



# Data Protection Solution Brief

---

Build a ransomware-resilient architecture and ensure  
business continuity



# How Data Loss Becomes a Business Crisis

---

Real-world incidents show how one failure can trigger the next

## Network Breach

After breaching network devices, a Japanese food company was attacked by ransomware and escalated to lateral movement<sup>1</sup>.

## Unusable Backup

Only 32% believe they can recover within a week<sup>2</sup>.

## Backup Destruction

Ransomware campaigns such as Storm-0501 now deliberately target and destroy backup data<sup>3</sup>.

## Operational Shutdown

A German mobile insurance provider was unable to recover after encryption and ultimately filed for bankruptcy<sup>4</sup>.

### Source:

1. "Investigation Results and Future Measures on Cyberattack Data Exposure" Asahi Group

2. Veeam Data Protection Trends Report

3. Storm-0501's evolving techniques lead to cloud-based ransomware

4. Ransomware plunges insurance company into bankruptcy

## What these incidents have in common

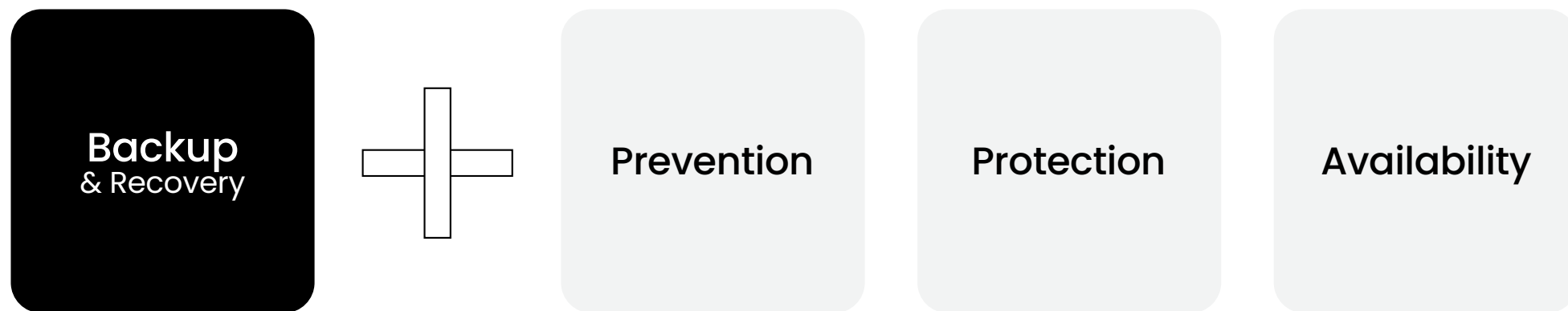
is that no single layer of defense was sufficient to stop the full chain of attacks and failures.



Then, how to avoid crisis? 

# 1 + 3 Data Protection Framework

The straightforward framework for ransomware-resilient architecture



- **Backup** remains the most direct and reliable mechanism for recovery following an incident.
- Recent incidents demonstrate that data loss and operational disruption are rarely the result of a single control failure. Modern data protection strategies are shifting from backup-centric thinking to multi-layered resilience architecture. By reinforcing backup with network-level **prevention**, system and data **protection**, and system-level **high availability**, organizations can reduce risk across multiple failure points and improve overall resilience.

# About QNAP

For over 20 years, QNAP has been a leading NAS storage vendor in the industry.

Driven by the mission to deliver trusted solutions across every layer of data protection, QNAP goes beyond storage to integrate networking, surveillance, cloud, and security. Through responsible product development, QNAP has proved itself as a comprehensive infrastructure solution provider that organizations can rely on.



