QNAP®

Global Enterprise Cyber Resilience Survey 2026



A self-assessment of 1,838 organizations across 93 countries, measuring eleven controls from backup to recovery to reveal the gaps enterprises most often overlook and the practical steps to close them.

Survey period 2026 | Enterprise sample size 1,838 | Online self-assessment, not a third-party audit

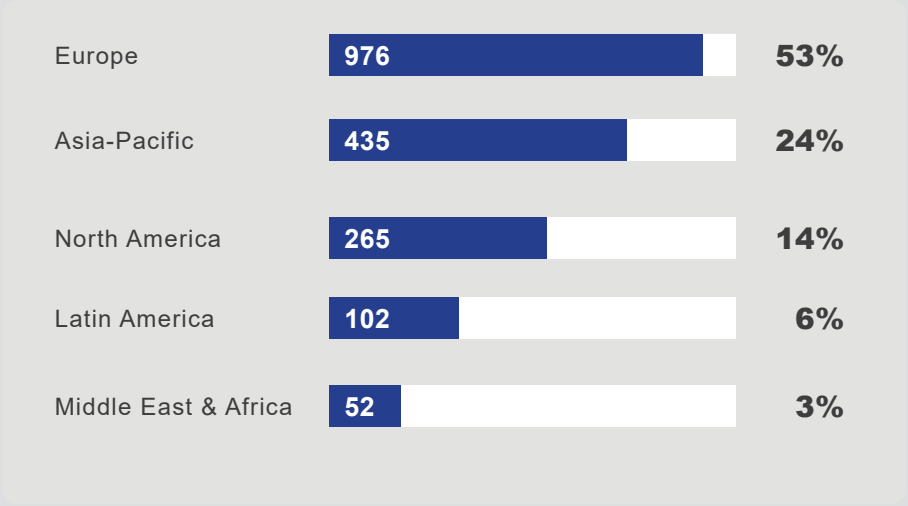
About This Survey

As ransomware and supply-chain attacks become routine, asking whether an organization "does security" no longer reveals much. What determines the scale of the damage is how mature each protection is: absent altogether, dependent on manual effort, or handled by a dedicated enterprise-grade mechanism.

To measure that maturity, QNAP invited its global community to complete an eleven-question self-assessment spanning four stages: data protection and backup, identity and access control, threat monitoring and active defense, and business continuity and recovery. Each answer scores 1, 3 or 5 points, giving a total between 11 and 55.

Of 3,236 responses, this report analyzes the 1,838 submitted on behalf of organizations. Individual and home users were excluded so that every figure describes a business environment. All external research is cited separately and never mixed with survey results.

Enterprise sample by region



Four stages and scoring

Data protection and backup	Question 1-4
Identity and access control	Question 5-6
Threat monitoring and active defense	Question 7-9
Business continuity and recovery	Question 10-11

1 point - No protection

3 points - Partial or manual

5 points - Enterprise-grade protection

What These Numbers Can and Cannot Tell You

Every self-assessment has a scope. The points below are not weaknesses of the report; they are the conditions under which its figures should be read and quoted. Statements about attack frequency and cost rely on published international research, not on incident data from this survey.

01

Self-assessed, not audited

Scores reflect each respondent's view of their own organization. The survey uses a descriptive scale in which every option names a concrete practice; this makes it easier to recognize controls already in place than a bare checklist would, so adoption rates here should not be compared directly with checkbox-style surveys.

02

Drawn from QNAP's own community

Respondents are QNAP customers, partners and prospects. The figures describe organizations already engaged with storage and backup, and should not be extrapolated to all businesses.

03

Enterprise sample definition

Of 3,236 responses, 1,398 from individual and home users were excluded. The sample retains enterprise users, companies whose staff also use QNAP personally, channel partners and former enterprise users.

04

Sample skews toward small organizations

Firms with 1 to 10 employees account for 49% of the enterprise sample. Because scores rise with company size, readers benchmarking against peers should use the size analysis rather than the overall average.

05

Regional weighting

Europe contributes 53% of responses. Within Asia-Pacific, Taiwan accounts for 42%. Latin America (102) and the Middle East and Africa (52) have smaller samples and should be read as indicative.

Five findings

Market Insights

01 Half of enterprises sit at Developing or below

The average score is 33.9 out of 55. In total, 922 organizations (50% of the sample) fall into the two lower tiers, and 64% leave at least one of the eleven controls completely unprotected.

02 Nearly half of enterprises keep backups an attacker could delete

Although 83% keep an offsite backup, 896 organizations, or 49% of all respondents, keep that backup online with no immutable copy. More than a third of them score Established or above.

03 Ransomware can spread unseen in most networks

Only 13% of enterprises have enterprise-grade internal threat detection, the lowest of all eleven controls, and 29% would notice ransomware only after files are encrypted.

04 Asia-Pacific trails the other regions

Asia-Pacific averages 31.1, against 34.5 to 35.0 for the other four regions, and its share of High-Risk organizations (23%) is roughly double theirs. The gap persists, and even widens, among organizations with 11 or more employees.

