

Carta bianca sulla sicurezza di MyQ X 10.x

ITALIANO

Generato da docs.myq-solution.com
agosto/2026
Copyright © 2026 MyQ spol. s r.o. Tutti i diritti riservati.

Avviso sulla traduzione

Questa traduzione è stata realizzata con l'assistenza dell'intelligenza artificiale. In caso di discrepanze o ambiguità, fa fede il documento originale in lingua inglese.

Indice

1 Architettura Zero Trust 7
2 Struttura di protezione trifase 8
2.1 Protezione dell'infrastruttura di stampa 8
2.2 Protezione dei flussi di lavoro di stampa 8
2.3 Protezione della stampa 8
3 Privacy fin dalla progettazione 9
4 Evoluzione continua della sicurezza 10
5 Miglioramenti chiave per la sicurezza in 10.2 11
5.1 Sicurezza TLS migliorata 11
5.2 Miglioramenti alla sicurezza dell'autenticazione 11
5.3 Aggiornamenti alla sicurezza del database 11
5.4 Risoluzione delle vulnerabilità 12
5.5 Sicurezza API e integrazione 12
5.6 Sicurezza amministrativa 12
6 Valore aziendale della gestione sicura della stampa 13
6.1 Mitigazione dei rischi e riduzione dei costi 13
6.2 Principi di sicurezza avanzati 13
6.3 Efficienza operativa 14
6.4 Vantaggi strategici per l'azienda 14
7 Conformità 15
7.1 Certificazione e implementazione ISO 27001:2022 15
7.2 Quadro di conformità al GDPR e misure di protezione dei dati 15
7.3 Requisiti di conformità regionali (HIPAA, SOX) 16
7.4 Pratiche SSDLC (Secure Software Development Lifecycle) 17
7.5 Audit di sicurezza regolari e test di penetrazione 18
7.6 Distinta dei materiali software e gestione delle vulnerabilità 18
8 Implementazione dell’architettura Zero Trust 20
8.1 Principi Zero Trust nella gestione della stampa 20
8.2 Metodologia "Non fidarti mai, verifica sempre" 20
8.3 Segmentazione e isolamento della rete 21
8.4 Autenticazione e verifica robuste 21
8.5 Verifica dei dispositivi e degli endpoint 22

9 Gestione dell’identità e dell’accesso 24
9.1 Implementazione dell'autenticazione a più fattori 24
9.2 Concessione dell'autorizzazione del dispositivo OAuth 2.0 24
9.3 Funzionalità di integrazione Single Sign-On 25
9.4 Controllo degli accessi basato sui ruoli (RBAC) 25
9.5 Supporto multi-tenant Entra ID 26
9.6 Integrazione LDAP e Active Directory 26
9.7 Gestione dei PIN temporanei e politiche di sicurezza 27
9.8 Supporto dell'autenticazione biometrica 27
10 Sicurezza dell’infrastruttura 28
10.1 Rafforzamento della sicurezza dei Print Server 28
10.2 Crittografia del database (implementazione Firebird 4.0) 28
10.3 Applicazione TLS 1.2/1.3 e gestione dei certificati 29
10.4 Sicurezza delle comunicazioni di rete 29
10.5 Configurazione del firewall e gestione delle porte 29
10.6 Sicurezza API e token di autenticazione 29
10.7 Isolamento dei processi e sandboxing 30
10.8 Firma del codice e verifica dell'integrità 30
11 Protezione e crittografia dei dati 31
11.1 Implementazione della crittografia end-to-end 31
11.2 Crittografia dei dati inattivi 31
11.3 Protezione dei dati in transito (crittografia TLS) 32
11.4 Crittografia dei lavori di stampa e archiviazione sicura 32
11.5 Miglioramenti alla crittografia del database 32
11.6 Crittografia dei backup e archiviazione sicura 33
11.7 Politiche di gestione e rotazione delle chiavi 33
11.8 Minimizzazione dei dati e privacy by design 34
12 Flussi di lavoro di stampa sicuri 35
12.1 Implementazione del rilascio sicuro della stampa 35
12.2 Flussi di lavoro di Pull Printing 35
12.3 Timeout del lavoro di stampa ed eliminazione automatica 36
12.4 Filigrane e firme digitali 36
12.5 Anteprima di stampa e convalida dei contenuti 37
12.6 Gestione degli errori e ripristino sicuro dei lavori di stampa 37
13 Sicurezza dei dispositivi e della rete 38

13.1 Rafforzamento della sicurezza dei dispositivi multifunzione 38
13.2 Segmentazione della rete e configurazione VLAN 38
13.3 Implementazione della sicurezza SNMP v3 39
13.4 Gestione delle credenziali della stampante 39
13.5 Sicurezza del firmware e gestione degli aggiornamenti 39
13.6 Gestione e restrizioni delle porte USB 40
14 Audit e monitoraggio 41
14.1 Monitoraggio e avvisi in tempo reale 41
14.2 Registrazione e analisi delle attività di stampa 41
14.3 Analisi del comportamento degli utenti 42
14.4 Rilevamento e risposta agli incidenti 42
14.5 Politiche di conservazione e archiviazione dei log 43
14.6 Funzionalità avanzate di filtraggio e ricerca 43
14.7 Registro di controllo per le azioni amministrative 44
15 Risposta agli incidenti e recupero 45
15.1 Procedure di risposta agli incidenti di sicurezza 45
15.2 Procedure di ripristino e recupero 45
15.3 Alta disponibilità e failover 46
15.4 Analisi post-incidente e miglioramento 46

Panoramica delle funzionalità di sicurezza di MyQ X

MyQ X offre una serie di funzionalità volte a migliorare la sicurezza e la privacy degli utenti finali e dell'azienda. Queste funzionalità includono la stampa sicura dal dispositivo multifunzione, la personalizzazione della sessione utente e continuano ad avere un impatto anche dopo la stampa del documento grazie all'utilizzo di filigrane.

Di seguito è riportato un breve riassunto delle funzionalità di sicurezza di MyQ X:

- Conformità al GDPR
- Stampa sicura
- Sessioni utente con diverse opzioni di autenticazione, compresa l'autenticazione a due fattori.
- Logout manuale e automatico dalle sessioni utente
- Crittografia dei dati end-to-end, compresa la crittografia dei dati inattivi (database, lavori, registri)
- Cartelle di destinazione della scansione predefinite dall'amministratore MyQ
- Code private per l'eliminazione immediata dei lavori di stampa dopo il rilascio
- Modalità privacy per l'anonimizzazione dei nomi dei lavori di stampa
- Accesso limitato alle opzioni di configurazione del Print Server sull'interfaccia web MyQ X
- Diritti personalizzabili per l'accesso a diverse opzioni di configurazione
- Livelli multipli di complessità delle password
- Registro di controllo delle modifiche alle impostazioni
- Supporto per l'autorità di certificazione aziendale
- Applicazione di filigrane ai documenti stampati
- Anteprima del lavoro
- Controllo dei documenti digitalizzati tramite sistemi OCR e DMS
- Archiviazione dei lavori di stampa

L'approccio alla sicurezza di MyQ X si basa sul principio che **La sicurezza non è un elemento secondario, ma parte integrante dell'intero ecosistema di gestione della stampa.**La piattaforma implementa una strategia di difesa completa che protegge i dati e i flussi di lavoro in ogni fase del ciclo di vita dei documenti.

1 Architettura Zero Trust

Seguendo la metodologia "non fidarti mai, verifica sempre", MyQ X parte dal presupposto che le minacce possano provenire sia dall'interno che dall'esterno di una rete. Ogni connessione, utente e dispositivo deve essere autenticato e autorizzato prima di accedere alle risorse di stampa, garantendo una verifica continua durante tutte le interazioni.

2 Struttura di protezione trifase

MyQ X affronta la questione della sicurezza attraverso tre fasi fondamentali:

2.1 Protezione dell'infrastruttura di stampa

Tutte le infrastrutture di supporto sono adeguatamente protette prima della stampa di qualsiasi documento, comprese le workstation, i dispositivi mobili, i server, le reti e i dispositivi di stampa.

2.2 Protezione dei flussi di lavoro di stampa

Flussi di lavoro sicuri e comprovati, tra cui il rilascio di stampe autenticate, l'isolamento dei lavori e la reportistica completa, prevengono le vulnerabilità che potrebbero esporre le organizzazioni a rischi.

2.3 Protezione della stampa

Protezione continua tramite filigrana, firme digitali e registri di controllo completi che garantiscono la tracciabilità e incoraggiano un comportamento responsabile da parte degli utenti.

3 Privacy fin dalla progettazione

La protezione dei dati è integrata nell'architettura di MyQ X sin dalla sua concezione. Il sistema riduce al minimo la raccolta di dati, implementa una crittografia avanzata e offre agli utenti il controllo sulle proprie informazioni personali per garantire la conformità al GDPR e la protezione della privacy.

4 Evoluzione continua della sicurezza

MyQ X garantisce la sicurezza attraverso aggiornamenti regolari, risoluzione tempestiva delle vulnerabilità, integrazione delle informazioni sulle minacce e valutazioni e certificazioni di sicurezza continue da parte di terzi.

Questo approccio incentrato sulla sicurezza garantisce alle organizzazioni la possibilità di implementare MyQ X con la certezza che le loro informazioni sensibili, i requisiti di conformità e la continuità operativa siano protetti da misure di sicurezza leader nel settore.

5 Miglioramenti chiave per la sicurezza in 10.2

MyQ X 10.2 introduce significativi miglioramenti alla sicurezza progettati per rafforzare la protezione contro le minacce informatiche in continua evoluzione, mantenendo al contempo l'efficienza operativa. Questi miglioramenti risolvono vulnerabilità critiche e implementano standard di sicurezza moderni.

5.1 Sicurezza TLS migliorata

Versione minima TLS 1.2 predefinita: MyQ X 10.2 aumenta la versione TLS minima predefinita da 1.1 a 1.2, con supporto per TLS 1.3. Ciò elimina il supporto per i protocolli SSL obsoleti e i codici di cifratura deboli che comportano rischi per la sicurezza.

