MyQ Roger Data Security Whitepaper

March/2025
Revision 13

Table of Contents

1 Introduction

The purpose of this document is to inform the customers of MyQ Roger about processes that involve establishing connections in the system and about security measures taken to protect consequent data transfer.

2 Glossary

- **IPP/s (Internet Printing Protocol over Secure TLS)**:
  - MyQ Roger ensures secure printing by utilizing the Internet Printing Protocol (IPP) over a TLS-encrypted channel, preventing unauthorized access and ensuring data integrity in transit.
  - MyQ Roger optimizes network traffic through efficient packet handling, reducing unnecessary data transmission and ensuring secure communication between endpoints.
- **TLS (Transport Layer Security)**:
  MyQ Roger enforces TLS 1.2/1.3 for secure data encryption in all communications, ensuring protection against interception and man-in-the-middle (MITM) attacks.
- **Data at Rest, Data in Transit**:
  - **Data at Rest**: MyQ Roger encrypts stored data using AES-256, ensuring that sensitive information remains secure against unauthorized access.
  - **Data in Transit**: All data transferred between clients, servers, and cloud services is encrypted using TLS to maintain integrity and confidentiality.
- **Zero Trust Infrastructure**:
  MyQ Roger follows a **Zero Trust** security model by implementing continuous authentication, device verification, and least privilege access for users and services.
- **IAM (Identity and Access Management)**:
  MyQ Roger integrates IAM best practices by enforcing secure user authentication, multi-factor authentication (MFA), and identity-based access controls.
- **RBAC (Role-Based Access Control)**:
  MyQ Roger implements RBAC to restrict permissions based on user roles, ensuring that only authorized personnel can access critical functions and sensitive data.
- **SSO (Single Sign-On)**:
  MyQ Roger supports **SSO** via OAuth2 integration, enabling seamless authentication across enterprise applications while maintaining security and compliance.

3 Operations Security

3.1 Introduction

Security is a top priority at MyQ Roger. We enforce a **security-first** approach at every stage of development, deployment, and operations. Given the critical nature of cloud environments, security must be **proactive, automated, and continuously monitored** to prevent breaches and unauthorized access.

Our **Secure Operations strategy** integrates **continuous monitoring, vulnerability management, infrastructure security, and compliance** to ensure the integrity of applications and infrastructure.

3.2 Monitoring

Continuous monitoring is essential for detecting and responding to threats in real time. MyQ implements a **multi-layered monitoring approach:**

3.2.1 Endpoint Detection and Response (EDR)

- Monitors all endpoints (servers, VMs, and containers) for suspicious activity.
- Uses **behavioral analytics and threat intelligence** to detect advanced threats.
- Automatically isolates compromised endpoints to prevent lateral movement.

3.2.2 Azure Defender (Now Defender for Cloud)

- Protects **Azure AKS, SQL Server, Virtual Machines, and Storage**.
- Provides **real-time threat detection** and security configuration recommendations.
- Integrates with **Microsoft Sentinel (SIEM)** for centralized alerting.

3.2.3 Host Scanning

- Scans **VMs, cloud instances, and on-premises servers** for misconfigurations and outdated software.
- Detects **privilege escalation risks, unauthorized access points, and outdated dependencies**.

3.2.4 Log Collection & Analysis

- **Centralized logging** on a separate cluster for scalability and isolation.
- **Logs from Kubernetes, applications, and infrastructure** are labeled for efficient retrieval.
- **Long-term retention policies** ensure compliance and security analysis.
- **Alerting mechanisms** detect anomalies and security incidents, integrating with SIEM.
- **Real-time log correlation** for API requests, authentication events, database queries, and firewall traffic.

3.2.5 Port Scanning

- Detects unauthorized **open ports** that expose services to threats.
- Uses **automated tools like Nmap and ZMap** to scan for **unexpected port changes**.

3.2.6 Container Scanning

- **Static and dynamic scanning** of Docker containers before deployment.
- Identifies vulnerabilities in **base images, application layers, and runtime permissions**.
- Integrated with **Trivy** for **image security scanning**.

3.2.7 Kubernetes Monitoring

- Uses **Azure Kubernetes Service (AKS) built-in monitoring** with **Prometheus & Grafana**.
- Monitors **Kubernetes API calls, RBAC policies, and pod security**.
- Alerts on **container privilege escalations, excessive resource usage, and lateral movement attempts**.