05 Size and sector shape maturity

Scores climb steadily with company size, from 32.5 for firms with 1 to 10 employees to 39.5 for those with more than 1,000, and the share reaching the Leading tier triples. By industry, IT services leads at 36.7 and media and communications trails at 30.4.

50%

of enterprises score at Developing or below, short of a stable security baseline

Total scores divide the sample into four tiers: High Risk (260 organizations), Developing (662), Established (599) and Leading (317). The two lower tiers together hold 922 organizations, just over half of the sample, and they leave an average of 4.6 controls with no protection at all. These organizations are not a fringe minority but the mainstream. The median score is 33, exactly the upper boundary of the Developing tier: the typicalorganization sits right on the line between exposed and established.

The average score is 33.9 out of 55, or about 62% of the maximum, with a median of 33. Only 17% reach Leading, and 64% leave at least one of the eleven controls with no protection at all.

What separates the tiers is easier to see in unprotected controls than in points. High-Risk organizations leave an average of 8.3 of the eleven controls completely unprotected; Developing organizations 3.1; Established 0.7; Leading 0.1. Every one of the 260 High-Risk organizations has six or more controls with no protection. For this group the missing piece is not a single tool but a basic layer across every stage, so QNAP recommends starting with identity and backup fundamentals before moving to advanced defenses.



Source: this survey, enterprise sample (n = 1,838). Total score is the sum of eleven questions scored 1, 3 or 5.

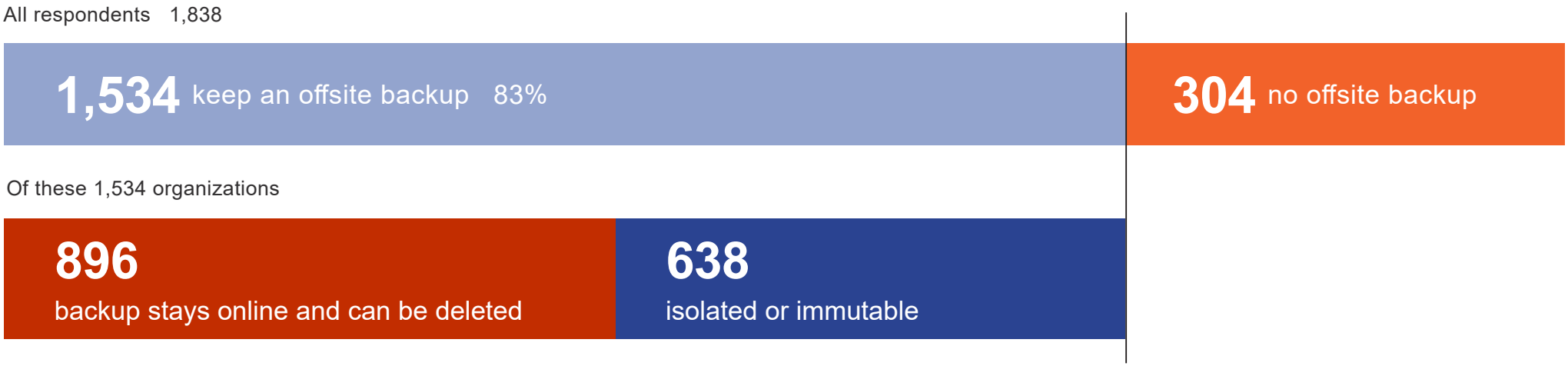
49%

of enterprises keep backups that could be deleted or encrypted along with their production data: nearly one in two

Offsite backup is the most widely adopted control in the survey: 1,534 of 1,838 organizations (83%) have one. But having a backup and having one that survives an attack are two different things. In Sophos research, 94% of organizations hit by ransomware said attackers tried to compromise their backups, and organizations whose backups were compromised paid the ransom 67% of the time, against 36% for those whose backups held. The backup is now the first target in the attack chain, not a safety net outside it.

Of the 1,534 organizations with an offsite backup, 896 show both weaknesses at once: the backup server stays connected to the network around the clock, and nothing prevents a stolen administrator account from deleting it. That is 49% of all respondents.

This is not a problem confined to laggards. The 896 organizations average 31.1 points, only 2.8 below the overall 33.9; 323 of them already score Established or above, and 53 have more than 1,000 employees. Once a backup job runs successfully, it tends to be treated as done, and the protections around the backup itself receive far less attention.



Definition of the 896: Q1 (offsite backup) scored 3 or higher, while Q3(ransomware-proof architecture) and Q4 (immutable backup) both scored below 5.Sophos research is an external source; see References.