Convalida dei certificati migliorata: la convalida dei certificati migliorata impedisce l'uso di certificati scaduti o emessi in modo improprio, proteggendo dagli attacchi man-in-the-middle e da altre vulnerabilità. Il sistema ora si fida automaticamente dei certificati CA radice provenienti dall'archivio dei certificati di sistema del server.

5.2 Miglioramenti alla sicurezza dell'autenticazione

Maggiore sicurezza di password e PIN: gli algoritmi di hashing delle password migliorati rafforzano la protezione delle credenziali. Il sistema introduce nuove regole di sicurezza per i PIN, tra cui la lunghezza minima obbligatoria di 6 cifre e la prevenzione di combinazioni facilmente intuibili come "1234" o "1111".

Protezione dei tentativi di accesso: i tentativi di autenticazione non riusciti sono ora limitati per motivi di sicurezza. Per impostazione predefinita, i client/dispositivi vengono bloccati per 5 minuti dopo più di 5 tentativi di accesso non validi entro 60 secondi, con periodi di tempo configurabili.

Miglioramento della registrazione degli eventi di accesso: la registrazione avanzata degli eventi di accesso, in particolare dei tentativi di autenticazione non riusciti, semplifica il filtraggio e il monitoraggio degli eventi di sicurezza in MyQ Log per gli amministratori.

5.3 Aggiornamenti alla sicurezza del database

Implementazione di Firebird 4.0: l'aggiornamento al motore di database Firebird 4.0 offre funzionalità di sicurezza avanzate e prestazioni migliorate. Le password del database sono ora oscurate nei file di log per impedire l'esposizione delle credenziali.

Protezione dei dati migliorata: accesso limitato ai dati sensibili tramite report personalizzati e account di reporting esterni, garantendo la riservatezza dei dati a diversi livelli di accesso.

5.4 Risoluzione delle vulnerabilità

Correzioni CVE critiche: MyQ X 10.2 risolve diverse vulnerabilità critiche, tra cui:

- CVE-2024-28059: vulnerabilità di esecuzione di codice remoto non autenticato.
- CVE-2024-22076: Miglioramenti alla sicurezza dello scripting PHP.
- CVE-2023-45853, CVE-2023-5678, CVE-2023-49316: vulnerabilità dei componenti di terze parti.

Aggiornamenti di sicurezza dei componenti: le versioni aggiornate di componenti critici, tra cui OpenSSL 3.1.0, PHP 8.3.14 e Apache 2.4.57, risolvono vulnerabilità di sicurezza note.

5.5 Sicurezza API e integrazione

Restrizioni API REST: ambiti limitati per client noti e rimozione delle funzionalità per operazioni sensibili come la modifica dei server di autenticazione degli utenti, rafforzando la sicurezza delle API.

Controlli di scripting PHP: le nuove impostazioni Easy Config consentono agli amministratori di bloccare/sbloccare l'accesso allo scripting PHP, migliorando la sicurezza mantenendo queste impostazioni in modalità di sola lettura.

5.6 Sicurezza amministrativa

Maggiore sicurezza degli account amministrativi: la password amministrativa predefinita è stata rimossa per le nuove installazioni. Gli amministratori possono ora disabilitare gli account amministrativi quando non sono necessari, promuovendo l'uso di account utente specifici con diritti appropriati piuttosto che account amministrativi condivisi.

Questi miglioramenti alla sicurezza dimostrano l'impegno di MyQ X nel mantenere standard di sicurezza di livello aziendale, affrontando al contempo le sfide contemporanee della sicurezza informatica. Aggiornamenti di sicurezza regolari e una gestione proattiva delle vulnerabilità garantiscono alle organizzazioni di poter implementare MyQ X con fiducia nella propria sicurezza.

6 Valore aziendale della gestione sicura della stampa

La gestione sicura della stampa offre un valore aziendale misurabile trasformando l'infrastruttura di stampa da una potenziale responsabilità a una risorsa strategica per la sicurezza. MyQ X fornisce alle organizzazioni una protezione completa che affronta l'intera gamma di rischi legati alla stampa, migliorando al contempo l'efficienza operativa.

6.1 Mitigazione dei rischi e riduzione dei costi

Prevenzione della violazione dei dati: Secure Print Release garantisce che i documenti riservati non vengano mai lasciati incustoditi nei vassoi delle stampanti, eliminando l'accesso non autorizzato alle informazioni sensibili. Gli utenti effettuano l'autenticazione prima che i loro lavori di stampa vengano rilasciati, mantenendo il controllo completo sulla sicurezza dei documenti.

Evitare i costi di conformità: le funzionalità di conformità GDPR, HIPAA e SOX integrate aiutano le organizzazioni a evitare sanzioni normative e a ridurre i costi di preparazione degli audit attraverso controlli di conformità automatizzati e audit trail completi.

Continuità operativa: la funzione Device Spooling di MyQ mantiene le capacità di stampa durante le interruzioni del server, memorizzando i lavori crittografati localmente per un massimo di una settimana su 10 dispositivi, evitando interruzioni dell'attività durante la manutenzione del sistema o tempi di inattività imprevisti.

6.2 Principi di sicurezza avanzati

Implementazione Zero Trust: richiedendo l'autenticazione per ogni lavoro di stampa, MyQ X applica i principi "non fidarti mai, verifica sempre" in tutto l'ambiente di stampa, rafforzando la sicurezza complessiva dell'organizzazione.

Tracciabilità dei documenti: la filigrana e le firme digitali consentono alle organizzazioni di tracciare i documenti riservati durante tutto il loro ciclo di vita, garantendo la responsabilità e scoraggiando l'uso improprio delle informazioni sensibili.

Crittografia completa: la crittografia end-to-end dei dati di stampa, dei database e dei lavori di stampa memorizzati garantisce che le informazioni sensibili rimangano

protette durante l'intero flusso di lavoro dei documenti, soddisfacendo i rigorosi requisiti di sicurezza.

6.3 Efficienza operativa

Ottimizzazione della larghezza di banda: il client spooling riduce il traffico di rete elaborando i lavori a livello locale, migliorando le prestazioni in ambienti con larghezza di banda limitata, come uffici remoti e filiali.

Autenticazione flessibile: diverse opzioni di autenticazione, tra cui carte d'identità, PIN, password e autenticazione tramite app mobile, offrono agli utenti metodi di accesso comodi ma sicuri che si adattano alle diverse esigenze aziendali. È disponibile anche l'autenticazione a più fattori (MFA), che combina questi metodi.

Gestione centralizzata: le politiche di sicurezza unificate su tutti i dispositivi semplificano l'amministrazione, garantendo al contempo standard di protezione coerenti in tutta l'organizzazione.

6.4 Vantaggi strategici per l'azienda

Vantaggio competitivo: dimostrare solide capacità di sicurezza di stampa può differenziare le organizzazioni nei mercati competitivi, in particolare nei settori che trattano dati sensibili o servono clienti attenti alla sicurezza.

Fiducia dei dipendenti: i flussi di lavoro di stampa sicuri danno agli utenti la certezza che i loro documenti sono protetti, migliorando la produttività e riducendo le preoccupazioni relative alla sicurezza che possono influire sull'efficienza sul posto di lavoro.

Infrastruttura pronta per il futuro: il framework di sicurezza completo di MyQ X consente alle organizzazioni di adattarsi alle minacce alla sicurezza informatica in continua evoluzione e ai requisiti normativi senza grandi revisioni dell'infrastruttura.

La gestione sicura della stampa con MyQ X trasforma la stampa da una potenziale vulnerabilità di sicurezza in un processo aziendale controllato, verificabile e conforme che supporta gli obiettivi organizzativi proteggendo al contempo le preziose risorse informative.

7 Conformità

Il quadro di conformità completo di MyQ X dimostra il suo impegno a soddisfare i più elevati standard di sicurezza internazionali e i requisiti normativi. Questo approccio multilivello garantisce alle organizzazioni di poter implementare MyQ X con fiducia, soddisfacendo al contempo i diversi requisiti di conformità in tutti i settori e giurisdizioni.

7.1 Certificazione e implementazione ISO 27001:2022

MyQ ha ottenuto **la certificazione ISO/IEC 27001:2022**, stabilendo un approccio sistematico alla gestione della sicurezza delle informazioni che soddisfa le migliori pratiche internazionali. L'implementazione comprende:

Quadro di gestione dei rischi: processi completi di valutazione dei rischi che identificano, valutano e mitigano i rischi per la sicurezza delle informazioni in tutte le operazioni aziendali e nelle implementazioni dei clienti.

Implementazione dei controlli di sicurezza: implementazione strutturata di controlli di sicurezza tecnici, amministrativi e fisici che proteggono le risorse informative durante tutto il loro ciclo di vita.

Processo di miglioramento continuo: revisioni e aggiornamenti regolari delle politiche, delle procedure e dei controlli di sicurezza per affrontare le minacce in evoluzione e mantenere la conformità alla certificazione.

Impegno della direzione: supervisione a livello esecutivo che garantisce che la sicurezza rimanga integrata nella strategia aziendale e nei processi decisionali operativi.

La certificazione convalida l'approccio sistematico di MyQ alla protezione dei dati dei clienti e al mantenimento della riservatezza, dell'integrità e della disponibilità dei sistemi informativi.

7.2 Quadro di conformità al GDPR e misure di protezione dei dati

MyQ X implementa **una conformità** completa **al GDPR** attraverso principi di privacy by design integrati nell'architettura del sistema:

Minimizzazione dei dati: il sistema raccoglie solo i metadati essenziali necessari per la funzionalità operativa, evitando il trattamento superfluo dei dati personali che potrebbe aumentare i rischi di conformità.

Gestione dei diritti degli utenti: implementazione completa dei diritti degli utenti GDPR, tra cui:

- Diritto di accesso ai dati personali
- Diritto di rettifica delle informazioni inesatte
- Diritto alla cancellazione ("diritto all'oblio")
- Diritto alla portabilità dei dati
- Diritto di limitazione del trattamento

Valutazioni d'impatto sulla protezione dei dati: valutazione sistematica dei rischi per la privacy relativi a nuove funzionalità e implementazioni, garantendo il mantenimento della conformità al GDPR durante l'evoluzione del sistema.

