RGPD

DOCUMENTO TÉCNICO

Novo regulamento europeu sobre a proteção de dados pessoais (Regulamento Geral de Proteção de Dados - RGPD): todas as ofertas da QNAP para apoiar as empresas durante e após as adaptações necessárias para cumprir o regulamento.

O que é o RGPD?

O RGPD (Regulamento Geral de Proteção de Dados) é o Regulamento Europeu 2016/679 trata sobre a proteção das pessoas no que diz respeito ao processamento de dados pessoais e à livre circulação desses dados. Esse regulamento substitui a Diretiva Europeia sobre a proteção de dados pessoais (Diretiva 95/46/CE) adotada em 1995 e revogará regras conflitantes estabelecidas no Código de proteção de dados pessoais (Decreto Legislativo 196/2003). O regulamento foi adotado em 27 de abril de 2016 e será totalmente implementado nos países da UE a partir de 25 de maio de 2018, após um período de transição de dois anos e, ao contrário das Diretivas, nenhuma lei de aplicação é exigida dos países-membros.

O RGPD visa unificar e padronizar na União Europeia as diferentes regras que regem o processamento de dados pessoais, determinando definitivamente as maneiras como dados e informações devem ser armazenados, protegidos e disponibilizados pelas Empresas. O RGPD aplica-se a empresas não pertencentes à UE se elas fornecerem produtos ou serviços a pessoas que residem na União Europeia.

Convém salientar que as regras do RGPD serão aplicáveis de maneira geral e não preveem requisitos específicos ou diferentes dependendo do tamanho, do tipo ou do setor em que a Empresa atua.

De acordo com a Comissão Europeia, dados pessoais são qualquer informação sobre uma pessoa relacionada à sua vida privada, profissional ou pública. Eles podem representar qualquer informação: nomes, fotos, endereços de e-mail, dados bancários, publicações em sites de redes sociais, registros médicos ou endereços IP de computadores.

Medidas a serem tomadas: do registro das atividades de processamento ao plano de adaptação para estar em conformidade

A principal finalidade do RGPD é garantir que os dados pessoais não sejam divulgados e que sejam protegidos e monitorados. As alterações introduzidas pelo RGPD, que podem incluir alterações na forma como os processos são organizados, obrigam as empresas a realizar um planejamento cuidadoso durante um período muito limitado de tempo, pois o prazo de adaptação está muito perto de ser atingido (cerca de seis meses).

As empresas devem criar um plano de adaptação para cumprir os requisitos do RGPD. Nesta etapa, o modelo atual da organização deve ser avaliado a fim de definir um plano que detalhe as medidas a serem implementadas na empresa.

O plano de adaptação a ser implementado de acordo com uma abordagem estruturada deve levar em conta duas importantes áreas de tecnologia e TI:

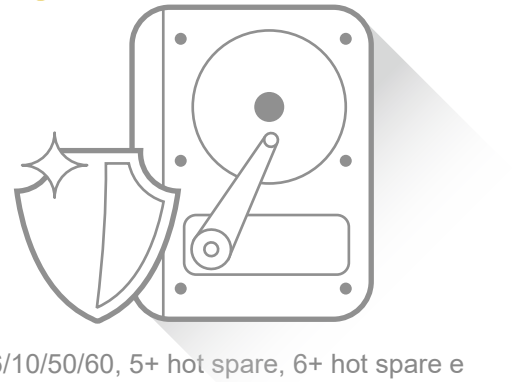
• A área de processos e regras. Esta é, sem dúvida, uma das áreas mais afetadas pelas exigências de adaptação do RGPD. Por exemplo, portabilidade de dados, gerenciamento de violação de dados, registro de atividades de processamento e os direitos dos titulares dos dados. A privacidade por natureza é outro aspecto fundamental; em outras palavras, uma nova abordagem exigida pelo RGPD que impôs às empresas a obrigação de iniciar um projeto, planejamento desde o início as ferramentas para proteger os dados pessoais.

• A área de tecnologia e ferramentas. Esta é uma área fundamental, mesmo considerando o investimento a ser estimado no plano de adaptação. Medidas de segurança de TI (antivírus, recuperação de desastres, firewall, pseudonimização de dados, criptografia de dados, prevenção e detecção de violação de dados, gerenciamento de identidade etc.), segurança física (por exemplo, controles de acesso), a adoção de ferramentas de GRC (governança, risco e conformidade).

