myQ X

White paper de segurança do MyQ X 1.0

PORTUGUÊS (BRASIL)

Gerado a partir de docs.myq-solution.com
agosto/2026

Aviso sobre a tradução

Esta tradução foi criada com o auxílio de inteligência artificial. Em caso de discrepância ou ambiguidade, prevalece o documento original em inglês.

Sumário

1 Arquitetura Zero Trust 7
2 Estrutura de Proteção em Três Fases 8
2.1 Proteção da infraestrutura de impressão 8
2.2 Proteção dos fluxos de trabalho de impressão 8
2.3 Proteção dos documentos impressos 8
3 Privacidade desde a concepção 9
4 Evolução contínua da segurança 10
5 Principais melhorias de segurança na versão 10.2 11
5.1 Segurança TLS aprimorada 11
5.2 Aprimoramentos na segurança da autenticação 11
5.3 Atualizações de segurança do banco de dados 12
5.4 Resolução de vulnerabilidades 12
5.5 Segurança de API e integração 12
5.6 Segurança administrativa 12
6 Valor comercial do gerenciamento seguro de impressão 14
6.1 Mitigação de riscos e redução de custos 14
6.2 Princípios de segurança aprimorados 14
6.3 Eficiência operacional 15
6.4 Benefícios estratégicos para os negócios 15
7 Conformidade 16
7.1 Certificação e implementação da ISO 27001:2022 16
7.2 Estrutura de conformidade com o GDPR e medidas de proteção de dados 16
7.3 Requisitos regionais de conformidade (HIPAA, SOX) 17
7.4 Práticas do Ciclo de Vida de Desenvolvimento de Software Seguro (SSDLC) 18
7.5 Auditorias de segurança regulares e testes de penetração 19
7.6 Lista de Componentes de Software e Gerenciamento de Vulnerabilidades 19
8 Implementação da arquitetura Zero Trust 21
8.1 Princípios do Zero Trust no gerenciamento de impressão 21
8.2 Metodologia “Nunca confie, sempre verifique” 21
8.3 Segmentação e isolamento de rede 22
8.4 Autenticação e verificação robustas 22
8.5 Verificação de dispositivos e terminais 23

9 Gerenciamento de Identidade e Acesso 25
9.1 Implementação da autenticação multifatorial 25
9.2 Concessão de autorização de dispositivo OAuth 2.0 25
9.3 Recursos de integração de logon único (SSO) 26
9.4 Controle de Acesso Baseado em Função (RBAC) 26
9.5 Suporte a ambientes multilocatários do Entra ID 27
9.6 Integração com LDAP e Active Directory 27
9.7 Gerenciamento de PINs temporários e políticas de segurança 28
9.8 Suporte à autenticação biométrica 28
10 Segurança da infraestrutura 29
10.1 Fortalecimento da segurança do servidor de impressão 29
10.2 Criptografia de banco de dados (implementação no Firebird 4.0) 29
10.3 Aplicação do TLS 1.2/1.3 e gerenciamento de certificados 30
10.4 Segurança da comunicação de rede 30
10.5 Configuração do firewall e gerenciamento de portas 30
10.6 Segurança de API e tokens de autenticação 31
10.7 Isolamento de processos e sandboxing 31
10.8 Assinatura de código e verificação de integridade 31
11 Proteção e criptografia de dados 32
11.1 Implementação de criptografia de ponta a ponta 32
11.2 Criptografia de dados em repouso 32
11.3 Proteção de dados em trânsito (criptografia TLS) 33
11.4 Criptografia de trabalhos de impressão e armazenamento seguro 33
11.5 Aprimoramentos na criptografia de bancos de dados 34
11.6 Criptografia de backup e armazenamento seguro 34
11.7 Políticas de gerenciamento e rotação de chaves 34
11.8 Minimização de dados e privacidade desde a concepção 35
12 Fluxos de trabalho de impressão segura 36
12.1 Implementação da liberação segura de impressão 36
12.2 Fluxos de trabalho da impressão pull 36
12.3 Tempo limite do trabalho de impressão e exclusão automática 37
12.4 Marcas d’água e assinaturas digitais 37
12.5 Pré-visualização do trabalho e validação de conteúdo 38
12.6 Tratamento de erros e recuperação segura de trabalhos 38
13 Segurança de dispositivos e redes 39

13.1 Fortalecimento da segurança de dispositivos multifuncionais....39
13.2 Segmentação de rede e configuração de VLAN....39
13.3 Implementação de segurança do SNMP v3....40
13.4 Gerenciamento de credenciais da impressora....40
13.5 Segurança do firmware e gerenciamento de atualizações....41
13.6 Gerenciamento e restrições de portas USB....41
14 Auditoria e Monitoramento....42
14.1 Monitoramento e alertas em tempo real....42
14.2 Registro e análise de atividades de impressão....42
14.3 Análise de Comportamento do Usuário....43
14.4 Detecção e resposta a incidentes....43
14.5 Políticas de retenção e arquivamento de logs....44
14.6 Recursos avançados de filtragem e pesquisa....44
14.7 Log de auditoria para ações administrativas....45
15 Resposta a Incidentes e Recuperação....46
15.1 Procedimentos de resposta a incidentes de segurança....46
15.2 Procedimentos de recuperação e restauração....46
15.3 Alta disponibilidade e failover....47
15.4 Análise e melhoria pós-incidente....48

Visão geral dos recursos de segurança do MyQ X

O MyQ X oferece uma variedade de recursos para aprimorar a segurança e a privacidade dos usuários finais e também da empresa. Esses recursos começam com a impressão segura no multifuncional, a personalização da sessão do usuário e têm um impacto contínuo mesmo após a impressão de um documento, com a ajuda de marcas d'água.

Aqui está um breve resumo dos recursos de segurança do MyQ X:

- Conformidade com o GDPR
- Impressão segura
- Sessões de usuário com várias opções de autenticação, incluindo autenticação de dois fatores
- Logout manual e automático das sessões de usuário
- Criptografia de ponta a ponta, incluindo criptografia de dados em repouso (banco de dados, tarefas, logs)
- Pastas de destino de digitalização fixas, predefinidas pelo administrador do MyQ
- Filas privadas para exclusão imediata de trabalhos de impressão após a liberação
- Modo de privacidade para tornar anônimos os nomes dos trabalhos de impressão
- Acesso restrito às opções de configuração do servidor de impressão na interface web do MyQ X
- Direitos personalizáveis para acesso a diferentes opções de configuração
- Vários níveis de complexidade de senha
- Registro de auditoria para alterações nas configurações
- Suporte para autoridade certificadora da empresa
- Inserção de marca d'água em documentos impressos
- Pré-visualização de trabalhos
- Controle de documentos digitalizados por meio de sistemas de OCR e DMS
- Arquivamento de trabalhos

A abordagem de segurança do MyQ X baseia-se no princípio de que **a segurança não é uma consideração secundária, mas parte integrante de todo o ecossistema de gerenciamento de impressão**. A plataforma implementa uma estratégia de defesa abrangente que protege dados e fluxos de trabalho em todas as etapas do ciclo de vida do documento.

1 Arquitetura Zero Trust

Seguindo a metodologia “nunca confie, sempre verifique”, o MyQ X parte do princípio de que ameaças podem existir tanto dentro quanto fora de uma rede. Cada conexão, usuário e dispositivo deve ser autenticado e autorizado antes de acessar os recursos de impressão, garantindo verificação contínua em todas as interações.

2 Estrutura de Proteção em Três Fases

O MyQ X aborda a segurança por meio de três fases essenciais:

2.1 Proteção da infraestrutura de impressão

Toda a infraestrutura de suporte é devidamente protegida antes que qualquer documento seja impresso, incluindo estações de trabalho, dispositivos móveis, servidores, redes e dispositivos de impressão.

2.2 Proteção dos fluxos de trabalho de impressão

Fluxos de trabalho seguros e comprovados, incluindo liberação de impressão autenticada, isolamento de tarefas e relatórios abrangentes, evitam vulnerabilidades que poderiam deixar as organizações expostas.

2.3 Proteção dos documentos impressos

Proteção contínua por meio de marcas d’água, assinaturas digitais e registros de auditoria abrangentes que mantêm a rastreabilidade e incentivam o comportamento responsável dos usuários.

3 Privacidade desde a concepção

A proteção de dados está incorporada à arquitetura do MyQ X desde o início. O sistema minimiza a coleta de dados, implementa criptografia robusta e oferece aos usuários controle sobre suas informações pessoais para garantir a conformidade com o GDPR e a proteção da privacidade.

4 Evolução contínua da segurança

O MyQ X mantém sua segurança por meio de atualizações regulares, correção imediata de vulnerabilidades, integração de inteligência contra ameaças e avaliações e certificações contínuas de segurança realizadas por terceiros.

Essa abordagem que prioriza a segurança garante que as organizações possam implantar o MyQ X com confiança, sabendo que suas informações confidenciais, requisitos de conformidade e continuidade operacional estão protegidos por medidas de segurança líderes do setor.

5 Principais melhorias de segurança na versão 10.2

O MyQ X 10.2 apresenta melhorias significativas de segurança, projetadas para fortalecer a proteção contra ameaças cibernéticas em constante evolução, mantendo a eficiência operacional. Essas melhorias corrigem vulnerabilidades críticas e implementam padrões modernos de segurança.

5.1 Segurança TLS aprimorada

Versão mínima padrão do TLS 1.2: O MyQ X 10.2 aumenta a versão mínima padrão do TLS de 1.1 para 1.2, com suporte para o TLS 1.3. Isso elimina o suporte a protocolos SSL obsoletos e algoritmos de criptografia fracos que representam riscos à segurança.

Validação de certificados aprimorada: a validação aprimorada de certificados impede o uso de certificados vencidos ou emitidos incorretamente, protegendo contra ataques do tipo “man-in-the-middle” e outras vulnerabilidades. O sistema agora reconhece automaticamente como confiáveis os certificados de CA raiz do armazenamento de certificados do sistema do servidor.

