GDPR

WHITE PAPER

QNAP

Il nuovo Regolamento Europeo sulla Protezione dei Dati (GDPR): L’offerta QNAP completa per supportare le imprese durante e dopo il piano di adeguamento al Regolamento.

GDPR: di cosa si tratta

GDPR (General Data Protection Regulation) è il Regolamento europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati: tale Regolamento andrà a sostituire la Direttiva Europea sulla protezione dei dati (Direttiva 95/46/EC) istituita nel 1995 e abrogherà le norme del Codice per la protezione dei dati personali (D.lgs. n.196/2003) che risulteranno con esso incompatibili. Il Regolamento è stato adottato il 27 aprile 2016 e diverrà pienamente operativo nei paesi UE a partire dal 25 maggio 2018 dopo un periodo di transizione di due anni e, a differenza di una Direttiva, non richiede alcuna forma di legislazione applicativa da parte degli stati membri.

Il GDPR si pone l'obiettivo di uniformare e normalizzare, nell'ambito dell'Unione Europea, le diverse norme che regolano il trattamento dei dati personali, disciplinando in via definitiva le modalità con cui i dati e le informazioni dovranno essere archiviate, protette e rese accessibili da parte delle aziende: si applica anche ad aziende extra-UE che forniscano beni o servizi a residenti nell'Unione Europea.

E' importante sottolineare come le norme del GDPR abbiano una valenza generale e non prevedano obblighi specifici o differenziati per dimensioni, tipologia o settore di attività dell'azienda.

Secondo la Commissione Europea "i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica. Può riguardare qualunque cosa: nomi, foto, indirizzi email, dettagli bancari, interventi su siti web di social network, informazioni mediche o indirizzi IP di computer."

I passi da compiere: dal registro delle attività di trattamento al piano di adeguamento

L'obiettivo principale del GDPR è di garantire che i dati personali non siano divulgati, siano protetti e costantemente monitorati: le novità del GDPR, che possono comportare modifiche organizzative significative e investimenti di natura tecnologica, impongono alle aziende un'attenta pianificazione in tempi molto stretti, dato che il termine entro il quale potersi adeguare è ormai prossimo (circa sei mesi).

Le aziende devono predisporre un Piano di adeguamento al GDPR. Questa fase prevede l'assessment del modello attuale dell'organizzazione, al fine di definire un piano di azioni opportunamente dettagliate e calate sulla realtà aziendale.

Tale Piano di adeguamento, da realizzare con un approccio strutturato, dovrebbe considerare sicuramente due importanti aree in ambito tecnologico e informatico:

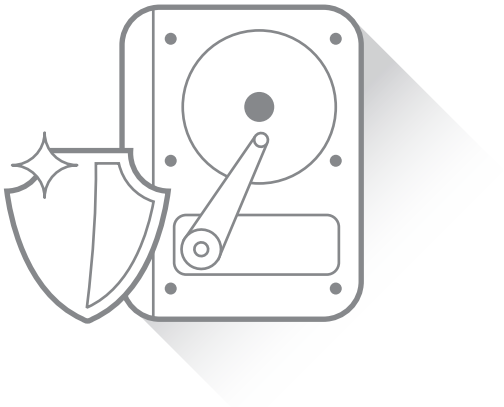
• L'area dei processi e delle regole. È senza dubbio una delle aree maggiormente coinvolte nelle richieste di adeguamento del GDPR: basti ricordare la portabilità dei dati, la gestione dei data breach, del registro dei trattamenti e dei diritti degli interessati. Molto importante la Privacy by design, ovvero un nuovo approccio richiesto dal GDPR che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti a tutela dei dati personali.

• L'area della tecnologia e degli strumenti. Area di cruciale importanza, anche dal punto di vista degli investimenti da prevedere nel piano di adeguamento: misure di sicurezza informatica (antivirus, disaster recovery, firewall, pseudonimizzazione dati, cifratura dati, prevenzione e rilevazione data breach, Identity Management, ecc.), di sicurezza fisica (es. controllo accessi), di adozione di tool IT GRC (Governance, Risk & Compliance).