See QNAP Data Protection Solution 

# QNAP's End-to-end Data Protection

A unified software suite designed to protect business data across workloads, platforms, and locations

## Backup multiple workloads



### Hyper Data Protection

New

License-free backup for Windows PCs, servers, VMs, SaaS, and more



### Qsync

Real-time file backup for PC/Mac

## Backup NAS data



### Hybrid Backup Sync (HBS 3)

Reliable backup and sync of NAS data to other NAS, remote servers, or 20+ cloud services

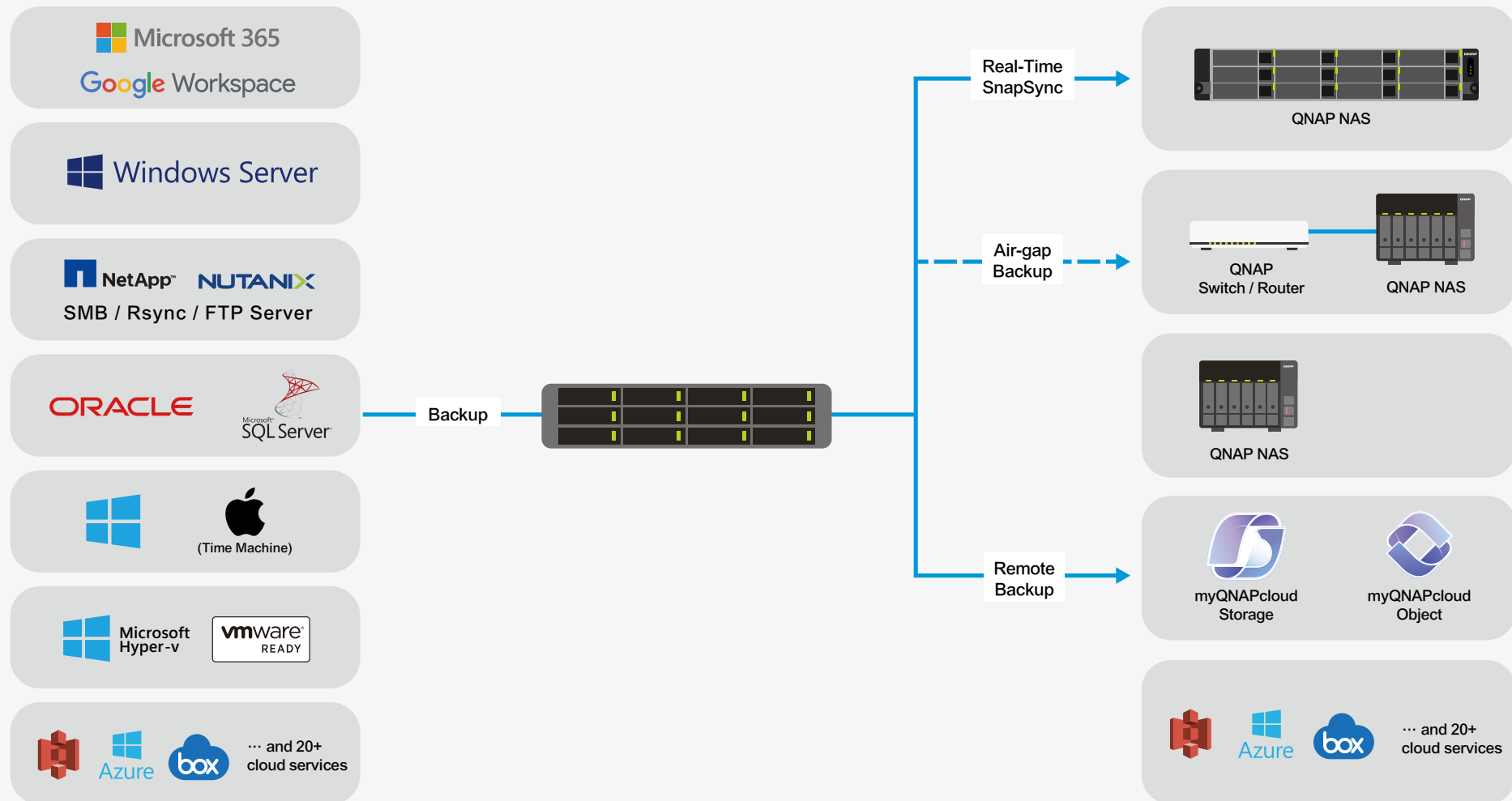
## Management platform



### Hybrid Backup Center

Centralized cloud dashboard for monitoring and managing cross-site, cross-device backup tasks

# Unified Backup Architecture Across Devices, Sites, and Clouds





# Engineered for Reliable Data Protection

Empowering global enterprises with a foundation of uncompromising reliability

## Why QNAP?

Because we don't just store your data, we ensure your business never stops, combining industry-leading hardware with a resilient software ecosystem.