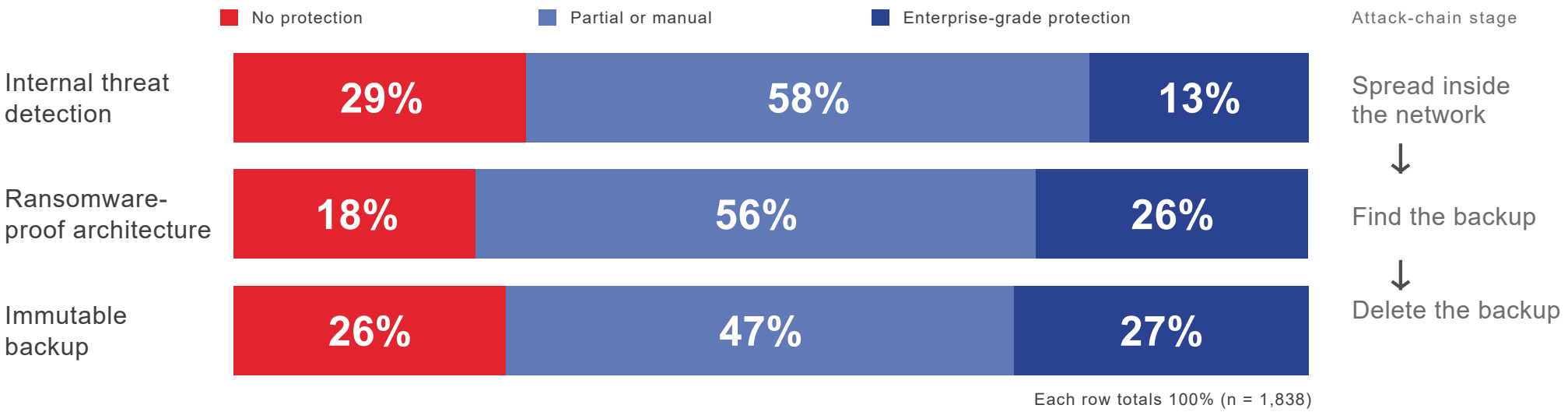
29%

of enterprises have no protection against ransomware spreading inside their network, the first step of the attack chain

In this survey, 29% of enterprises have no internal threat detection at all, 18% have no ransomware-proof backup architecture and 26% have no immutable backup. The other end is more telling: only 13%, 26% and 27% reach enterprise grade, and internal threat detection, at 13%, is the lowest of all eleven controls.

These three controls were chosen not by score but by the attack chain described in external research, each mapped to one attacker move: spreading inside the network, finding the backup and deleting it.

QNAP observes that beyond the organizations with no protection, most gaps come from reliance on manual handling. Attackers typically begin moving laterally within 29 minutes of initial access, while organizations take a median of 11 days to detect an intrusion; any step that waits for a human decision can fail at the moment it matters. For these three controls, QNAP recommends approaches that are configured once and then run automatically.

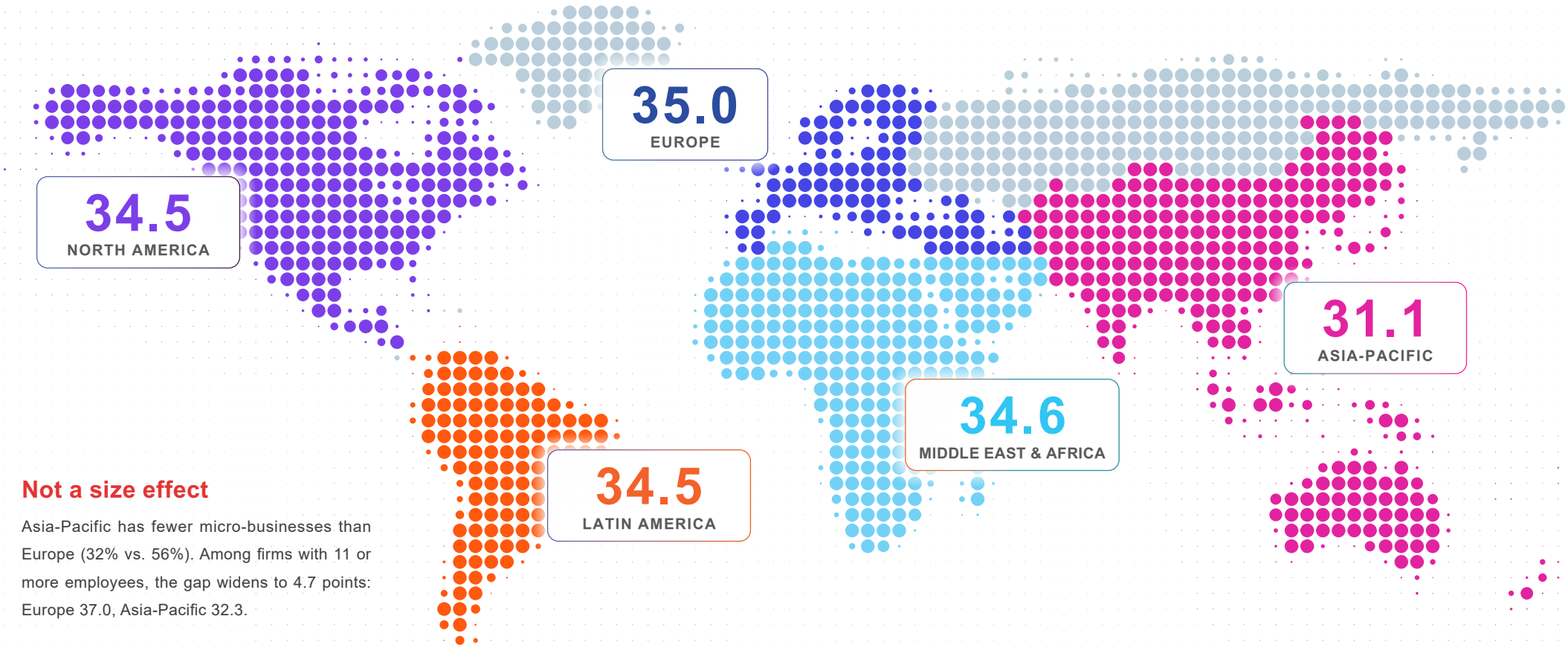


Each row totals 100% (n = 1,838)

External sources: CrowdStrike 2026 Global Threat Report; Google Mandiant M-Trends 2025.