5.2 Aprimoramentos na segurança da autenticação

Segurança aprimorada de senhas e PINs: Algoritmos aprimorados de hash de senha fortalecem a proteção de credenciais. O sistema introduz novas regras de segurança para PINs, incluindo comprimento mínimo obrigatório de 6 dígitos e prevenção de combinações facilmente adivinháveis, como “1234” ou “1111”.

Proteção contra tentativas de login: as tentativas de autenticação malsucedidas agora são limitadas por motivos de segurança. Por padrão, os clientes/dispositivos ficam bloqueados por 5 minutos após mais de 5 tentativas inválidas de login em 60 segundos, com períodos de tempo configuráveis.

Registro aprimorado de eventos de login: O registro aprimorado de eventos de login, especialmente tentativas de autenticação malsucedidas, facilita aos administradores a filtragem e o monitoramento de eventos de segurança no MyQ Log.

5.3 Atualizações de segurança do banco de dados

Implementação do Firebird 4.0: a atualização para o mecanismo de banco de dados Firebird 4.0 traz recursos de segurança aprimorados e melhor desempenho. As senhas do banco de dados agora são ofuscadas nos arquivos de log para evitar a exposição de credenciais.

Proteção de dados aprimorada: acesso restrito a dados confidenciais por meio de relatórios personalizados e contas externas de relatórios, garantindo a confidencialidade dos dados em diferentes níveis de acesso.

5.4 Resolução de vulnerabilidades

Correções de vulnerabilidades CVE críticas: O MyQ X 10.2 corrige várias vulnerabilidades críticas, incluindo:

- CVE-2024-28059: Vulnerabilidade de execução remota de código sem autenticação.
- CVE-2024-22076: Melhorias de segurança em scripts PHP.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316: Vulnerabilidades em componentes de terceiros.

Atualizações de segurança de componentes: Versões atualizadas de componentes críticos, incluindo OpenSSL 3.1.0, PHP 8.3.14 e Apache 2.4.57, corrigem vulnerabilidades de segurança conhecidas.

5.5 Segurança de API e integração

Restrições da API REST: escopos limitados para clientes conhecidos e recursos removidos para operações confidenciais, como a alteração de servidores de autenticação de usuários, reforçando a segurança da API.

Controles de scripts PHP: Novas configurações do Easy Config permitem que os administradores bloqueiem/desbloqueiem o acesso a scripts PHP, melhorando a segurança ao manter essas configurações no modo somente leitura.

5.6 Segurança administrativa

Segurança aprimorada da conta de administrador: a senha padrão de administrador foi removida para novas instalações. Os administradores agora podem desativar contas de administrador quando não forem necessárias, promovendo o uso de contas de usuário específicas com direitos apropriados, em vez de contas administrativas compartilhadas.

Essas melhorias de segurança demonstram o compromisso do MyQ X em manter padrões de segurança de nível empresarial ao mesmo tempo em que enfrenta os desafios contemporâneos de segurança cibernética. Atualizações regulares de segurança e gerenciamento proativo de vulnerabilidades garantem que as organizações possam implantar o MyQ X com confiança em sua segurança.

6 Valor comercial do gerenciamento seguro de impressão

O gerenciamento seguro de impressão oferece valor comercial mensurável ao transformar a infraestrutura de impressão de um risco potencial em um ativo estratégico de segurança. O MyQ X oferece às organizações proteção abrangente que aborda todo o espectro de riscos relacionados à impressão, ao mesmo tempo em que aumenta a eficiência operacional.

6.1 Mitigação de riscos e redução de custos

Prevenção de vazamento de dados: a liberação segura de impressão garante que documentos confidenciais nunca sejam deixados sem supervisão nas bandejas das impressoras, eliminando o acesso não autorizado a informações confidenciais. Os usuários se autenticam antes que seus trabalhos sejam liberados, mantendo controle total sobre a segurança dos documentos.

Prevenção de custos de conformidade: os recursos integrados de conformidade com o GDPR, HIPAA e SOX ajudam as organizações a evitar penalidades regulatórias e reduzir os custos de preparação para auditorias por meio de controles automatizados de conformidade e trilhas de auditoria abrangentes.

Continuidade operacional: o recurso de spooling de dispositivos do MyQ mantém os recursos de impressão durante interrupções no servidor, armazenando trabalhos criptografados localmente por até uma semana em 10 dispositivos, evitando interrupções nos negócios durante a manutenção do sistema ou paradas inesperadas.

6.2 Princípios de segurança aprimorados

Implementação do modelo "Zero Trust": Ao exigir autenticação para cada trabalho de impressão, o MyQ X aplica os princípios de "nunca confiar, sempre verificar" em todo o ambiente de impressão, fortalecendo a postura geral de segurança da organização.

Rastreabilidade de documentos: marcas d'água e assinaturas digitais permitem que as organizações rastreiem documentos confidenciais ao longo de todo o seu ciclo de vida, garantindo a prestação de contas e impedindo o uso indevido de informações confidenciais.

Criptografia abrangente: a criptografia de ponta a ponta de dados de impressão, bancos de dados e trabalhos armazenados garante que as informações confidenciais

permaneçam protegidas ao longo de todo o fluxo de trabalho de documentos, atendendo a rigorosos requisitos de segurança.

6.3 Eficiência operacional

Otimização da largura de banda: o spooling no cliente reduz o tráfego de rede ao processar trabalhos localmente, melhorando o desempenho em ambientes com largura de banda limitada, como escritórios remotos e filiais.

Autenticação flexível: Várias opções de autenticação, incluindo cartões de identificação, PINs, senhas e autenticação por aplicativo móvel, oferecem aos usuários métodos de acesso convenientes e seguros que atendem às diversas necessidades organizacionais. A autenticação multifatorial (MFA), que combina esses métodos, também está disponível.

Gerenciamento centralizado: políticas de segurança unificadas em todos os dispositivos simplificam a administração, ao mesmo tempo em que garantem padrões de proteção consistentes em toda a organização.

6.4 Benefícios estratégicos para os negócios

Vantagem competitiva: Demonstrar recursos robustos de segurança de impressão pode diferenciar as organizações em mercados competitivos, especialmente em setores que lidam com dados confidenciais ou atendem a clientes preocupados com a segurança.

Confiança dos funcionários: fluxos de trabalho de impressão seguros dão aos usuários a confiança de que seus documentos estão protegidos, melhorando a produtividade e reduzindo preocupações relacionadas à segurança que podem afetar a eficiência no local de trabalho.

Infraestrutura preparada para o futuro: a estrutura de segurança abrangente do MyQ X posiciona as organizações para se adaptarem às ameaças de cibersegurança em constante evolução e aos requisitos regulatórios, sem grandes reformulações na infraestrutura.

O gerenciamento seguro de impressão com o MyQ X transforma a impressão de uma vulnerabilidade de segurança em potencial em um processo de negócios controlado, auditável e em conformidade, que apoia as metas organizacionais ao mesmo tempo em que protege ativos de informação valiosos.

7 Conformidade

A abrangente estrutura de conformidade do MyQ X demonstra seu compromisso em atender aos mais altos padrões internacionais de segurança e requisitos regulatórios. Essa abordagem em várias camadas garante que as organizações possam implantar o MyQ X com confiança, ao mesmo tempo em que cumprem diversas exigências de conformidade em diversos setores e jurisdições.

7.1 Certificação e implementação da ISO 27001:2022

O MyQ obteve **a certificação ISO/IEC 27001:2022**, estabelecendo uma abordagem sistemática para a gestão da segurança da informação que atende às melhores práticas internacionais. A implementação abrange:

Estrutura de gestão de riscos: processos abrangentes de avaliação de riscos que identificam, avaliam e mitigam riscos à segurança da informação em todas as operações comerciais e implantações de clientes.

Implementação de controles de segurança: implantação estruturada de controles de segurança técnicos, administrativos e físicos que protegem os ativos de informação ao longo de todo o seu ciclo de vida.

Processo de melhoria contínua: revisões e atualizações regulares das políticas, procedimentos e controles de segurança para lidar com ameaças em constante evolução e manter a conformidade com a certificação.

Compromisso da Administração: Supervisão por parte da alta administração, garantindo que a segurança permaneça integrada à estratégia empresarial e aos processos de tomada de decisão operacional.

A certificação valida a abordagem sistemática da MyQ para proteger os dados dos clientes e manter a confidencialidade, a integridade e a disponibilidade dos sistemas de informação.

7.2 Estrutura de conformidade com o GDPR e medidas de proteção de dados

O MyQ X implementa **conformidade** abrangente **com o GDPR** por meio de princípios de privacidade desde a concepção (privacy-by-design) incorporados em toda a arquitetura do sistema:

Minimização de Dados: O sistema coleta apenas os metadados essenciais necessários para a funcionalidade operacional, evitando o processamento desnecessário de dados pessoais que poderia aumentar os riscos de conformidade.

Gerenciamento de direitos do usuário: Implementação completa dos direitos do usuário previstos no GDPR, incluindo:

- Direito de acesso aos dados pessoais
- Direito à retificação de informações incorretas
- Direito ao apagamento (“direito ao esquecimento”)
- Direito à portabilidade dos dados
- Direito de restringir o tratamento

Avaliações de Impacto sobre a Proteção de Dados: Avaliação sistemática dos riscos à privacidade para novos recursos e implantações, garantindo que a conformidade com o GDPR seja mantida ao longo da evolução do sistema.