## High-Performance Infrastructure

- Intel® / AMD® multi-core processing power
- High-speed 25/10GbE connectivity, ready for 100GbE
- Scalable, PB-scale storage for long-term data growth

## Reliable ZFS-based System

- Self-healing capabilities to prevent silent data corruption
- Real-time SnapSync for zero-RPO disaster recovery
- Immutable snapshots to ensure ransomware-resistant recovery points

[Learn more](#) | [QuTS hero](#)

**QuTS** hero

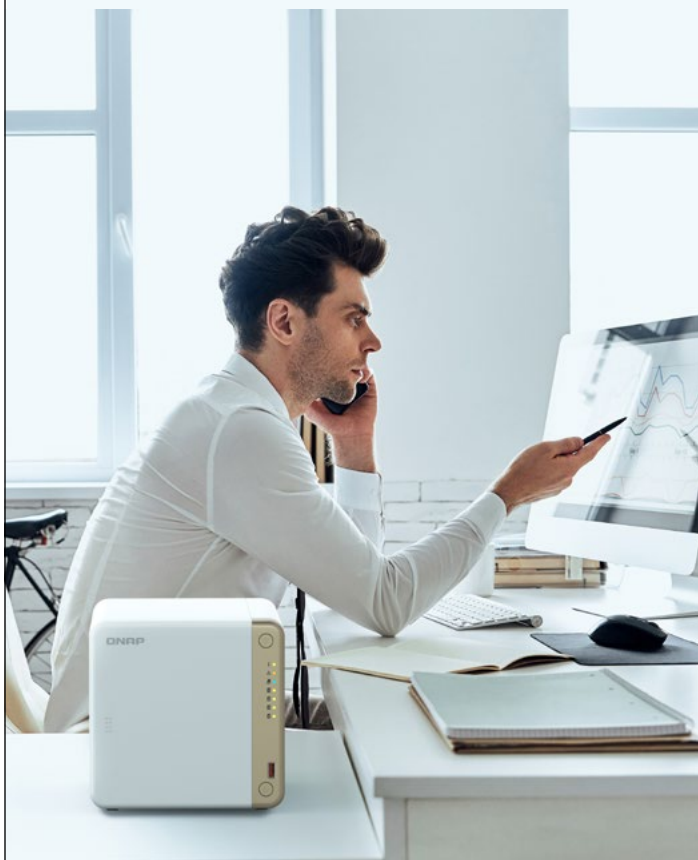


**myQNAPcloud** One

## Secure Hybrid Cloud Strategy

- Simplified offsite backup with QNAP-hosted cloud
- S3-compatible object storage optimizes data management
- Enhanced security with WORM (Write Once, Read Many) and Object Lock

[Learn more](#) | [myQNAPcloud One](#)





# Ransomware-Resilient Backup

Immutability and isolation as the last line of defense

In ransomware attacks, the greatest risk is often the deletion or alteration of backups, rendering them unrecoverable. QNAP ensures data remains inviolable through both immutability and isolation, even if system administrative privileges are compromised.

## Immutable Backup

Enforces immutability on backup data at rest, establishing trusted recovery baselines against ransomware and operational errors.