Il GDPR istituisce un quadro normativo tutto incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di "accountability"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti, ma anche di essere in grado di comprovarlo, adottando una serie di strumenti che lo stesso GDPR indica.

Come QNAP protegge i tuoi dati

Grazie alla funzione di codifica dei dati su QNAP NAS consente di codificare i volumi disco su NAS con codifica AES a 256-bit. I volumi codificati possono solo essere usati per il normale accesso lettura/scrittura con una password autorizzata. La codifica protegge i dati confidenziali da accessi non autorizzati anche quando vengono rubati i dischi rigidi o l'intero NAS.



• Crittografia AES 256-bit per unità interna

Turbo NAS supporta crittografia su base volume per proteggere i dati sensibili.Un codice di sicurezza o la password sono necessari per montare un volume crittografato all'avvio di Turbo NAS. Non è possibile accedere a tutti i dati senza la chiave crittografica, la quale impedisce l'accesso non autorizzato e la violazione dei dati sensibili di Turbo NAS anche se i dischi rigidi o il dispositivo vengono rubati. Alcuni modelli NAS inoltre supportano il motore di crittografia hardware AES-NI che scarica efficacemente i dati crittografati dal carico della CPU, per una protezione dei dati più rapida, economica e sicura.

• Crittografia dell'unità USB/eSATA esterna

Una unità esterna collegata a Turbo NAS significa rimozione rapida.È necessario proteggere dati importanti dell'unità da furto.Turbo NAS supporta ora la crittografia dei dischi rigidi USB/eSATA per evitare l'accesso non autorizzato ai contenuti in caso di perdita o furto. L'amministratore IT può scegliere se crittografare un volume del disco o una partizione specifica dell'unità esterna condiversi livelli di crittografia: AES-128, AES-192, AES-256.

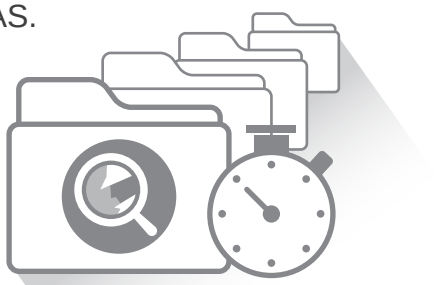
• Protezione di livello militare

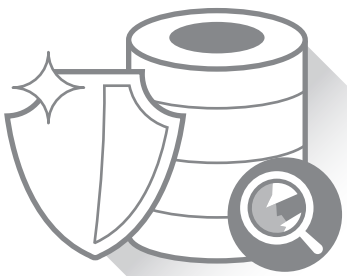
Per la crittografia del disco rigido interno ed esterno è stata adottata automaticamente una crittografia di livello militare FIPS 140-2, che è considerata la certificazione più elevata per la conformità.

Come QNAP gestisce i tuoi dati

• Qsirch - Qsirch è un potente motore di ricerca nel NAS.

Per le aziende, i benefici sono molteplici, in particolare la possibilità di trovare i documenti e i file desiderati per creare proposte, report, contratti e molto altro. Qsirch permette di aumentare immediatamente la produttività e l'efficienza lavorativa.

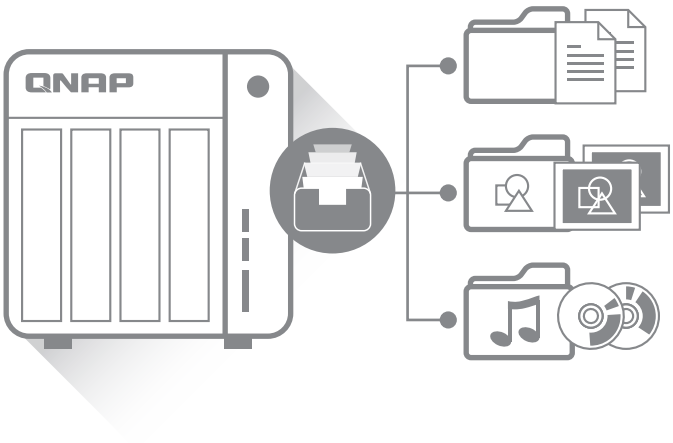




Qsirch opera in linea con le autorizzazioni di cartelle condivise e account utente del QTS. Protegge efficacemente la privacy dei dati e i risultati della ricerca restituiscono solo i file autorizzati per ogni utente. Gli amministratori possono aggiungere e rimuovere le cartelle condivise specifiche per Qsirch. Esclude in modo flessibile le cartelle condivise da indicizzazione per garantire la sicurezza dei dati.