7.3 Requisitos regionais de conformidade (HIPAA, SOX)

O MyQ X oferece suporte a estruturas de conformidade essenciais específicas do setor por meio de recursos robustos de proteção de dados e auditoria:

Conformidade com a HIPAA para o setor de saúde:

- Criptografia de Informações de Saúde Protegidas (PHI) em repouso e em trânsito.
- Registro abrangente de auditoria de todos os acessos a dados sensíveis de saúde.
- Controles de acesso baseados em funções, restringindo o acesso às PHI apenas ao pessoal autorizado.
- Procedimentos seguros de backup e recuperação para atender aos requisitos de retenção de dados da área da saúde.

Conformidade com a SOX para serviços financeiros:

- Registros de auditoria detalhados para o processamento e impressão de documentos financeiros.
- Controles de acesso que impedem a modificação não autorizada de registros financeiros.
- Recursos de arquivamento seguro que atendem aos requisitos regulatórios de retenção.
- Segregação de funções por meio de permissões baseadas em funções e fluxos de trabalho de aprovação.

Controles de segurança adicionais:

- Criptografia de banco de dados utilizando algoritmos padrão do setor.

- Protocolos de comunicação seguros para toda a transmissão de dados.
- Procedimentos automatizados de backup com criptografia e verificação de integridade.
- Registro e monitoramento de acessos para relatórios de conformidade.

7.4 Práticas do Ciclo de Vida de Desenvolvimento de Software Seguro (SSDLC)

A MyQ implementa um Ciclo de Vida de Desenvolvimento de Software Seguro, alinhado aos padrões do setor e aos requisitos da cadeia de suprimentos **da SLSA**, garantindo que as práticas de segurança sejam incorporadas em todas as fases do ciclo de vida do software.

Análise

A MyQ realiza **uma modelagem** rigorosa **de ameaças** e define **requisitos de segurança** claros durante a fase inicial de análise, permitindo a identificação precoce de riscos e estabelecendo uma base sólida de segurança antes do início do projeto.

Projeto

Todas as propostas arquitetônicas passam por **revisões** formais **da arquitetura de segurança** para validar a adesão a princípios como **Privilégio Mínimo**, **Confiança Zero** e **Defesa em Profundidade**, garantindo que a segurança seja sistematicamente incorporada ao projeto do sistema.

Desenvolvimento

Os desenvolvedores seguem **práticas seguras de codificação** e processos de revisão por pares, enquanto todas as compilações são executadas em **servidores de compilação** dedicados, isolados e **em conformidade com a SLSA**, garantindo a proteção da integridade do código-fonte e dos artefatos de compilação.

Testes

Os testes de segurança incluem **SAST** automatizado e **varredura de dependências** integrados aos pipelines de CI, permitindo a detecção precoce de vulnerabilidades tanto no código personalizado quanto em componentes de terceiros.

Implantação

Todos os artefatos de lançamento são protegidos por meio de **assinatura de código** e verificados durante a implantação, garantindo **integridade**, **autenticidade** e entrega controlada em ambientes de produção.

Manutenção

Após a implantação, os sistemas passam por **monitoramento** contínuo e **gerenciamento** estruturado **de patches**, garantindo o alinhamento constante com as ameaças em constante evolução e **as melhores práticas de segurança**.

7.5 Auditorias de segurança regulares e testes de penetração

A MyQ mantém uma validação de segurança robusta por meio de programas sistemáticos de testes e avaliações:

Testes de penetração automatizados: a integração com a plataforma de segurança Qualys oferece avaliação contínua de vulnerabilidades e testes de penetração para todas as versões de software.

Avaliações de segurança por terceiros: auditorias de segurança independentes conduzidas por organizações externas qualificadas para validar os controles de segurança e identificar possíveis melhorias.

Revisões internas de segurança: Avaliações internas regulares das políticas, procedimentos e controles técnicos de segurança para garantir a eficácia e a conformidade contínuas.

Processo de resposta a vulnerabilidades: procedimentos estruturados para lidar com problemas de segurança identificados, incluindo prazos para o desenvolvimento e a implantação de patches.

7.6 Lista de Componentes de Software e Gerenciamento de Vulnerabilidades

A MyQ implementa uma segurança abrangente da cadeia de suprimentos por meio do rastreamento detalhado de componentes e do gerenciamento de vulnerabilidades:

Publicação da SBOM: Documentação completa da Lista de Componentes de Software (SBOM) que identifica todos os componentes, bibliotecas e dependências de terceiros utilizados nos sistemas MyQ X.

Varredura automatizada de vulnerabilidades: monitoramento contínuo de bancos de dados de componentes para detectar vulnerabilidades recém-identificadas que afetem as dependências do MyQ X.

Gerenciamento Rápido de Patches: Processo sistemático para avaliar, testar e implantar atualizações de segurança para componentes de terceiros, com priorização baseada na avaliação de riscos.

Controle de versão de componentes: Rastreamento detalhado de todos os componentes de software, incluindo números de versão, níveis de patches de segurança e cronogramas de atualização, conforme documentado nas notas de lançamento.

Avaliação de segurança de fornecedores: Avaliação de fornecedores de software de terceiros para garantir que mantenham padrões de segurança adequados e processos de divulgação de vulnerabilidades.

Essa estrutura abrangente de conformidade garante que o MyQ X atenda a diversos requisitos regulatórios, mantendo os mais altos padrões de segurança da informação e proteção de dados em todos os ambientes operacionais.

8 Implementação da arquitetura Zero Trust

O MyQ X implementa a Arquitetura Zero Trust como uma abordagem de segurança fundamental que elimina a confiança implícita e valida continuamente todas as transações. Essa estrutura abrangente garante que nenhum usuário, dispositivo ou conexão de rede seja considerado confiável por padrão, independentemente de sua localização ou status de autenticação anterior.

8.1 Princípios do Zero Trust no gerenciamento de impressão

A implementação do Zero Trust no MyQ X baseia-se no princípio de **"nunca confiar, sempre verificar"** em todo o sistema de gerenciamento de impressão. O sistema exige verificação explícita para cada solicitação de acesso, garantindo que:

Canais de comunicação criptografados: todo o tráfego de rede utiliza criptografia TLS obrigatória, com versão mínima 1.2, impedindo a interceptação e a adulteração durante a transmissão de dados. Os certificados HTTPS devem ser devidamente configurados e validados para evitar ataques do tipo "man-in-the-middle".

Aplicação de protocolos seguros: O MyQ X bloqueia o tráfego HTTP não criptografado e impõe protocolos de segurança robustos em todos os canais de comunicação, incluindo conexões SMTP, LDAP e SNMP. Protocolos legados, como o SNMPv1, são proibidos, sendo preferido o SNMPv3 com autenticação robusta.

Controles de segurança da API: O acesso à API REST requer tokens de autenticação com filtragem de endereços IP, garantindo que as chamadas à API sejam autenticadas e tenham origem em fontes confiáveis. Os segredos do cliente passam por rotação periódica para manter a integridade da segurança.

8.2 Metodologia "Nunca confie, sempre verifique"

A metodologia Zero Trust permeia todos os aspectos das operações do MyQ X por meio de mecanismos de verificação contínua:

Verificação de identidade: toda interação do usuário requer autenticação, independentemente da localização na rede ou do status de confiança do dispositivo. Os usuários devem se autenticar em cada dispositivo de impressão, mesmo que já tenham feito login em outro local da organização.

Autenticação de dispositivos: os próprios dispositivos de impressão devem se autenticar antes de acessar recursos de rede, com credenciais e certificados exclusivos que impedem a falsificação não autorizada de dispositivos.

Gerenciamento de sessões: as sessões dos usuários implementam funcionalidades automáticas de tempo limite e logout, garantindo que sessões abandonadas não possam ser exploradas por pessoas não autorizadas.

8.3 Segmentação e isolamento de rede

O MyQ X implementa uma segmentação abrangente da rede para limitar as superfícies de ataque e conter possíveis violações de segurança:

Controles de limite de rede: O sistema aplica regras rígidas de firewall que bloqueiam portas não utilizadas e limitam o acesso à rede apenas aos canais de comunicação necessários. As configurações padrão desativam serviços e protocolos desnecessários.

Segmentação baseada em certificados: O MyQ X oferece suporte a três modos de gerenciamento de certificados — Autoridade Certificadora Integrada, Autoridade Certificadora da Empresa e Gerenciamento Manual de Certificados —, permitindo que as organizações implementem limites de confiança adequados com base em suas políticas de segurança.

Aplicação de FQDN: Todas as comunicações de rede devem utilizar nomes de domínio totalmente qualificados (FQDN) em vez de endereços IP ou nomes de rótulo único, prevenindo ataques man-in-the-middle baseados em DNS e garantindo a validação adequada dos certificados.

Gerenciamento de portas: O sistema gerencia automaticamente as regras do firewall e oferece controle explícito sobre quais portas de rede estão acessíveis, reduzindo a superfície de ataque por meio do bloqueio sistemático de portas.

8.4 Autenticação e verificação robustas

O MyQ X mantém a validação contínua de segurança por meio de múltiplas camadas de autenticação e monitoramento em tempo real:

Autenticação por vários métodos: O sistema suporta diversos métodos de autenticação, incluindo LDAP, Microsoft Entra ID, RADIUS e autenticação local do MyQ, com recursos de failover automático que garantem o controle de acesso contínuo.

Integração com servidores de autenticação: a integração segura com servidores de autenticação externos utiliza conexões criptografadas (TLS para LDAP, protocolos seguros para RADIUS) e impõe segredos compartilhados robustos, específicos para cada implantação do MyQ.

Monitoramento de login: O registro aprimorado de eventos de autenticação, especialmente tentativas de login malsucedidas, permite que os administradores detectem e respondam a possíveis ameaças à segurança. Tentativas de autenticação malsucedidas acionam mecanismos de bloqueio automático — por padrão, os dispositivos são bloqueados por 5 minutos após mais de 5 tentativas inválidas em 60 segundos.

Controles de persistência de sessão: O sistema implementa políticas configuráveis de tempo limite de sessão e funcionalidade de logout automático, garantindo que sessões inativas não possam ser exploradas.