## Immutable Snapshot

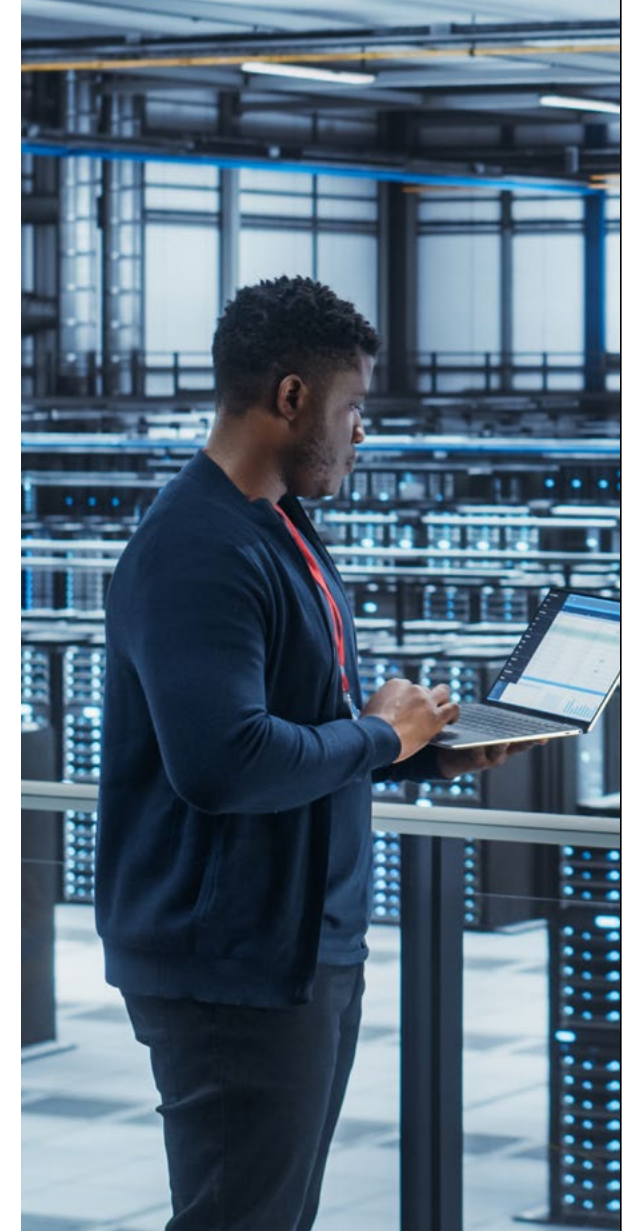
Creates read-only, point-in-time snapshots that preserve data state and enable fast rollback from accidental changes or ransomware impact.

## myQNAPcloud One

Extends immutability to the cloud with WORM and object lock technologies, supporting long-term data retention and compliance requirements.