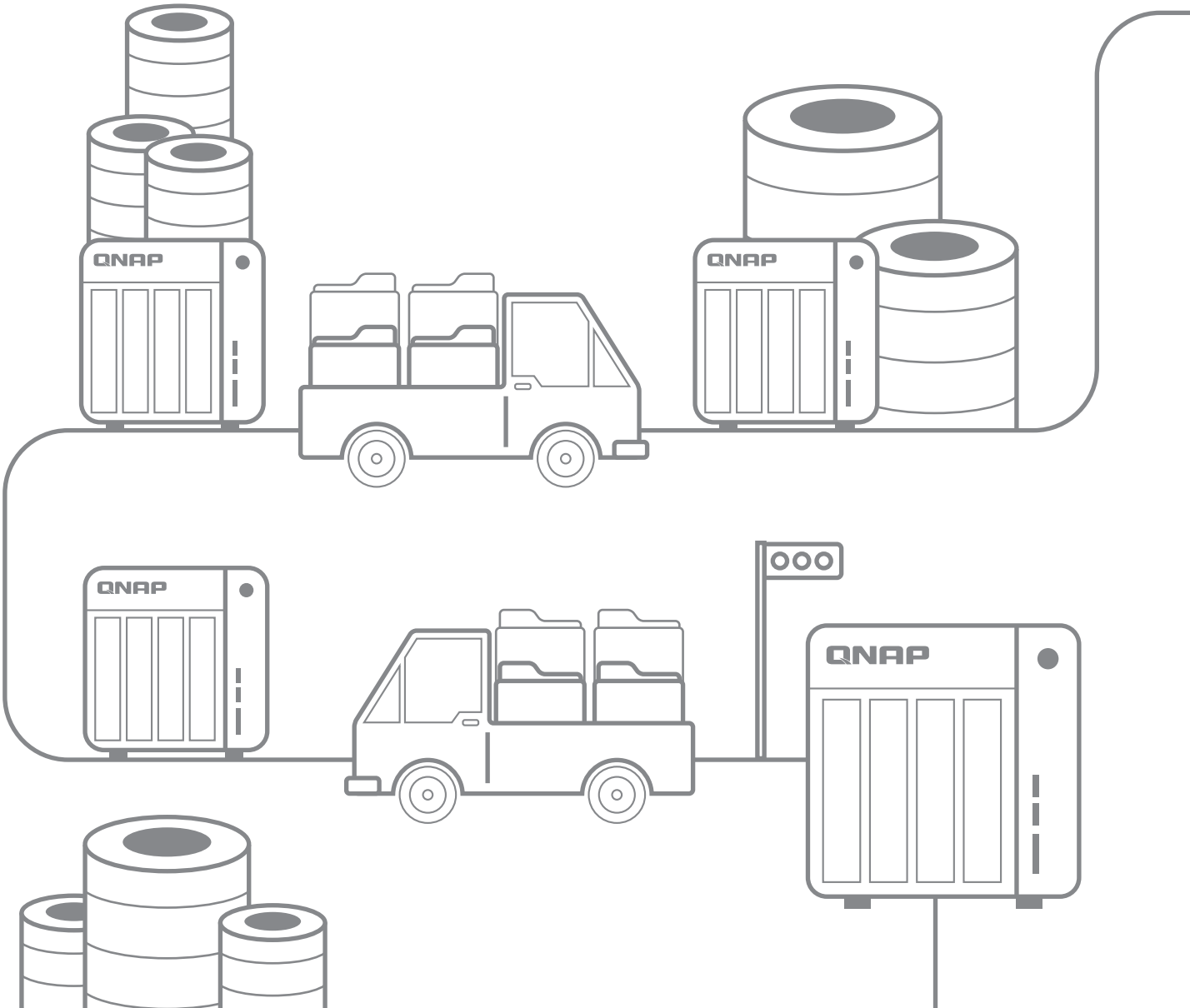
• Qfiling - Qfiling automatizza l'organizzazione dei file in modo efficiente