8.5 Verificação de dispositivos e terminais

O MyQ X aplica protocolos rigorosos de verificação de dispositivos para garantir que apenas terminais autorizados possam acessar os recursos de impressão:

Gerenciamento de certificados de dispositivos: Todos os dispositivos conectados devem apresentar certificados válidos para comunicação em rede. O sistema mantém um repositório abrangente de certificados com validação adequada da cadeia e oferece suporte à implantação automática de certificados por meio de Política de Grupo ou Gerenciamento de Dispositivos Móveis (MDM).

Controles de segurança de terminais: Os dispositivos de impressão passam por validação de segurança contínua, incluindo autenticação SNMP v3 com senhas fortes e algoritmos criptográficos (SHA1 e AES). As credenciais das impressoras são gerenciadas por meio de protocolos de segurança específicos do fabricante, com senhas fortes geradas aleatoriamente.

Autenticação de dispositivos móveis: O MyQ X Mobile Client implementa a concessão de autorização de dispositivo OAuth 2.0 para autenticação segura de dispositivos móveis, substituindo sistemas legados baseados em PIN por segurança moderna com recursos biométricos.

Estrutura de segurança BYOD: O sistema oferece suporte a ambientes “Traga seu próprio dispositivo” (BYOD) por meio da propagação segura de impressão via AirPrint e Mopria, mantendo os princípios de confiança zero mesmo em redes sem visibilidade direta do servidor de impressão.

Gerenciamento de tokens de acesso: tokens de acesso exclusivos são emitidos para cada tipo de dispositivo, sendo a Segurança da Camada de Transporte (TLS) obrigatória para todas as comunicações. O sistema implementa controles de acesso

Just-in-Time (JIT) que ajustam dinamicamente os privilégios com base no contexto e na avaliação contínua de riscos.

Essa implementação abrangente do modelo Zero Trust garante que o MyQ X mantenha os mais altos padrões de segurança, ao mesmo tempo em que atende a diversas necessidades organizacionais e cenários de implantação. A arquitetura oferece proteção em profundidade que se adapta ao cenário de ameaças em constante evolução, mantendo a eficiência operacional e a experiência do usuário.

9 Gerenciamento de Identidade e Acesso

O MyQ X oferece uma estrutura abrangente de Gerenciamento de Identidade e Acesso (IAM) que se integra perfeitamente aos sistemas de autenticação corporativos existentes, ao mesmo tempo em que oferece suporte aos padrões modernos de segurança. A arquitetura de IAM garante uma autenticação de usuários segura, escalável e flexível em diversos ambientes organizacionais.

9.1 Implementação da autenticação multifatorial

O MyQ X implementa recursos robustos **de autenticação multifatorial (MFA)** que aumentam significativamente a segurança ao exigir múltiplos fatores de verificação:

Autenticação por terminal integrado: os métodos padrão de MFA incluem combinações de cartão de identificação e PIN, nas quais os usuários primeiro apresentam seu cartão de identificação físico e, em seguida, confirmam sua identidade com um código PIN. Alternativamente, a autenticação por cartão de identificação e senha oferece segurança de dois fatores semelhante, com verificação por senha em vez de PIN.

Autenticação por dispositivo móvel: O MyQ X Mobile Client permite uma MFA sofisticada por meio da leitura de código QR combinada com verificação biométrica. Os usuários se autenticam lendo um código QR exibido no terminal integrado, com segurança adicional fornecida por meio de bloqueios biométricos (Face ID ou impressão digital) em seus dispositivos móveis.

Integração com o Cliente para Desktop: As organizações que utilizam os serviços do Microsoft 365 se beneficiam da MFA integrada por meio da autenticação do Entra ID. Os usuários com a autenticação de dois fatores ativada em suas contas do Entra ID são automaticamente solicitados a verificar sua identidade usando aplicativos autenticadores ao acessar o Cliente para Desktop.

9.2 Concessão de autorização de dispositivo OAuth 2.0

O MyQ X suporta o padrão **de concessão de código de autorização OAuth 2.0**, permitindo a integração segura com provedores de identidade modernos e aplicativos de terceiros:

Fluxo OAuth padrão: O sistema implementa a estrutura completa de autorização OAuth 2.0, incluindo a exibição da página de login, a geração de código de acesso único e a recuperação segura de tokens. Os aplicativos clientes recebem tokens de portador com prazos de validade configuráveis e escopos concedidos.

Segurança na integração de API: tokens OAuth devem ser fornecidos para todo acesso a endpoints de API, garantindo que integrações de terceiros mantenham a autenticação adequada. O sistema suporta a validação de ID e segredo do cliente com correspondência segura de URI de redirecionamento.

Gerenciamento de tokens: Os tokens de acesso incluem controles de validade (padrão de 1.800 segundos) e restrições de escopo, proporcionando controle granular sobre as permissões de acesso à API, ao mesmo tempo em que mantêm a segurança por meio da rotação de tokens.

9.3 Recursos de integração de logon único (SSO)

O MyQ X oferece integração abrangente **de Logon Único (SSO)** que simplifica a autenticação de usuários em ambientes corporativos:

Integração com o Microsoft 365: a integração profunda com o Microsoft Entra ID permite um SSO contínuo para organizações que utilizam os serviços do Microsoft 365. Os usuários podem se autenticar usando suas credenciais existentes da Microsoft, eliminando a necessidade de senhas separadas para o MyQ.

Serviços de diretório corporativo: os recursos de SSO se estendem a vários servidores de autenticação, incluindo Active Directory, OpenLDAP e Novell eDirectory, permitindo que os usuários utilizem suas credenciais corporativas existentes para acessar o MyQ.

Autenticação multiplataforma: a funcionalidade de SSO funciona em todos os componentes do MyQ X, incluindo o Cliente para Desktop, o Cliente Móvel e terminais embutidos, proporcionando experiências de autenticação consistentes, independentemente do método de acesso.

9.4 Controle de Acesso Baseado em Função (RBAC)

O MyQ X implementa **um** sofisticado **Controle de Acesso Baseado em Funções** que se alinha aos requisitos de segurança corporativos:

Gerenciamento granular de permissões: O sistema oferece controle detalhado sobre as permissões dos usuários, permitindo que os administradores definam direitos de acesso específicos com base nas funções e responsabilidades organizacionais.

Administração baseada em grupos: a implementação do RBAC oferece suporte tanto a permissões individuais de usuários quanto ao controle de acesso baseado em

grupos, permitindo o gerenciamento eficiente de grandes contingentes de usuários por meio da atribuição a grupos de segurança.

Aplicação do princípio do privilégio mínimo: os controles de acesso seguem o princípio do privilégio mínimo, garantindo que os usuários recebam apenas as permissões mínimas necessárias para suas funções de trabalho, mantendo a eficiência operacional.

9.5 Suporte a ambientes multilocatários do Entra ID

O MyQ X oferece suporte robusto a **ambientes multilocatários do Microsoft Entra ID**:

Autenticação entre locatários: o sistema pode autenticar usuários em vários locatários do Entra ID, oferecendo suporte a estruturas organizacionais complexas com várias instâncias do Azure AD.

Isolamento de locatários: o suporte multilocatário inclui mecanismos de isolamento adequados que impedem o acesso a dados entre locatários, mantendo os recursos centralizados de gerenciamento do MyQ.

Gerenciamento híbrido de identidades: a integração oferece suporte tanto a cenários de identidade exclusivamente na nuvem quanto a cenários híbridos, atendendo a organizações com Active Directory local sincronizado com o Entra ID.

9.6 Integração com LDAP e Active Directory

O MyQ X oferece recursos abrangentes **de integração com LDAP e Active Directory**:

Opções flexíveis de sincronização: O sistema oferece suporte a vários métodos de sincronização, incluindo sincronização completa, sincronização seletiva de atributos e sincronização condicional com base em filtros LDAP. Os administradores podem escolher entre substituição completa, adição exclusiva ou atualizações condicionais para propriedades de cartões e PINs.

Recursos avançados de filtragem: a sincronização LDAP inclui opções sofisticadas de filtragem que utilizam a sintaxe padrão de filtros LDAP, permitindo a importação seletiva de usuários com base em unidades organizacionais, associações a grupos ou atributos personalizados.

Importação de estrutura de grupos: O sistema pode importar estruturas organizacionais completas, incluindo grupos de segurança, grupos de distribuição e

hierarquias de grupos aninhadas do Active Directory, mantendo as relações organizacionais dentro do MyQ.

Autenticação segura: Todas as comunicações LDAP utilizam criptografia TLS para proteger credenciais e dados do usuário durante a sincronização. O sistema oferece suporte tanto ao LDAP tradicional sobre TLS quanto a conexões LDAP seguras.

9.7 Gerenciamento de PINs temporários e políticas de segurança

O MyQ X implementa **um gerenciamento** abrangente **de PINs e políticas de segurança**:

Segurança aprimorada de PINs: A versão 10.2 introduz segurança reforçada para PINs, incluindo comprimento mínimo obrigatório de 6 dígitos e prevenção de combinações facilmente adivinháveis, como “1234” ou “1111”.

Emissão de PINs temporários: O sistema oferece suporte a códigos PIN temporários que podem ser emitidos para períodos específicos ou cenários de uso único, proporcionando segurança adicional para acesso de visitantes ou funcionários temporários.

Aplicação de políticas de PIN: políticas de PIN configuráveis permitem que as organizações definam requisitos de complexidade, períodos de validade e restrições de reutilização que estejam alinhados aos padrões de segurança corporativos.

Proteção contra falhas de autenticação: a segurança aprimorada inclui o bloqueio automático de tentativas de autenticação após falhas repetidas (padrão: bloqueio de 5 minutos após 5 tentativas malsucedidas em 60 segundos).