O RGPD estabelece um quadro jurídico centrado em tarefas e na responsabilidade do controlador de dados. As novas regras exigem que o controlador garanta a conformidade com os princípios estabelecidos no regulamento e também que seja capaz de comprovar tal conformidade, adotando uma série de ferramentas especificadas no RGPD.

Como a QNAP pode ajudar a proteger seus dados

O QNAP NAS permite criptografar todos os seus dados ou pastas específicas com a criptografia AES de 256 bits. Outros mecanismos de proteção de dados incluem configurações de RAID, instantâneos e o S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology ou tecnologia de monitoramento automático, análise e relatório).



• Configuração de RAID flexível

O QNAP NAS suporta tipos de RAID abrangentes, incluindo RAID 1/5/6/10/50/60, 5+ hot spare, 6+ hot spare e 10+ hot spare. Você pode ativar a configuração de RAID mais adequada para reduzir efetivamente o risco de perda de dados provocada por falhas inesperadas no disco rígido, além de manter um desempenho ideal do sistema.

• Proteção com instantâneos

Os instantâneos permitem que o seu QNAP NAS registre o estado do sistema a qualquer momento. Se um problema inesperado ocorrer no sistema, você pode reverter para um estado anterior registrado pelo instantâneo. O Gerenciador de Armazenamento adiciona uma ferramenta de instantâneo on-line fácil de usar para que você possa facilmente fazer backup e restaurar dados para qualquer ponto no tempo a fim de evitar a perda de dados importantes.

• Verificação da integridade de discos rígidos S.M.A.R.T.

O S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology ou tecnologia de monitoramento automático, análise e relatório) exibe o status dos discos rígidos instalados no QNAP NAS, permitindo que você tome medidas imediatas se qualquer um dos valores S.M.A.R.T. forem indicados como anormais, além de reduzir o risco de perda de dados causada por falhas no disco rígido físico.

• Criptografia AES de 256 bits de todo o NAS

O QNAP NAS suporta criptografia de volume para proteger dados confidenciais. Um código de segurança e uma senha são necessários para montar um volume codificado ao iniciar o QNAP NAS. Nem todos os dados podem ser acessados sem a chave de criptografia que protege contra o acesso não autorizado e a violação de dados confidenciais no QNAP NAS, mesmo se os discos rígidos e o NAS forem roubados. Alguns modelos de NAS suportam a criptografia acelerada por hardware que remove os dados codificados da carga de trabalho da CPU, proporcionando um desempenho mais rápido e garantindo a proteção dos dados.

• Criptografia de unidades externas

O QNAP NAS também pode criptografar dispositivos de armazenamento externos para proteger contra o acesso não autorizado. A equipe de TI tem a opção de criptografar os volumes de disco em uma partição específica do dispositivo externo usando criptografia AES-128, AES-192 e AES-256.

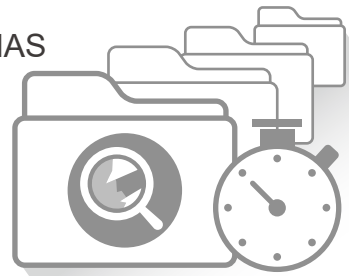
• Proteção de nível militar

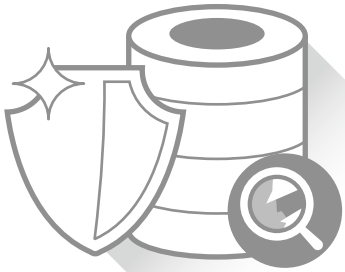
Para criptografar unidades de armazenamento internas e externas, o método de criptografia AES de 256 bits de nível militar é utilizado. Esse método é validado pelo CAVP (programa de validação de algoritmo criptográfico) do FIPS 140-2 e ajuda a evitar que dados confidenciais sejam acessados se os discos rígidos ou todo o sistema NAS for roubado.

Como a QNAP pode ajudar a gerenciar seus dados

• O Qsirch é um avançado mecanismo de pesquisa no NAS

Há muitas vantagens para as empresas, particularmente a possibilidade de recuperar documentos e arquivos para criar propostas, relatórios, contratos e muito mais. É possível aumentar consideravelmente a produtividade e a eficácia com o Qsirch.

