GDPR

WHITE PAPER

QNAP

The new European Regulation on the Protection of Personal Data (GDPR - General Data Protection Regulation): The whole QNAP offering to support Companies during and after the required adaptations to comply with the Regulation.

What is the GDPR?

The GDPR (General Data Protection Regulation) is European Regulation 2016/679 that covers the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This Regulation replaces the European Directive on the protection of personal data (Directive 95/46/EC) adopted in 1995 and will repeal conflicting rules established in the Code on the protection of personal data (Legislative Decree #196/2003). The Regulation was adopted on April 27, 2016 and it will be fully implemented in the EU Countries from May 25, 2018 after a two-year transition period and differently from Directives, no application law is required from the Member States.

The GDPR aims at unifying and standardizing, within the European Union the different rules governing the processing of personal data, definitely determining the ways in which data and information should be stored, protected and made accessible by Companies. The GDPR applies to non-EU Companies if they provide goods or services to individuals residing within the European Union.

It should be underlined that the rules in the GDPR shall be generally applicable and do not foresee specific or different requirements depending on the size, type or sector where the Company operates.

According to the European Commission, personal data is any information on an individual, related both to their private, professional or public life. They may concern any information: names, photos, email addresses, bank details, posts on websites of social networks, medical records or computer IP addresses.

The steps to be performed: from the Record of Processing Activities to the Adaptation Plan to achieve compliance

The main purpose of the GDPR is to ensure that personal data should not be disclosed, should be protected and monitored. The changes introduced by the GDPR, that may involve changes to the way processes are organized, requires companies to carefully plan over a very limited period of time, because the term for adaptation is now very close (about six months).

Companies must set up an Adaptation Plan to comply with the requirements of the GDPR. In this step, the current model of the organization shall be assessed, to define a plan with detailed actions to be implemented in the Company.

The Adaptation Plan, to be implemented following a structured approach, should take into account two important areas in Technology and IT:

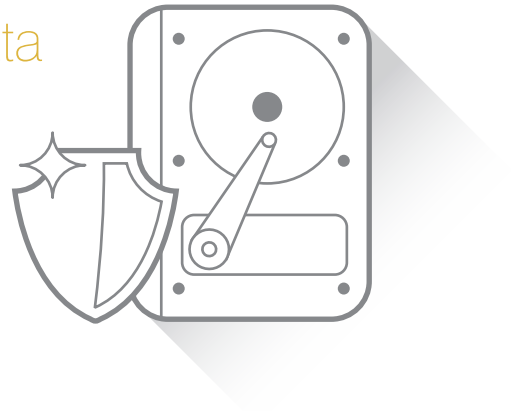
• The area of Processes and Rules. This is undoubtedly one of the areas greatly affected by the adaptation requirements in the GDPR. For example data portability, data breach management, record of processing activities and the rights of data subjects. Privacy by design is another crucial aspect, in other words a new approach required by the GDPR that established the obligation for companies to begin a project, planning from the start the tools to protect personal data.

• The area of Technology and Tools. This is a crucial area, even considering investment to be budgeted in the Adaptation Plan. IT security measures (anti-virus, disaster recovery, firewall, data pseudonymization, data cryptography, data breach prevention and detection, Identity Management, etc.), Physical Security (e.g. Access controls), adoption of IT GRC tools (Governance, Risk & Compliance).

The GDPR establishes a legal framework centered on tasks and accountability of the Data Controller. The new rules require that the Controller ensures compliance with principles established in the Regulation, and also to be able to prove such compliance, adopting a number of tools specified in the GDPR.

How QNAP can help protect your data

QNAP NAS allows you to encrypt all of your data, or individual folders, using AES 256-bit encryption. Other data protection mechanisms include RAID configurations, snapshots, and S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology).



• Flexible RAID configuration

QNAP NAS supports comprehensive RAID types, including RAID 1/5/6/10/50/60, 5+ hot spare, 6+ hot spare and 10+ hot spare. You can enable the most suitable RAID configuration to effectively reduce the risk of data loss caused by unexpected hard disk failure while also maintaining optimal system performance.

• Snapshot protection

Snapshots allow your QNAP NAS to record the state of the system at any time. If an unexpected situation arises on your system, you can revert back to a previous state that the snapshot has recorded. The Storage Manager adds an easy-to-use web-based snapshot tool for you to easily backup and restore data back to any point of time to prevent loss of important data.

