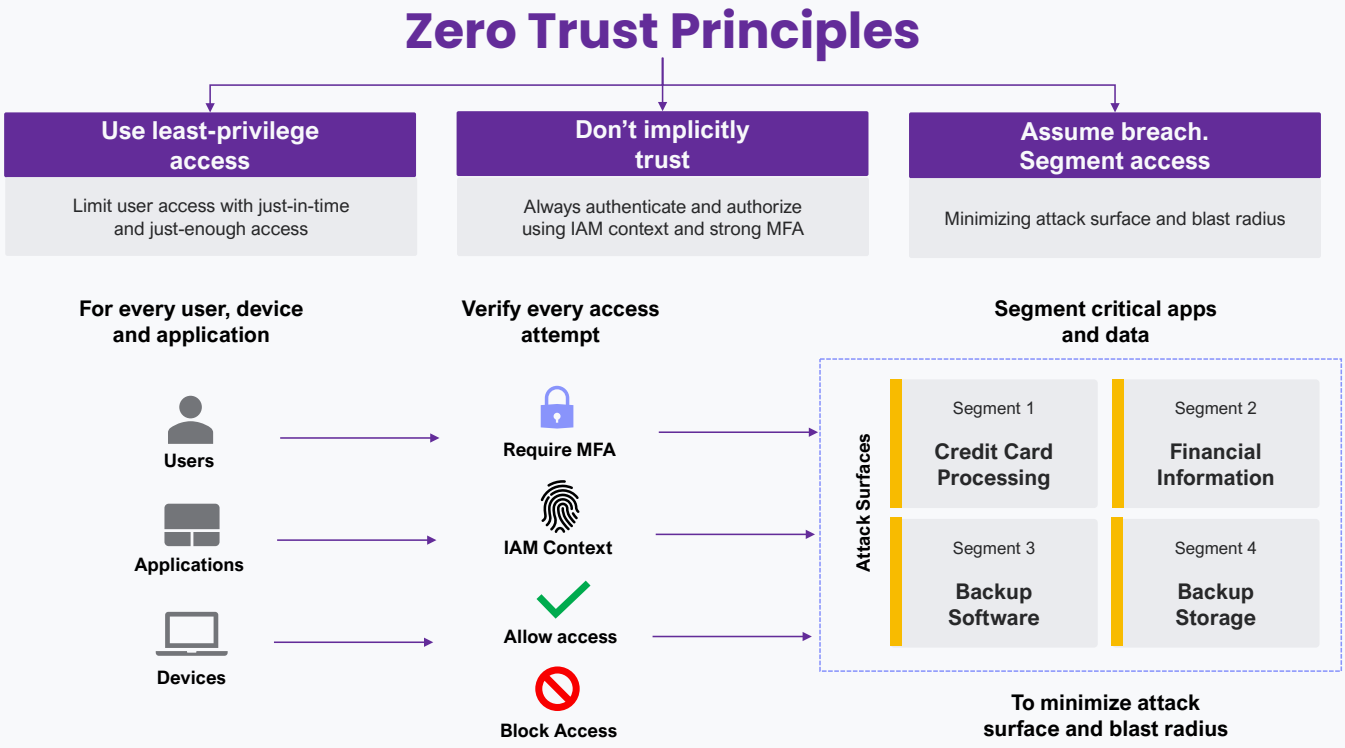
Zero Trust is a security paradigm replacing the more traditional and increasingly ineffective perimeter-based security approach. Zero Trust is being adopted as the best-in-class IT security standard by the US government and enterprises worldwide.

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.
- **Don't implicitly trust.** Always authenticate and authorize by leveraging Identity and Access Management (IAM) context (location, time, etc.) and strong MFA-based authentication.
- **Apply least-privilege access**, with just-in-time and just-enough access.

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



The Object First Approach

Following ZTDR principles, Object First recommends the following best practices for your backup data storage security:

- **Segmentation** — separation of Backup Software and Backup Storage.
- **Multiple data resilience zones or security domains** to ensure multi-layered security.
- **S3-native object storage immutability.**
- **S3-native security**, least-privilege access, IAM, and MFA-based authentication.
- **S3-native communication protocol** with minimal attack surface for Backup Storage.
- **Zero access to root and OS**, protecting against malicious or compromised administrators.
- **Open design and architecture**, simplifying enterprise adoption and deployment.

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 security domains — such as Backup Software, Primary Backup Storage, and Secondary Backup Storage – each with its 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. This ensures the efficacy of the multi-layered security strategy. (See Figure 1).

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

Object First built Ootbi around these principles to meet these requirements and to be part of an enterprise's Zero Trust strategy. Specifically, we have incorporated Zero Trust Data Resilience principles as explained below and in the Numberline Security research paper.

