IBM Guardium

IBM Quantum Safe Remediator

Version 1.1.1

Transform your enterprise with quantum-safe cryptography and build crypto-agility.

Highlights
Adaptive Proxy – Enable crypto-agility with limited changes

Adaptive Proxy Manager – Unified adaptive proxy monitoring

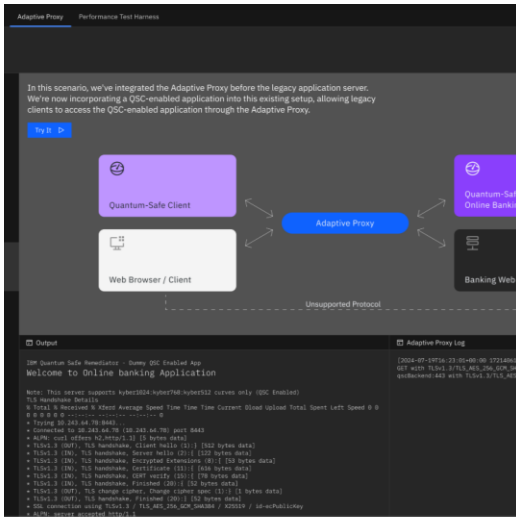
Forward Proxy – Securing outbound traffic

Performance Harness – Free insights before actions

Quantum computing is no longer a distant concept—it’s a looming cybersecurity threat. Cybercriminals are likely to be engaging in “harvest now, decrypt later” attacks, collecting encrypted data today in anticipation of breaking it with quantum capabilities when cryptographically relevant quantum computing becomes available. The transition to quantum-safe cryptography (QSC) has become a business and leadership imperative.

For enterprises with complex IT environment, heterogeneous environments, and mission critical legacy applications, transitioning to quantum-safe cryptography presents a unique set of challenges. These environments often cannot be easily updated, and introducing changes to application code or network configurations carries risk and cost. Organizations need a solution that protects their infrastructure today—without disruptions.

IBM Quantum Safe™ Explorer empowers organizations to strengthen cyber resiliency and accelerate their transition towards using quantum-safe cryptography—with limited need to rewrite lines of application code. It enables hybrid cryptographic environments that support both classical and post-quantum algorithms, defends against "harvest now, decrypt later" attacks, and allows teams to test remediation patterns while evaluating algorithm performance in real-world conditions. With centralized cryptography management and seamless infrastructure integration, IBM Quantum Safe Remediator helps modernize security—ensuring enterprises can upgrade to using quantum-safe cryptography with agility, efficiency, and confidence.



In this scenario, we've integrated the Adaptive Proxy before the legacy application server. We're now incorporating a QSC-enabled application into this existing setup, allowing legacy clients to access the QSC-enabled application through the Adaptive Proxy.

```
IBM Quantum Safe Remediator - Dummy QSC Enabled App
Welcome to Online banking Application

Note: This server supports kyber1024:kyber768:kyber512 curves only (QSC Enabled)
TLS Handshake Details
% Total % Received % Xferd Average Speed Time Time Time Current Dload Upload Total Spent Left Speed 0 0
0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0
* Trying 10.243.64.78:8443...
* Connected to 10.243.64.78 (10.243.64.78) port 8443
* ALPN: curl offers h2,http/1.1] [5 bytes data]
* TLSv1.3 (OUT), TLS handshake, Client hello (1):} [512 bytes data]
* TLSv1.3 (IN), TLS handshake, Server hello (2):{ [122 bytes data]
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):{ [53 bytes data]
* TLSv1.3 (IN), TLS handshake, Certificate (11):{ [616 bytes data]
* TLSv1.3 (IN), TLS handshake, CERT verify (15):{ [78 bytes data]
* TLSv1.3 (IN), TLS handshake, Finished (20):{ [52 bytes data]
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):} [1 bytes data]
* TLSv1.3 (OUT), TLS handshake, Finished (20):} [52 bytes data]
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / X25519 / id-ecPublicKey
* ALPN: server accepted http/1.1
```

```
[2024-07-19T16:23:01+00:00 17214061
GET with TLSv1.3/TLS_AES_256_GCM_SH
qscBackend:443 with TLSv1.3/TLS_AES
```

Adaptive Proxy – Enable crypto-agility with limited changes

The Adaptive Proxy is designed to seamlessly handle both legacy and Post-Quantum ready clients and servers by enabling backward compatibility and smooth interoperability. Whether the request comes from a legacy browser, a hybrid system, or a quantum-safe device, the proxy ensures the transition to using post-quantum cryptography (PQC) and helps enterprises defend against "harvest now, decrypt later" scenarios without disrupting mission-critical systems or workflows. With support for modern NIST-approved cryptographic curves, the Adaptive Proxy offers centralized control over TLS protocols and policies. Hence streamlining the management of complex environments.

A key use case is protecting the information in transit between Internet of Things (IoT) devices, which often lack the resources to implement PQC themselves. In these cases, the Adaptive Proxy acts as a shield, ensuring secure communication between IoT devices and enterprise services without compromising performance.