7.3 Requisiti di conformità regionali (HIPAA, SOX)

MyQ X supporta i framework di conformità specifici del settore attraverso solide funzionalità di protezione dei dati e di audit:

Conformità HIPAA per il settore sanitario:

- Crittografia delle informazioni sanitarie protette (PHI) inattive e in transito.
- Registrazione completa di tutti gli accessi ai dati sanitari sensibili.
- Controlli di accesso basati sui ruoli che limitano l'accesso alle PHI solo al personale autorizzato.
- Procedure di backup e ripristino sicure per i requisiti di conservazione dei dati sanitari.

Conformità SOX per i servizi finanziari:

- Audit trail dettagliati per l'elaborazione e la stampa di documenti finanziari.
- Controlli di accesso che impediscono la modifica non autorizzata dei registri finanziari.
- Funzionalità di archiviazione sicure che supportano i requisiti normativi di conservazione.
- Separazione dei compiti attraverso autorizzazioni basate sui ruoli e flussi di lavoro di approvazione.

Controlli di sicurezza aggiuntivi:

- Crittografia del database utilizzando algoritmi standard del settore.
- Protocolli di comunicazione sicuri per tutte le trasmissioni di dati.
- Procedure di backup automatizzate con crittografia e verifica dell'integrità.
- Registrazione e monitoraggio degli accessi per la reportistica di conformità.

7.4 Pratiche SSDLC (Secure Software Development Lifecycle)

MyQ implementa un ciclo di vita dello sviluppo software sicuro in linea con gli standard di settore e i requisiti della catena di fornitura **SLSA**, garantendo che le pratiche di sicurezza siano integrate in tutte le fasi del ciclo di vita del software.

Analisi

MyQ esegue **una** rigorosa **modellazione delle minacce** e definisce chiari **requisiti di sicurezza** durante la fase di analisi iniziale, consentendo l'identificazione precoce dei rischi e stabilendo una solida base di sicurezza prima dell'inizio della progettazione.

Progettazione

Tutte le proposte architetturali sono sottoposte a **revisioni** formali **dell'architettura di sicurezza** per convalidare l'aderenza a principi quali **il privilegio minimo**, **lo zero trust** e **la difesa in profondità**, garantendo che la sicurezza sia sistematicamente integrata nella progettazione del sistema.

Sviluppo

Gli sviluppatori seguono **pratiche di codifica sicure** e processi di revisione tra pari, mentre tutte le build vengono eseguite su **server di build** dedicati, isolati **e conformi allo standard SLSA**, garantendo la protezione dell'integrità del codice sorgente e degli artefatti di build.

Test

I test di sicurezza includono **SAST** automatizzato e **scansione delle dipendenze** integrati nelle pipeline CI, consentendo il rilevamento tempestivo delle vulnerabilità sia nel codice personalizzato che nei componenti di terze parti.

Distribuzione

Tutti gli artefatti di rilascio sono protetti tramite **la firma del codice** e verificati durante la distribuzione, garantendo **integrità**, **autenticità** e consegna controllata negli ambienti di produzione.

Manutenzione

Dopo la distribuzione, i sistemi sono sottoposti a **monitoraggio** continuo e **gestione** strutturata **delle patch**, garantendo un allineamento costante con le minacce in evoluzione e **le migliori pratiche di sicurezza**.

7.5 Audit di sicurezza regolari e test di penetrazione

MyQ mantiene una solida convalida della sicurezza attraverso programmi sistematici di test e valutazione:

Test di penetrazione automatizzati: l'integrazione con la piattaforma di sicurezza Qualys fornisce una valutazione continua delle vulnerabilità e test di penetrazione per tutte le versioni del software.

Valutazioni di sicurezza di terze parti: audit di sicurezza indipendenti condotti da organizzazioni esterne qualificate per convalidare i controlli di sicurezza e identificare potenziali miglioramenti.

Revisioni interne di sicurezza: valutazioni interne regolari delle politiche di sicurezza, delle procedure e dei controlli tecnici per garantire l'efficacia e la conformità continue.

Processo di risposta alle vulnerabilità: procedure strutturate per affrontare i problemi di sicurezza identificati, compresi i requisiti temporali per lo sviluppo e l'implementazione delle patch.

7.6 Distinta dei materiali software e gestione delle vulnerabilità

MyQ implementa una sicurezza completa della catena di fornitura attraverso il monitoraggio dettagliato dei componenti e la gestione delle vulnerabilità:

Pubblicazione SBOM: documentazione completa della distinta dei materiali software che identifica tutti i componenti, le librerie e le dipendenze di terze parti utilizzati nei sistemi MyQ X.

Scansione automatizzata delle vulnerabilità: monitoraggio continuo dei database dei componenti per individuare nuove vulnerabilità che interessano le dipendenze di MyQ X.

Gestione rapida delle patch: processo sistematico per la valutazione, il test e la distribuzione degli aggiornamenti di sicurezza per i componenti di terze parti, con priorità basata sulla valutazione dei rischi.

Controllo della versione dei componenti: tracciamento dettagliato di tutti i componenti software, inclusi i numeri di versione, i livelli delle patch di sicurezza e i programmi di aggiornamento, come documentato nelle note di rilascio.

Valutazione della sicurezza dei fornitori: valutazione dei fornitori di software di terze parti per garantire che mantengano standard di sicurezza e processi di divulgazione delle vulnerabilità adeguati.

Questo quadro di conformità completo garantisce che MyQ X soddisfi diversi requisiti normativi, mantenendo i più elevati standard di sicurezza delle informazioni e protezione dei dati in tutti gli ambienti operativi.

8 Implementazione dell’architettura Zero Trust

MyQ X implementa l'architettura Zero Trust come approccio di sicurezza fondamentale che elimina la fiducia implicita e convalida continuamente ogni transazione. Questo framework completo garantisce che nessun utente, dispositivo o connessione di rete sia considerato affidabile per impostazione predefinita, indipendentemente dalla loro posizione o dallo stato di autenticazione precedente.

8.1 Principi Zero Trust nella gestione della stampa

L'implementazione Zero Trust di MyQ X si basa sul principio **"non fidarti mai, verifica sempre"** in tutto il sistema di gestione della stampa. Il sistema richiede una verifica esplicita per ogni richiesta di accesso, garantendo che:

Canali di comunicazione crittografati: tutto il traffico di rete utilizza la crittografia TLS obbligatoria con versione minima 1.2, impedendo l'intercettazione e la manomissione durante la trasmissione dei dati. I certificati HTTPS devono essere configurati e convalidati correttamente per prevenire attacchi man-in-the-middle.

Applicazione di protocolli sicuri: MyQ X blocca il traffico HTTP non crittografato e applica protocolli di sicurezza rigorosi su tutti i canali di comunicazione, comprese le connessioni SMTP, LDAP e SNMP. I protocolli legacy come SNMPv1 sono vietati a favore di SNMPv3 con autenticazione forte.

Controlli di sicurezza API: l'accesso all'API REST richiede token di autenticazione con filtraggio degli indirizzi IP, garantendo che le chiamate API siano autenticate e provengano da fonti affidabili. I segreti dei client vengono sottoposti a rotazione periodica per mantenere l'integrità della sicurezza.

8.2 Metodologia "Non fidarti mai, verifica sempre"

La metodologia Zero Trust permea ogni aspetto delle operazioni di MyQ X attraverso meccanismi di verifica continua:

Verifica dell'identità: ogni interazione dell'utente richiede l'autenticazione, indipendentemente dalla posizione di rete o dallo stato di affidabilità del dispositivo. Gli utenti devono autenticarsi su ogni dispositivo di stampa, anche se hanno già effettuato l'accesso altrove nell'organizzazione.

Autenticazione dei dispositivi: i dispositivi di stampa stessi devono autenticarsi prima di accedere alle risorse di rete, con credenziali e certificati univoci che impediscono lo spoofing non autorizzato dei dispositivi.

Gestione delle sessioni: le sessioni degli utenti implementano la funzionalità di timeout e logout automatici, garantendo che le sessioni abbandonate non possano essere sfruttate da persone non autorizzate.

8.3 Segmentazione e isolamento della rete

MyQ X implementa una segmentazione completa della rete per limitare le superfici di attacco e contenere potenziali violazioni della sicurezza:

Controlli dei confini di rete: il sistema applica rigide regole firewall che bloccano le porte inutilizzate e limitano l'accesso alla rete solo ai canali di comunicazione necessari. Le configurazioni predefinite disabilitano i servizi e i protocolli non necessari.

Segmentazione basata su certificati: MyQ X supporta tre modalità di gestione dei certificati - Autorità di certificazione integrata, Autorità di certificazione aziendale e Gestione manuale dei certificati - consentendo alle organizzazioni di implementare confini di fiducia appropriati in base alle loro politiche di sicurezza.

Applicazione FQDN: tutte le comunicazioni di rete devono utilizzare nomi di dominio completi (FQDN) anziché indirizzi IP o nomi a etichetta singola, impedendo attacchi man-in-the-middle basati su DNS e garantendo una corretta convalida dei certificati.

Gestione delle porte: il sistema gestisce automaticamente le regole del firewall e fornisce un controllo esplicito sulle porte di rete accessibili, riducendo la superficie di attacco attraverso il blocco sistematico delle porte.

8.4 Autenticazione e verifica robuste

MyQ X mantiene una convalida continua della sicurezza attraverso più livelli di autenticazione e monitoraggio in tempo reale:

Autenticazione multimodale: il sistema supporta diversi metodi di autenticazione, tra cui LDAP, Microsoft Entra ID, RADIUS e autenticazione MyQ locale, con funzionalità di failover automatico che garantiscono un controllo continuo degli accessi.

Integrazione del server di autenticazione: l'integrazione sicura con server di autenticazione esterni utilizza connessioni crittografate (TLS per LDAP, protocolli

sicuri per RADIUS) e applica segreti condivisi forti specifici per ogni implementazione MyQ.

Monitoraggio degli accessi: la registrazione avanzata degli eventi di autenticazione, in particolare dei tentativi di accesso non riusciti, consente agli amministratori di rilevare e rispondere a potenziali minacce alla sicurezza. I tentativi di autenticazione non riusciti attivano meccanismi di blocco automatico: per impostazione predefinita, i dispositivi vengono bloccati per 5 minuti dopo più di 5 tentativi non validi entro 60 secondi.