## Airgap+

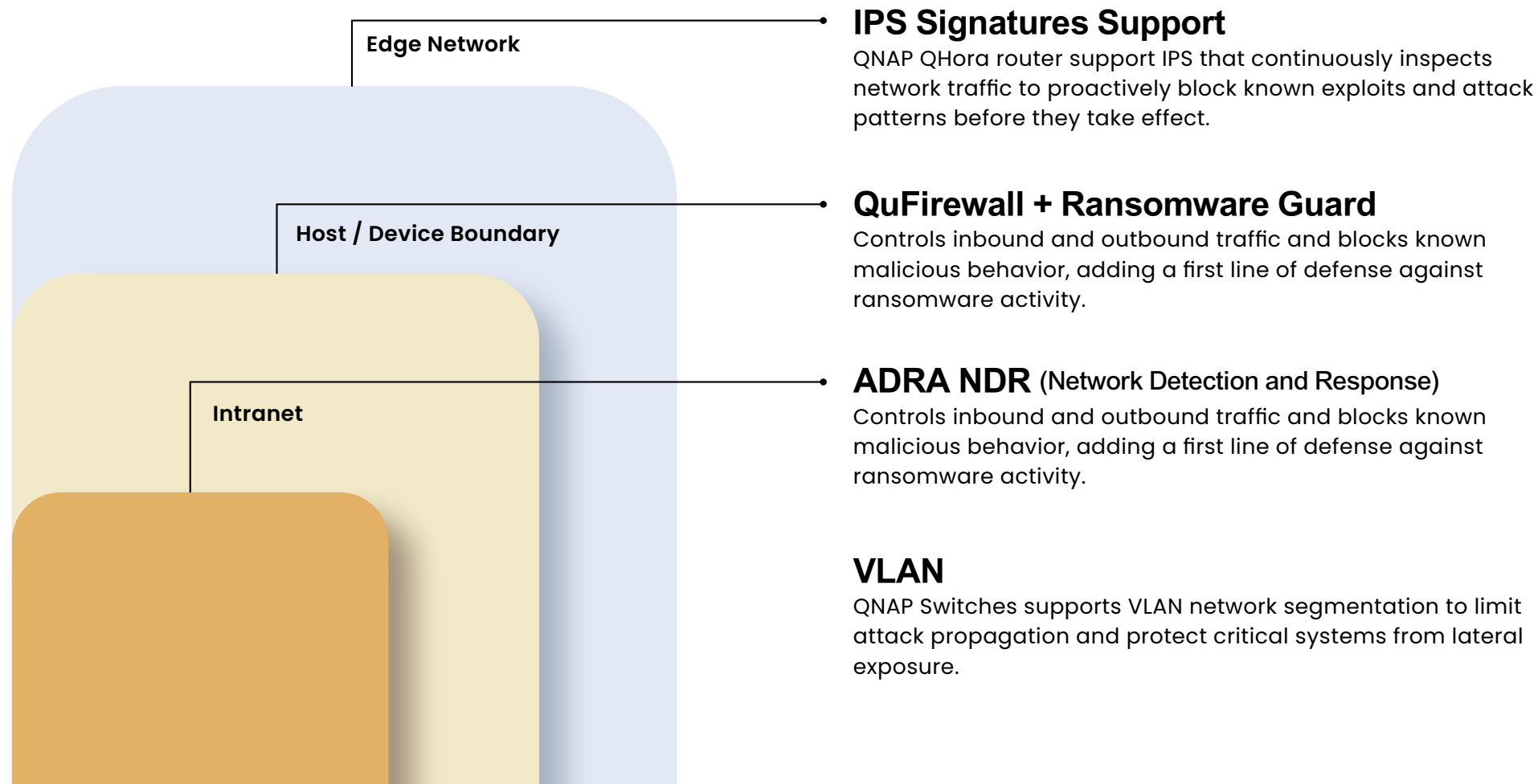
Physically and logically isolates backup targets during non-backup periods, reducing exposure to network-based attacks.



# Network-Level Prevention

Stop lateral movement before threats escalate

Effective data protection begins at the network layer, where most attacks first gain a foothold and begin to spread. QNAP NAS and network solutions integrate anomaly detection and response, segmentation and isolation, and secure connection architecture to contain risks before attacks escalate and keep incidents manageable.



# System-Level Protection

Preventing system and permission abuse to maintain operational control

To defend against ransomware and internal threats, organizations must address both unauthorized access and malicious data modification. By enforcing least-privilege access, separating administrative duties, and protecting data at the system level, enterprises can significantly reduce the operational impact of an attack, even after initial compromise.

## Access Control



### RBAC with Microsoft Entra ID & ACL

Integrates Entra ID (Formerly Azure AD) and Windows ACL to enforce role-based least privilege.



### Delegated Administration

Segregates duties to minimize administrative privilege abuse and insider misuse.



### Multi-Factor Authentication (MFA)

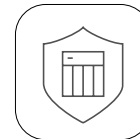
Adds multi-layered verification to protect against unauthorized access and credential leaks.

## NAS System Protection



### Snapshots & Versioning

Enable nearline recovery of files and systems from accidental changes or ransomware impact.



### Security Center

Monitors abnormal file activity and detects suspicious behavior, providing early warning of potential threats.



### Data Immutability

Enforce data immutability to prevent unauthorized encryption. (Go Page 9 to learn more)

# High-Availability (HA)

HA ensuring business continuity through multiple HA models

While backup and protection reduce data loss, availability ensures that business operations do not stop in the first place. QNAP NAS supports multiple high-availability architectures, allowing organizations to select the appropriate model based on workload requirements, performance needs, and scale.