9.8 Suporte à autenticação biométrica

O MyQ X aproveita **recursos** modernos **de autenticação biométrica** por meio da integração com dispositivos móveis:

Integração biométrica móvel: O MyQ X Mobile Client oferece suporte a métodos de autenticação biométrica, incluindo Face ID em dispositivos iOS e reconhecimento de impressão digital em dispositivos Android, proporcionando um controle de acesso integrado e seguro.

Autenticação multimodal: A autenticação biométrica funciona em conjunto com a segurança baseada no dispositivo, criando um sistema de autenticação multimodal que combina algo que o usuário possui (dispositivo móvel) com algo que ele é (características biométricas).

10 Segurança da infraestrutura

O MyQ X oferece uma segurança de infraestrutura robusta que protege todo o ambiente de gerenciamento de impressão contra ameaças cibernéticas em constante evolução. A plataforma incorpora múltiplas camadas de defesa para proteger servidores, bancos de dados, comunicação de rede e integridade do software, garantindo confiabilidade operacional e confidencialidade dos dados.

10.1 Fortalecimento da segurança do servidor de impressão

Os servidores de impressão MyQ X são fortalecidos por meio de configurações de segurança baseadas nas melhores práticas, definidas nas configurações do arquivo **config.ini**, incluindo:

- Restrição de serviços e processos para limitar a superfície de ataque.
- Ativação de protocolos de comunicação seguros e desativação de opções legadas e inseguras.
- Atribuição rigorosa de privilégios de usuário, evitando privilégios de administrador quando desnecessários.
- Atualizações automáticas regulares e aplicação de patches de segurança para corrigir vulnerabilidades recém-descobertas.
- Configuração de regras de firewall e restrições de portas para bloquear o tráfego de rede não autorizado.

Essas medidas reduzem o risco de exploração e mantêm a disponibilidade do sistema mesmo em condições de ataque.

10.2 Criptografia de banco de dados (implementação no Firebird 4.0)

O MyQ X utiliza o mecanismo de banco de dados **Firebird 4.0**, que oferece recursos avançados de criptografia para proteger dados confidenciais em repouso e durante operações de backup. Os principais recursos de criptografia incluem:

- Criptografia AES-256 dos arquivos do banco de dados para impedir o acesso não autorizado aos dados.
- Armazenamento criptografado de senhas e chaves dentro do sistema de banco de dados.
- Ofuscação do conteúdo confidencial do banco de dados em logs e diagnósticos.

Isso garante a conformidade com as regulamentações de proteção de dados e evita o comprometimento da contabilidade de trabalhos de impressão e das informações dos usuários.

10.3 Aplicação do TLS 1.2/1.3 e gerenciamento de certificados

Para proteger os dados em trânsito, o MyQ X impõe, por padrão, o protocolo **TLS 1.2** como mínimo, com atualização opcional para TLS 1.3 para maior segurança e desempenho. A plataforma oferece modos flexíveis de gerenciamento de certificados:

- Geração automática de uma Autoridade Certificadora (CA) raiz privada que assina certificados de servidor e de cliente.
- Integração de CAs intermediárias gerenciadas pela organização, permitindo cadeias de confiança corporativas e controle centralizado de certificados.
- Suporte à instalação manual de certificados, incluindo certificados de CAs de terceiros ou públicas.

Os certificados e as chaves privadas são armazenados com segurança por meio de proteção criptografada, e os clientes recebem certificados confiáveis por meio da Política de Grupo ou do Gerenciamento de Dispositivos Móveis.

10.4 Segurança da comunicação de rede

O MyQ X protege todos os canais de comunicação de rede ao:

- Bloqueio de todo o tráfego HTTP não criptografado, impondo o uso exclusivo de HTTPS.
- Criptografar o tráfego SMTP, LDAP e RADIUS usando TLS para proteger a autenticação e o fluxo de e-mails.
- Desativar protocolos obsoletos e vulneráveis, como o POP3 e seus substitutos do STARTTLS.
- Utilizar o SNMPv3 com autenticação forte e algoritmos criptográficos para monitorar e gerenciar dispositivos com segurança.

Esses controles impedem a interceptação, a falsificação de identidade e ataques do tipo “man-in-the-middle” em toda a rede.

10.5 Configuração do firewall e gerenciamento de portas

O MyQ X reduz as superfícies de ataque ao:

- Desativar regras de firewall para portas de rede e protocolos não utilizados.
- Permitir o controle granular de quais portas ficam expostas com base nas políticas de rede da organização.

Isso limita os pontos de entrada apenas àqueles essenciais para os serviços de impressão, reforçando as defesas do perímetro.

10.6 Segurança de API e tokens de autenticação

As APIs aplicam várias camadas de segurança:

- A estrutura de concessão de código de autorização OAuth 2.0 protege o acesso à API por meio de tokens de portador de curta duração e restrições de escopo.
- Os tokens são validados em relação aos endereços IP dos clientes e exigem credenciais seguras dos clientes.
- A rotação periódica de segredos protege contra vazamentos de credenciais.

Isso protege os pontos de extremidade da API contra solicitações não autorizadas e abusos.

10.7 Isolamento de processos e sandboxing

Os aplicativos de gerenciamento de impressão MyQ X são executados com **isolamento de processos** para impedir que componentes comprometidos afetem todo o sistema. O uso de sandboxing em máquinas virtuais ou contêineres é empregado sempre que viável para conter violações de segurança e limitar o movimento lateral dentro do ambiente.

10.8 Assinatura de código e verificação de integridade

Todos os binários e instaladores do software MyQ são **assinados** para garantir autenticidade e integridade. Isso assegura que os clientes instalem versões verificadas do software, livres de adulteração ou modificações não autorizadas.

11 Proteção e criptografia de dados

O MyQ X implementa proteção e criptografia abrangentes de dados ao longo de todo o ciclo de vida do documento, garantindo confidencialidade e integridade desde o envio inicial para impressão até a saída final e o arquivamento.

11.1 Implementação de criptografia de ponta a ponta

O MyQ X oferece **criptografia de ponta a ponta** em todos os canais de comunicação e pontos de armazenamento de dados:

Canais de comunicação criptografados: todo o tráfego de rede utiliza criptografia TLS obrigatória, com versão mínima 1.2 por padrão. O protocolo HTTPS é obrigatório para todas as interfaces web, comunicação entre servidores e conexões de clientes.

Segurança baseada em certificados: vários modos de gerenciamento de certificados atendem aos requisitos organizacionais, desde a Autoridade Certificadora (CA) integrada até a integração com a infraestrutura de chaves públicas (PKI) corporativa e certificados de CAs públicas. As chaves privadas são protegidas por senhas geradas aleatoriamente e armazenadas de forma criptografada no banco de dados Firebird.

Segurança de protocolos: A criptografia TLS é aplicada nos protocolos SMTP, LDAP, RADIUS e SNMP, garantindo que nenhum dado confidencial seja transmitido em texto não criptografado.

11.2 Criptografia de dados em repouso

O MyQ X protege os dados armazenados por meio de múltiplas camadas de criptografia:

Criptografia do banco de dados: O banco de dados Firebird 4.0 suporta criptografia usando certificados personalizados com o recurso “Encrypting File System” (EKU – Enhanced Key Usage). Os certificados devem estar localizados em repositórios de certificados designados no computador, sendo preferível o repositório Pessoal.

Proteção do sistema de arquivos: Os arquivos de tarefas de impressão e digitalização armazenados no servidor de impressão MyQ X podem ser criptografados usando certificados personalizados fornecidos pelos administradores, adicionando uma camada extra de proteção além das permissões do sistema de arquivos.

Criptografia completa do disco: O MyQ X oferece suporte à integração com tecnologias de criptografia completa do disco, como o Microsoft BitLocker, para proteger todos os dados em repouso no servidor de impressão, incluindo o banco de dados, certificados e arquivos temporários.

11.3 Proteção de dados em trânsito (criptografia TLS)

O MyQ X aplica **padrões** rigorosos **de criptografia TLS** para todas as comunicações de rede:

TLS 1.2 como mínimo: a configuração padrão exige, no mínimo, o TLS 1.2, com atualização opcional para o TLS 1.3 para maior segurança e desempenho. Protocolos legados, incluindo SSL e versões mais antigas do TLS, são bloqueados.

Gerenciamento de conjuntos de criptografia: o sistema implementa conjuntos de criptografia robustos e desativa algoritmos vulneráveis para prevenir ataques criptográficos. As comunicações SNMPv3 utilizam criptografia SHA1 e AES.

Validação de certificados: Todas as conexões TLS exigem validação adequada de certificados por meio de nomes de domínio totalmente qualificados (FQDN) para evitar ataques do tipo “man-in-the-middle”. O uso do START TLS é evitado devido às vulnerabilidades de MITM.

11.4 Criptografia de trabalhos de impressão e armazenamento seguro

O MyQ X oferece vários mecanismos para proteger os trabalhos de impressão ao longo de todo o seu ciclo de vida:

Liberação segura de impressão: os trabalhos de impressão são armazenados com segurança no servidor MyQ até que os usuários se autentiquem no dispositivo, impedindo o acesso não autorizado aos documentos que se encontram nas bandejas de saída da impressora.

Criptografia de arquivos de tarefas: Os administradores podem ativar a criptografia de tarefas fornecendo certificados personalizados, garantindo que os arquivos das tarefas de impressão permaneçam criptografados enquanto estiverem armazenados no servidor aguardando liberação.

Filas privadas: Para documentos altamente confidenciais, as filas privadas excluem automaticamente os trabalhos de impressão imediatamente após a liberação, eliminando o risco de acesso não autorizado prolongado.

Modo de Privacidade: Quando ativado, o modo de privacidade oculta os nomes dos documentos de todos os usuários, exceto do proprietário do documento, impedindo a divulgação de informações por meio dos nomes dos trabalhos. Nem mesmo os administradores podem visualizar os nomes dos trabalhos de outros usuários.