Controlli di persistenza della sessione: il sistema implementa politiche di timeout della sessione configurabili e funzionalità di logout automatico, garantendo che le sessioni inattive non possano essere sfruttate.

8.5 Verifica dei dispositivi e degli endpoint

MyQ X applica rigorosi protocolli di verifica dei dispositivi per garantire che solo gli endpoint autorizzati possano accedere alle risorse di stampa:

Gestione dei certificati dei dispositivi: tutti i dispositivi collegati devono presentare certificati validi per la comunicazione di rete. Il sistema mantiene un archivio completo di certificati con una corretta convalida della catena e supporta la distribuzione automatica dei certificati tramite Group Policy o Mobile Device Management (MDM).

Controlli di sicurezza degli endpoint: i dispositivi di stampa sono sottoposti a una continua convalida della sicurezza, inclusa l'autenticazione SNMP v3 con password complesse e algoritmi crittografici (SHA1 e AES). Le credenziali della stampante sono gestite tramite protocolli di sicurezza specifici del fornitore con password complesse generate in modo casuale.

Autenticazione dei dispositivi mobili: MyQ X Mobile Client implementa OAuth 2.0 Device Authorization Grant per l'autenticazione sicura dei dispositivi mobili, sostituendo i sistemi legacy basati su PIN con una moderna sicurezza biometrica.

Struttura di sicurezza BYOD: il sistema supporta gli ambienti Bring-Your-Own-Device (BYOD) attraverso la propagazione sicura della stampa tramite AirPrint e Mopria, mantenendo i principi zero-trust anche nelle reti senza visibilità diretta del Print Server.

Gestione dei token di accesso: vengono emessi token di accesso univoci per ogni tipo di dispositivo, con Transport Layer Security (TLS) obbligatorio per tutte le comunicazioni. Il sistema implementa controlli di accesso Just-in-Time (JIT) che

regolano dinamicamente i privilegi in base al contesto e alla valutazione continua del rischio.

Questa implementazione completa Zero Trust garantisce che MyQ X mantenga i più elevati standard di sicurezza, supportando al contempo diverse esigenze organizzative e scenari di implementazione. L'architettura fornisce una protezione approfondita che si adatta all'evoluzione delle minacce, mantenendo l'efficienza operativa e l'esperienza utente.

9 Gestione dell’identità e dell’accesso

MyQ X fornisce un framework completo per la gestione delle identità e degli accessi che si integra perfettamente con i sistemi di autenticazione aziendali esistenti, supportando al contempo i moderni standard di sicurezza. L'architettura IAM garantisce un'autenticazione degli utenti sicura, scalabile e flessibile in diversi ambienti organizzativi.

9.1 Implementazione dell'autenticazione a più fattori

MyQ X implementa solide funzionalità **di autenticazione a più fattori (MFA)** che migliorano significativamente la sicurezza richiedendo più fattori di verifica:

Autenticazione tramite Embedded Terminal: i metodi MFA standard includono combinazioni di carta d'identità e PIN, in cui gli utenti presentano prima la loro carta d'identità fisica e poi confermano la loro identità con un codice PIN. In alternativa, l'autenticazione tramite carta d'identità e password fornisce una sicurezza a due fattori simile con la verifica della password al posto del PIN.

Autenticazione basata su dispositivi mobili: MyQ X Mobile Client consente una sofisticata autenticazione MFA tramite la scansione di codici QR combinata con la verifica biometrica. Gli utenti si autenticano scansionando un codice QR visualizzato sul terminale integrato, con una sicurezza aggiuntiva fornita tramite blocchi biometrici (Face ID o impronta digitale) sui loro dispositivi mobili.

Integrazione del Desktop Client: le organizzazioni che utilizzano i servizi Microsoft 365 beneficiano dell'autenticazione MFA integrata tramite Entra ID. Agli utenti con l'autenticazione a due fattori abilitata nei propri account Entra ID viene automaticamente richiesto di verificare la propria identità utilizzando applicazioni di autenticazione quando accedono al Desktop Client.

9.2 Concessione dell'autorizzazione del dispositivo OAuth 2.0

MyQ X supporta lo standard **OAuth 2.0 Authorization Code Grant**, consentendo l'integrazione sicura con i moderni provider di identità e le applicazioni di terze parti:

Flusso OAuth standard: il sistema implementa il framework di autorizzazione OAuth 2.0 completo, compresa la presentazione della pagina di accesso, la generazione di codici di accesso monouso e il recupero sicuro dei token. Le applicazioni client ricevono token bearer con tempi di scadenza configurabili e ambiti concessi.

Sicurezza dell'integrazione API: i token OAuth devono essere forniti per tutti gli accessi agli endpoint API, garantendo che le integrazioni di terze parti mantengano un'autenticazione adeguata. Il sistema supporta la convalida dell'ID client e del segreto client con corrispondenza URI di reindirizzamento sicura.

Gestione dei token: i token di accesso includono controlli di scadenza (1800 secondi di default) e restrizioni di ambito, fornendo un controllo granulare sui permessi di accesso alle API e mantenendo la sicurezza attraverso la rotazione dei token.

9.3 Funzionalità di integrazione Single Sign-On

MyQ X fornisce un'integrazione **Single Sign-On (SSO)** completa che semplifica l'autenticazione degli utenti in tutti gli ambienti aziendali:

Integrazione con Microsoft 365: la profonda integrazione con Microsoft Entra ID consente un SSO senza soluzione di continuità per le organizzazioni che utilizzano i servizi Microsoft 365. Gli utenti possono autenticarsi utilizzando le loro credenziali Microsoft esistenti, eliminando la necessità di password MyQ separate.

Servizi di directory aziendali: le funzionalità SSO si estendono a vari server di autenticazione, tra cui Active Directory, OpenLDAP e Novell eDirectory, consentendo agli utenti di sfruttare le credenziali aziendali esistenti per l'accesso a MyQ.

Autenticazione multipiattaforma: la funzionalità SSO funziona su tutti i componenti MyQ X, inclusi Desktop Client, Mobile Client e Embedded Terminal, fornendo esperienze di autenticazione coerenti indipendentemente dal metodo di accesso.

9.4 Controllo degli accessi basato sui ruoli (RBAC)

MyQ X implementa **un** sofisticato **controllo degli accessi basato sui ruoli** che si allinea ai requisiti di sicurezza aziendali:

Gestione granulare delle autorizzazioni: il sistema fornisce un controllo dettagliato delle autorizzazioni degli utenti, consentendo agli amministratori di definire diritti di accesso specifici in base ai ruoli e alle responsabilità organizzative.

Amministrazione basata sui gruppi: l'implementazione RBAC supporta sia le autorizzazioni dei singoli utenti che il controllo degli accessi basato sui gruppi, consentendo una gestione efficiente di grandi popolazioni di utenti attraverso l'assegnazione di gruppi di sicurezza.

Applicazione del principio del privilegio minimo: i controlli di accesso seguono il principio del privilegio minimo, garantendo che gli utenti ricevano solo le

autorizzazioni minime necessarie per le loro funzioni lavorative, mantenendo al contempo l'efficienza operativa.

9.5 Supporto multi-tenant Entra ID

MyQ X fornisce un solido supporto per **gli ambienti multi-tenant Microsoft Entra ID**:

Autenticazione cross-tenant: il sistema è in grado di autenticare gli utenti su più tenant Entra ID, supportando strutture organizzative complesse con più istanze Azure AD.

Isolamento tenant: il supporto multi-tenant include adeguati meccanismi di isolamento che impediscono l'accesso ai dati tra tenant, mantenendo al contempo le funzionalità di gestione centralizzata di MyQ.

Gestione ibrida delle identità: l'integrazione supporta sia scenari di identità solo cloud che ibridi, adattandosi alle organizzazioni con Active Directory on-premise sincronizzato con Entra ID.

9.6 Integrazione LDAP e Active Directory

MyQ X offre funzionalità complete **di integrazione LDAP e Active Directory**:

Opzioni di sincronizzazione flessibili: il sistema supporta diversi metodi di sincronizzazione, tra cui la sincronizzazione completa, la sincronizzazione selettiva degli attributi e la sincronizzazione condizionale basata su filtri LDAP. Gli amministratori possono scegliere tra la sostituzione completa, l'aggiunta o gli aggiornamenti condizionali per le proprietà delle schede e dei PIN.

Funzionalità di filtraggio avanzate: la sincronizzazione LDAP include sofisticate opzioni di filtraggio che utilizzano la sintassi standard dei filtri LDAP, consentendo l'importazione selettiva degli utenti in base alle unità organizzative, all'appartenenza a gruppi o ad attributi personalizzati.

Importazione della struttura di gruppo: il sistema può importare strutture organizzative complete, inclusi gruppi di sicurezza, gruppi di distribuzione e gerarchie di gruppi nidificati da Active Directory, mantenendo le relazioni organizzative all'interno di MyQ.

Autenticazione sicura: tutte le comunicazioni LDAP utilizzano la crittografia TLS per proteggere le credenziali e i dati degli utenti durante la sincronizzazione. Il sistema supporta sia il tradizionale LDAP su TLS che le connessioni LDAP sicure.

9.7 Gestione dei PIN temporanei e politiche di sicurezza

MyQ X implementa **una gestione** completa **dei PIN e politiche di sicurezza**:

Sicurezza PIN migliorata: la versione 10.2 introduce una maggiore sicurezza dei PIN, tra cui la lunghezza minima obbligatoria di 6 cifre e la prevenzione di combinazioni facilmente intuibili come "1234" o "1111".

Emissione di PIN temporanei: il sistema supporta codici PIN temporanei che possono essere emessi per periodi di tempo specifici o scenari di utilizzo singolo, fornendo ulteriore sicurezza per l'accesso degli ospiti o dei dipendenti temporanei.

Applicazione delle politiche relative ai PIN: le politiche configurabili relative ai PIN consentono alle organizzazioni di definire requisiti di complessità, periodi di scadenza e restrizioni di riutilizzo in linea con gli standard di sicurezza aziendali.

Protezione in caso di autenticazione non riuscita: la sicurezza avanzata include il blocco automatico dei tentativi di autenticazione dopo ripetuti fallimenti (impostazione predefinita: blocco di 5 minuti dopo 5 tentativi non riusciti entro 60 secondi).