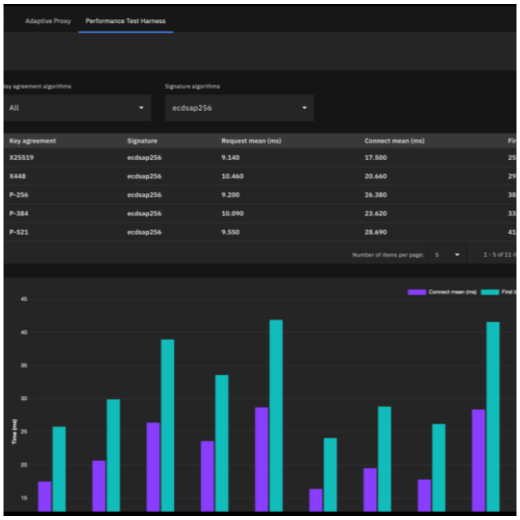
The Adaptive Proxy also offers flexible deployment options within Kubernetes or OpenShift clusters. It can be deployed as a pre-ingress controller; processing traffic before it reaches the cluster's ingress. Or as a post-ingress controller that handles TLS re-encryption and protocol translation while preserving existing routing functions. These deployment options provide enhanced flexibility without significant infrastructure costs.

Adaptive Proxy Manager – Unified adaptive proxy monitoring

IBM Quantum Safe Remediator Adaptive Proxy Manager offers administrators a centralized interface to monitor all Adaptive Proxy instances across the network. Through this manager, administrators can easily view the configuration and health status of deployed proxies. It also enables selective configuration updates, allowing efficient management and maintenance of installed Adaptive Proxies.

Forward Proxy – Securing outbound traffic

The Forward Proxy acts as a critical intermediary, securing outgoing traffic between clients and the internet. It intercepts TLS requests, ensuring that all data leaving the network is encrypted. This is essential when parts of the supply chain aren't yet quantum-safe, providing an added layer of protection against quantum threats. For example, financial institutions can secure sensitive transactions to organizations with non-compliant supply chain partners and still ensure their communications remain safe by encrypting outgoing traffic with the NIST PQC algorithms before it reaches third-party systems. Forward Proxy ensures that your outgoing traffic is always quantum-safe, no matter where it's going. The client app adds flexibility, allowing users to turn the proxy on or off as needed, depending on their security environment.



ey agreement algorithms: All

Signature algorithms: ecdsap256

Key agreement	Signature	Request mean (ms)	Connect mean (ms)	Fi
X25519	ecdsap256	9.140	17.500	25
X448	ecdsap256	10.460	20.660	29
P-256	ecdsap256	9.200	26.380	38
P-384	ecdsap256	10.090	23.620	33
P-521	ecdsap256	9.550	28.690	41

Number of items per page: 5 1 - 5 of 11 i

Performance Harness – Free insights before actions

Performance Harness enables the enterprise to measure HTTP traffic and allow users to understand how the algorithms are impacting behaviors. The analysis can help the enterprise take actions that optimize the performance of cryptographic algorithms in both client infrastructure and cloud environments. By running tests using OpenSSL and the benchmarking tool h2load, the Performance Harness allows a security infrastructure architect to gather specific environment performance metrics and compare them to standardized benchmarks, providing valuable insights that guide your quantum-safe transformation efforts.

With a dashboard view, users can benchmark various algorithm combinations and select from a range of test scenarios to run performance tests in the environment. The results, stored in a file system, can be compared to determine how different cryptographic algorithms impact performance. This data-driven approach improves the enterprise transition to using quantum-safe cryptography.

IBM Quantum Safe Remediator pre-requisites:

	Adaptive Proxy / Adaptive Proxy Manager / Performance Harness	Forward Proxy
System Requirements	**Virtual Server Instance / Virtual Machine** CPU: 8-core CPU or similar RAM: 64GB Free disk space: 10GB , 100GB (for Adaptive Proxy Manager) **Operating System** Red Hat Enterprise Linux v7.1 or later Ubuntu v20.04 or later	**Operating System** Windows 11 or later or Ubuntu Linux
Software Requirements	Docker Engine v25.0.3 or Later Web browser - Chrome, Safari, Firefox or Edge Internet connection will be needed for Adaptive Proxy Manager VPN connection may be needed for Adaptive Proxy Manager, as per the requirement of the target environment.	PowerShell for Windows /Bash shell for Linux Podman client v4.9.3 or above (for Windows/Linux) or Docker Client v25.0.3 or above
Red Hat Open Shift (RHOS)/Kubernetes cluster installation requirements	**Cluster deployment for Adaptive Proxy only** Kubernetes v1.28 or above CPU 500 millicore for each running pod RAM 128 MB per running pod Helm v3.15.2 or later Kubectl v1.30 or later	

Conclusion

IBM Quantum Safe Remediator helps enterprises transition to quantum-safe cryptography with minimal disruption by enabling hybrid environments, securing communications, and defending against future decryption threats. It delivers crypto-agility while preserving operational stability, making modernization both secure and seamless.

For more information

To learn more about IBM Quantum Safe Explorer and IBM Guardium, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/guardium-quantum-safe.

Produced in the
United States of America
June 2025

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.