3.2.8 Regular TLS Scans

- MyQ performs **TLS security scans using Qualys SSL Labs** to ensure best practices.
- TLS configurations are evaluated to maintain an **A+ security rating**, mitigating risks from weak protocols.
- Automated tools verify **certificate validity, expiration tracking, and protocol strength**.

3.3 Vulnerability Management

3.3.1 Vulnerability Scanning

- **Regular scans** detect security flaws in applications and infrastructure.
- Includes **automated CVE scanning** for cloud-deployed components.
- Integrates with **DefectDojo, SonarQube, and Trivy** for risk assessment.

3.3.2 Penetration Testing

- Conducted regularly to identify security weaknesses before exploitation.
- Combines **automated and manual testing methodologies** for comprehensive assessment.
- Findings are **documented, prioritized, and remediated** accordingly.

3.4 Infrastructure Security

A **hardened infrastructure** ensures security beyond just monitoring. MyQ employs:

3.4.1 SIEM (Security Information and Event Management)

- **Microsoft Sentinel SIEM** collect security events for real-time detection.

- Analyzes logs from **firewalls, identity systems, application logs, audit logs, and threat feeds**.
- Enables **automated responses to detected threats**.

3.4.2 Security Tracking & Management

- **Jira Bug Database** tracks, categorizes, and prioritizes security vulnerabilities.
- **DefectDojo** consolidates test results, ensuring structured tracking of security engagements.
- Regular **patching and remediation** maintain a strong security posture.

3.4.3 Identity and Access Management (IAM)

- Enforces **Zero Trust** with **role-based access control (RBAC) and multi-factor authentication (MFA)**.
- Uses **Azure AD** for identity governance.
- **Privilege escalation alerts** detect unauthorized admin access.

3.5 Development Workflow

Secure software development is a critical aspect of MyQ's security strategy. The following measures ensure the integrity of code, pipelines, and cloud environments:

3.5.1 Secure Development Environment

- MyQ developers use **security-hardened environments** with endpoint protection.
- Developers must follow **secure coding practices and regular security training**.

3.5.2 GitLab Secure Pipelines

- GitLab CI/CD pipelines include **automated security checks, code reviews, and testing**.
- **Static Application Security Testing (SAST)** and **Dynamic Application Security Testing (DAST)** detect vulnerabilities.
- **Container Image Signing** ensures only trusted images are deployed.

3.5.3 IAM & Access Control

- Only **Selected DevOps and SecOps personnel** have access to Azure cloud environments.
- **Role-based access control (RBAC) with Just-In-Time (JIT) least privilege elevation** is enforced.

3.5.4 Azure Kubernetes & Container Security

- MyQ’s **AKS clusters pull images only from Azure Container Registry (ACR)**.
- AKS environments enforce **network policies and Pod Security Standards (PSS)** to isolate workloads.

3.5.5 Secrets Management

- **All secrets and API keys are stored in Azure Key Vault**, accessible only to IAM-authorized personnel.
- **Trivy filesystem scans** are conducted before committing to Git to detect and prevent sensitive secrets.

3.6 Conclusion

MyQ's **Secure Operations strategy** is built on a foundation of **continuous monitoring, proactive threat management, and strong infrastructure security**. By leveraging **advanced security tools, strict access controls, and automated testing**, MyQ ensures a **secure, resilient cloud environment**.

With the **integration of TLS security scans, penetration testing, and centralized logging**, MyQ enhances its ability to **detect, respond to, and mitigate security risks** effectively.

Security is an **evolving challenge**, and MyQ remains committed to **enhancing security measures through regular updates, compliance audits, and security best practices**. By maintaining a **security-first mindset**, MyQ upholds the **integrity and confidentiality** of its services, ensuring **trust and reliability** for all stakeholders.

4 Applications Security

4.1 The Evolution of Security Threats

In the early days, before the internet was widespread, printers were directly connected via LPT cables, and security concerns were minimal. The biggest risk was physical—someone looking over a user's shoulder to see printed documents. The security landscape was straightforward, and cyber threats were virtually nonexistent.

However, as printers and devices became network-connected, the threat landscape changed drastically. With printers now accessible over local area networks (LANs) and even the internet, attackers no longer need physical access. Threats such as man-in-the-middle (MITM) attacks, unauthorized data interception, and remote exploits have become prevalent. Cybercriminals have evolved from looking over shoulders to eavesdropping on network traffic and exploiting vulnerabilities.