9.8 Supporto dell'autenticazione biometrica

MyQ X sfrutta **le** moderne **funzionalità di autenticazione biometrica** attraverso l'integrazione dei dispositivi mobili:

Integrazione biometrica mobile: il client mobile MyQ X supporta metodi di autenticazione biometrica, tra cui Face ID sui dispositivi iOS e riconoscimento delle impronte digitali sui dispositivi Android, fornendo un controllo degli accessi sicuro e senza interruzioni.

Autenticazione multimodale: l'autenticazione biometrica funziona in combinazione con la sicurezza basata sul dispositivo, creando un sistema di autenticazione multimodale che combina qualcosa che l'utente possiede (dispositivo mobile) con qualcosa che l'utente è (caratteristiche biometriche).

10 Sicurezza dell’infrastruttura

MyQ X fornisce una solida sicurezza dell'infrastruttura che protegge l'intero ambiente di gestione della stampa dalle minacce informatiche in continua evoluzione. La piattaforma incorpora più livelli di difesa per salvaguardare i server, i database, la comunicazione di rete e l'integrità del software, garantendo l'affidabilità operativa e la riservatezza dei dati.

10.1 Rafforzamento della sicurezza dei Print Server

I server di stampa MyQ X sono rafforzati utilizzando configurazioni di sicurezza basate sulle migliori pratiche definite nelle impostazioni del file **config.ini**, tra cui:

- Restrizione dei servizi e dei processi per limitare la superficie di attacco.
- Abilitazione di protocolli di comunicazione sicuri e disabilitazione delle opzioni legacy non sicure.
- Assegnazione rigorosa dei privilegi agli utenti, evitando i privilegi di amministratore quando non sono necessari.
- Aggiornamenti automatici regolari e patch di sicurezza per risolvere le vulnerabilità appena scoperte.
- Configurazione delle regole del firewall e delle restrizioni delle porte per bloccare il traffico di rete non autorizzato.

Queste misure riducono il rischio di sfruttamento e mantengono la disponibilità del sistema anche in condizioni di attacco.

10.2 Crittografia del database (implementazione Firebird 4.0)

MyQ X utilizza il motore di database **Firebird 4.0**, che fornisce funzionalità di crittografia avanzate per proteggere i dati sensibili inattivi e durante le operazioni di backup. Le principali funzionalità di crittografia includono:

- Crittografia AES-256 dei file del database per impedire l'accesso non autorizzato ai dati.
- Archiviazione crittografata di password e chiavi all'interno del sistema di database.
- Offuscamento dei contenuti sensibili del database nei log e nelle diagnostiche.

Ciò garantisce la conformità alle normative sulla protezione dei dati e impedisce la compromissione della contabilità dei lavori di stampa e delle informazioni degli utenti.

10.3 Applicazione TLS 1.2/1.3 e gestione dei certificati

Per proteggere i dati in transito, MyQ X applica di default un protocollo **TLS 1.2** minimo, con aggiornamento opzionale a TLS 1.3 per una maggiore sicurezza e prestazioni migliori. La piattaforma supporta modalità di gestione dei certificati flessibili:

- Generazione automatica di un'autorità di certificazione (CA) privata che firma i certificati del server e del client.
- Integrazione di CA intermedie gestite dall'organizzazione, che consentono catene di fiducia aziendali e controllo centralizzato dei certificati.
- Supporto per l'installazione manuale dei certificati, compresi i certificati CA di terze parti/pubblici.

I certificati e le chiavi private sono archiviati in modo sicuro con protezione crittografata e i clienti ricevono certificati affidabili tramite Criteri di gruppo o Gestione dispositivi mobili.

10.4 Sicurezza delle comunicazioni di rete

MyQ X protegge tutti i canali di comunicazione di rete:

- Bloccando tutto il traffico HTTP non crittografato, applicando solo HTTPS.
- Crittografando il traffico SMTP, LDAP e RADIUS utilizzando TLS per proteggere l'autenticazione e il flusso di posta.
- Disabilitazione dei protocolli obsoleti e vulnerabili come POP3 e STARTTLS.
- Utilizzando SNMPv3 con autenticazione forte e algoritmi crittografici per monitorare e gestire in modo sicuro i dispositivi.

Questi controlli impediscono intercettazioni, spoofing e attacchi man-in-the-middle sulla rete.

10.5 Configurazione del firewall e gestione delle porte

MyQ X riduce le superfici di attacco tramite:

- Disabilitando le regole del firewall per le porte e i protocolli di rete inutilizzati.
- Consentendo un controllo granulare delle porte esposte in base alle politiche di rete dell'organizzazione.

Ciò limita i punti di ingresso solo a quelli essenziali per i servizi di stampa, migliorando le difese perimetrali.

10.6 Sicurezza API e token di autenticazione

Le API applicano più livelli di sicurezza:

- Il framework OAuth 2.0 Authorization Code Grant protegge l'accesso alle API tramite token bearer di breve durata e restrizioni di ambito.
- I token vengono convalidati rispetto agli indirizzi IP dei client e richiedono credenziali client sicure.
- Le rotazioni periodiche dei segreti proteggono dalla fuga delle credenziali.

Ciò protegge gli endpoint API da richieste non autorizzate e abusi.

10.7 Isolamento dei processi e sandboxing

Le applicazioni di gestione della stampa MyQ X funzionano con **l'isolamento dei processi** per impedire che i componenti compromessi influenzino l'intero sistema. Laddove possibile, viene utilizzato il sandboxing con macchine virtuali o container per contenere le violazioni della sicurezza e limitare i movimenti laterali all'interno dell'ambiente.

10.8 Firma del codice e verifica dell'integrità

Tutti i file binari e gli installer del software MyQ sono **firmati** per garantirne l'autenticità e l'integrità. Ciò assicura che i clienti installino versioni del software verificate, prive di manomissioni o modifiche non autorizzate.

11 Protezione e crittografia dei dati

MyQ X implementa una protezione e una crittografia complete dei dati durante l'intero ciclo di vita del documento, garantendo la riservatezza e l'integrità dalla richiesta di stampa iniziale fino all'output finale e all'archiviazione.

11.1 Implementazione della crittografia end-to-end

MyQ X fornisce **una crittografia end-to-end** su tutti i canali di comunicazione e i punti di archiviazione dei dati:

Canali di comunicazione crittografati: tutto il traffico di rete utilizza la crittografia TLS obbligatoria con versione minima 1.2 per impostazione predefinita. HTTPS è applicato a tutte le interfacce web, alle comunicazioni da server a server e alle connessioni client.

Sicurezza basata su certificati: diverse modalità di gestione dei certificati supportano i requisiti organizzativi, dall'autorità di certificazione integrata all'integrazione PKI aziendale e ai certificati CA pubblici. Le chiavi private sono protette da password generate in modo casuale e memorizzate in forma crittografata nel database Firebird.

Sicurezza del protocollo: la crittografia TLS è applicata ai protocolli SMTP, LDAP, RADIUS e SNMP, garantendo che nessun dato sensibile venga trasmesso in chiaro.

11.2 Crittografia dei dati inattivi

MyQ X protegge i dati archiviati attraverso più livelli di crittografia:

Crittografia del database: il database Firebird 4.0 supporta la crittografia utilizzando certificati personalizzati con "Encrypting File System" Enhanced Key Usage (EKU). I certificati devono essere collocati in archivi di certificati designati, preferibilmente nell'archivio personale.

Protezione del file system: i file dei lavori di stampa e scansione archiviati sul Print Server MyQ X possono essere crittografati utilizzando certificati personalizzati forniti dagli amministratori, aggiungendo un ulteriore livello di protezione oltre alle autorizzazioni del file system.

Crittografia completa del disco: MyQ X supporta l'integrazione con tecnologie di crittografia completa del disco come Microsoft BitLocker per proteggere tutti i dati inattivi sul Print Server, inclusi database, certificati e file temporanei.

11.3 Protezione dei dati in transito (crittografia TLS)

MyQ X applica rigorosi **standard di crittografia TLS** per tutte le comunicazioni di rete:

TLS 1.2 minimo: la configurazione predefinita richiede almeno TLS 1.2, con aggiornamento opzionale a TLS 1.3 per una maggiore sicurezza e prestazioni migliori. I protocolli legacy, inclusi SSL e versioni TLS precedenti, sono bloccati.

Gestione delle suite di cifratura: il sistema implementa suite di cifratura avanzate e disabilita gli algoritmi vulnerabili per prevenire attacchi crittografici. Le comunicazioni SNMPv3 utilizzano la crittografia SHA1 e AES.

Convalida dei certificati: tutte le connessioni TLS richiedono una corretta convalida dei certificati utilizzando nomi di dominio completi (FQDN) per prevenire attacchi man-in-the-middle. START TLS viene evitato a causa delle vulnerabilità MITM.

11.4 Crittografia dei lavori di stampa e archiviazione sicura

MyQ X fornisce diversi meccanismi per proteggere i lavori di stampa durante il loro ciclo di vita:

Rilascio sicuro della stampa: i lavori di stampa vengono archiviati in modo sicuro sul server MyQ fino a quando gli utenti non effettuano l'autenticazione sul dispositivo, impedendo l'accesso non autorizzato ai documenti presenti nei vassoi di uscita della stampante.

Crittografia dei file di lavoro: gli amministratori possono abilitare la crittografia dei lavori fornendo certificati personalizzati, garantendo che i file dei lavori di stampa rimangano crittografati mentre sono archiviati sul server in attesa di essere rilasciati.

Code private: per i documenti altamente riservati, le code private eliminano automaticamente i lavori di stampa subito dopo il rilascio, eliminando il rischio di un accesso non autorizzato prolungato.

Modalità privacy: quando è abilitata, la modalità privacy nasconde i nomi dei documenti a tutti gli utenti tranne al proprietario del documento, impedendo la divulgazione di informazioni attraverso i nomi dei lavori. Anche gli amministratori non possono visualizzare i nomi dei lavori di altri utenti.

11.5 Miglioramenti alla crittografia del database

L'implementazione del database **Firebird 4.0** offre funzionalità di crittografia avanzate:

Crittografia con certificati personalizzati: i file del database vengono crittografati utilizzando certificati con EFS Extended Key Usage, fornendo una protezione efficace contro l'accesso non autorizzato al database.