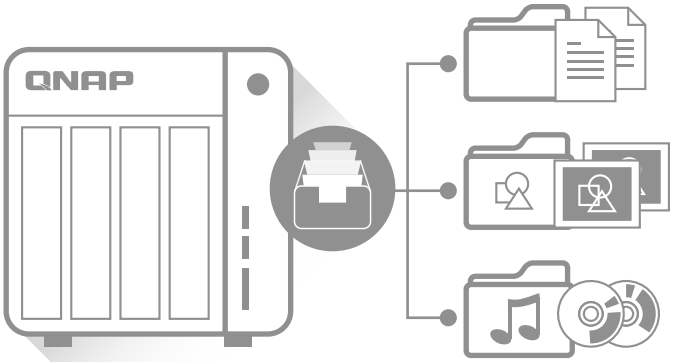




O Qsirch funciona monitorando os direitos de acesso a pastas compartilhadas e contas de usuário. O Qsirch protege a privacidade dos dados, e os resultados de pesquisa retornam apenas os arquivos que podem ser acessados pelo usuário. Os administradores podem facilmente adicionar e remover pastas específicas do Qsirch. As pastas compartilhadas podem ser excluídas seletivamente do processo de indexação para garantir a segurança dos dados.

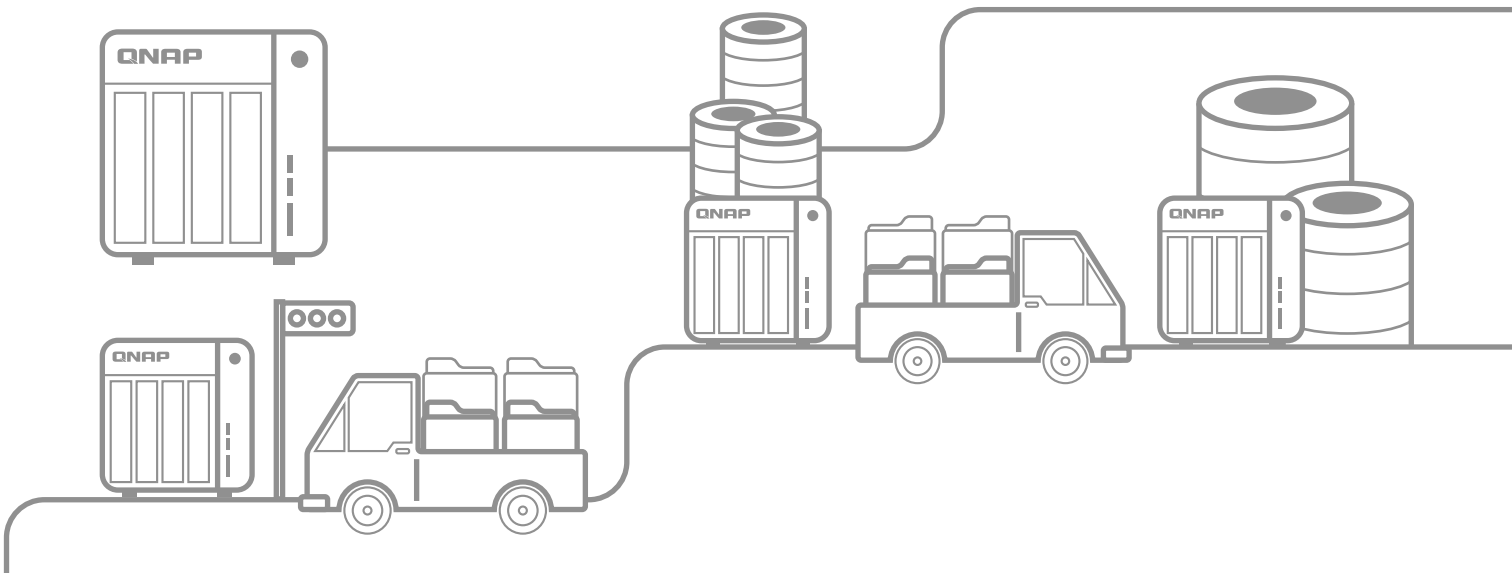
• O Qfiling automatiza a organização dos arquivos com eficiência

Quando o QNAP NAS é utilizado como armazenamento central de arquivos, a possibilidade de organizar os arquivos de forma eficiente é ideal para gerenciar e usar os arquivos. No entanto, quando há um grande número de arquivos distribuídos em várias pastas, a classificação e o armazenamento desses arquivos pode se tornar um processo difícil, demorado e cansativo. Com o Qfiling, a organização de arquivos é automatizada e eficiente.