Mitigating these risks is a continuous challenge, as new threats emerge frequently. To address these evolving security challenges, MyQ Roger implements continuous security practices, proactive monitoring, and strong defense mechanisms.

4.2 MyQ Roger's Security Approach

MyQ Roger is built with a security-first approach, ensuring that innovation and user experience are always aligned with the highest security standards. Our commitment to security is reflected in our continuous efforts to integrate robust security measures at every stage of development. We adopt a "secure-by-default" philosophy, embedding security within our products and services from the ground up.

To achieve this, MyQ Roger leverages automation, data-driven risk assessments, and best-in-class security practices to proactively identify and mitigate threats. By implementing security controls early in the development cycle, following a **shift-left approach**, we ensure vulnerabilities are detected and remediated before they reach production. This proactive integration allows us to scale efficiently, reduce risks, and minimize security threats. Our approach reinforces our dedication to safeguarding customer data, workflows, and overall security posture.

4.3 Shifting Left in Security

Shifting security left means integrating security early in the software development lifecycle (SDLC) rather than addressing vulnerabilities later. By catching security issues in the initial development stages, we prevent costly fixes and mitigate potential breaches. This proactive strategy ensures that every line of code meets the highest security standards before it reaches production, reducing risks and strengthening our overall security posture.

4.4 MyQ Security Responsibilities

MyQ Roger is committed to safeguarding customer data and ensuring a secure operational environment. Our core security responsibilities include:

- **Data Protection**: MyQ ensures customer data is securely stored and encrypted, preventing unauthorized access and ensuring data confidentiality.
- **Regular Security Patching**: We proactively apply security patches and updates to all systems to eliminate vulnerabilities before they can be exploited.
- **Access Control Management**: We enforce strict access policies following the principle of least privilege, ensuring that only authorized personnel can access sensitive resources.

By upholding these security principles, MyQ Roger fosters a culture of security, protecting users from potential threats while ensuring compliance with industry standards.

4.5 MyQ Roger Security Control/Management

While we rely on secure cloud infrastructure, MyQ Roger takes direct responsibility for implementing additional security layers and adhering to industry best practices. Our approach includes:

- **Key Management with Azure Key Vault**: We utilize Azure Key Vault to store and manage all secrets, private keys, and certificates securely, ensuring strict access controls and encryption.
- **ISO 27001 Certification**: We adhere to ISO 27001 standards to maintain a structured and consistent approach to information security.
- **Endpoint Detection and Response (EDR)**: We leverage advanced EDR solutions to detect, analyze, and mitigate security threats in real time, reducing response time and minimizing risks.
- **Secure Development Practices**: Our secure software development lifecycle includes vulnerability assessments, continuous monitoring, and automated security scans to detect and fix security flaws.
- **Regular Security Audits**: We conduct both internal and third-party audits to ensure compliance and proactively address security risks.
- **SIEM with Azure Sentinel**: We use Azure Sentinel for real-time threat detection, automated response, and continuous security monitoring across all cloud and network environments.

By implementing these security measures, MyQ Roger strengthens its overall security framework, ensuring that customer data remains protected at all times.

4.6 Microsoft Azure and Compliance

MyQ Roger runs on Microsoft Azure, leveraging Azure Kubernetes Service (AKS), Azure SQL Servers, and Azure Cosmos DB for MongoDB. By operating within Azure's infrastructure, we benefit from Microsoft's industry-leading security, compliance, and reliability standards.

4.6.1 Microsoft's Security and Compliance Responsibilities

- Azure adheres to global compliance frameworks such as ISO 27001, SOC 2, and GDPR in the EU, ensuring adherence to strict regulatory standards.

- Microsoft provides built-in security features such as network isolation, identity protection, and continuous threat detection, reducing attack surfaces.
- Azure services undergo rigorous security assessments and penetration testing to proactively identify and remediate vulnerabilities.

By leveraging Azure's secure infrastructure, MyQ Roger adds its own security layers to create a robust and resilient security model that protects customer applications and data.