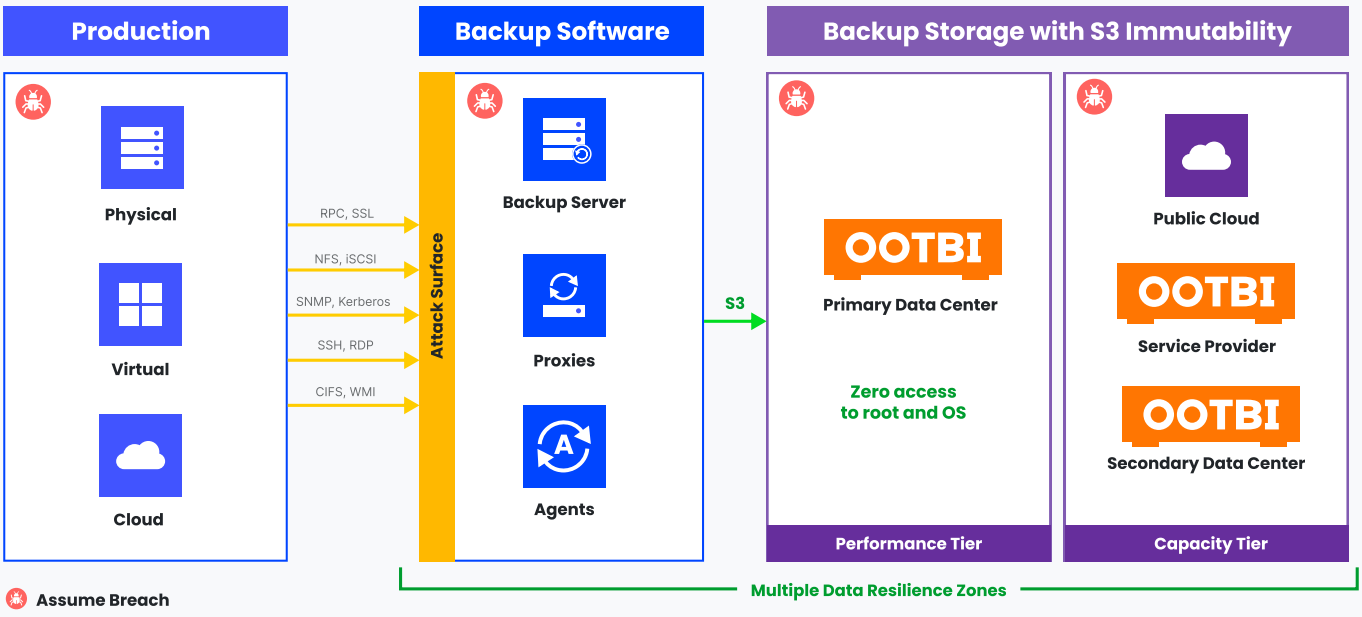
Resilience Zones

A core Zero Trust concept for networking is microsegmentation to break up security perimeters into smaller zones, thus reducing 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.

A well-architected 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.

Figure 1

Zero Trust Data Resilience (ZTDR) Architecture



Not Zero Trust Architectures

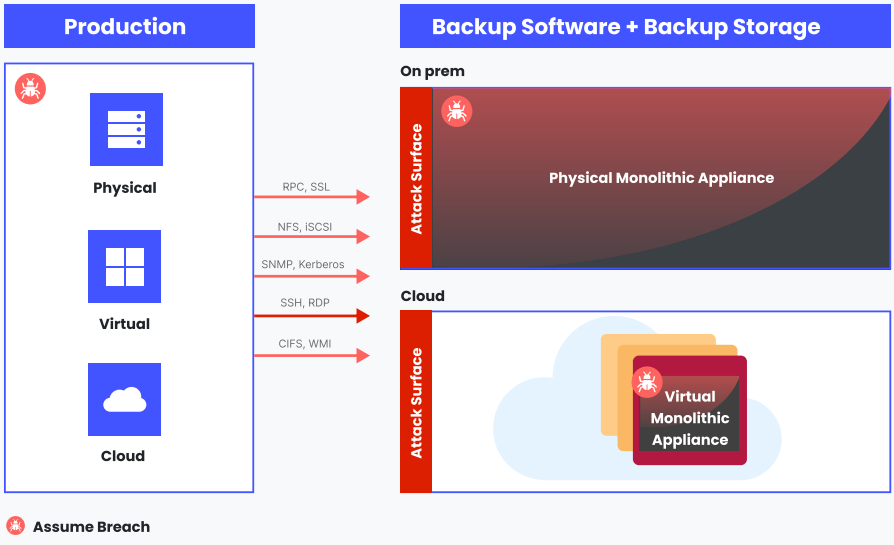
Alternative architectures, including Monolithic Appliances and Direct-Attached Storage (DAS), do not meet the requirements of Zero Trust Data Resilience as there is no separation of Backup Software and Backup Storage. These architectures do not provide true immutability because, upon breach, an attacker will have full access to the Backup Software and Storage. The attacker may now be able to modify, delete, or render your backup data inaccessible. In other words, the blast radius of an attack would include the full backup and recovery system.