Protezione con password: le password del database sono oscurate nei file di log, impedendo l'esposizione delle credenziali durante le attività di risoluzione dei problemi e monitoraggio.

Rafforzamento delle autorizzazioni: la cartella dati MyQ, contenente il database degli utenti e le chiavi private dei certificati TLS, è limitata solo agli amministratori, al SISTEMA e all'account di servizio MyQ, rimuovendo l'accesso di lettura predefinito per tutti gli utenti.

11.6 Crittografia dei backup e archiviazione sicura

MyQ X garantisce che i backup mantengano lo stesso livello di sicurezza dei dati di produzione:

Backup crittografati: i backup del database sono protetti da password sicure generate in modo casuale che impediscono il ripristino o l'accesso non autorizzato ai file di backup.

Archiviazione sicura dei backup: i file di backup devono essere archiviati in luoghi sicuri con controlli di accesso appropriati e crittografia a riposo per mantenere la riservatezza dei dati durante il ciclo di vita del backup.

11.7 Politiche di gestione e rotazione delle chiavi

MyQ X implementa pratiche di gestione sicura delle chiavi:

Rotazione dei certificati: i certificati possono essere ruotati regolarmente in base alle politiche di sicurezza dell'organizzazione, con supporto per la distribuzione automatizzata tramite Criteri di gruppo o Gestione dispositivi mobili.

Protezione delle chiavi private: tutte le chiavi private per i certificati e le operazioni CA sono protette da password generate in modo casuale e archiviate in forma crittografata all'interno del database.

Rotazione dei segreti API: i segreti dei client API REST devono essere sottoposti a rotazione periodica per mantenere la sicurezza. Il sistema supporta il rollover dei segreti senza interruzione del servizio.

11.8 Minimizzazione dei dati e privacy by design

MyQ X implementa **principi di privacy by design conformi al GDPR**:

Raccolta limitata dei dati: il sistema raccoglie solo i metadati essenziali necessari per la funzionalità operativa, evitando il trattamento superfluo dei dati personali che potrebbe aumentare i rischi per la privacy.

Cancellazione automatica: gli amministratori possono configurare periodi di cancellazione automatica per i file di stampa e scansione, garantendo che i dati vengano conservati solo per il tempo necessario alle finalità aziendali.

Diritti dei dati degli utenti: implementazione completa dei diritti degli utenti GDPR, inclusi l'accesso ai dati, l'anonimizzazione e il diritto all'oblio, con informative sulla privacy personalizzabili sulle interfacce utente.

Gestione delle sessioni: la funzionalità di logout automatico garantisce che le sessioni degli utenti vengano terminate correttamente, impedendo accessi non autorizzati attraverso sessioni abbandonate.

Questo quadro completo di protezione e crittografia dei dati garantisce che MyQ X mantenga i più elevati standard di riservatezza e integrità dei dati, supportando al contempo i requisiti di conformità normativa in diversi ambienti organizzativi.

12 Flussi di lavoro di stampa sicuri

MyQ X fornisce flussi di lavoro di stampa sicuri e completi che mantengono il pieno controllo dell'utente sul rilascio dei documenti, impedendo al contempo che le informazioni sensibili vengano esposte nei vassoi di uscita della stampante. Questi flussi di lavoro sono essenziali per le organizzazioni che richiedono una rigorosa sicurezza dei documenti e la responsabilità degli utenti.

12.1 Implementazione del rilascio sicuro della stampa

Hold Print garantisce che i lavori di stampa non vengano mai rilasciati immediatamente alla stampante. I documenti vengono archiviati in modo sicuro sul server MyQ e stampati solo dopo che l'utente autorizzato ha effettuato l'autenticazione sul dispositivo di stampa, impedendo che documenti incustoditi vengano lasciati nei vassoi di uscita.

Pull Print estende ulteriormente questa funzionalità consentendo agli utenti di rilasciare i propri lavori su qualsiasi dispositivo compatibile all'interno del sistema di stampa, non solo sul dispositivo a cui hanno originariamente inviato il lavoro. Questa flessibilità è particolarmente preziosa durante la manutenzione delle apparecchiature o quando gli utenti devono stampare da luoghi diversi.

I metodi di autenticazione multipli supportano il rilascio sicuro della stampa, inclusi codici PIN, tessere identificative, password, codici QR con verifica biometrica e combinazioni di autenticazione a due fattori. Questa flessibilità soddisfa i diversi requisiti di sicurezza delle organizzazioni.

12.2 Flussi di lavoro di Pull Printing

Pull Print offre vantaggi significativi sia per gli amministratori che per gli utenti finali:

Vantaggi amministrativi:

- Eliminazione delle pile di documenti incustoditi sulle stampanti dell'ufficio
- Applicazione di comportamenti di stampa responsabili e politiche di sicurezza dei documenti
- Gestione di tutte le stampe tramite un'unica coda di stampa unificata
- Riduzione degli sprechi di stampa e dei costi associati grazie alle opzioni di anteprima e regolazione
- Supporta la stampa flessibile su più dispositivi

Vantaggi per l'utente:

- I documenti riservati rimangono protetti fino al momento dell'esplicita autorizzazione alla stampa
- Stampa su qualsiasi dispositivo autorizzato nell'organizzazione
- Anteprima dei documenti sull'Embedded Terminal prima del rilascio
- Modifica delle opzioni di stampa (colore, fronte/retro, finitura) anche dopo l'invio del lavoro
- Modifica delle destinazioni di stampa sul dispositivo se la stampante originale non è disponibile

12.3 Timeout del lavoro di stampa ed eliminazione automatica

MyQ X implementa procedure di pulizia automatica per impedire l'esposizione prolungata dei documenti:

Periodi di conservazione configurabili: gli amministratori definiscono per quanto tempo i file dei lavori di stampa vengono conservati sul server MyQ prima della cancellazione automatica, bilanciando le esigenze operative con quelle di sicurezza.

Gestione del timeout dei lavori di stampa: i lavori di stampa non rilasciati entro i tempi specificati vengono automaticamente rimossi dalla coda di attesa, impedendo l'accumulo di documenti dimenticati o abbandonati sui server.

Logout automatico: le sessioni dei dispositivi scadono automaticamente dopo periodi definiti dall'amministratore, impedendo l'accesso non autorizzato ai documenti sui terminali abbandonati.

12.4 Filigrane e firme digitali

La filigrana consente la tracciabilità dei documenti aggiungendo sovrapposizioni personalizzabili alle pagine stampate che possono includere:

- Indicazioni di riservatezza
- Date di stampa e timestamp
- Nome della persona che stampa il documento
- Informazioni di identificazione della stampante

Queste filigrane possono essere applicate a tutte le pagine o solo a quelle selezionate, creando una traccia di controllo che aiuta a identificare i documenti trapelati e a risalire alla loro fonte.

12.5 Anteprima di stampa e convalida dei contenuti

Il motore **di anteprima del lavoro** consente agli amministratori di rivedere i lavori di stampa prima del rilascio:

Formati supportati: la funzionalità di anteprima supporta i tre linguaggi di descrizione pagina più comuni: PCL 5, PCL 6 e PostScript.

Controllo preventivo: gli amministratori possono rifiutare i lavori di stampa non autorizzati prima che raggiungano il dispositivo di stampa, prevenendo violazioni delle politiche e proteggendo le informazioni sensibili.

Filtraggio basato sul contenuto: l'integrazione con i sistemi OCR e di gestione dei documenti consente di applicare le politiche di scansione in base all'analisi del contenuto dei documenti.

12.6 Gestione degli errori e ripristino sicuro dei lavori di stampa

MyQ X implementa una solida gestione degli errori per mantenere la sicurezza durante i malfunzionamenti del dispositivo:

Protezione dagli errori del dispositivo: quando un dispositivo di stampa entra in uno stato di errore (inceppamento della carta, toner esaurito), i documenti vengono trattenuti anziché stampati automaticamente una volta risolto l'errore, mantenendo il controllo dell'utente sui tempi di rilascio.

Conservazione della sessione: se un dispositivo diventa indisponibile durante una sessione, il sistema MyQ conserva la sessione dell'utente e consente di continuare su dispositivi alternativi senza perdere lo stato del documento.

Logout automatico dal dispositivo: quando si verificano errori del dispositivo, il logout automatico cancella la memoria del dispositivo per impedire l'accesso non autorizzato ai documenti da parte del personale di manutenzione o di altri utenti.

Questa architettura completa e sicura del flusso di lavoro di stampa garantisce alle organizzazioni un controllo rigoroso sulla sicurezza dei documenti durante l'intero ciclo di vita della stampa, supportando al contempo la flessibilità operativa e la produttività degli utenti.

13 Sicurezza dei dispositivi e della rete

MyQ X fornisce controlli completi di sicurezza dei dispositivi e della rete per proteggere i dispositivi multifunzione (MFD), le stampanti e l'infrastruttura di rete da accessi non autorizzati e sfruttamento.

13.1 Rafforzamento della sicurezza dei dispositivi multifunzione

Le organizzazioni che implementano MyQ X con dispositivi multifunzione dovrebbero adottare le migliori pratiche di sicurezza, tra cui:

Controlli di accesso ai dispositivi: limitare l'accesso fisico alle stampanti solo alle sedi e al personale autorizzati, riducendo l'esposizione a manomissioni o furti.

Disattivazione dei protocolli inutilizzati: disattivare i protocolli e i servizi dei dispositivi non necessari e non richiesti da MyQ X, riducendo la superficie di attacco di ciascun dispositivo.

Gestione delle credenziali predefinite: modificare tutte le password amministratore predefinite sui dispositivi con credenziali complesse generate in modo casuale. Le impostazioni predefinite di fabbrica sono comunemente note agli aggressori.

Protezione del disco rigido interno: se i dispositivi supportano l'archiviazione interna dei lavori di stampa per la ristampa, implementare la crittografia (AES) e le funzioni di sovrascrittura automatica dei dati per impedire l'accesso non autorizzato ai documenti archiviati.