4.7 Customer Security Responsibilities

While MyQ Roger provides a secure infrastructure and best-in-class security measures, customers also have key responsibilities to ensure the security of their environment. These include:

- **Maintaining an Active User List**: Customers should continuously manage user access by leveraging automated user synchronization or manually disabling inactive accounts to minimize risk.
- **Role-Based Access Control (RBAC) Enforcement**: Customers must apply RBAC principles to restrict user access to only necessary permissions, ensuring stronger security and operational efficiency.
- **Securing the Local Network**: Even though MyQ Roger operates with a zero-trust model, customers should ensure that their local network adheres to best security practices, such as firewall configurations, network segmentation, and endpoint protection.
- **Proper Resource Maintenance**: All connected devices, including printers and multifunction devices (MFPs), should be regularly updated with the latest firmware and security patches to prevent vulnerabilities.

By adhering to these responsibilities, customers strengthen their security posture while benefiting from MyQ Roger's comprehensive security framework.

4.8 Security Automation

To further enhance security across the development lifecycle, MyQ Roger integrates automated security testing and external security assessments:

- **SAST (Static Application Security Testing)**: Conducted on every commit to detect security vulnerabilities early in the development cycle, reducing the likelihood of insecure code reaching production.
- **DAST (Dynamic Application Security Testing)**: Performed in sandbox environments to identify and mitigate runtime security risks before deployment.
- **External Penetration Testing**: We engage independent security experts to perform penetration testing, ensuring that our security defenses can withstand real-world attack scenarios.

By automating security testing and conducting regular external assessments, MyQ Roger maintains a proactive and resilient security posture.

4.9 Conclusion

At MyQ Roger, security is not an afterthought—it is an integral part of our product and development lifecycle. By combining secure-by-design principles, industry best practices, and a strong compliance framework, we provide a robust security posture that protects our customers' data and operations. Our commitment to continuous security improvements ensures that MyQ Roger remains resilient against evolving threats while maintaining the highest standards of reliability and trust. We will continue to evolve our security strategy, adapting to new challenges and leveraging the latest technologies to uphold our mission of providing a secure and seamless user experience.

5 Data Protection

5.1 Overview

Data protection is at the core of **MyQ Roger's** approach to security, ensuring that every aspect of its cloud-based printing and scanning solution adheres to the highest industry standards. A fundamental principle of MyQ Roger is that **no print or scan job data is ever transferred through its servers**. Instead, MyQ Roger strictly limits its data collection to essential **metadata**, such as **job file names, file sizes, and page count information**. This ensures operational efficiency while safeguarding user privacy.

5.2 Multi-Tenant Cloud Security

As a **multi-tenant cloud product**, MyQ Roger provides customers with an environment that is **logically isolated** to prevent cross-tenant data exposure.

To provide resilience, MyQ Roger relies on **Azure SQL** and **Azure Cosmos DB**, both of which offer built-in security features such as **data encryption at rest and in transit, automated threat detection, and access monitoring**. The cloud infrastructure undergoes continuous security assessments to mitigate risks associated with multi-tenant environments.

5.3 Encryption & Secure Communication

Security is embedded at every level of MyQ Roger’s operations. All communication between clients, cloud services, and printers is **encrypted using TLS (Transport Layer Security)** to prevent unauthorized access or tampering.

To further strengthen security, **publicly trusted Certificate Authorities (CAs)** sign all certificates used within MyQ Roger, ensuring the highest level of trust. Additionally, certificates are **rotated every three months**, reducing the risk of potential compromise and maintaining compliance with security best practices.

5.4 Compliance & Identity Management

MyQ Roger aligns with internationally recognized security standards, holding **ISO 27001 certification**, which demonstrates its commitment to implementing robust information security management practices.

To enforce strict access controls, **Role-Based Access Control (RBAC)** is implemented, ensuring that users are granted **only the permissions necessary for their role**. This minimizes exposure to sensitive data and reduces the risk of accidental or intentional misuse.

5.5 GDPR Compliance

Ensuring compliance with the **General Data Protection Regulation (GDPR)** is a top priority for MyQ Roger. In accordance with GDPR principles, MyQ Roger follows stringent data protection measures to safeguard user privacy:

- **Data Minimization**: Only essential metadata is collected, eliminating the risk of storing sensitive user documents.
- **User Rights & Control**: Users have the ability to request **access, correction, deletion, or anonymization** of their personal data, as mandated by GDPR.
- **Transparency in Data Processing**: Clear and concise privacy policies outline how metadata is handled, stored, and protected.
- **Secure Data Storage**: All data is **encrypted at rest and in transit**, ensuring full compliance with GDPR’s strict security requirements.
- **Anonymization Measures**: When required, MyQ Roger implements **data anonymization techniques** to ensure that personal data can no longer be attributed to a specific user, reinforcing privacy protection.