Principais recursos do Qfiling:

- Velocidade ▶ O Qfiling pode ser configurado em poucos cliques.
- Organização ▶ Os arquivos são organizados com base nas configurações do usuário.
- Aumento da produtividade ▶ A organização de arquivos é automática e ocorre em intervalos regulares, sem perda de tempo ou esforço.
- Gerenciamento otimizado ▶ Mantém os arquivos organizados para que os usuários possam localizá-los com facilidade.



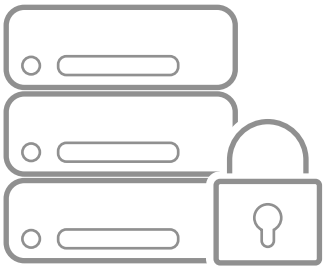
Como a QNAP pode ajudar a gerenciar seus usuários

O QNAP NAS suporta vários recursos de segurança para o sistema, o acesso aos dados e os arquivos armazenados. O acesso criptografado protege o sistema e as conexões de comunicação, o bloqueio de IPs impede o acesso de usuários suspeitos e a criptografia de dispositivos de armazenamento externos reduz o risco de extravio de dados caso os discos rígidos sejam roubados. Configurações avançadas de privilégio, como ACLs do Windows, Windows Active Directory (AD) e o serviço de diretório LDAP são suportados para simplificar o gerenciamento de controle de acesso. Soluções antivírus também são suportadas. Todas essas medidas tornam o QNAP NAS um local seguro para arquivos importantes.

Proteção de acesso à rede

Os administradores de TI podem definir uma lista de conexões não autorizadas e autorizadas para permitir o acesso de vários usuários ao QNAP NAS usando um endereço IP. Ele funciona como um bloqueio de IPs baseado em critérios automáticos e protege o acesso à rede. Por exemplo, esse comando pode ser definido como "em 1 minuto, depois de 5 tentativas malsucedidas, bloquear o IP por 1 hora, 1 dia ou para sempre".
Se um endereço IP for recusado, o host não poderá mais se conectar ao servidor, independentemente das portas de conexão que usadas.