Quando si usa QNAP NAS come archivio file centrale, la possibilità di organizzare i file in modo efficiente è un principio fondamentale per gestire e usare file ogni giorno. Tuttavia, di fronte a un numero elevato di file distribuiti su più cartelle, diventa sempre più difficile, dispendioso in termini di tempo e stancante classificarli e archiviarli. Adesso, con Qfiling l'organizzazione dei file è automatica ed efficiente.



Le caratteristiche principali di Qfiling sono:

- Velocità ▶ Completare tutte le impostazioni con pochi clic.. Veloce e semplice
- Organizzazione ▶ I file sono ben organizzati e archiviati in base alle impostazioni
- Produttività aumentata ▶ L'organizzazione dei file diventa automatica e periodica senza altro tempo o impegno.
- Gestione ottimizzata ▶ Mantenere i file organizzati semplifica l'individuazione dei file necessari e ottenere il massimo da ogni file.



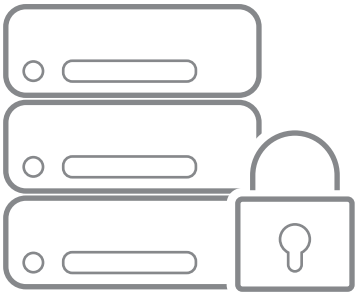
Come QNAP gestisce i tuoi utenti

QNAP Turbo NAS supporta numerose funzioni per fornire la sicurezza per il sistema, l'accesso ai dati e ai file archiviati. L'accesso crittografato protegge le connessioni di sistema e le comunicazioni, il blocco di IP impedisce l'ingresso di utenti sospetti e la crittografia dell'unità esterna riduce il rischio di appropriazione dei dati in caso di furto dei dischi rigidi. Inoltre, è supportato il rilevamento degli ultimi virus. Tutte queste misure sono volte a rendere Turbo NAS un luogo sicuro per i file importanti.

Protezione di accesso alla rete

Gli amministratori IT possono impostare l'elenco di connessioni non consentite o consentite per autorizzare l'accesso adeguato da parte di diversi utenti a Turbo NAS tramite indirizzo IP. Funziona come un blocco degli IP automatico basato su criteri, consentendo il comando di protezione di accesso alla rete. Ad esempio, il comando può essere impostato con "fra 1 minuto, dopo 5 tentativi non riusciti, bloccare l'IP per 1 ora, 1 giorno o sempre".
Una volta che un indirizzo IP viene rifiutato, per l'host non sarà più possibile connettersi al server, indipendentemente dalle porte di connessione che utilizza.

Protegge i dati in ambienti misti



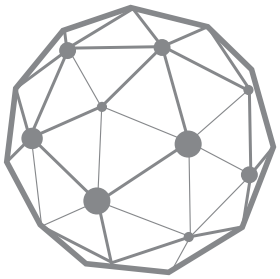
In genere, tutti gli utenti aziendali installano in tempo reale un software antivirus adeguato. Tuttavia, i virus si sviluppano al di là di ogni previsione e i tentativi intenzionali degli utenti di connessione a siti Internet pericolosi sono difficili da evitare. Poiché i file infetti da virus in un ambiente misto possono causare danni rilevanti, è essenziale disporre di una soluzione antivirus su Turbo NAS che fornisce condivisione dei file cross-platform.
Rilevamento intelligente: La soluzione antivirus integrata per Turbo NAS assicura la continuità aziendale tramite il rilevamento dei virus, malware, worm e Trojan più recenti con continui aggiornamenti gratuiti del database dei virus. Oltre alle varie attività di scansione con selezione della cartella personalizzata e la scansione programmata, viene fornito un avviso tramite e-mail al termine dell'attività o al rilevamento dei virus.