11.5 Aprimoramentos na criptografia de bancos de dados

A implementação do banco de dados **Firebird 4.0** oferece recursos avançados de criptografia:

Criptografia com certificado personalizado: os arquivos do banco de dados são criptografados usando certificados com EFS Extended Key Usage, oferecendo forte proteção contra acesso não autorizado ao banco de dados.

Proteção por senha: as senhas do banco de dados são ofuscadas nos arquivos de log, impedindo a exposição de credenciais durante atividades de solução de problemas e monitoramento.

Reforço de permissões: a pasta de dados do MyQ, que contém o banco de dados de usuários e as chaves privadas dos certificados TLS, é restrita apenas a administradores, ao grupo SYSTEM e à conta de serviço do MyQ, removendo o acesso de leitura padrão para todos os usuários.

11.6 Criptografia de backup e armazenamento seguro

O MyQ X garante que os backups mantenham o mesmo nível de segurança dos dados de produção:

Backups criptografados: os backups do banco de dados são protegidos por senhas seguras e geradas aleatoriamente, que impedem a restauração ou o acesso não autorizado aos arquivos de backup.

Armazenamento seguro de backups: os arquivos de backup devem ser armazenados em locais seguros, com controles de acesso adequados e criptografia em repouso, para manter a confidencialidade dos dados durante todo o ciclo de vida do backup.

11.7 Políticas de gerenciamento e rotação de chaves

O MyQ X implementa práticas seguras de gerenciamento de chaves:

Rotação de certificados: os certificados podem ser rotacionados regularmente de acordo com as políticas de segurança da organização, com suporte para implantação automatizada por meio de Política de Grupo ou Gerenciamento de Dispositivos Móveis.

Proteção de chaves privadas: Todas as chaves privadas para certificados e operações de CA são protegidas por senhas geradas aleatoriamente e armazenadas de forma criptografada no banco de dados.

Rotação de segredos da API: Os segredos do cliente da API REST devem passar por rotação periódica para manter a segurança. O sistema oferece suporte à renovação de segredos sem interrupção do serviço.

11.8 Minimização de dados e privacidade desde a concepção

O MyQ X implementa **princípios de privacidade desde a concepção em conformidade com o GDPR**:

Coleta limitada de dados: O sistema coleta apenas os metadados essenciais necessários para a funcionalidade operacional, evitando o processamento desnecessário de dados pessoais que poderia aumentar os riscos à privacidade.

Exclusão automática: Os administradores podem configurar períodos de exclusão automática para arquivos de tarefas de impressão e digitalização, garantindo que os dados sejam retidos apenas pelo tempo necessário para fins comerciais.

Direitos do usuário sobre os dados: implementação completa dos direitos do usuário previstos no GDPR, incluindo acesso aos dados, anonimização e o direito ao esquecimento, com avisos de privacidade personalizáveis nas interfaces do usuário.

Gerenciamento de sessões: a funcionalidade de logout automático garante que as sessões dos usuários sejam encerradas corretamente, impedindo o acesso não autorizado por meio de sessões abandonadas.

Essa estrutura abrangente de proteção e criptografia de dados garante que o MyQ X mantenha os mais altos padrões de confidencialidade e integridade dos dados, ao mesmo tempo em que atende aos requisitos de conformidade regulatória em diversos ambientes organizacionais.

12 Fluxos de trabalho de impressão segura

O MyQ X oferece fluxos de trabalho abrangentes de impressão segura que mantêm o controle total do usuário sobre a liberação de documentos, ao mesmo tempo em que evitam que informações confidenciais sejam expostas nas bandejas de saída da impressora. Esses fluxos de trabalho são essenciais para organizações que exigem segurança rigorosa dos documentos e responsabilização dos usuários.

12.1 Implementação da liberação segura de impressão

A função "Hold Print" garante que os trabalhos de impressão nunca sejam liberados imediatamente para a impressora. Os documentos são armazenados com segurança no servidor MyQ e impressos somente após o usuário autorizado se autenticar no dispositivo de impressão, evitando que documentos sejam deixados sem supervisão nas bandejas de saída.

A "Pull Print" amplia ainda mais essa funcionalidade, permitindo que os usuários liberem seus trabalhos em qualquer dispositivo compatível dentro do sistema de impressão, não apenas no dispositivo para o qual enviaram originalmente o trabalho. Essa flexibilidade é particularmente valiosa durante a manutenção de equipamentos ou quando os usuários precisam imprimir de locais diferentes.

Vários métodos de autenticação oferecem suporte à liberação segura de impressão, incluindo códigos PIN, cartões de identificação, senhas, códigos QR com verificação biométrica e combinações de autenticação de dois fatores. Essa flexibilidade atende a diversos requisitos de segurança organizacionais.

12.2 Fluxos de trabalho da impressão pull

A impressão pull oferece benefícios significativos tanto para administradores quanto para usuários finais:

Benefícios administrativos:

- Eliminam pilhas de documentos abandonados nas impressoras do escritório
- Promova um comportamento responsável na impressão e o cumprimento das políticas de segurança de documentos
- Gerenciar todas as impressões por meio de uma única fila de impressão unificada
- Reduzir o desperdício de impressão e os custos associados por meio de opções de visualização prévia e ajuste
- Oferecer suporte à impressão flexível em vários dispositivos

Benefícios para o usuário:

- Documentos confidenciais permanecem protegidos até que sejam explicitamente liberados
- Imprima em qualquer dispositivo autorizado na organização
- Visualize os documentos no terminal integrado antes da liberação
- Modifique as opções de impressão (cor, frente e verso, acabamento) mesmo após o envio do trabalho
- Alterar os destinos de impressão no próprio dispositivo caso a impressora original não esteja disponível

12.3 Tempo limite do trabalho de impressão e exclusão automática

O MyQ X implementa procedimentos de limpeza automática para evitar a exposição prolongada de documentos:

Períodos de retenção configuráveis: os administradores definem por quanto tempo os arquivos de trabalhos de impressão ficam armazenados no servidor MyQ antes da exclusão automática, equilibrando os requisitos operacionais com as necessidades de segurança.

Gerenciamento de tempo limite de trabalhos: os trabalhos não liberados dentro dos prazos especificados são automaticamente removidos da fila de espera, evitando que documentos esquecidos ou abandonados se acumulem nos servidores.

Logout automático: as sessões nos dispositivos expiram automaticamente após períodos definidos pelo administrador, impedindo o acesso não autorizado a documentos em terminais abandonados.

12.4 Marcas d’água e assinaturas digitais

A marca d’água permite a rastreabilidade dos documentos ao adicionar sobreposições personalizáveis às páginas impressas, que podem incluir:

- Designações de confidencialidade
- Datas e carimbos de hora de impressão
- Nome da pessoa que está imprimindo o documento
- Informações de identificação da impressora

Essas marcas d’água podem ser aplicadas a todas as páginas ou a páginas selecionadas, criando uma trilha de auditoria que ajuda a identificar documentos vazados e rastreá-los até sua origem.

12.5 Pré-visualização do trabalho e validação de conteúdo

O mecanismo **de visualização de trabalhos** permite que os administradores revisem os trabalhos de impressão antes da liberação:

Suporte a formatos: a funcionalidade de pré-visualização suporta as três linguagens de descrição de página mais comuns — PCL 5, PCL 6 e PostScript.

Controle preventivo: os administradores podem rejeitar trabalhos de impressão não autorizados antes que cheguem ao dispositivo de impressão, evitando violações de políticas e protegendo informações confidenciais.

Filtragem baseada em conteúdo: a integração com sistemas de OCR e de gerenciamento de documentos permite que políticas de digitalização sejam aplicadas com base na análise do conteúdo do documento.

12.6 Tratamento de erros e recuperação segura de trabalhos

O MyQ X implementa um tratamento robusto de erros para manter a segurança durante falhas no dispositivo:

Proteção contra erros do dispositivo: quando um dispositivo de impressão entra em estado de erro (atolamento de papel, falta de toner), os documentos são retidos em vez de serem impressos automaticamente quando o erro for resolvido, mantendo o controle do usuário sobre o momento da liberação.

Preservação da sessão: se um dispositivo ficar indisponível no meio de uma sessão, o sistema MyQ preserva a sessão do usuário e permite a continuação em dispositivos alternativos sem perder o estado do documento.

Logout automático do dispositivo: quando ocorrem erros no dispositivo, o logout automático limpa a memória do dispositivo para impedir o acesso não autorizado aos documentos por parte da equipe de manutenção ou de outros usuários.

Essa arquitetura abrangente de fluxo de trabalho de impressão segura garante que as organizações mantenham um controle rigoroso sobre a segurança dos documentos ao longo de todo o ciclo de vida da impressão, ao mesmo tempo em que promove a flexibilidade operacional e a produtividade do usuário.

13 Segurança de dispositivos e redes

O MyQ X oferece controles abrangentes de segurança de dispositivos e rede para proteger dispositivos multifuncionais (MFDs), impressoras e infraestrutura de rede contra acesso não autorizado e exploração.

13.1 Fortalecimento da segurança de dispositivos multifuncionais

Organizações que implantam o MyQ X com MFDs devem implementar as melhores práticas de segurança, incluindo:

Controles de acesso aos dispositivos: restringir o acesso físico às impressoras apenas a locais e pessoal autorizados, reduzindo a exposição a adulterações ou roubos.

Desativação de protocolos não utilizados: desative protocolos e serviços desnecessários nos dispositivos que não sejam exigidos pelo MyQ X, reduzindo a superfície de ataque de cada dispositivo.

Gerenciamento de credenciais padrão: Altere todas as senhas padrão de administrador nos dispositivos para credenciais fortes e geradas aleatoriamente. As configurações padrão de fábrica são comumente conhecidas pelos invasores.