Availability

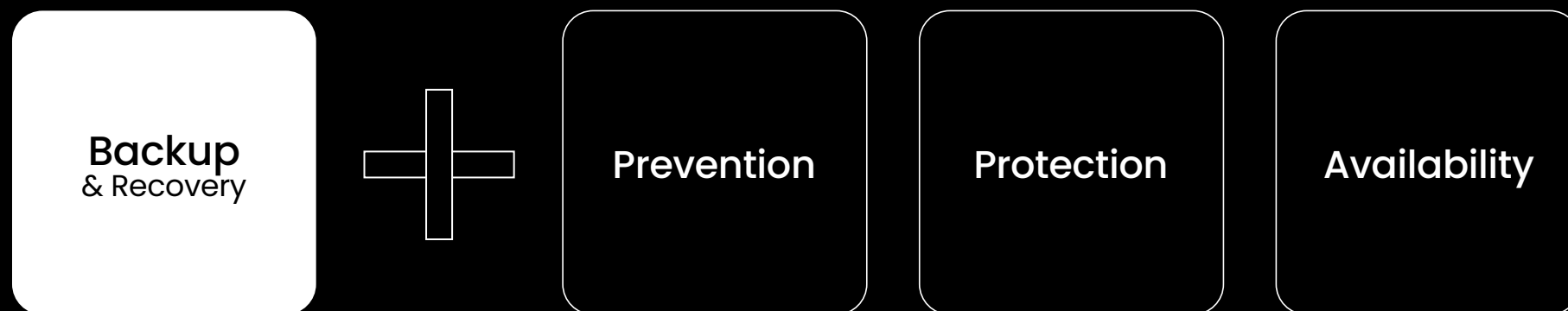
NAS HA			Network HA	VM HA
Active-Active	Active-Passive	MEGA Scale-out NAS	MC-LAG	VM Failover
Dual-active controller architecture for optimized performance and zero-downtime storage services.	Dual-NAS HA architecture designed for fault tolerance, enabling automatic failover to maintain uninterrupted services.	Multiple nodes operate as a unified cluster – Providing both high availability and horizontal scalability.	Enhances switch-level availability to deliver always-on connectivity and a resilient network backbone.	Continuous VM operations during failures, maintenance, and system upgrades.
Best suited for				
Mission-critical services requiring maximum uptime and performance.	Core business systems that require reliability with simpler architecture.	Growing workloads and data volumes.	High-traffic environments and redundant network backbones.	Hosting critical virtualized services and application.





# QNAP's 1 + 3 Data Protection

integrates multiple layers of protection—from securing endpoints to ensuring rapid recovery—into a unified, manageable solution.



**Contact us today** 

to schedule a personalized demo or consultation





A large, 3D shield-shaped icon is positioned on the left side of the page. The shield is metallic and has a glowing orange circuitry pattern on its surface. It is set against a dark background with a pattern of glowing orange binary code (0s and 1s).

# Data Protection Solution Brief

Build a ransomware-resilient architecture and ensure business continuity

## **QNAP Systems, Inc.**

New Taipei City  
Email: [sales@qnap.com](mailto:sales@qnap.com)  
Tel: +886 2 2641 2000

## **QNAP Inc. (USA)**

Pomona CA  
Email: [usasales@qnap.com](mailto:usasales@qnap.com)  
Tel: +1-909-595-2782

## **QNAP Inc. (Canada)**

Markham, Ontario  
Email: [canadasales@qnap.com](mailto:canadasales@qnap.com)  
Tel: +1-905-947-1000

## **QNAP GmbH (Germany)**

Willich  
Email: [desales@qnap.com](mailto:desales@qnap.com)  
Tel: +49-2154-88428-0

## **QNAP SRL (Italy)**

Roma  
Email: [eusales@qnap.com](mailto:eusales@qnap.com)  
Tel: +39-(0)687-738456

## **QNAP UK Limited**

Swindon  
Email: [uksales@qnap.com](mailto:uksales@qnap.com)  
Tel: +44-(0)333-344-2522

## **QNAP Japan**

Tokyo  
Email: [jpsales@qnap.com](mailto:jpsales@qnap.com)  
Tel: +81-3-5901-9735

## **QNAP Korea**

Seoul  
Email: [krsales@qnap.com](mailto:krsales@qnap.com)