• S.M.A.R.T. hard disk health check

S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology) displays the status of hard disks installed in the QNAP NAS, allowing you to take early actions if any of the S.M.A.R.T. values are reported as abnormal and mitigating the risk of data loss caused by physical hard disk failure.

• AES 256-bit encryption of the whole NAS

QNAP NAS supports volume-based encryption to protect sensitive data. A security code and a password are required to mount an encoded volume when starting the QNAP NAS. Not all data can be accessed without the encryption key that protects against unauthorized access and the breach of sensitive data on the QNAP NAS, even if the hard disks and the NAS are stolen. Some NAS models support hardware-accelerated encryption that removes the encoded data from the workload of the CPU, providing faster performance while ensuring secure data protection.

• Encrypting external drives

QNAP NAS can also encrypt external storage devices to protect against unauthorized access. IT staff have the option to encrypt disk volumes on a specific partition of the external device using AES-128, AES-192, or AES-256.

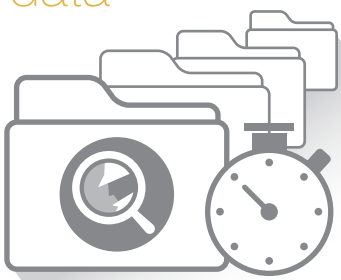
• Military-grade protection

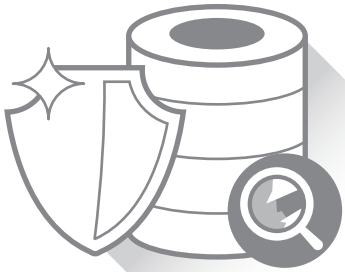
To encrypt internal and external storage units, the military-grade AES 256-bit encryption method is utilized. This method is validated by FIPS 140-2 CAVP (Cryptographic Algorithm Validation Program) and helps to prevent sensitive business data from being accessed if the hard drives or the entire NAS system were stolen.

How QNAP can help manage your data

• Qsirch is a powerful NAS search engine

There many advantages for companies, in particular the possibility to retrieve documents and files to create proposals, reports, contracts and more. Productivity and effectiveness can be greatly increased with Qsirch.

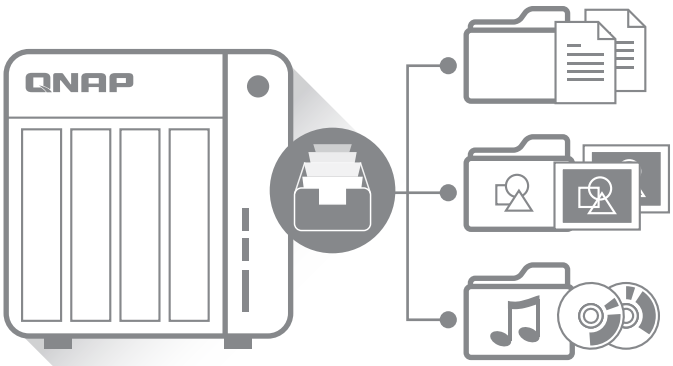




Qsirch works following the access rights for shared folders and user accounts. Qsirch effectively protects the privacy of data and the results of searches only return files that can be accessed by that user. Administrators can easily add and remove specific shared folders for Qsirch. Shared folders can be selectively excluded from indexing to ensure the security of data.