Asia-Pacific Scores Lowest of All Five Regions

Average total score by region, enterprise sample (maximum 55). Every region shares the same two weakest links by average score: internal threat detection and recovery time.



Not a size effect

Asia-Pacific has fewer micro-businesses than Europe (32% vs. 56%). Among firms with 11 or more employees, the gap widens to 4.7 points: Europe 37.0, Asia-Pacific 32.3.

EUROPE	MIDDLE EAST & AFRICA	NORTH AMERICA	LATIN AMERICA	ASIA-PACIFIC
35.0	34.6	34.5	34.5	31.1
n=976	n=52	n=265	n=102	n=435
Leading 18%	Leading 21%	Leading 18%	Leading 20%	Leading 14%
High Risk 11%	High Risk 13%	High Risk 13%	High Risk 13%	High Risk 23%

Colors show regional averages, not country scores. Russia, Belarus, Central Asia, Mongolia and Greenland appear in gray because together they account for only 3 responses; those responses are still included in the regional averages. Taiwan accounts for 42% of the Asia-Pacific sample.

7.0 pts

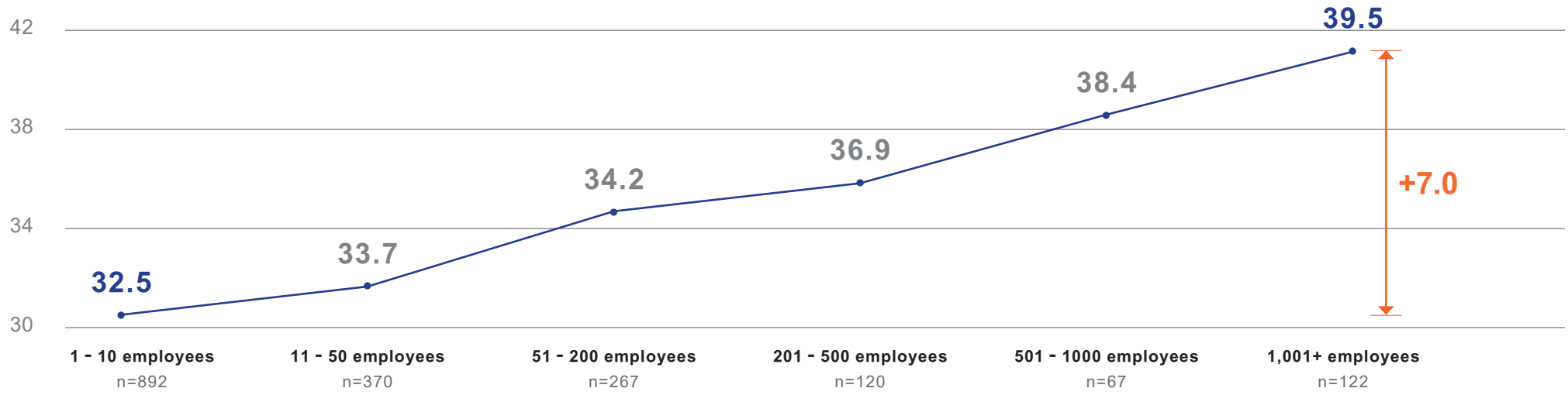
separate the smallest and largest organizations: a gap in resources, not awareness

Scores rise with every step up in company size: from 32.5 among organizations with 1 to 10 employees (892 responses) to 39.5 among those with more than 1,000 (122 responses). The share reaching the Leading tier triples over the same range, from 13% to 39%.

The pattern has two practical implications. In small organizations, low scores rarely reflect a lack of concern; more often one person handles IT, purchasing and day-to-day operations at once. For that reason, solutions that work for smaller businesses must be simple to deploy and able to run on their own once configured, rather than adding another recurring task to the same person's list.

The weakest link also shifts with size. Up to 200 employees, internal threat detection is the lowest-scoring control; from 201 employees upward, recovery time takes its place. Smaller organizations struggle to see what is happening inside the network; larger ones struggle to stop the clock once something breaks. Even among organizations with more than 1,000 employees, only 26% have automated internal threat detection. QNAP ADRA NDR X is built for exactly this situation: a proactive internal threat detection solution that plugs directly into the existing network and lowers the cost of strengthening security.