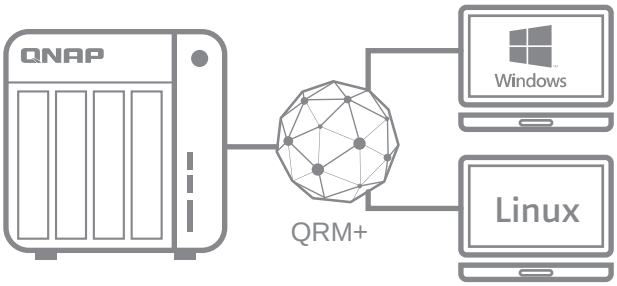
Protezione di sistema migliorata

Di solito, un NAS con varie porte LAN consente tutti i servizi di rete abilitati per accedere ai contenuti del server attraverso ciascuna porta LAN. Ciò riduce la protezione dei dati. Nelle aziende, i dati importanti devono essere accessibili solo ad alcune persone tramite protocollo di rete predefinito, ovvero, un indirizzo IP interno. Il supporto dell'associazione del servizio Turbo NAS offre agli amministratori IT la flessibilità per consentire o bloccare servizi specifici dalle interfacce di rete designate per garantire la protezione del sistema.

Come QNAP gestisce il tuo Sistema

QRM+ (QNAP Remote Manager Plus), è la soluzione di gestione remota centralizzata di QNAP studiata per i team IT di tutti i settori che si affidano a dispositivi computerizzati connessi in rete. Fornisce una soluzione single-point per rilevare, mappare, monitorare e gestire tutti i dispositivi cruciali, quali server/PC/Thin Client, ecc. nella rete. QRM+ contribuisce a gestire con facilità la propria infrastruttura IT, attraverso un'interfaccia singola e nel giro di pochi istanti.

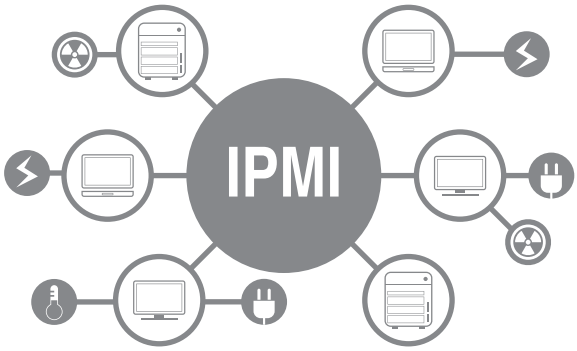


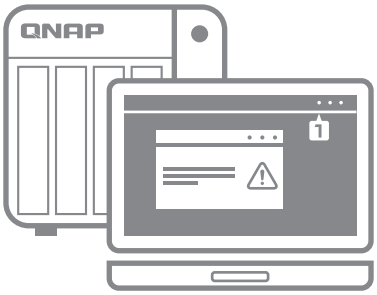


QRM+ può generare un elenco dei dispositvi IT collegati consentendo agli amministratori IT di monitorare rapidamente ciascun dispositivo collegato e garantendo l'integrità di tutti i dispostivi. QRM+ inoltre consente il monitoraggio in tempo reale, in modo da poter verificare lo stato di ciascun end-point tutte le volte che è necessario. Con QRM+, la gestione remota dei dispositivi IT è sicura, rapida e semplice.

Monitorare tutti i parametri di server cruciali tramite IPMI

QRM+, una delle poche soluzioni disponibili sul mercato per la gestione centralizzata di dispositivi compatibili IPMI, fornisce una soluzione come punto singolo per il rilevamento, la mappatura, il monitoraggio e la gestione di tutti i dispositivi IPMI nella rete. QRM+ supporta IPMI 2.0, che consente la gestione dei propri dispositivi compatibili IPMI , a prescindere e dallo stato del sistema operativo. Contribuisce a monitorare i sensori di sistema cruciali, quali i sensori di temperatura, velocità delle ventole, sensori di tensione, stato di alimentazione e notifiche di evento IPMI.