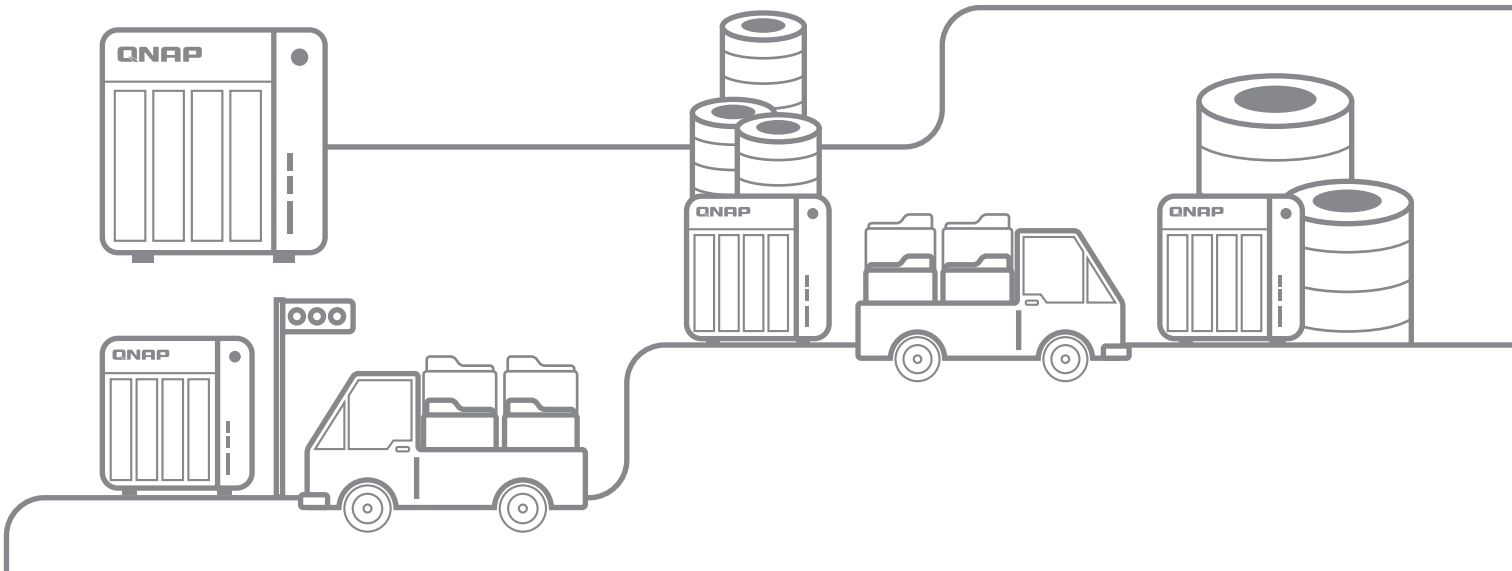
• Qfiling efficiently automates file organization

When the QNAP NAS is used as central file storage, the possibility to efficiently organize files is a key point to manage and use files. However, when faced with a large number of files distributed across many folders, classifying and storing them can become difficult, time consuming and tiring. With Qfiling file organization is automated and efficient.



The main features of Qfiling are:

- Speed ▶ Qfiling can be set up within a few clicks.
- Organization ▶ Files are organized based on user settings.
- Increased productivity ▶ The organization of files is automatic and at regular intervals, without wasting time or effort.
- Optimized management ▶ Keeps files organized for users to easily locate them.



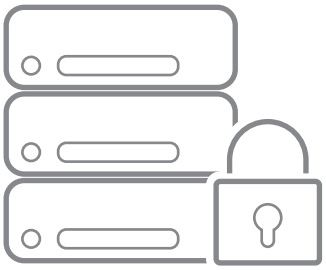
How QNAP can help manage your users

QNAP NAS supports several security features for the system, access to data, and stored files. Encrypted access protects system and communication connections, IP blocking prevents access to suspected users, and the encryption of the external storage devices reduces the risk that data may be misappropriated if hard drives are stolen. Advanced privilege settings such as Windows ACL, Windows Active Directory (AD), and LDAP Directory Service are supported to simplify access control management. Anti-virus solutions are also supported. All these measures make QNAP NAS a safe location for important files.

Network access protection

IT administrators can define a list of unauthorized and authorized connections to allow access to several users to the QNAP NAS using an IP address. It operates as an automatic criteria-based block of IPs, and protects network access. For example, this command can be set as "in 1 minute, after 5 unsuccessful attempts, block the IP for 1 hour, 1 day or forever".
If an IP address is refused, the host can no longer connect to the server, regardless of the connection ports that are used.