Average total score by company size (maximum 55)



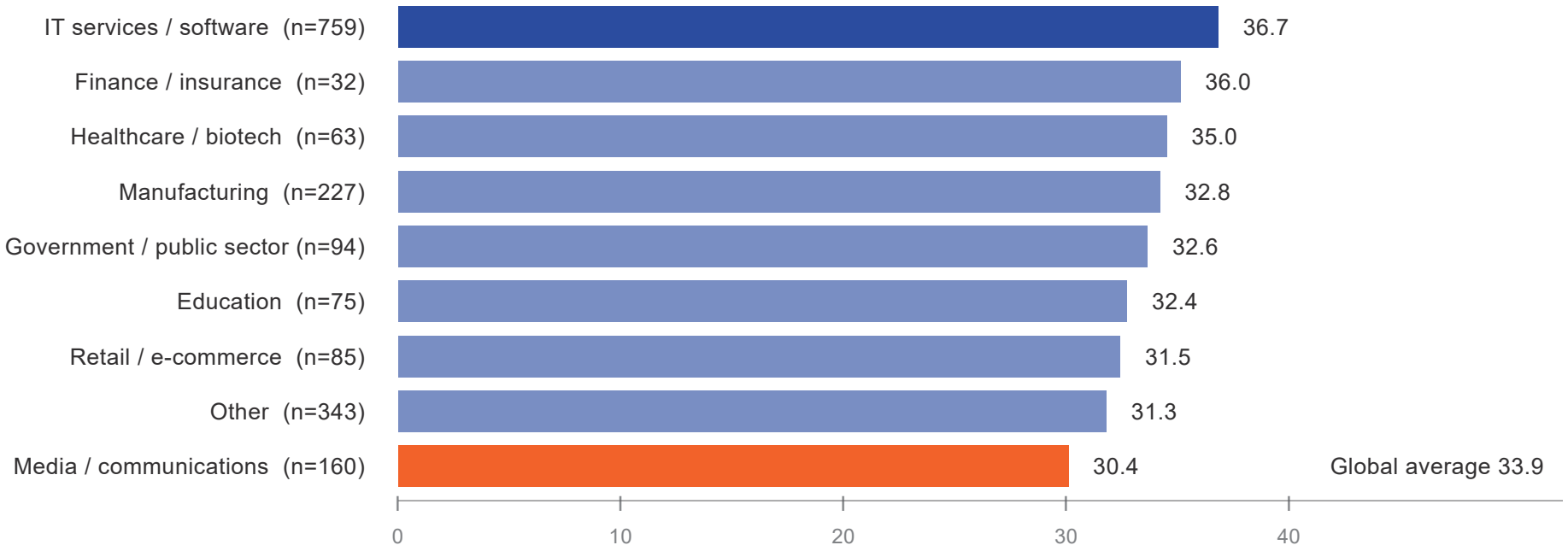
How Security Varies by Industry

Tech, Finance and Healthcare Lead in Cyber Resilience; Media and Retail Trail

IT services and software leads at 36.7 points and, with 759 responses, is also by far the largest group. Finance and insurance follows at 36.0, then healthcare at 35.0. At the other end sit media and communications at 30.4 and retail at 31.5.

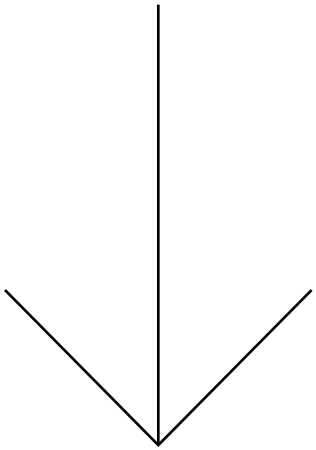
The ranking follows a recognizable pattern. Sectors where IT is the core business, or where regulators scrutinize data handling, cluster near the top. Sectors in which data volumes tend to grow faster than dedicated IT staff, such as media, retail and education, cluster near the bottom. This is an observation drawn from the ranking rather than a measured cause, but it matches what the size analysis shows: maturity tracks available resources.

The "Other" group, 343 organizations from sectors outside the eight named categories, averages 31.3 and has the lowest share at the Leading tier of any group (6%). Organizations without sector-specific regulation or guidance appear to have the least external pressure, and the least external help, to move forward.



*Sectors with fewer than 100 responses (finance 32, healthcare 63, education 75, retail 85, government 94) should be read as indicative.

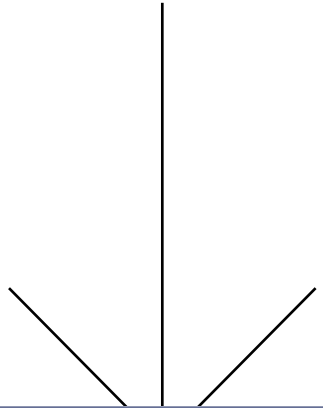
Insights



- Data protection and backup
- Identity and access control

Action

- Threat monitoring and active defense



- Business continuity and recovery

36%

of enterprises still back up manually to an external drive or another device

QNAP HBS 3 turns 3-2-1-1-0 from a rule into a schedule

A backup is not simply one more copy; it is a rule that can be verified. The industry's working definition of a usable backup is 3-2-1-1-0: three copies of the data, on two different types of media, one stored offsite, one kept offline or isolated, and zero errors when a restore is tested.

This survey evaluates three key conditions: offsite storage, isolation, and restore verification. While enterprise adoption reaches 47% for offsite backup, it drops to just 26% for both isolation and verification—revealing that most backup strategies are still built for hardware failure, not active ransomware attacks.