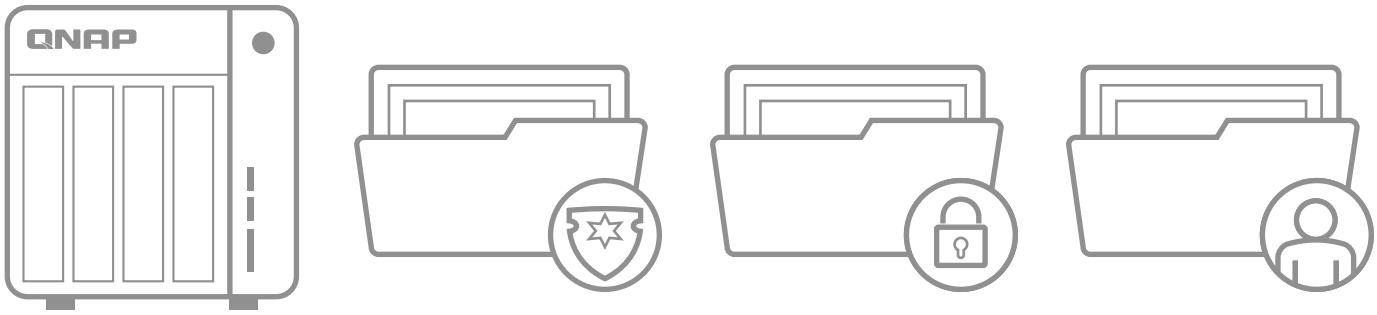
Proteção em ambientes mistos



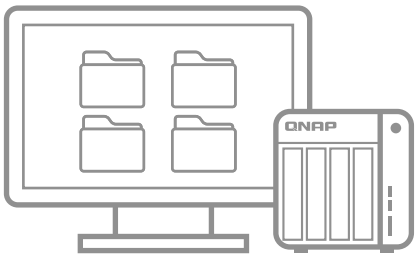
Normalmente todos os usuários corporativos usam um antivírus. No entanto, não é possível prever o desenvolvimento dos vírus nem impedir tentativas deliberadas dos usuários de conectar-se a sites perigosos. Como os arquivos infectados em um ambiente misto podem causar danos consideráveis, é importante ter uma solução de antivírus no QNAP NAS que ofereça compartilhamento de arquivos entre plataformas.
Detecção inteligente: A solução de antivírus integrada do QNAP NAS garante a operação contínua das atividades empresariais através da detecção dos mais recentes vírus, malwares, worms e cavalos de Troia com atualizações regulares gratuitas do banco de dados de vírus. As varreduras de vírus podem ser personalizadas e configuradas para seguir uma programação específica, com notificações por e-mail caso um vírus seja detectado.

Melhor proteção do sistema

Geralmente, um NAS com várias portas LAN permite que todos os serviços de rede ativados acessem conteúdo no servidor através de cada porta LAN. A proteção de dados é reduzida. Em empresas, apenas pessoas específicas devem ter acesso aos dados importantes usando um protocolo de rede definido que é um endereço IP interno. A correspondência do serviço do QNAP NAS oferece aos administradores de TI a opção de permitir ou bloquear serviços selecionados nas interfaces de rede definidas para garantir a proteção do sistema.



Configuração de permissões de ACLs do Windows



O QNAP NAS agora suporta ACLs do Windows, permitindo que você facilmente aproveite as configurações de permissão de pastas compartilhadas do sistema Windows e os controles de acesso ao NAS. Permissões básicas e 13 permissões avançadas podem ser configuradas no Windows e sincronizadas com as configurações de permissão de pastas compartilhadas do NAS. Também há suporte para permissões de subpastas e configurações de privilégio no nível de arquivo. As mesmas permissões podem ser aplicadas ao AFP, FTP, File Station e Samba quando as permissões de pasta avançadas estão ativadas para implementar um controle de acesso rigoroso a fim de aumentar a segurança dos dados.

Windows Active Directory (AD)

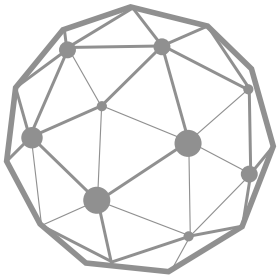
O QNAP NAS pode ser facilmente conectado ao Windows AD para permitir um gerenciamento de contas eficaz. Os administradores de TI podem aproveitar a verificação centralizada de direitos de acesso para reduzir configurações de privilégio complexas, enquanto os usuários do domínio podem facilmente usar seu nome de conta e sua senha do Windows AD para se conectar a diferentes sistemas QNAP NAS na rede local. O QNAP NAS suporta a implantação do AD em grande escala com até 200 mil usuários e grupos do AD.

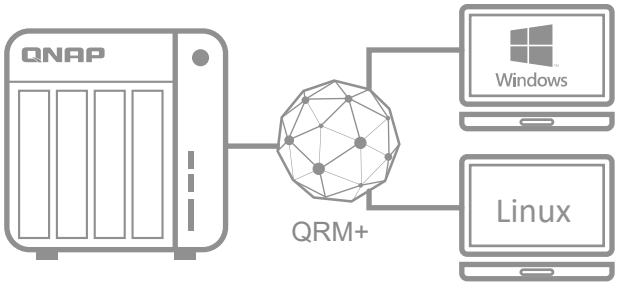
Serviço de diretório LDAP

O suporte a LDAP da QNAP permite que o NAS seja adicionado a serviços de diretório LDAP, como o OpenLDAP. Assim, os usuários são autenticados centralmente pelo servidor LDAP e podem usar o mesmo nome de conta e senha LDAP para acessar qualquer QNAP NAS que tenha sido adicionado ao servidor LDAP. Com um servidor LDAP integrado e fácil de usar, o QNAP NAS também pode ser utilizado como um servidor LDAP para autenticar centralmente usuários e grupos para todos os outros dispositivos e aplicativos com LDAP para reduzir o esforço de gerenciamento, além de aumentar a segurança dos dados.