Protection in mixed environments

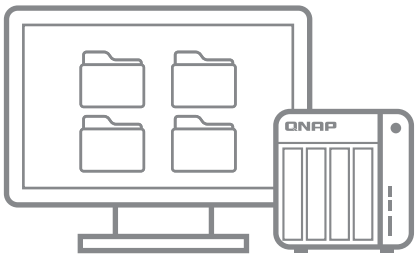


Usually all business users use an appropriate anti-virus. However, it is not possible to forecast the development of viruses and it is not possible to stop the voluntary attempts of users to connect to dangerous Internet sites. Because infected files in a mixed environment may cause substantial damages, it is important to have an anti-virus solution on the QNAP NAS that offers cross-platform file sharing.
Smart detection: The integrated anti-virus solution for QNAP NAS ensures seamless operation of business activities through detection of the latest viruses, malware, worms and Trojans with continuous free updates of the virus database. Virus scans can be customized and set to run on a schedule, with email notifications if a virus is detected.

Better system protection

Usually, a NAS with several LAN ports allows to all enabled network services to access content in the server through each LAN port. Data protection is reduced. In companies, only selected people should be able to access important data using a set network protocol that is an internal IP address. The matching of the QNAP NAS service offers IT administrators the option to allow or block selected services from defined network interfaces to ensure system protection.

Windows ACL permission setting



QNAP NAS supports Windows ACL, allowing you to easily leverage the Windows system's shared folder permission settings and access controls to the NAS. Basic permissions and 13 advanced permissions can be set up from Windows and synchronized to the NAS shared folder permission settings. Sub-folder permissions and file-level privilege settings are also supported. The same permissions can be applied to AFP, FTP, File Station and Samba when Advanced Folder Permissions is enabled to enforce strict access control for higher data security.

Windows Active Directory (AD)

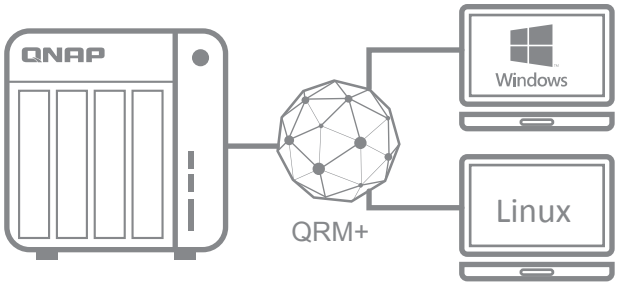
QNAP NAS can be easily joined to the Windows AD for efficient user account management. IT administrators can benefit from centralized access right verification to reduce complex privilege settings while domain users can easily use their Windows AD account name and password to connect to different QNAP NAS on the local network. QNAP NAS supports large-scale AD deployment of up to 200,000 AD users and groups.

LDAP Directory Service

QNAP's LDAP support allows the NAS to be added to LDAP-based directory services, such as OpenLDAP. Users are then centrally authenticated by the LDAP server, and can use the same LDAP account name and password to access any QNAP NAS that has been added the LDAP server. With a built-in and easy-to-use LDAP Server, the QNAP NAS can also be used as a LDAP server to centrally authenticate users and groups for all the other LDAP-enabled devices and applications to save on management effort while also enhancing data security.

How QNAP can help manage your systems

QNAP QRM+ (QNAP Remote Manager Plus) and Q'center are centralized, single-interface management solutions for IT teams to centrally detect, map, monitor and manage networked devices such as PCs, servers, thin clients and QNAP NAS. The QNAP NAS also provides web-based display logs for efficient tracking and can be used as a Syslog server to centrally store system logs for all networked devices.

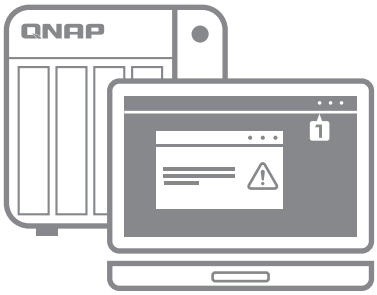


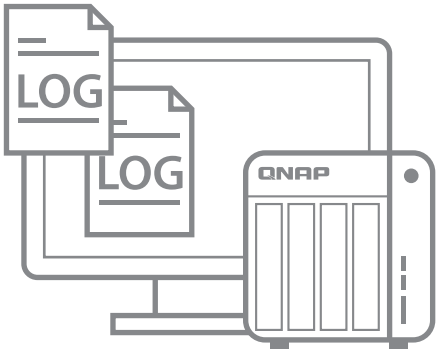
QRM+: Centralized monitoring and management of networked devices

QRM+ can create a list of connected devices for administrators to quickly monitor their status - including IPMI-compatible devices. QRM+ can be used for real-time monitoring, to assess device status (including temperature, fan speed, sensors, power supply, and IPMI event notifications) of each end-point whenever necessary. With QRM+, remotely managing IT devices is secure, fast and easy.