These measures ensure that MyQ Roger fully aligns with GDPR's core requirements, giving users control over their personal data while maintaining a secure and compliant environment.

5.6 Data Backups

To protect against data loss and ensure service reliability, MyQ Roger implements a **comprehensive data backup strategy**. This includes:

- **Automated Backups**: Regularly scheduled **incremental and full backups** ensure that data remains recoverable in the event of an incident.
- **Secure Storage**: Backups are encrypted using **AES-256 encryption**, ensuring that even in the unlikely event of unauthorized access, data remains unreadable.
- **Retention Policies**: Backups are **stored for a defined period** in alignment with compliance requirements, allowing for efficient recovery in case of system failure or disaster recovery scenarios.
- **Integrity Testing & Verification**: Regular **backup integrity tests** are conducted to confirm that stored backups are functional and reliable, ensuring seamless data restoration when needed.

By implementing these robust security, compliance, and backup measures, **MyQ Roger provides a secure, private, and highly efficient cloud-based printing and scanning solution** that meets the highest data protection standards in the industry.

6 Server Uptime, Data Backup, and Disaster Recovery

6.1 Server Uptime

MyQ Roger is dedicated to maintaining a 99.9% uptime target; however, service level agreements (SLAs) are tailored per customer and do not explicitly guarantee this metric. We employ advanced high-availability (HA) strategies, leveraging multi-zone deployments and multi-pod architectures to ensure service continuity and minimize potential downtime in the event of operational disruptions.

6.2 Real-Time System Status Monitoring

To enhance transparency and provide real-time visibility into system performance, we maintain a dedicated status site that delivers up-to-date insights on service health. This platform enables customers to:

- **Monitor Live System Status**: View real-time operational metrics and incident updates.
- **Receive Proactive Notifications**: Subscribe to alerts for service degradation or planned maintenance events.
- **Access Historical Uptime Reports**: Review past incidents and performance trends to assess reliability.

By offering a centralized status site, we empower customers with timely and accurate information, reinforcing trust and enabling proactive decision-making in the event of disruptions.

6.3 Backup Strategies

6.3.1 Azure SQL Backup Strategy

We employ a geo-redundant backup strategy for Azure SQL databases, ensuring data resilience and recoverability. Key aspects include:

- **Geo-Redundant Storage**: Backups are replicated across multiple regions for disaster recovery.
- **Retention Policy**: Backups are retained for several months, allowing historical data recovery.
- **Incremental Backups**: A 14-day point-in-time recovery (PITR) window enables granular restoration of lost data.
- **SLA-Based Customization**: Retention periods and recovery time objectives (RTO) vary based on cluster-specific SLAs and can be tailored to meet customer needs.

6.3.2 Azure Cosmos DB Backup Strategy

For Azure Cosmos DB, we implement comprehensive data protection mechanisms, particularly for accounting records, ensuring data integrity and traceability:

- **Full Accounting Data Reports**: All accounting transactions, including job accounting for print, scan, copy, and fax activities, are fully recorded.

- **Historical Data Retracing**: Our system allows tracking and retracing of any reported accounting records to ensure compliance and auditability.
- **High Availability and Redundancy**: Built-in multi-region replication ensures continuity and minimizes data loss risks.

By implementing these robust backup strategies, we safeguard critical business data while providing flexible recovery options tailored to customer-specific SLAs.

6.4 Disaster Scenarios & Response Plan

Disaster Scenario	Mitigation Strategy	Recovery Process
Data Corruption	PITR (Point-in-Time Recovery)	Restore database to last known good state
Cloud Region Outage	Geo-redundant backups & failover	Switch to secondary Azure region
Kubernetes Node Failure	Auto-replication of services in AKS	Pods are rescheduled to healthy nodes
Cyberattack (DDoS, Ransomware, etc.)	WAF, Azure DDoS Protection, and security monitoring	Isolate compromised systems, restore from clean backups

7 Zero Trust

7.1 Understanding Zero Trust Security

Trust is a complex construct. For example, I trust my mother to cook a perfect dinner, but I would never trust her with network security. In cybersecurity, misplaced trust can lead to significant vulnerabilities, which is why the Zero Trust model exists.