13.2 Segmentazione della rete e configurazione VLAN

MyQ X supporta strategie di segmentazione della rete per contenere potenziali compromissioni dei dispositivi:

Isolamento VLAN: separare il traffico di rete delle stampanti e dei dispositivi dalle reti generali degli utenti e amministrative utilizzando LAN virtuali, limitando il movimento laterale se un dispositivo viene compromesso.

Sottoreti e elenchi di controllo degli accessi: implementare controlli di accesso a livello di rete utilizzando elenchi di controllo degli accessi (ACL) per garantire che solo i sistemi autorizzati possano comunicare con i dispositivi di stampa e i server.

Regole firewall: blocca il traffico in entrata e in uscita non necessario dalle sottoreti delle stampanti, limitando la connettività solo ai servizi essenziali e impedendo ai dispositivi infetti di accedere ad altre risorse di rete.

Applicazione FQDN: tutte le comunicazioni di rete devono utilizzare nomi di dominio completi (FQDN) anziché indirizzi IP o nomi host abbreviati, impedendo attacchi man-in-the-middle basati su DNS e garantendo la corretta convalida dei certificati.

13.3 Implementazione della sicurezza SNMP v3

MyQ X applica i moderni protocolli **SNMPv3** con crittografia avanzata per la gestione dei dispositivi:

Divieto di SNMPv1 non sicuro: la comunicazione SNMPv1 legacy deve essere completamente disabilitata, poiché trasmette le credenziali in chiaro e non dispone di crittografia.

Configurazione SNMPv3: tutte le comunicazioni SNMP devono utilizzare SNMPv3 con:

- Password complesse generate in modo casuale per l'autenticazione
- Algoritmi di hashing SHA1 o più potenti
- Crittografia AES per la riservatezza dei dati
- Credenziali uniche per dispositivo specifiche per ogni implementazione MyQ

13.4 Gestione delle credenziali della stampante

MyQ X riconosce che **la gestione delle credenziali della stampante è specifica del fornitore** e richiede l'implementazione da parte del cliente:

Requisiti di password complesse: tutte le credenziali amministrative della stampante devono utilizzare password complesse generate in modo casuale anziché credenziali predefinite o semplici.

Rotazione delle credenziali: aggiornare periodicamente le password delle stampanti in base alle politiche di sicurezza dell'organizzazione per ridurre il rischio di compromissione delle credenziali.

Restrizioni di accesso: limitare l'accesso alla gestione della stampante al solo personale autorizzato tramite regole firewall, controlli di accesso fisico e autorizzazioni basate sui ruoli.

13.5 Sicurezza del firmware e gestione degli aggiornamenti

Mantenere aggiornato il firmware dei dispositivi è fondamentale per la sicurezza:

Aggiornamenti automatici: configurare i dispositivi in modo che ricevano e applichino automaticamente gli aggiornamenti del firmware del produttore che risolvono le vulnerabilità di sicurezza appena scoperte.

Avvisi di sicurezza dei fornitori: monitorare le notifiche di sicurezza del produttore relative a vulnerabilità critiche che interessano i dispositivi distribuiti e applicare tempestivamente le patch.

Test degli aggiornamenti: testare gli aggiornamenti del firmware in ambienti non di produzione prima di distribuirli alle stampanti di produzione per garantirne la compatibilità e la funzionalità.

13.6 Gestione e restrizioni delle porte USB

MyQ X supporta i controlli amministrativi per la connettività USB dei dispositivi:

Disabilitazione delle porte USB: gli amministratori devono disabilitare le porte USB in entrata sui dispositivi multifunzione per impedire:

- La stampa diretta tramite USB, aggirando i controlli di sicurezza MyQ
- Accesso diretto ai dischi rigidi dei dispositivi e ai dati memorizzati
- Uso non autorizzato delle funzionalità del dispositivo

Alternative di stampa diretta sicure: abilitare solo metodi di stampa sicuri approvati (IPP/S, AirPrint con integrazione MyQ) bloccando l'accesso USB diretto non sicuro.

Questo quadro completo di sicurezza dei dispositivi e della rete garantisce che i dispositivi di stampa rimangano componenti sicuri dell'infrastruttura MyQ X, mantenendo al contempo l'efficienza operativa e la sicurezza dell'organizzazione.

14 Audit e monitoraggio

MyQ X offre funzionalità complete di audit e monitoraggio che consentono agli amministratori di mantenere la visibilità sulle operazioni di stampa, rilevare incidenti di sicurezza e garantire la conformità alle politiche e alle normative aziendali.

14.1 Monitoraggio e avvisi in tempo reale

MyQ X monitora tutti i componenti dell'infrastruttura di stampa in tempo reale attraverso diversi canali di monitoraggio:

Monitoraggio dello stato dei dispositivi: monitoraggio continuo dello stato delle stampanti e dei dispositivi multifunzione, inclusi i livelli di toner, la disponibilità di carta, le condizioni di errore e la connettività dei dispositivi. Gli amministratori ricevono informazioni immediate sullo stato di salute e sullo stato operativo dei dispositivi.

Gestione degli avvisi: gli avvisi automatici informano gli amministratori di eventi critici, tra cui errori dei dispositivi, scorte in esaurimento, problemi di connettività e altri problemi operativi. Le notifiche di avviso possono essere inviate tramite e-mail o integrate con il Visualizzatore eventi di Windows.

Notifiche degli eventi: le notifiche personalizzabili basate sugli eventi attivano azioni in risposta a condizioni specifiche del dispositivo o del sistema, consentendo la risoluzione proattiva dei problemi prima che questi abbiano un impatto sulle operazioni.

14.2 Registrazione e analisi delle attività di stampa

MyQ X mantiene **registri di controllo dettagliati di tutte le attività di stampa, copia, scansione e fax**:

Contabilità basata sui lavori: la contabilità avanzata tiene traccia di ogni lavoro in modo indipendente, consentendo l'attribuzione dettagliata a utenti, dispositivi, progetti e centri di costo specifici. I lavori eseguiti durante una singola sessione utente vengono contabilizzati separatamente, fornendo dati di utilizzo precisi.

Metadati delle attività: la registrazione completa cattura la data di invio del lavoro, la data di rilascio del lavoro, l'identificazione del dispositivo, il formato della carta, le impostazioni simplex/duplex, le impostazioni del colore e tutti gli altri parametri rilevanti del lavoro.

Registro MyQ: il registro di sistema in tempo reale visualizza tutte le attività del server, inclusi eventi di sistema, errori, avvisi, tentativi di autenticazione, modifiche di configurazione e azioni amministrative. I messaggi di registro sono classificati in base alla gravità (critico, errore, avviso, informazione, notifica, debug, traccia) e filtrabili per periodo di tempo e sottosistema.

14.3 Analisi del comportamento degli utenti

MyQ X offre sofisticate funzionalità di analisi per comprendere i modelli di stampa e rilevare anomalie:

Generazione di report personalizzati: le funzionalità avanzate di reporting consentono agli amministratori di creare report personalizzati basati su qualsiasi combinazione di parametri tracciati, consentendo l'analisi del comportamento di stampa per utente, reparto, progetto, dispositivo o periodo di tempo.

Monitoraggio dei centri di costo: l'attribuzione dettagliata dei lavori di stampa ai centri di costo, ai progetti e ai gruppi di utenti consente una rendicontazione trasparente delle spese e supporta decisioni informate in merito alle politiche di stampa.

Monitoraggio del comportamento: gli amministratori possono analizzare i modelli di stampa per identificare attività insolite, utilizzi eccessivi o violazioni delle politiche che richiedono ulteriori indagini.

14.4 Rilevamento e risposta agli incidenti

MyQ X supporta il monitoraggio incentrato sulla sicurezza attraverso la registrazione strutturata e gli avvisi:

Registrazione delle autenticazioni non riuscite: la registrazione avanzata dei tentativi di autenticazione, in particolare dei tentativi di accesso non riusciti, consente agli amministratori di rilevare e rispondere a potenziali minacce alla sicurezza. A partire dalla versione 10.2, i registri dei tentativi di accesso sono stati migliorati per facilitare il filtraggio nel registro MyQ.

Regole di notifica dei registri: regole personalizzabili attivano notifiche automatiche basate su tipi di eventi, sottosistemi e modelli di messaggi specifici, consentendo il rilevamento rapido di eventi rilevanti per la sicurezza. Le regole possono utilizzare espressioni regolari per cercare modelli specifici nei messaggi di registro.

Avvisi di eventi critici: il sistema avvisa automaticamente gli amministratori in caso di eventi critici, tra cui violazioni della sicurezza, errori di autenticazione, tentativi di accesso non autorizzati e modifiche alla configurazione.

14.5 Politiche di conservazione e archiviazione dei log

MyQ X implementa una gestione flessibile dei log per bilanciare le esigenze operative con i requisiti di conformità:

Periodi di conservazione configurabili: gli amministratori definiscono il numero di giorni prima che i log vengano automaticamente eliminati, allineando la conservazione alle politiche di governance dei dati dell'organizzazione e ai requisiti normativi.

Esportazione e archiviazione dei log: i log possono essere esportati in formato Excel o CSV per l'archiviazione e l'analisi esterna. Le esportazioni pianificate consentono l'archiviazione automatica dei log a intervalli regolari.

Conservazione a lungo termine: i log esportati possono essere archiviati in repository sicuri e crittografati per conservare i registri storici a fini di audit, verifica della conformità e indagine sugli incidenti.

14.6 Funzionalità avanzate di filtraggio e ricerca

MyQ X fornisce strumenti sofisticati per l'analisi e l'investigazione dei log:

Ricerche salvate: gli amministratori possono creare, salvare e condividere filtri di ricerca di uso comune per un accesso rapido ai dati di log rilevanti. Le ricerche salvate possono essere organizzate in cartelle per una facile gestione.

Filtraggio per **periodo di tempo**: filtrare i log per intervalli di date specifici o periodi predefiniti per concentrare l'analisi su intervalli di tempo rilevanti.

Filtraggio per sottosistema e contesto: ricerca per specifici sottosistemi MyQ (interfaccia utente web, terminale, server SMTP, ecc.) e contesti (stampa diretta, dispositivi specifici) per isolare gli eventi rilevanti.

Controllo della verbosità: selezionare quali livelli di gravità dei log (critico, errore, avviso, informazioni, ecc.) vengono visualizzati, riducendo il rumore e concentrandosi sugli eventi significativi.