Alerts and notifications: Receive alerts in advance before a disaster occurs

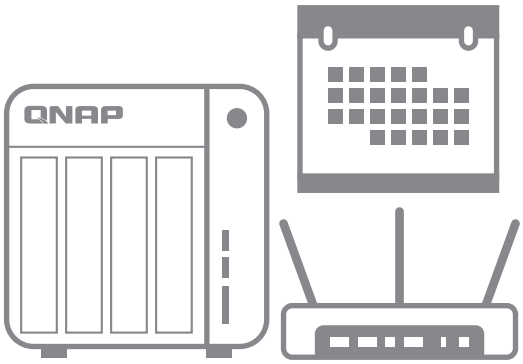
QRM+ has alerts to assist IT staff in correcting performance issues before users, applications, and the company are affected.





Comprehensive log system

QNAP NAS assists IT administrators in effective system tracking by providing web-based display logs: the system event logs keep IT administrators aware of the information, warning, and error events of the QNAP NAS; the system connection logs enable IT administrators to view the access history of each file (who, when, and what actions were performed). In addition, an online user list is available for monitoring user access. If a suspicious connection is detected, administrators can right click on the user to immediately add them to the block list or the disconnect list.



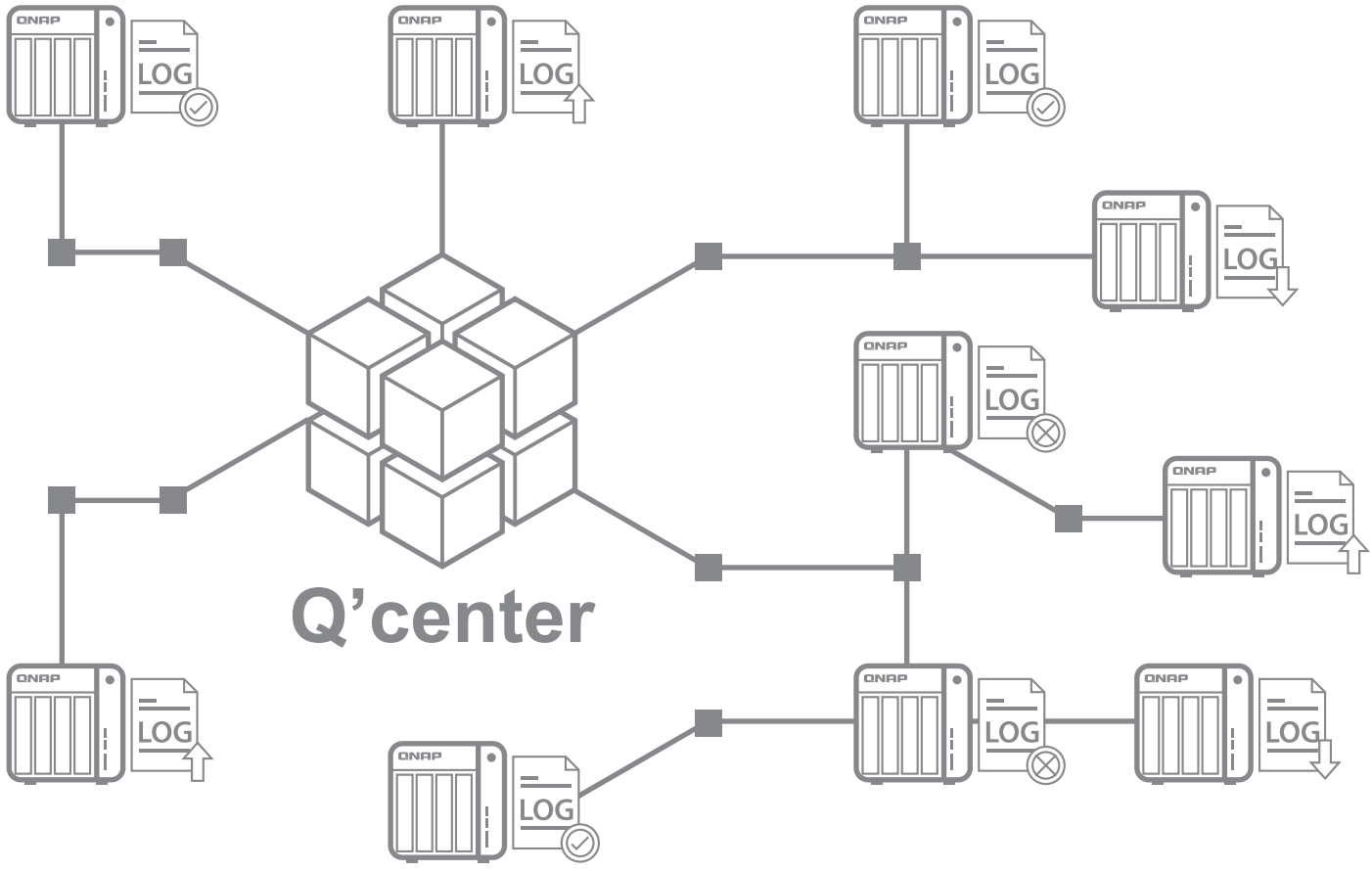
QNAP NAS as a Syslog server

A central repository of log data from various network devices allows efficient management and security auditing in businesses. By supporting UDP and TCP protocols, QNAP NAS can serve as a Syslog server, allowing IT administrators to easily collect and store logs from other networked devices to QNAP NAS to improve efficiency on management and troubleshooting when necessary. Advanced filters and email notifications are provided to help quickly identify failures or security threats.

Besides playing the role as a server for collecting logs from other devices, QNAP NAS can also act as a client to send its own logs to the Syslog server.

Q’center: Centrally monitor and manage all your NAS