Proteção do disco rígido interno: Se os dispositivos suportarem o armazenamento interno de trabalhos de impressão para reimpressão, implemente criptografia (AES) e recursos de sobrescrita automática de dados para impedir o acesso não autorizado aos documentos armazenados.

13.2 Segmentação de rede e configuração de VLAN

O MyQ X oferece suporte a estratégias de segmentação de rede para conter possíveis comprometimentos de dispositivos:

Isolamento de VLAN: Separe o tráfego de rede de impressoras e dispositivos das redes gerais de usuários e administrativas usando LANs virtuais, limitando o movimento lateral caso um dispositivo seja comprometido.

Sub-redes e listas de controle de acesso: Implemente controles de acesso no nível da rede usando listas de controle de acesso (ACLs) para garantir que apenas sistemas autorizados possam se comunicar com dispositivos de impressão e servidores.

Regras de firewall: bloqueie o tráfego de entrada e saída desnecessário das sub-redes das impressoras, limitando a conectividade apenas aos serviços essenciais e impedindo que dispositivos infectados acessem outros recursos da rede.

Aplicação de FQDN: Todas as comunicações de rede devem utilizar nomes de domínio totalmente qualificados (FQDN) em vez de endereços IP ou nomes de host abreviados, evitando ataques “man-in-the-middle” baseados em DNS e garantindo a validação adequada dos certificados.

13.3 Implementação de segurança do SNMP v3

O MyQ X impõe protocolos **SNMPv3** modernos com criptografia robusta para o gerenciamento de dispositivos:

Proibição do SNMPv1 inseguro: a comunicação legada por SNMPv1 deve ser totalmente desativada, pois transmite credenciais em texto simples e não possui criptografia.

Configuração do SNMPv3: Todas as comunicações SNMP devem utilizar o SNMPv3 com:

- Senhas fortes e geradas aleatoriamente para autenticação
- Algoritmos de hash SHA1 ou mais robustos
- Criptografia AES para garantir a confidencialidade dos dados
- Credenciais únicas por dispositivo, específicas para cada implantação do MyQ

13.4 Gerenciamento de credenciais da impressora

O MyQ X reconhece que **o gerenciamento de credenciais de impressoras é específico de cada fabricante** e requer implementação por parte do cliente:

Requisitos de senhas fortes: todas as credenciais administrativas da impressora devem usar senhas fortes, geradas aleatoriamente, em vez de credenciais padrão ou simples.

Rotação de credenciais: atualize periodicamente as senhas das impressoras de acordo com as políticas de segurança da organização para reduzir o risco de comprometimento das credenciais.

Restrições de acesso: Limite o acesso à gestão da impressora apenas ao pessoal autorizado por meio de regras de firewall, controles de acesso físico e permissões baseadas em funções.

13.5 Segurança do firmware e gerenciamento de atualizações

Manter o firmware dos dispositivos atualizado é fundamental para a segurança:

Atualizações automáticas: Configure os dispositivos para receber e aplicar automaticamente as atualizações de firmware do fabricante que corrigem vulnerabilidades de segurança recém-descobertas.

Alertas de segurança do fabricante: Monitore as notificações de segurança do fabricante sobre vulnerabilidades críticas que afetem os dispositivos implantados e aplique os patches imediatamente.

Testes de atualização: Teste as atualizações de firmware em ambientes que não sejam de produção antes de implantá-las nas impressoras de produção, para garantir compatibilidade e funcionalidade.

13.6 Gerenciamento e restrições de portas USB

O MyQ X oferece controles administrativos para a conectividade USB dos dispositivos:

Desativação de portas USB: Os administradores devem desativar as portas USB de entrada nos MFDs para impedir:

- Impressão direta via USB, contornando os controles de segurança do MyQ
- Acesso direto aos discos rígidos dos dispositivos e aos dados armazenados
- Uso não autorizado das funcionalidades do dispositivo

Alternativas seguras para impressão direta: habilite apenas métodos de impressão seguros aprovados (IPP/S, AirPrint com integração ao MyQ), bloqueando o acesso USB direto não seguro.

Essa estrutura abrangente de segurança de dispositivos e rede garante que os dispositivos de impressão continuem sendo componentes seguros da infraestrutura do MyQ X, mantendo a eficiência operacional e a postura de segurança da organização.

14 Auditoria e Monitoramento

O MyQ X oferece recursos abrangentes de auditoria e monitoramento que permitem aos administradores manter a visibilidade sobre as operações de impressão, detectar incidentes de segurança e garantir a conformidade com as políticas e regulamentações organizacionais.

14.1 Monitoramento e alertas em tempo real

O MyQ X monitora todos os componentes da infraestrutura de impressão em tempo real por meio de vários canais de monitoramento:

Monitoramento do status dos dispositivos: monitoramento contínuo do status de impressoras e dispositivos multifuncionais, incluindo níveis de toner, disponibilidade de papel, condições de erro e conectividade dos dispositivos. Os administradores recebem informações imediatas sobre a integridade e o status operacional dos dispositivos.

Gerenciamento de alertas: alertas automatizados notificam os administradores sobre eventos críticos, incluindo erros nos dispositivos, baixo nível de consumíveis, problemas de conectividade e outras falhas operacionais. As notificações de alerta podem ser enviadas por e-mail ou integradas ao Visualizador de Eventos do Windows.

Notificações de eventos: Notificações personalizáveis baseadas em eventos acionam ações em resposta a condições específicas do dispositivo ou do sistema, permitindo a resolução proativa de problemas antes que eles afetem as operações.

14.2 Registro e análise de atividades de impressão

O MyQ X mantém **registros de auditoria detalhados de todas as atividades de impressão, cópia, digitalização e fax**:

Contabilidade por trabalho: a contabilidade avançada rastreia cada trabalho de forma independente, permitindo a atribuição detalhada a usuários, dispositivos, projetos e centros de custo específicos. Os trabalhos realizados durante uma única sessão de usuário são contabilizados separadamente, fornecendo dados precisos de uso.

Metadados de atividade: O registro abrangente captura a data de envio do trabalho, a data de liberação do trabalho, a identificação do dispositivo, o formato do papel, as

configurações de simplex/duplex, as configurações de cor e todos os outros parâmetros relevantes do trabalho.

Log do MyQ: O log do sistema em tempo real exibe toda a atividade do servidor, incluindo eventos do sistema, erros, avisos, tentativas de autenticação, alterações de configuração e ações administrativas. As mensagens de log são categorizadas por gravidade (Crítico, Erro, Aviso, Informação, Notificação, Depuração, Rastreamento) e podem ser filtradas por período de tempo e subsistema.

14.3 Análise de Comportamento do Usuário

O MyQ X oferece recursos sofisticados de análise para compreender padrões de impressão e detectar anomalias:

Geração de Relatórios Personalizados: Recursos avançados de relatórios permitem que os administradores criem relatórios personalizados com base em qualquer combinação de parâmetros monitorados, possibilitando a análise do comportamento de impressão por usuário, departamento, projeto, dispositivo ou período de tempo.

Acompanhamento de Centros de Custo: a atribuição detalhada de trabalhos de impressão a centros de custo, projetos e grupos de usuários permite a geração de relatórios de despesas transparentes e apoia decisões bem fundamentadas em relação às políticas de impressão.

Monitoramento de comportamento: os administradores podem analisar padrões de impressão para identificar atividades incomuns, uso excessivo ou violações de políticas que justifiquem uma investigação mais aprofundada.

14.4 Detecção e resposta a incidentes

O MyQ X oferece suporte ao monitoramento com foco em segurança por meio de registros e alertas estruturados:

Registros de autenticação com falha: O registro aprimorado de tentativas de autenticação, especialmente tentativas de login com falha, permite que os administradores detectem e respondam a possíveis ameaças à segurança. Desde a versão 10.2, os registros de tentativas de login foram aprimorados para facilitar a filtragem no MyQ Log.

Regras de Notificação de Logs: Regras personalizáveis acionam notificações automatizadas com base em tipos específicos de eventos, subsistemas e padrões de mensagens, permitindo a detecção rápida de eventos relevantes para a segurança. As

regras podem usar expressões regulares para pesquisar padrões específicos em mensagens de log.

Alertas de eventos críticos: O sistema alerta automaticamente os administradores sobre eventos críticos, incluindo violações de segurança, falhas de autenticação, tentativas de acesso não autorizado e alterações de configuração.

14.5 Políticas de retenção e arquivamento de logs

O MyQ X implementa um gerenciamento flexível de logs para equilibrar as necessidades operacionais com os requisitos de conformidade:

Períodos de retenção configuráveis: os administradores definem o número de dias antes que os logs sejam excluídos automaticamente, alinhando a retenção às políticas de governança de dados da organização e aos requisitos regulatórios.

Exportação e arquivamento de logs: os logs podem ser exportados nos formatos Excel ou CSV para armazenamento externo e análise. As exportações programadas permitem o arquivamento automatizado dos logs em intervalos regulares.

Preservação de longo prazo: os logs exportados podem ser armazenados em repositórios seguros e criptografados para manter registros históricos para fins de auditoria, verificação de conformidade e investigação de incidentes.

14.6 Recursos avançados de filtragem e pesquisa

O MyQ X oferece ferramentas sofisticadas para análise e investigação de logs:

Pesquisas salvas: os administradores podem criar, salvar e compartilhar filtros de pesquisa comumente usados para acesso rápido a dados de logs relevantes. As pesquisas salvas podem ser organizadas em pastas para facilitar o gerenciamento.

Filtragem por Período: Filtre logs por intervalos de datas específicos ou períodos predefinidos para concentrar a análise em intervalos de tempo relevantes.

Filtragem por subsistema e contexto: pesquise por subsistemas específicos do MyQ (interface web, terminal, servidor SMTP etc.) e contextos (impressão direta, dispositivos específicos) para isolar eventos relevantes.

Controle de detalhamento: Selecione quais níveis de gravidade de log (Crítico, Erro, Aviso, Informação etc.) serão exibidos, reduzindo o ruído e concentrando-se em eventos significativos.