Como a QNAP pode ajudar a gerenciar seus sistemas

O QNAP QRM+ (QNAP Remote Manager Plus) e o Q'center são soluções de gerenciamento centralizadas com uma única interface que ajudam as equipes de TI a detectar, mapear, monitorar e gerenciar dispositivos em rede, como PCs, servidores, thin clients e QNAP NAS. O QNAP NAS também oferece registros de exibição na Web para monitoramento eficiente e pode ser usado como um servidor Syslog para armazenar registros de sistema centralmente para todos os dispositivos em rede.



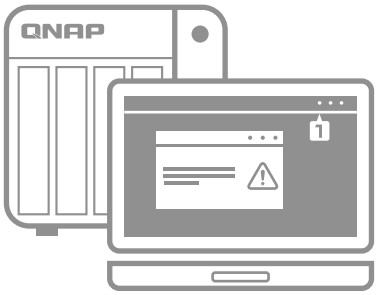


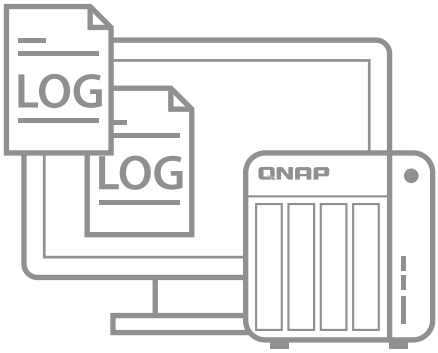
QRM+: Monitoramento e gerenciamento centralizados dos dispositivos em rede

O QRM+ pode criar uma lista de dispositivos conectados para que os administradores monitorem rapidamente seu estado, incluindo dispositivos compatíveis com IPMI. O QRM+ pode ser usado para monitoramento em tempo real, para avaliar o status do dispositivo (incluindo temperatura, velocidade do ventilador, sensores, fonte de alimentação e notificações de eventos IPMI) de cada terminal sempre que necessário. Com o QRM+, o gerenciamento remoto dos dispositivos de TI é seguro, rápido e fácil.

Alertas e notificações: Receba alertas antes que um desastre ocorra

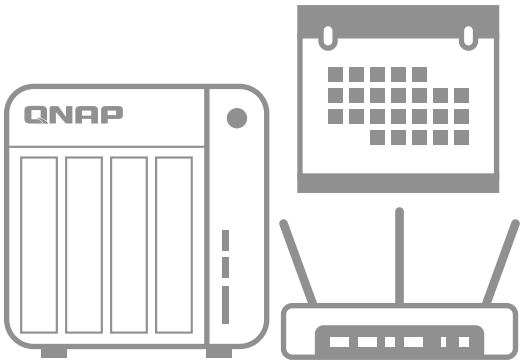
O QRM+ oferece alertas para ajudar a equipe de TI a resolver problemas de desempenho antes que os usuários, os aplicativos e a empresa sejam prejudicados.





Sistema de registro abrangente

O QNAP NAS ajuda os administradores de TI a monitorar o sistema de forma eficaz oferecendo registros de exibição na Web: os registros de eventos do sistema mantêm os administradores de IT a par de eventos de informação, aviso e erro no QNAP NAS. Os registros de conexão do sistema permitem que os administradores de TI visualizem o histórico de acesso a cada arquivo (quem, quando e que ações foram executadas). Além disso, uma lista de usuários on-line está disponível para monitorar o acesso dos usuários. Se uma conexão suspeita for detectada, os administradores podem clicar com o botão direito no usuário para adicioná-lo imediatamente à lista de bloqueio ou à lista de desconexão.

