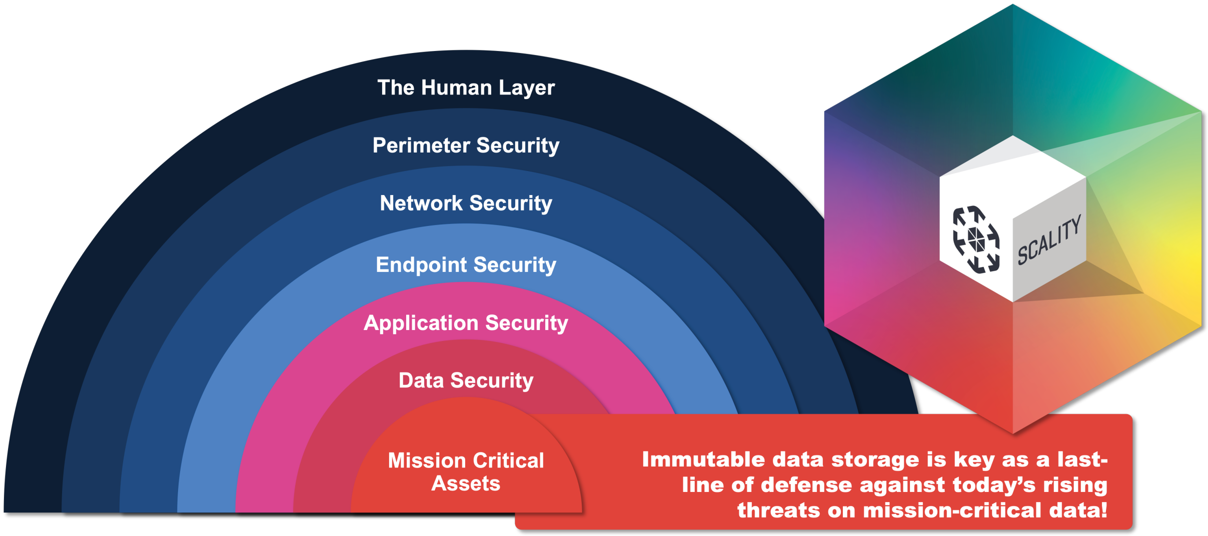
SCALITY

How Scality protects data

with 5 levels of unbreakable cyber resiliency

Cyber resiliency. It's top-of-mind for business leaders — and a top priority for CIOs/CISOs.

With 85% of organizations suffering at least one cyber attack in the last year and 93% of ransomware attacks targeting backup repositories[1], a strategic plan to thwart data loss and ensure business continuity must include immutable data storage — a cornerstone of multi-layered cybersecurity.



Immutable data storage is key as a last-line of defense against today's rising threats on mission-critical data!

Why is immutable data storage a must-have?

Delivers the ability to store data, once written, in a way that can't be modified or deleted (for a fixed time or indefinitely)

Defends data against both inadvertent and malicious actions, including ransomware exfiltration, modification or destruction

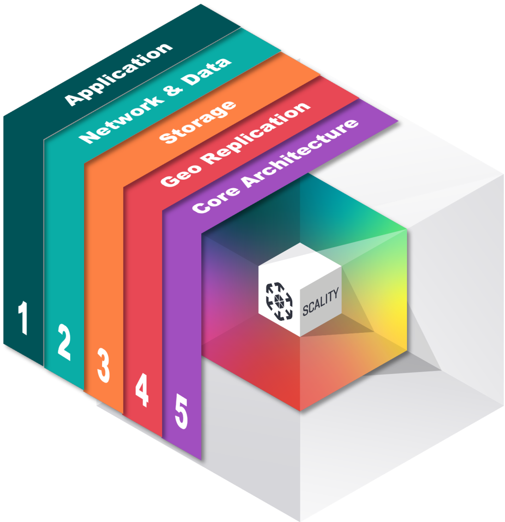
Helps meet regulatory requirements that require a write-once-read-many (WORM) model

Ensures swift, simple recovery of data and business operations when an event occurs

For maximum protection against the widest possible range of current and future threats, Scality's software-defined object storage solutions are thoughtfully designed to provide five distinct levels of unbreakable cyber resiliency.

[1] 2023 Global Ransomware Trends Report, Veeam.

Scality's 5 levels of unbreakable cyber resiliency



1. Application-level resiliency

Scality supports S3 Object Locking APIs to protect against intentional or inadvertent attempts to overwrite data by a user or application issuing S3 commands against a data set (as might be the case in a ransomware attack).

- Amazon S3 object locking immutability with configurable data retention policies and compliance mode to ensures object locks and data retention policies cannot be overridden, even by the system super admin
- Veeam v12 "Direct to object" backups and SOSAPI support, plus automated enforcement of validated IAM access control policies

2. Network & data resiliency

To prevent an authenticated user from reading and accessing data, such as publishing (exfiltrating) the data with malicious intent, Scality applies additional layers of protection via state-of-the-art encryption schemes.

- Secure HTTPS/TLS S3 termination and AES 256-bit data encryption-at-rest with KMS
- Multi-factor authentication (MFA) for secure UI logins, plus automated firewall rules on deployment

3. Storage resiliency

What if attackers are able to penetrate the system below the API layer and actually read or write data on the physical disk drives? Scality's approach makes their success virtually impossible.

- Distributed erasure coding renders data indecipherable to low-level and data exfiltration attacks; metadata in secure repository on intrinsically immutable object storage layer
- Scale-out from TB to 100PB+ with 14 nines data protection and self-healing

4. Geographic replication resiliency

To eliminate vulnerabilities of storing all data in a single location, Scality enables storage across multiple sites, availability zones or physical data centers to create multiple "security domains." With just one copy of data intact, restoration and recovery are assured.

- Async replication to separate security and management domain for "air-gapped" offsite storage
- Eliminates the "all data in one place" problem

5. Core architecture-level resiliency

Scality's object storage solutions are inherently immutable at the core architecture level, meaning the system implements the proper protocols to preserve data in its original form once written.

- Integrated, security-hardened Linux operating system precludes root access, reduces exposure to CVEs to limit a wide range of attack threats

Visit **www.scality.com**

San Francisco • Paris • Washington, D.C • Tokyo • London