Monolithic Appliance: Not Zero Trust

Monolithic appliances represented the next step in data protection and security for many.By integrating the Backup Software and Backup Storage layers, they appeared to streamline the infrastructure. However, this architecture comes with the high cost of compromised security, as the failure to separate the Backup Software and Backup Storage layers according to ZTDR principles means the blast radius of any breach encompasses the full appliance. (see Figure 2).

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**

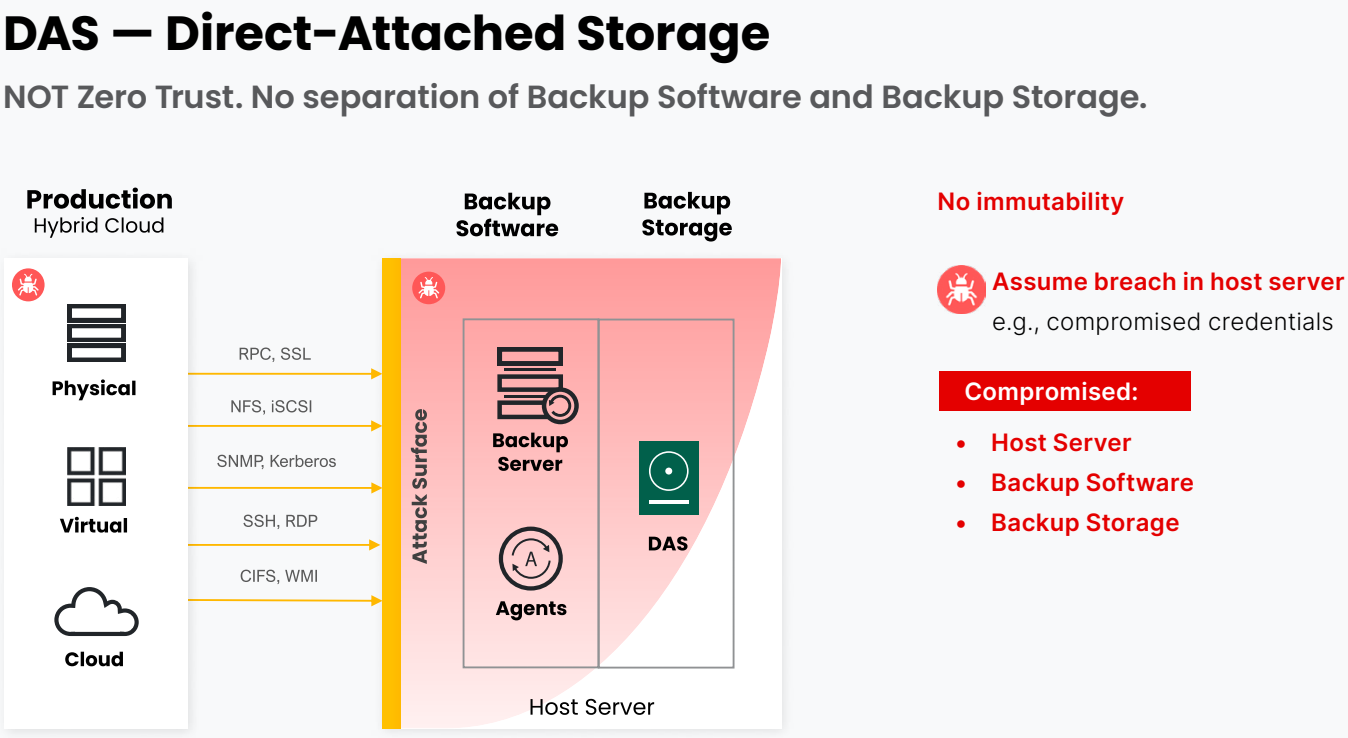
Due to their inherent single-purpose nature, admins are forced to trust monolithic appliances far beyond acceptable levels. A monolithic vendor's proprietary file system immutability can be well intended and designed, but when the box itself can be compromised, it represents a significant and inviting attack surface.

It's critical 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 conducting data backup within the confines of a proprietary storage system housed within the virtual appliance rather than directly securing immutable cloud object storage external to the instance. This weakness arises from an architectural misalignment with ZTDR.

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 data backup and recovery.

Zero Trust Data Resilience (ZTDR) is a model that extends the principles of ZTMM to address the backup and recovery use case. The foundational principle of ZTDR is segregating Backup Software and Backup Storage. This segmentation establishes multiple data resilience zones, ensuring true immutability, multi-layered security, a reduced attack surface, and a minimized blast radius. Incorporating industry-standard S3 immutability and security further fortifies the recommended best practices. This white paper delves into ZTDR principles, emphasizing the pivotal role of immutability and reinforcing Object First's approach to delivering optimal storage solutions for realizing 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.

NOTE

This document represents Object First's perspective on the Zero Trust research conducted by Veeam and Numberline Security. The original research and Veeam's white paper: "Zero Trust Data Resilience — A Pragmatic Approach to Implementing Zero Trust" is available at: https://go.veeam.com/zero-trust-data-resilience