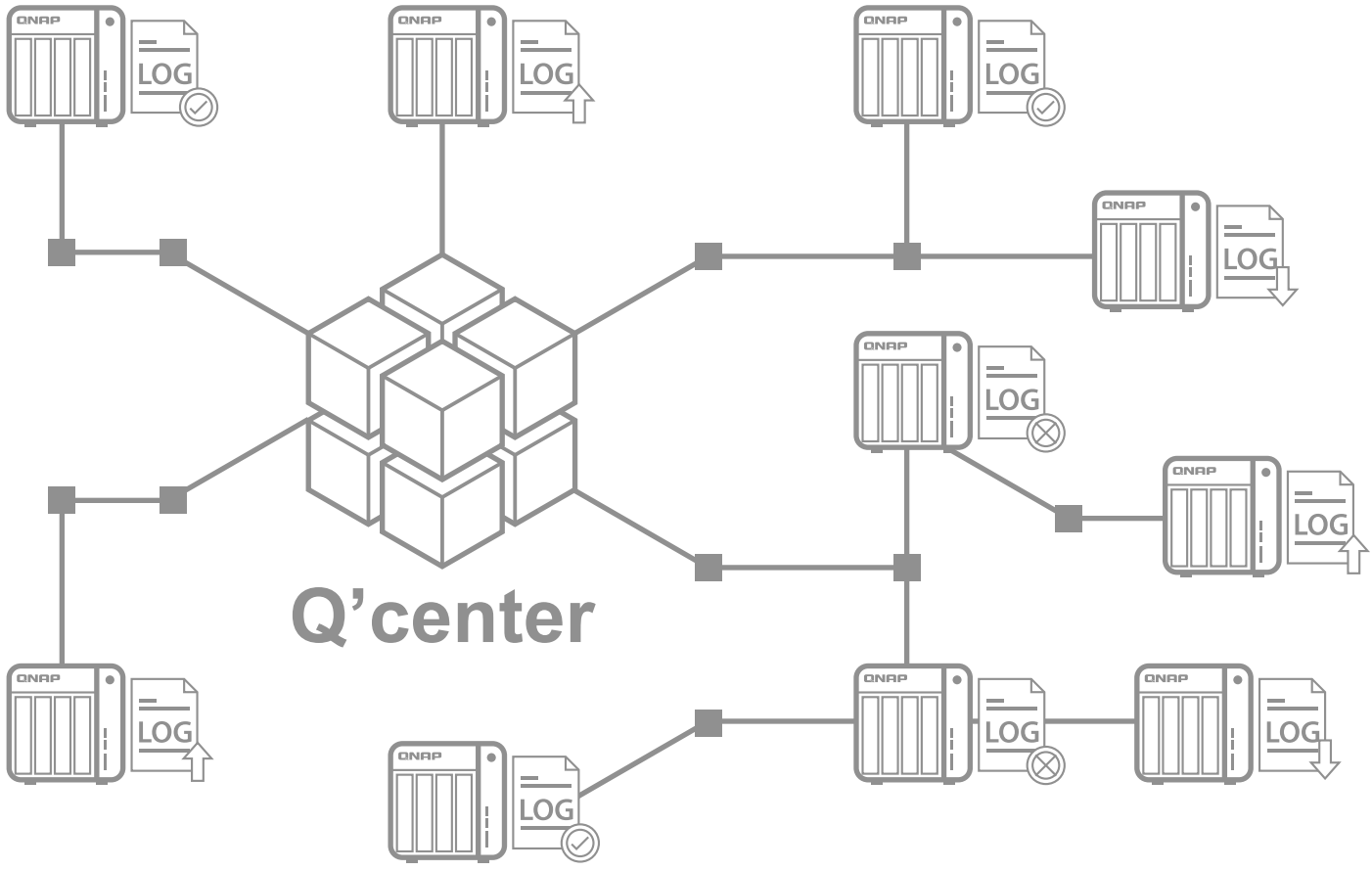


QNAP NAS como servidor Syslog

Um repositório central de dados de registro de vários dispositivos de rede permite um gerenciamento eficaz e auditorias de segurança nas empresas. Com suporte aos protocolos UDP e TCP, o QNAP NAS pode atuar como um servidor Syslog, permitindo que os administradores de TI facilmente coletem e armazenem no QNAP NAS registros de outros dispositivos conectados em rede para aumentar a eficiência do gerenciamento e da solução de problemas, quando necessário. Filtros avançados e notificações por e-mail estão disponíveis para ajudar a rapidamente identificar falhas ou ameaças à segurança.
Além de desempenhar o papel de um servidor de coleta de registros de outros dispositivos, o QNAP NAS também pode atuar como um cliente para enviar seus próprios registros para o servidor Syslog.