7.1.1 Real-World Example: The Danger of Implicit Trust

One of the most well-known breaches where a lack of Zero Trust principles played a role was the **Colonial Pipeline attack** in 2021. Attackers gained access through a compromised VPN credential, which did not have Multi-Factor Authentication (MFA) enabled. Since the network implicitly trusted authenticated users, the attackers were able to move laterally and deploy ransomware, causing widespread fuel shortages across the U.S. This incident highlights why "never trust, always verify" is critical to modern cybersecurity.

7.2 What is Zero Trust?

Zero Trust is a cybersecurity paradigm built on the principle of "never trust, always verify." It ensures that users and devices are not trusted by default, even if they are connected to a secured corporate network or were previously verified. Instead, trust must be continually assessed and validated based on various security signals.

7.2.1 The Core Principles of Zero Trust

Zero Trust is defined in **NIST SP 800-207** as a framework focused on resource protection through continuous verification. This security model applies to:

- **Identity and Access Management**: Ensuring users and devices authenticate securely.
- **Network and Endpoint Security**: Protecting communication and enforcing strict access controls.
- **Data Protection**: Ensuring sensitive data is encrypted and securely stored.
- **Continuous Monitoring**: Detecting anomalies and responding to potential threats in real time.

7.3 How Zero Trust Applies to MyQ Roger

7.3.1 Explicit Verification

- Authentication is required even on authorized devices (phones/desktops).
- Uses modern authentication standards.
- Multi-Factor Authentication (MFA) is enforced for mobile and Multi-Function Printer (MFP) logins.
- OAuth2 Device Flow is implemented for device authorization.

- **Continuous authentication mechanisms** track changes in user behavior to detect anomalies.

7.3.2 Access Management

- **Role-Based Access Control (RBAC)** ensures users have only the minimum necessary access.
- **Least Privilege Principle** is enforced to reduce security risks.
- **Micro-Segmentation** is implemented to limit lateral movement within the network.
- **Just-in-Time (JIT) Access Controls** dynamically adjust user privileges based on the context.

7.3.3 Device & Endpoint Security

- Unique access tokens are issued for each device type.
- Transport Layer Security (TLS) is mandatory for all communications.
- **Endpoint Detection and Response (EDR) solutions** monitor and analyze device behavior.
- **Zero Trust Network Access (ZTNA)** ensures that only authorized devices can access specific resources.

7.3.4 Data Protection

- All data is securely stored using encrypted storage solutions.
- Policies ensure data is accessed only by authorized entities.
- **Data Loss Prevention (DLP) solutions** monitor and prevent unauthorized data exfiltration.
- **Secure Enclaves** protect highly sensitive data from unauthorized access.

7.4 Addressing Cyber Threats with Zero Trust

Zero Trust helps mitigate the following threats:

- **Insider threats**: Prevents employees or compromised accounts from gaining unauthorized access.
- **Credential stuffing and phishing attacks**: Reduces the impact of compromised credentials through continuous authentication.
- **Lateral movement attacks**: Micro-segmentation restricts attackers from moving laterally across networks.
- **Supply chain attacks**: Ensures strict verification of third-party access and integrations.

7.5 Compliance and Regulatory Considerations

Zero Trust aligns with various cybersecurity regulations and frameworks:

- **ISO 27001**: Enforces secure access management and data protection.
- **GDPR**: Ensures secure processing and storage of personal data.
- **HIPAA**: Protects sensitive healthcare information.
- **NIST Cybersecurity Framework**: Provides guidelines for Zero Trust implementation.

7.6 Why Zero Trust Matters

Adopting Zero Trust minimizes the risk of security breaches, insider threats, and unauthorized access. In an era of increasing cyber threats, a Zero Trust architecture provides robust protection by ensuring continuous verification and strict access controls across all resources.

By implementing these principles, MyQ Roger ensures a secure, resilient, and adaptive security posture that aligns with modern cybersecurity best practices. Additionally, continuous monitoring, access controls, and real-time threat detection enhance the organization's ability to respond to evolving cyber threats effectively.