QNAP recommends HBS 3 as the starting point. It is built into QTS and QuTS hero at no additional license cost. The questions that matter are whether backups run on an automatic schedule, how many historical versions are kept, and how often a restore is confirmed to work. Organizations that already back up offsite should also watch frequency: the less often a backup runs, the more data is lost when a restore is needed. QuDedup deduplicates and encrypts at the source, shortening each job so backups can run more often with multiple versions, and immutable backup adds tamper protection on top.

QNAP RECOMMENDS

HBS 3 (Hybrid Backup Sync)

Backup, sync and restore | Built into QTS / QuTS hero, license-free | 1.9 million+ users worldwide

01 Local, remote and cloud in one tool

Supports RTRR, Rsync, FTP, SMB, WebDAV and major cloud services. One tool covers every backup path, with no separate software for each destination.

02 Multi-version backup

Set how many versions to keep and for how long. If production data is encrypted by ransomware, an earlier clean version remains available, not just the latest copy.

03 Source-Side Encryption & Deduplication

QuDedup delivers block-level deduplication and encryption at the source. Proven in virtualized environments, it cuts backup sizes by up to 75%—slashing bandwidth usage and accelerating backup windows.

04 Immutable backup to WORM folders

When a backup job completes, the destination folder locks immediately, so the backup is tamper-proof from the moment it lands. Requires HBS v26 or later with a QuTS hero destination.

56%

of enterprises back up offsite but keep the backup server online around the clock

QNAP Airgap+ keeps backups beyond the reach of attackers

When backup and production share a network, a single intrusion can destroy both. Attackers need no special skill: with any account that holds administrator rights, they can reach, delete or encrypt backups exactly as a legitimate administrator would. Isolated backup has become a foundation of cyber defense rather than an optional extra.

In this survey, 18% of organizations have no isolation at all, and a further 56% keep offsite or cloud backups whose servers stay continuously connected to the network. Only 26% have physically isolated their backups.

QNAP recommends HBS x Airgap+ to automate the air gap. After each job, the backup is automatically cut off from the network, with no manual swapping of drives or rotation of tapes. A Bridge NAS sits between source and backup, and its two gates never open at the same time: data enters the bridge, the outer gate closes, and only then does the inner gate open. At no moment is there a direct path between source and backup, including during transfer, and once the job finishes the backup becomes invisible on the network again. Whatever happens to production, a clean isolated copy is always there to restore from.

QNAP RECOMMENDS

HBS x Airgap+

Air-gapped backup | QNAP NAS + QHora router or QSW managed switch

01 Five-stage airlock workflow

Standby, outer gate opens, data staged, inner gate opens, back to isolation. The full cycle runs on schedule, and the backup side becomes invisible on the network again when done.

02 The two gates never open together

Source and backup are never directly connected, not even during transfer. If the source is fully compromised, attackers still cannot reach the backup device.

03 The Bridge NAS is sealed too

It runs only HBS sync and backup tasks, offers no external services and accepts no inbound connections, so it adds no new attack surface.

04 Gate control secured with mutual TLS

HBS and QuRouter authenticate each other with certificates, so only verified systems can open or close the gates and the gate control itself cannot be spoofed.

26%

of enterprises cannot stop a privileged account from deleting their backups

of enterprises cannot stop a privileged account from deleting their backups

The most common ransomware technique is not breaking encryption. It is obtaining administrator rights and then deleting backups as a legitimate user. If a backup is protected only by account permissions, it falls the moment those permissions do.

Isolation keeps attackers from finding the backup; immutability means that even if they find it, they cannot touch it. WORM (Write Once, Read Many) locks data at the file-system level as soon as it is written, so it cannot be changed or deleted during the retention period, not even by an administrator. The technology originated in regulatory record-keeping for finance, healthcare and the public sector, and has since become a widely adopted defense against ransomware. In this survey, in addition to the 26% with no protection, another 47% rely on whatever older versions happen to remain in the cloud.

QNAP recommends keeping backup copies in WORM folders, where the lock is enforced by the ZFS file system rather than by account settings, so a compromised account changes nothing. Enabling immutable snapshots as well allows production to be rolled back directly to its pre-attack state, without waiting for a full restore. Retention can be set separately for each: short retention on snapshots to cover accidental deletion and single-system incidents, and long retention on WORM copies for incidents that require going further back.

QNAP RECOMMENDS

Immutable Storage & Snapshots

Tamper-proof storage and pre-attack recovery | Locked at the ZFS file-system level, independent of account permissions

01 ZFS-level locking

Data is locked by the file system the moment it is written. Even with the highest administrator rights, attackers cannot modify, delete or even move it to the recycle bin during the retention period.

02 Enterprise and Compliance modes

Enterprise mode preserves administrative flexibility: administrators can still delete an entire WORM share. Compliance mode prevents even administrators from deleting it, for the highest level of protection.

03 Immutable snapshots

Snapshots can also be locked for a retention period. If production data is encrypted, it can still be restored to a clean point before the attack, with no ransom paid.