14.7 Log de auditoria para ações administrativas

O MyQ X rastreia todas as alterações administrativas por meio de um **Log de Auditoria** dedicado:

Alterações de configuração: registra todas as modificações nas configurações do MyQ, incluindo quem fez a alteração, quando foi feita e qual componente do sistema foi afetado.

Gerenciamento de direitos do usuário: Rastreamento detalhado das alterações nas permissões do usuário, associações a grupos e controles de acesso, com a capacidade de visualizar informações detalhadas sobre cada alteração.

Gerenciamento de PINs e credenciais: Rastreamento aprimorado de adições, remoções e modificações de PINs para monitorar o ciclo de vida das credenciais.

Recursos de exportação: os registros de auditoria podem ser exportados sob demanda ou programados para exportação automática regular, atendendo aos requisitos de relatórios de conformidade e retenção de registros.

Essa estrutura abrangente de auditoria e monitoramento garante que o MyQ X forneça aos administradores a visibilidade necessária para manter a segurança, detectar ameaças, garantir a conformidade com políticas e solucionar problemas operacionais de maneira eficaz.

15 Resposta a Incidentes e Recuperação

O MyQ X oferece recursos abrangentes de resposta a incidentes e recuperação, projetados para manter a continuidade dos negócios durante interrupções planejadas e não planejadas. A plataforma combina procedimentos automatizados de backup, recursos de alta disponibilidade e mecanismos flexíveis de failover para garantir que os serviços de impressão permaneçam operacionais mesmo durante interrupções do sistema.

15.1 Procedimentos de resposta a incidentes de segurança

O MyQ X oferece suporte à resposta estruturada a incidentes por meio de diversos mecanismos de monitoramento e alerta:

Detecção de Incidentes em Tempo Real: O monitoramento automatizado acompanha continuamente a integridade do sistema, falhas de autenticação, alterações de configuração e eventos de segurança, permitindo a detecção rápida de possíveis incidentes de segurança.

Escalonamento de alertas: regras configuráveis do Log Notifier acionam notificações imediatas aos administradores quando ocorrem eventos críticos de segurança, incluindo tentativas de autenticação malsucedidas, tentativas de acesso não autorizado e anomalias no sistema.

Preservação da trilha de auditoria: o registro abrangente de todas as atividades do sistema garante que dados forenses completos estejam disponíveis para a investigação de incidentes. O Log de Auditoria do MyQ rastreia todas as ações administrativas, alterações de configuração e atividades dos usuários.

Procedimentos de contenção: No caso de um incidente de segurança, os administradores podem isolar rapidamente os componentes afetados, desativar contas comprometidas e implementar controles de acesso de emergência.

15.2 Procedimentos de recuperação e restauração

O MyQ X implementa recursos robustos de backup e restauração para garantir uma rápida recuperação em caso de falhas do sistema ou perda de dados:

Backup automatizado do banco de dados: Backups automatizados regulares do banco de dados do MyQ capturam todos os dados de configuração, informações de usuários e configurações do sistema. Os backups são protegidos por criptografia com senha e armazenados com segurança.

Restauração completa do sistema: O processo de restauração recupera todo o ambiente do MyQ, incluindo o banco de dados, certificados, arquivos de configuração e relatórios. Os administradores simplesmente selecionam o arquivo de backup e fornecem a senha, caso esteja protegido.

Backup e restauração com suporte a cluster: Para implantações de alta disponibilidade que utilizam o Microsoft Failover Clustering, o MyQ oferece suporte ao backup em armazenamento compartilhado do cluster e à restauração coordenada em todos os nós do cluster.

15.3 Alta disponibilidade e failover

O MyQ X oferece várias estratégias de failover para manter as operações de impressão durante o tempo de inatividade do servidor:

Integração com o Microsoft Failover Clustering: O MyQ X é implantado em configurações ativo-passivo dentro dos clusters de failover do Microsoft Windows Server. O software do cluster monitora continuamente a integridade dos nós e muda automaticamente para os nós passivos quando o nó ativo fica indisponível.

Impressão de reserva: Quando o MyQ Desktop Client detecta perda de conexão com o servidor, ele redireciona automaticamente os trabalhos de impressão para impressoras de reserva pré-configuradas. Assim que a conectividade com o servidor for restaurada, a contabilidade dos trabalhos é atualizada automaticamente.

Fila de impressão no dispositivo: os trabalhos de impressão podem ser armazenados de forma criptografada na memória do dispositivo durante interrupções no servidor. Quando a conectividade é restaurada, os dispositivos transmitem automaticamente os dados de contabilidade para o servidor.

Login offline: os terminais incorporados do MyQ X armazenam em cache as credenciais de autenticação do usuário, permitindo que os usuários façam login e acessem as funcionalidades do dispositivo mesmo quando o servidor estiver indisponível.

Fila de impressão no cliente: os trabalhos são processados localmente nas estações de trabalho dos usuários e armazenados em seus computadores, em vez de no servidor, reduzindo significativamente os requisitos de largura de banda e permitindo a impressão durante a manutenção do servidor ou em caso de problemas de rede.

15.4 Análise e melhoria pós-incidente

O MyQ X oferece suporte à melhoria contínua dos recursos de resposta a incidentes por meio de ferramentas de análise abrangentes:

Análise de registros históricos: os administradores podem revisar os registros exportados para compreender a sequência de eventos que levou a um incidente, identificar as causas-raiz e determinar as ações corretivas apropriadas.

Revisão da trilha de auditoria: O log de auditoria oferece visibilidade completa de todas as ações administrativas e alterações de configuração que possam ter contribuído para ou precedido incidentes de segurança.

Padrões de busca salvos: os administradores podem criar e salvar filtros de busca nos registros para padrões comuns de incidentes, permitindo a identificação rápida de eventos semelhantes no futuro.

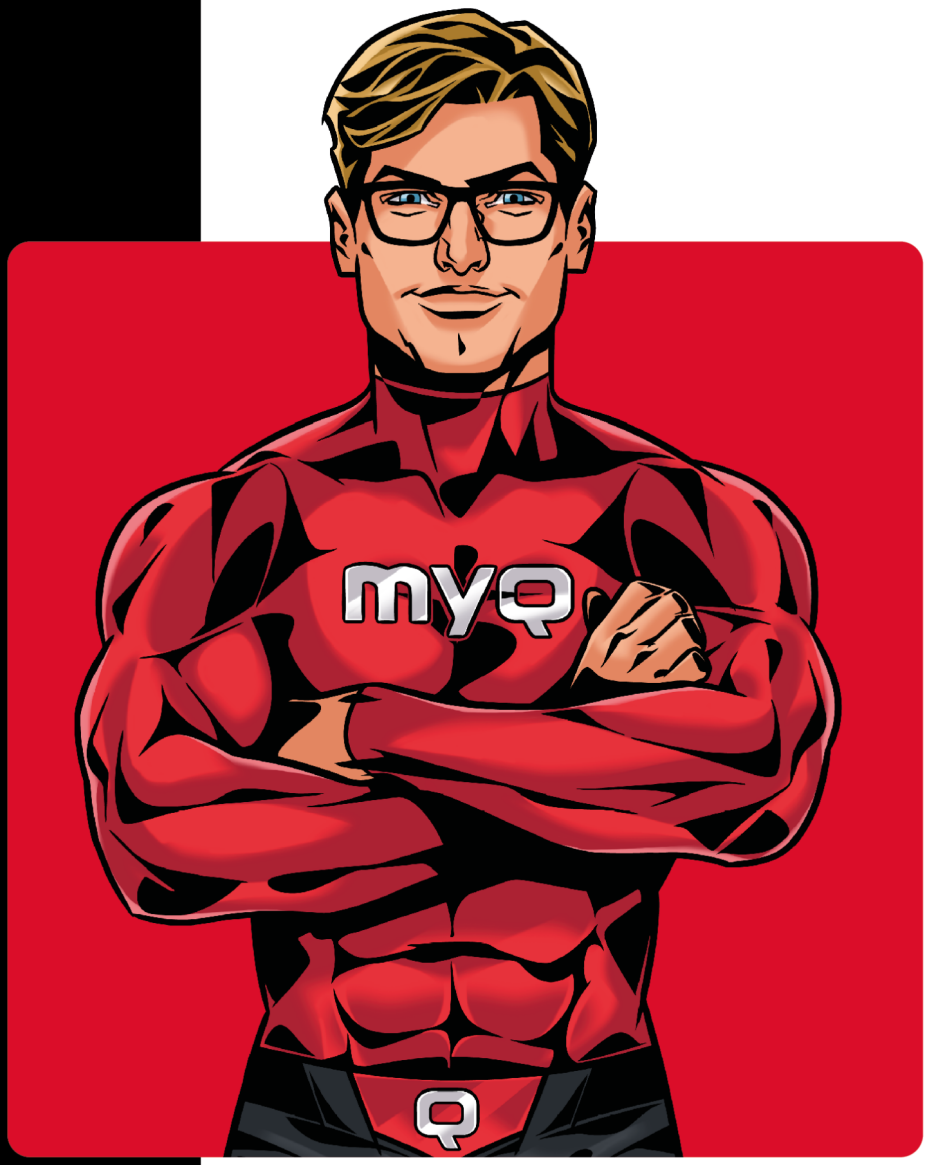
myQ X

POUPE TEMPO COM SOLUÇÕES DE IMPRESSÃO PERSONALIZADAS

MyQ X é uma solução premiada de gestão de impressão on-premises ou em cloud privada, na qual milhões de utilizadores confiam.

info@myq-solution.com

myq-solution.com



50+ milhões
Utilizadores que confiam na MyQ

1+ milhão
Dispositivos ativos

26+
Marcas suportadas

1000+
Parceiros certificados

Presente em **140+** países

Prémios e certificações

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001