8 Secure Login with MyQ Roger

8.1 Introduction

Using a PIN as the primary method of login was never truly secure. Early mobile phones relied on PINs, but as security concerns evolved, so did authentication methods. Today, biometrics have become the norm, offering a more secure and user-friendly approach to authentication.

MyQ Roger embraces this shift by implementing the latest OAuth 2.0 Device Authorization Grant (formerly known as the Device Flow). This modern authentication method requires users to log in using a one-time QR code scanned with their mobile phone, eliminating the need for static passwords or insecure PINs.

We recognize a user's mobile phone as one of the most secure means of authentication. By leveraging biometric authentication to unlock the phone and subsequently access the MyQ app, we ensure that the individual logging in is the legitimate owner of the account.

8.2 Secure Authentication with MyQ Roger

- **OAuth 2.0 Device Authorization Grant**: Instead of relying on traditional PINs, users authenticate using a dynamically generated QR code. This method significantly reduces the risk of credential theft or reuse attacks.
- **Biometric Verification**: Since modern smartphones require biometric verification (e.g., fingerprint or facial recognition) to unlock, this adds an extra layer of security before accessing MyQ Roger.

8.3 Legacy PIN Authentication

While MyQ Roger still provides PIN-based login as an option, it is considered an insecure method and is discouraged by default. Users who choose to enable PIN authentication must explicitly mark it as safe, acknowledging the associated security risks. Furthermore, enabling PIN login will disable some advanced security features to mitigate potential vulnerabilities.

8.4 Security Responsibility

If an organization opts to allow PIN-based login, the responsibility for maintaining a secure environment falls on the customer. Best practices such as enforcing strong PIN policies, implementing physical security measures, and monitoring access logs should be followed to minimize risks.

8.5 Conclusion

With MyQ Roger, we prioritize security by leveraging modern authentication standards. The adoption of mobile-based biometric authentication ensures a seamless yet secure user experience. While legacy PIN-based login remains available, it is not the recommended method, and customers must take additional precautions if they choose to use it. By embracing secure login mechanisms, organizations can enhance both security and usability for their users.

9 Secure Printing with MyQ Roger

9.1 The Challenge of Secure Printing

Traditional secure printing methods rely on physically tethered connections, such as LPT cables, where a dedicated printer is assigned to a single laptop. While this method ensures the highest level of security, it is impractical in modern environments that demand flexibility, mobility, and shared resources.

AirPrint and Mopria offer secure printing capabilities but are insufficient in scenarios where users can initiate remote print jobs without being physically present near the printer. This creates security vulnerabilities where sensitive documents might be left unattended.

9.2 MyQ Roger: A Comprehensive Secure Printing Solution

MyQ Roger integrates multiple printing workflows while enforcing security protocols to ensure that users must be physically present to authenticate and release print jobs. The system guarantees that print jobs are securely stored and transmitted while minimizing data exposure.

9.3 Secure Printing Methods in MyQ Roger

9.3.1 1) Direct PC-to-Printer Printing

- Utilizes **IPP/s (Internet Printing Protocol Secure)** to transfer print jobs securely.
- Supported printer brands: **Ricoh, Kyocera**.
- Print jobs remain stored directly on the printer until the user authenticates and releases the job.

9.3.2 2) MyQ Roger Client (MRC)

- Print jobs are **encrypted and stored locally** on the user's PC.
- The printer retrieves the encrypted file **only after user authentication**.
- Secure printing is executed via **IPP/s**.

9.3.3 3) Cloud Printing

- Print files are securely stored in the user's cloud storage (e.g., **OneDrive, Google Drive, Dropbox**).
- The printer downloads the document directly from cloud storage using a **short-lived access link**.
- **No document retention** on the printer after printing, ensuring data confidentiality.

9.3.4 4) Microsoft Universal Print Integration

- MyQ Roger implements a **Universal Print Connector** that enables printers to communicate directly with **Microsoft's Universal Print servers**.

- Print jobs are securely stored on **Microsoft servers** and retrieved on demand after user authentication.
- Printing is conducted through **Universal Print drivers**, ensuring seamless and secure job handling.

9.4 Conclusion

MyQ Roger delivers a **holistic, secure printing environment** by combining direct, local, and cloud-based printing workflows with robust security measures. By requiring users to authenticate in person before job execution, MyQ Roger eliminates the risks associated with unattended print jobs, ensuring maximum data protection in modern workplaces.