04 Automatic integration with HBS

WORM retention is applied automatically when a backup completes, with no manual configuration each time, eliminating the risk of enabling WORM but forgetting to apply the lock.

24%

of enterprises protect core storage with a username and password alone

MFA keeps a leaked password from becoming a breach; RBAC keeps a breach from becoming a disaster

According to the Verizon Data Breach Investigations Report, credential abuse is the most common single initial access vector (22%), with phishing at 16%, and the human element, including errors, is involved in 60% of breaches. Most attacks begin not with technical brilliance but with a set of credentials that still work.

Protecting credentials is really two separate problems. Authentication answers “whether a user is who they claim to be”; authorization answers “what that user can reach”. With only the first, a stolen account has no limits once inside. With only the second, an attacker can still simply log in.

Access control belongs at the top of the list because every other control depends on it: if an attacker can sign in as a legitimate user, backup protection and monitoring can both be bypassed. Among High-Risk organizations, 79% rely on passwords alone. Because MFA and RBAC are built into QTS and QuTS hero and require no additional hardware, this is also one of the fastest improvements any organization can make.

QNAP RECOMMENDS

MFA + RBAC

Multi-factor authentication and role-based access control | Built into QTS / QuTS hero

01 Passwordless sign-in and 2FA

QNAP Authenticator supports passwordless sign-in, removing the risk of stolen passwords, and also provides time-based one-time codes for two-factor authentication, balancing convenience and security.

02 Role-based access control

Assign shared-folder and application permissions by department or role, instead of everyone sharing one administrator account, to limit what a single compromised account can reach.

03 Directory integration

Connect to AD or LDAP so permission changes follow HR records, reducing the risk of accounts that remain active long after an employee has left.

04 Default-deny, Not default-allow

Audit the access list for each shared folder during deployment. Most over-permissioning stems from a "grant access first" mindset, rather than intentional design.

58%

of enterprises only rely on endpoint tools or firewalls that cannot see agentless devices

QNAP ADRA NDR X — Internal network detection for proactive defense

Endpoint detection and response (EDR) protects only devices that can run an agent: PCs, laptops and servers. Printers, IP cameras, IoT sensors, third-party NAS and production controllers cannot. EDR also observes behavior inside a single device, so it struggles to see relationships between devices; seen from any one host, lateral movement looks like an ordinary connection. Once attackers hold administrator rights, they can also disable the agent or exclude the paths they use.

In this survey, 29% of organizations would only notice ransomware after file extensions change or antivirus raises an alert. A further 58% have EDR or firewalls in place that cannot see agentless devices. Only 13% detect threats at the network layer.

Network detection and response (NDR) closes this gap by analyzing traffic between devices at the switch layer, with nothing to install on each device, and it complements endpoint protection rather than replacing it. QNAP ADRA NDR X runs license-free on a QNAP NAS with a compatible switch and needs no additional hardware. It detects, analyzes and isolates threats automatically, stopping lateral spread while the rest of the network keeps running.

QNAP RECOMMENDS

ADRA NDR X

Network detection and response | License-free on QNAP NAS with compatible switches

01 Threat Watch selective inspection

Rather than inspecting every packet, it analyzes only those with anomalous characteristics in depth, detecting lateral movement and abnormal connections while preserving network throughput.

02 Threat Trap decoys

Emulates common services such as SSH and SMB as decoys to draw out threats already hiding on the network, instead of waiting passively for an alert.

03 Automatic targeted isolation

When high-risk behavior is confirmed, only the affected device is isolated, stopping the spread without interrupting the rest of the network.

04 Agentless device coverage

Network-layer detection automatically covers devices that can't run agents, such as printers, IoT gear, and third-party NAS.

27%

of enterprises would need more than a day to restore service; only 14% fail over automatically

QNAP High Availability shrinks recovery from days to near zero

ITIC reports over 90% of mid-to-large enterprises lose $300K+ per hour of downtime, with 41% losing $1M–$5M. Recovery speeds vary dramatically even with backups: replacing hardware takes days, manual rebuilds take hours, but automatic failover renders downtime virtually imperceptible.

In this survey, 27% would need more than a day to recover, 59% could recover within hours but only through a manual restore by IT staff, and just 14% have near-zero downtime through a high-availability cluster. For organizations with more than 200 employees, recovery time is the lowest-scoring control of all.

QNAP advises enterprises to adopt High Availability (HA) to safeguard critical services. Operating in a clustered setup, the secondary NAS seamlessly executes automatic failover upon primary system failure without requiring manual action or IT duty coverage. This slashes service interruption from hours or days down to seconds, drastically reducing outage costs. However, HA and Backup target different vulnerabilities. While HA resolves hardware-induced downtime through dual-node synchronization, it does not defend against accidental deletion or ransomware attacks. Data protection requires dedicated backups and immutable storage. Together, they answer the two critical questions after any incident: Can we get our data back? and How fast can service be restored?"

QNAP RECOMMENDS

High Availability (HA)

Dual-node cluster | Automatic failover

01 Automatic failover

When the primary system fails unexpectedly, the standby takes over automatically, with no manual intervention and no dependence on staffing hours.

02 Near-zero RTO

Service interruption shrinks from days or hours to the time needed for switchover, directly reducing the cost of downtime.