14.7 Registro di controllo per le azioni amministrative

MyQ X tiene traccia di tutte le modifiche amministrative attraverso un **registro di controllo** dedicato:

Modifiche alla configurazione: registra tutte le modifiche alle impostazioni MyQ, inclusi chi ha apportato la modifica, quando è stata effettuata e quale componente del sistema è stato interessato.

Gestione dei diritti utente: tracciamento dettagliato delle modifiche alle autorizzazioni utente, alle appartenenze ai gruppi e ai controlli di accesso, con la possibilità di visualizzare informazioni dettagliate su ogni modifica.

Gestione dei PIN e delle credenziali: monitoraggio avanzato delle aggiunte, delle rimozioni e delle modifiche dei PIN per monitorare il ciclo di vita delle credenziali.

Funzionalità di esportazione: i registri di controllo possono essere esportati su richiesta o programmati per l'esportazione automatica regolare, supportando i requisiti di conformità e conservazione dei dati.

Questo quadro completo di audit e monitoraggio garantisce che MyQ X fornisca agli amministratori la visibilità necessaria per mantenere la sicurezza, rilevare le minacce, garantire la conformità alle politiche e risolvere efficacemente i problemi operativi.

15 Risposta agli incidenti e recupero

MyQ X offre funzionalità complete di risposta agli incidenti e ripristino progettate per mantenere la continuità operativa durante le interruzioni pianificate e non pianificate. La piattaforma combina procedure di backup automatizzate, funzionalità ad alta disponibilità e meccanismi di failover flessibili per garantire che i servizi di stampa rimangano operativi anche durante le interruzioni del sistema.

15.1 Procedure di risposta agli incidenti di sicurezza

MyQ X supporta una risposta strutturata agli incidenti attraverso molteplici meccanismi di monitoraggio e allerta:

Rilevamento degli incidenti in tempo reale: il monitoraggio automatizzato tiene traccia in modo continuo dell'Integrità del sistema, degli errori di autenticazione, delle modifiche di configurazione e degli eventi di sicurezza, consentendo il rilevamento rapido di potenziali incidenti di sicurezza.

Escalation degli avvisi: regole configurabili di Log Notifier attivano notifiche immediate agli amministratori quando si verificano eventi di sicurezza critici, inclusi tentativi di autenticazione non riusciti, tentativi di accesso non autorizzati e anomalie di sistema.

Conservazione della traccia di audit: la registrazione completa di tutte le attività di sistema garantisce la disponibilità di dati forensi completi per l'indagine sugli incidenti. Il registro di audit MyQ tiene traccia di tutte le azioni amministrative, le modifiche di configurazione e le attività degli utenti.

Procedure di contenimento: in caso di incidente di sicurezza, gli amministratori possono isolare rapidamente i componenti interessati, disabilitare gli account compromessi e implementare controlli di accesso di emergenza.

15.2 Procedure di ripristino e recupero

MyQ X implementa solide funzionalità di backup e ripristino per garantire un rapido recupero da guasti del sistema o perdita di dati:

Backup automatico del database: i backup automatici regolari del database MyQ acquisiscono tutti i dati di configurazione, le informazioni sugli utenti e le impostazioni di sistema. I backup sono protetti con crittografia a password e archiviati in modo sicuro.

Ripristino completo del sistema: il processo di ripristino recupera l'intero ambiente MyQ, inclusi database, certificati, file di configurazione e report. Gli amministratori devono semplicemente selezionare il file di backup e fornire la password, se protetto.

Backup e ripristino cluster-aware: per le distribuzioni ad alta disponibilità che utilizzano Microsoft Failover Clustering, MyQ supporta il backup su storage cluster condiviso e il ripristino coordinato su tutti i nodi del cluster.

15.3 Alta disponibilità e failover

MyQ X offre diverse strategie di failover per mantenere le operazioni di stampa durante i periodi di inattività del server:

Integrazione con Microsoft Failover Clustering: MyQ X viene distribuito in configurazioni attive-passive all'interno dei cluster di failover di Microsoft Windows Server. Il software del cluster monitora continuamente lo stato dei nodi e passa automaticamente ai nodi passivi quando il nodo attivo non è disponibile.

Stampa di fallback: quando il Desktop Client MyQ rileva la perdita di connessione al server, reindirizza automaticamente i lavori di stampa a stampanti di fallback preconfigurate. Una volta ripristinata la connettività del server, la contabilità dei lavori viene aggiornata automaticamente.

Spooling dei dispositivi: i lavori di stampa possono essere memorizzati in modo crittografato nella memoria del dispositivo durante le interruzioni del server. Quando la connettività viene ripristinata, i dispositivi trasmettono automaticamente i dati di contabilità al server.

Accesso offline: i terminali Embedded Terminal MyQ X memorizzano nella cache le credenziali di autenticazione degli utenti, consentendo loro di accedere e utilizzare le funzionalità del dispositivo anche quando il server non è disponibile.

Spooling client: i lavori di stampa vengono elaborati localmente sulle workstation degli utenti e memorizzati sui loro computer anziché sul server, riducendo significativamente i requisiti di larghezza di banda e consentendo la stampa durante la manutenzione del server o in caso di problemi di rete.

15.4 Analisi post-incidente e miglioramento

MyQ X supporta il miglioramento continuo delle capacità di risposta agli incidenti attraverso strumenti di analisi completi:

Analisi dei registri storici: gli amministratori possono esaminare i registri esportati per comprendere la sequenza di eventi che hanno portato a un incidente, identificare le cause alla radice e determinare le azioni correttive appropriate.

Revisione dell'audit trail: il registro di audit fornisce una visibilità completa di tutte le azioni amministrative e le modifiche di configurazione che potrebbero aver contribuito o preceduto gli incidenti di sicurezza.

Modelli di ricerca salvati: gli amministratori possono creare e salvare filtri di ricerca all'interno dei registri per modelli di incidenti comuni, consentendo una rapida identificazione di eventi simili in futuro.

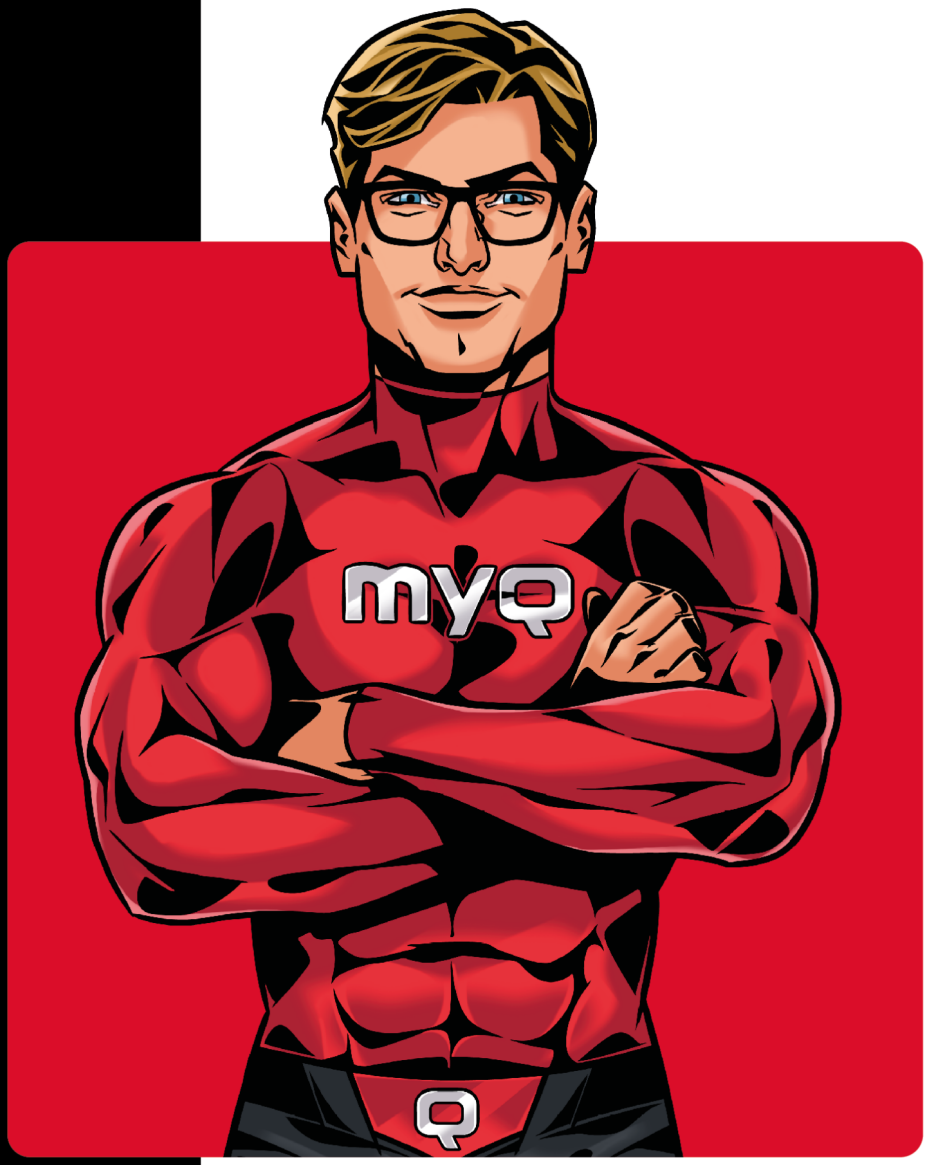
myQ X

RISPARMIA TEMPO CON SOLUZIONI DI STAMPA PERSONALIZZATE

MyQ X è una pluripremiata soluzione di gestione della stampa locale o su cloud privato, scelta da milioni di utenti.

info@myq-solution.com

myq-solution.com



50+ milioni
Utenti che si affidano a MyQ

1+ milione
Dispositivi attivi

26+
Marchi supportati

1000+
Partner certificati

Presente in **140+** paesi

Premi e certificazioni

BuyersLab PLATINUM TESTED SOLUTION 2023

BuyersLab PLATINUM TESTED SOLUTION 2022

BuyersLab PLATINUM TESTED SOLUTION 2021

ISO 9001 TÜV SÜD ISO 14001 ISO/IEC 27001