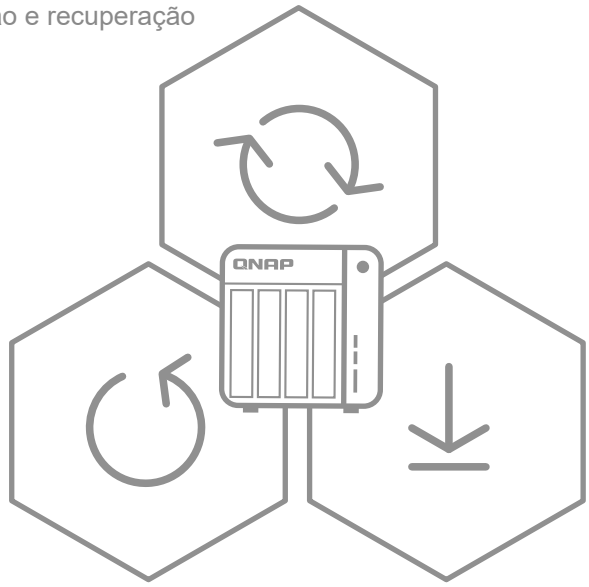
Q’center: Monitore e gerencie centralmente todos os seus sistemas NAS

O Q’center pode gerenciar e monitorar mutuamente vários sistemas NAS clientes, atendendo às necessidades de gerenciamento centralizado e às metas de controle segmentado ao mesmo tempo. Informações como a temperatura do sistema e a velocidade do ventilador permitem reduzir os riscos de falha do sistema utilizando condições de sala de controle. Você também pode ligar/desligar vários dispositivos NAS de uma só vez com as opções de energia predefinidas para melhorar a acessibilidade e a eficiência dos seus sistemas NAS. O Q’center também permite o monitoramento centralizado de registros de sistema e pode gerenciar as atualizações de firmware e a manutenção de todos os sistemas QNAP NAS com o mínimo de esforço.



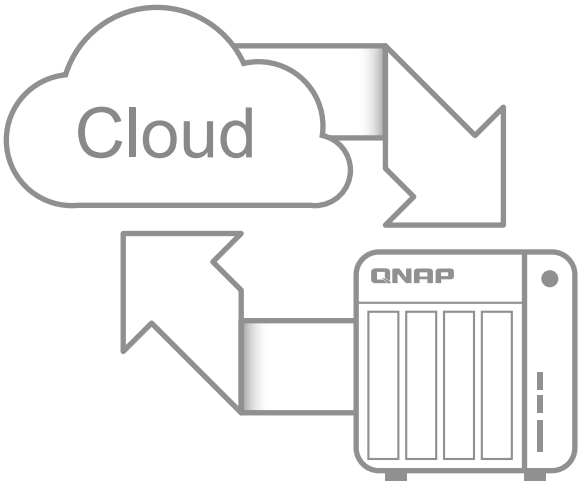
QNAP NAS: Uma eficiente solução de recuperação de desastres

O QNAP NAS suporta vários métodos de backup, sincronização e recuperação de dados.



Hybrid Backup Sync

O QNAP Hybrid Backup Sync consolida as funções de backup, restauração e sincronização em um único aplicativo para que os usuários finais possam facilmente transferir dados para ambientes de armazenamento locais, remotos e na nuvem usando RTRR (replicação remota em tempo real), rsync, FTP e CIFS/PME.



Backup em nuvem:

O QNAP NAS oferece soluções de backup em nuvem seguras, fáceis de usar e repletas de recursos para fazer backup dos dados em serviços de armazenamento oferecidos por nuvens públicas de nível empresarial, como Microsoft Azure, Amazon Glacier, Amazon S3, ElephantDrive, Google Drive, o Dropbox* e IBM SoftLayer. Até mesmo soluções de nuvem de armazenamento privado compatíveis com OpenStack Swift e WebDAV são suportadas.

Ao desenvolver um plano de adaptação para o RGPD, as empresas podem almejar simplesmente satisfazer os requisitos do regulamento atual ou encarar essa mudança como uma oportunidade de agregar valor à sua organização, contribuindo assim para a propagação de uma nova cultura de processamento de dados pessoais, bem como criar uma verdadeira transformação digital dos processos da empresa quanto ao gerenciamento de dados de clientes e funcionários.

Os hackers estão constantemente procurando pontos fracos e continuamente desenvolvendo ataques mais direcionados. As soluções de segurança sustentáveis devem evoluir e adaptar-se implementando as atualizações regulares e usando as informações sobre as ameaças assim que elas estiverem disponíveis. A segurança só é útil quando detecta ameaças, ativa uma reação imediata e garante uma proteção global para toda a estrutura, que inclui terminais, redes, nuvem híbrida etc.