Avvisi e notifiche: Ricevere in anticipo gli avvisi prima che avvenga il disastro

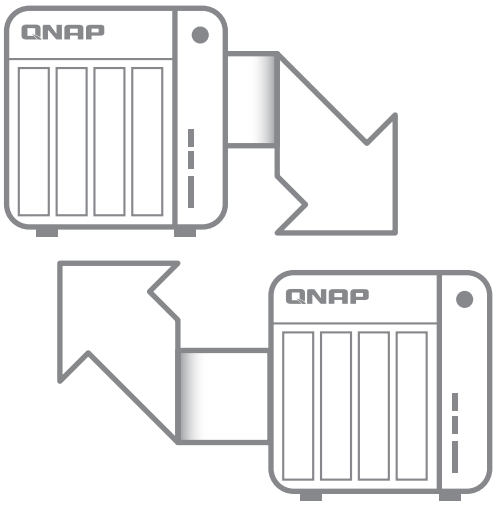
QRM+ offre avvisi per correggere problemi di prestazione prima che interessino utenti, applicazioni e l'azienda, consentendo di fruire di maggiore produttività, migliore collaborazione e recupero più veloce da tempi di inattività dei dispositivi o prestazioni del sistema.

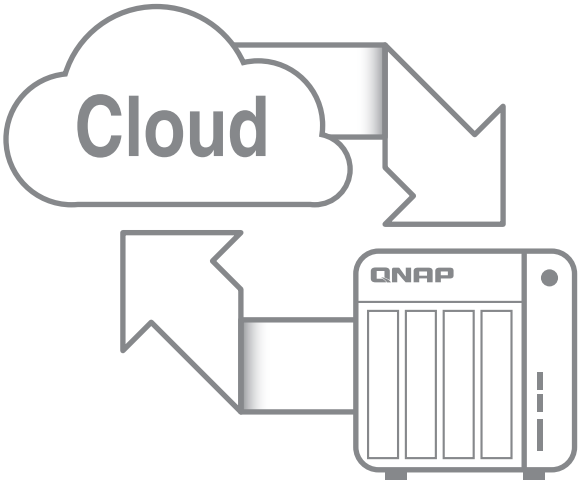
QNAP: una soluzione efficiente in caso di disaster recovery

In caso di perdita dei dati, Turbo NAS supporta diversi metodi di conservazione della copia per il recupero dei dati.

RTRR o rsync:

È possibile effettuare il backup dei dati di Turbo NAS su un altro Turbo NAS remoto o server FTP in tempo reale tramite il servizio RTRR (Real-Time Remote Replication) di QNAP od un server rsync standard schedulata tramite protocollo rsync.
Grazie a RTRR, il Turbo NAS sorgente monitora i file, inclusi i file nelle cartelle di backup Time Machine e Qsync, e sincronizza le modifiche sul server di destinazione. Gli amministratori IT possono effettuare attività di backup immediato e programmato.





Backup Cloud:

QTS offre soluzioni di backup su cloud sicure, facili da usare e ricche di funzioni che consentono di eseguire il backup dei dati su vari servizi di archiviazionei su cloud pubblici di classe aziendale, fra cui Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, Dropbox* e IBM SoftLayer. Supporta anche soluzioni di archiviazione su cloud private compatibili con OpenStack Swift e WebDAV. QTS è il gateway di archiviazione cloud che consente di creare piani di recupero semplici e accessibili oltre alla conservazione dei dati senza problemi a scopo normativo e di archiviazione.

In conclusione, nel disegnare il proprio piano di adeguamento al GDPR, le aziende possono scegliere se semplicemente lavorare per adempiere alla nuova normativa in senso stretto o sfruttare l'opportunità per creare valore per l'organizzazione nel suo complesso, contribuendo a diffondere una nuova cultura in materia di trattamento dei dati personali e a realizzare una vera e propria "digital transformation" dei processi aziendali che gestiscono i dati dei clienti e dei dipendenti.

I criminali informatici sono alla costante ricerca di punti deboli e sviluppano incessantemente attacchi sempre più mirati. Soluzioni di sicurezza sostenibili devono evolversi e adattarsi aggiornandosi di frequente e sfruttando le informazioni sulle minacce non appena queste si rendono disponibili. La sicurezza è veramente all'avanguardia solo se consente il rilevamento delle minacce, innesca una reazione e garantisce la protezione globale per l'intera struttura, dagli endpoint fino alle reti e al cloud ibrido.