IBM Quantum Safe Remediator

Seamlessly transition your enterprise to quantum-safe cryptography and build crypto-agility.

Highlights
Enhance cyber resiliency by protecting applications with an adaptive proxy while enabling communications with different browser clients on the network

Test various combinations of quantum-safe cryptographic algorithms to optimize performance before deploying to production

Build crypto-agility by centralizing cryptography management and implementing quantum-safe

Quantum-safe cryptography refers to encryption algorithms and protocols that are resistant against classical computers as well as future cryptographically relevant quantum computer (CRQC) driven decryption attacks. Even before a CRQC becomes available, “harvest now, decrypt later” attacks could enable cybercriminals to obtain and store data until they can decrypt it. Sensitive data with a long term data value, such as tax records, medical records, passports, as well as critical infrastructure systems, are at risk today. Preparedness is crucial. It is now possible to protect assets against future threats with quantum-safe cryptographic solutions.

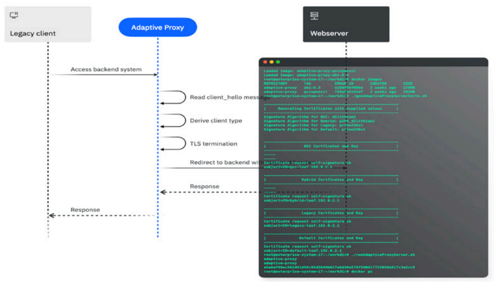
IBM Quantum Safe Remediator provides you with capabilities to seamlessly upgrading your existing IT infrastructure to quantum-safe. It offers a robust set of components and patterns for application, network, and third-party remediation across various client–server communication scenarios. Build crypto-agility as you centralize cryptography management while also exploring, testing, and applying best practices for remediation.

Secure communications between applications, data, and network systems.
Protect your applications and network endpoint without having to modify code or overhaul your existing IT infrastructure. By positioning an adaptive proxy as an intermediary between your server and clients of all types: legacy, hybrid, and quantum-safe-cryptography-enabled.

Centralize cryptographic management for agility.
Bring cryptography management into a centeralized function to enable crypto-agility for faster modifications, replacements (as needed) for encryption, and use of keys and certificates across enterprise.

Optimize deployment of PQC algorithms and remediation patterns with test harness.
Evaluate the performance of quantum-safe cryptography protocols as a means to gain insights on how to best use the algorithms and optimize performance accordingly before deploying changes to production.

Sign up to view a live demo at ibm.com/quantumsafe



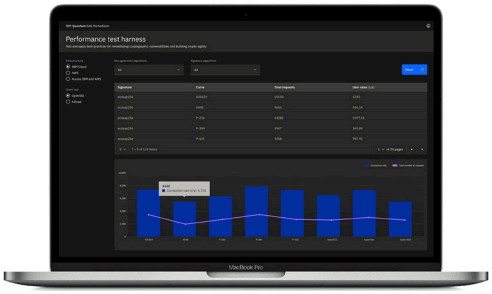
```
Loaded image: adaptive-proxy:qscopenssl
Loaded image: adaptive-proxy:ubi-9.3
root@enterprise-system-17:~/workdir# docker images
REPOSITORY       TAG          IMAGE ID       CREATED        SIZE
adaptive-proxy   ubi-9.3      e10df98f08be   2 weeks ago    278MB
adaptive-proxy   qscopenssl   728afe5341d7   2 weeks ago    283MB
root@enterprise-system-17:~/workdir# ./genAdaptiveProxyServerCerts.sh
----------------------------------------------------------
|     Generating Certificates with Supplied values       |
----------------------------------------------------------
Signature Algorithm for QSC: dilithium2
Signature Algorithm for Hybrid: p256_dilithium2
Signature Algorithm for Legacy: prime256v1
Signature Algorithm for Default: prime256v1

----------------------------------------------------------
|              QSC Certficates and Key                   |
----------------------------------------------------------
-----
-----
Certificate request self-signature ok
subject=CN=qsc-leaf.192.0.2.1
----------------------------------------------------------
|             Hybrid Certficates and Key                 |
----------------------------------------------------------
-----
Certificate request self-signature ok
subject=CN=hybrid-leaf.192.0.2.1
----------------------------------------------------------
|             Legacy Certficates and Key                 |
----------------------------------------------------------
Certificate request self-signature ok
subject=CN=legacy-leaf.192.0.2.1
----------------------------------------------------------
|             Default Certficates and Key                |
----------------------------------------------------------
Certificate request self-signature ok
subject=CN=default-leaf.192.0.2.1
root@enterprise-system-17:~/workdir# ./runAdaptiveProxyServer.sh
adaptive-proxy
adaptive-proxy
a5adaf99ec562d91d58c95d3690b827abd30a579f590417753856e817c3a2cc5
root@enterprise-system-17:~/workdir# docker ps
```