Q’center can mutually manage and monitor several client NAS, fulfilling needs for central management and segment control targets at the same time. Information such as system temperatures and fan speeds allows you to reduce system failure risks by using control room conditions. You can also power on/off multiple NAS at once with preset power options to enhance the accessibility and efficiency of your NAS. Q’center also allows central monitoring of system logs and can handle firmware updates and maintenance of all QNAP NAS with minimal effort.

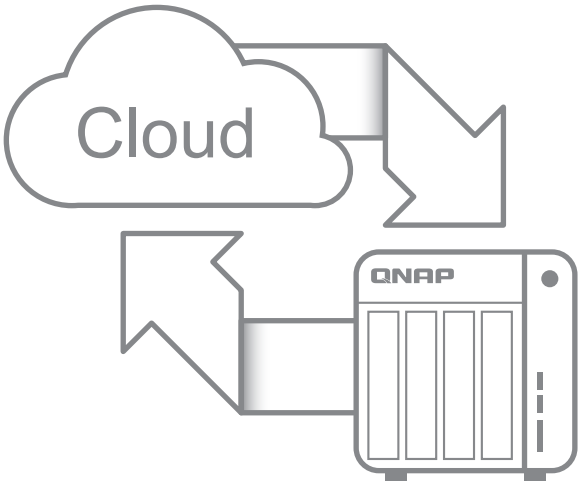


QNAP NAS: An efficient disaster recovery solution

QNAP NAS supports several methods to backup, sync, and recover data.

Hybrid backup sync

QNAP Hybrid Backup Sync consolidates backup, restoration and synchronization functions into a single application for users to easily transfer data to local, remote and cloud storage spaces using RTRR (Real-Time Remote Replication), rsync, FTP, and CIFS/SMB.



Cloud Backup:

QNAP NAS offers cloud backup solutions that are secure, easy to use and packed with features to backup data on the storage services available from enterprise-class public clouds such as Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, Dropbox* and IBM SoftLayer. Even private storage cloud solutions compatible with OpenStack Swift and WebDAV are supported.

When designing an Adaptation Plan for the GDPR, companies may choose to comply only with the requirements of current regulation or to change this into an opportunity to create value for their organization, thus contributing to spreading a new culture on personal data processing and create a real digital transformation of company processes managing client and employee data.

IT criminals are constantly searching weak points and are continuously developing more targeted attacks. Sustainable security solutions should evolve and adapt following frequent updates and using information on threats as soon as available. Security is only useful if it detects threats, triggers a reaction and guarantees global protection for the whole structure, from endpoints to networks and hybrid cloud.