03 HA complements backup - It doesn’t replace it

HA addresses hardware failure and keeps critical data consistent, while backup protects against data corruption, deletion, and ransomware encryption. Addressing fundamentally different risks, both are indispensable.

04 Recovery speed equals real dollars

When calculated against hourly downtime losses, every hour saved is direct cost avoidance—turning HA into a clear, quantifiable ROI.

Close the Most Critical Gap First

The most common reason security upgrades fail is not choosing the wrong tool but starting too many projects at once, so each one stalls halfway and gaps remain open. A more practical approach is to identify the organization's current tier and complete the one to three measures that matter most at that stage.

The data supports this sequence. Among High-Risk organizations, 79% rely on passwords alone and 57% have no offsite backup, so identity and backup come first. At the Established tier, only 8% have automated internal threat detection and 11% enterprise-grade recovery. Even at the Leading tier, these remain the last two gaps, at 59% and 58%, while every other control there exceeds 75%.

High Risk

Pts:11-22

260 (14%)

- **MFA / 2FA**
  Shut the most common entry point
- **RBAC**
  Limit what any one account can reach
- **HBS 3 Backup**
  Make sure a usable backup exists

Developing

Pts:23-33

662 (36%)

- **Airgap+ Isolated Backup**
  Keep backups offline and clean
- **Immutable Storage (WORM)**
  Backups stay undeletable, even if attackers find them
- **QuFirewall**
  Block brute-force attacks automatically

Established

Pts:34-44

599 (33%)

- **ADRA NDR X**
  Spot and stop threats moving inside the network
- **Self-encrypting Drives**
  Keep data safe on stolen or retired disks

Leading

Pts:45-55

317 (17%))

- **High Availability**
  Cut recovery time to near zero

Protecting Your Data Starts with a Certified, Compliant Vendor

QNAP is a trusted partner for your organization's security

Security & Privacy



Information Security Management System



Cloud Security Controls



Cloud Privacy Protection



EU General Data Protection Regulation

Supply Chain Security & Development Resilience



Secure Product Development Lifecycle Requirements



Open Source License Compliance OpenChain



Software Supply Chain Security Declaration



EU Cybersecurity Directive Compliance



EU Cyber Resilience Act Compliance



Japan IoT Security Label

Global Operations, Quality & Intellectual Property



Quality Management System



US Trade Agreements Act Compliance



Taiwan Intellectual Property Management System

Explore QNAP Trust Center >>

References

External research cited in this report, with original sources. None of these figures come from this survey; each is labeled where it appears.

Finding 02	Sophos, The Impact of Compromised Backups on Ransomware Outcomes	94% of organizations hit by ransomware said attackers tried to compromise their backups; organizations with compromised backups paid the ransom 67% of the time, versus 36% where backups held. sophos.com/en-us/blog/the-impact-of-compromised-backups-on-ransomware-outcomes
Rec. 04	Verizon, 2025 Data Breach Investigations Report (DBIR)	Credential abuse is the most common single initial access vector (22%), phishing 16%; the human element is involved in 60% of breaches. verizon.com/business/resources/reports/dbir/
Finding 03	CrowdStrike, 2026 Global Threat Report	Attackers begin lateral movement an average of 29 minutes after initial access, 65% faster than in 2024. crowdstrike.com/en-us/global-threat-report/
Finding 03	Google Mandiant, M-Trends 2025	Organizations take a median of 11 days to detect an intrusion: 10 days when detected internally, 26 days when notified externally. cloud.google.com/blog/topics/threat-intelligence/m-trends-2025/
Rec. 06	ITIC, 2024 Hourly Cost of Downtime Survey	More than 90% of mid-size and large enterprises lose over US$300,000 per hour of downtime; 41% lose US$1 million to US$5 million per hour. itic-corp.com/itic-2024-hourly-cost-of-downtime-report/

Survey data: 1,838 enterprise responses to an online self-assessment (2026), drawn from 3,236 total responses; not a third-party audit. See Research Limitations.

Get a Complete Cyber Resilience Check-up

If your organization sees itself in these findings, the QNAP team can help. Using the eleven controls in this report, we provide a dedicated assessment and tailored recommendations for your environment.



Contact Us

For more information,
contact marketing.tw@qnap.com

QNAP Systems, Inc.
New Taipei City
Email: sales@qnap.com
Tel: +886 2 2641 2000

QNAP Inc. (USA)
Pomona CA
Email: usasales@qnap.com
Tel: +1-909-595-2782

QNAP Inc. (Canada)
Markham, Ontario
Email: canadasales@qnap.com
Tel: +1-905-947-1000

QNAP GmbH (Germany)
Willich
Email: desales@qnap.com
Tel: +49-2154-88428-0

QNAP SRL (Italy)
Roma
Email: eusales@qnap.com
Tel: +39-(0)687-738456

QNAP UK Limited
Swindon
Email: uksales@qnap.com
Tel: +44-(0)333-344-2522

QNAP Japan
Tokyo
Email: jpsales@qnap.com
Tel: +81-3-5901-9735

QNAP Korea
Seoul
Email: krsales@qnap.com