Adaptive Proxy

The Adaptive Proxy will analyze if a request is coming from either a quantum-safe browser or a non-quantum-safe browers, and automatically establish a secure connection to an application. A common use case scenario is when an application, server, or endpoint cannot be remediated. Adaptive proxy can ensure a quantum safe connectivity, thus creating an agile solution to protect against "harvest now, decrypt later" situations.

It is achieved by enabling fully backward compatible quantum-safe communication across applications or servers. It involves positioning an adaptive proxy as an intermediary between clients and servers and implementing quantum-safe encryption, decryption, and key exchange mechanisms to ensure confidentiality, integrity, and authentication of the transmitted data. It is deployable on VMs, in containers, or to protect entire Kubernetes or Open Shift clusters.



IBM Quantum Safe Remediator

Performance test harness

Test and apply best practices for remediating cryptographic vulnerabilities and building crypto-agility

Infrastructure
● IBM Cloud
○ AWS
○ Across IBM and AWS

Client tool
● OpenSSL
○ h2load

Key agreement algorithms: All
Signature algorithms: All

Signature	Curve	Total requests	User rates (c/s)
ecdsap256	X25519	15150	1250
ecdsap256	X448	9665	656.14
ecdsap256	P-256	14282	1197.15
ecdsap256	P-384	5947	369.84
ecdsap256	P-521	9258	787.91

5 | 1 – 5 of 119 items | 1 of 24 pages

Performance test harness - Insight before Action

The performance test harness provides a testbed for gathering insights and conducting independent performance benchmarks, such as OpenSSL and h2load, and establishes baselines across public networks before implementation on your client environment to obtain targeted performance metrics. Using a suite of test scripts and software packages along with a dashboard, the performance test harness enables the client to know exact behavior of the algorithms used and compare standardized benchmarks against the tests executed in your environment to guide your remediation actions as you transition to quantum-safe cryptography.

IBM Quantum Safe Remediator prerequisites

The Adaptive Proxy and performance test harness requires the following system and software:

	Adaptive Proxy	**Performance test harness**
System requirements (50GB memory)	Virtual Server Instance/Virtual Machine CPU: 8 CORE: 4 RAM: 64GB Operating System: RHEL- Version 7.1 or later Ubuntu - Version 20.04 or later	Virtual Server Instance/ Virtual Machine CPU: 8 CORE: 4 RAM: 64GB Operating System: RHEL- Version 7.1 or later Ubuntu - Version 20.04 or later
Software requirements	Docker client Version: 25.0.3+	Docker client Version: 25.0.3+

Note: The number of virtual machine (VM) instances required for the performance test harness depends on the test scenario(s) you select—for example, if there are client components on one VM and server components on another VM, or if both are on the same VM, etc. Also, these configurations may vary depending on the expected traffic and usage.

Begin your quantum-safe transition today

Take the next steps to transform your cryptography for the quantum era with IBM Quantum Safe Remediator.
Get started today at ibm.com/quantumsafe

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
May 2024

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.