Dynamic Data and Secrets Protection: Are We Ready for the Post-Quantum Encryption Era?



Petras Kazlauskas
Partner Technical Specialist (PTS-P)

Guardium Data Security Center
Guardium Quantum-safe
HashiCorp Vault

Guardium®

HashiCorp Vault

IBM

Bad examples set things in motion

LSM Latvian Public Service Media

Politics Society Culture Economy Features Weather

Important 15th Saeima elections Border Defence airBaltic Drones Rail Baltica Coalition War in Ukr

Data of 1.2 million people breached in recent CSDD cyberattack

Share

Follow LSM on Google



August 18, 15:15 | Update 18. august, 21:37 | Crime | **Authors:** LSM English *(Latvian Public Media)*

The Road Traffic Safety Directorate (CSDD) reported on August 18 that personal data relating to 1.2 million people was obtained in a cyberattack. Latvia's total population is a little over 1.8 million, so as a proportion of the population, the breach is enormous.

Major Polish data breach aimed at extorting ransom, PM says

13.08.2026 19:30

A massive cyberattack on a Polish medical services company appears to have been motivated by an attempt to extort a ransom, Prime Minister Donald Tusk said on Thursday, as authorities probe a data breach that may have exposed the medical information of nearly 19 million people.



Polish Prime Minister Donald Tusk PAP/Piotr Nowak

"The motivation appears to be purely criminal; much indicates that this was an attempt to extort a ransom from the company," Tusk told reporters.

He said the investigation was ongoing and that state security services were involved.

Tusk told a news conference in Warsaw that "no private company anywhere in the world can guarantee 100-percent protection" against cyberattacks.

"We are focusing on making sure there are no leaks, or as few leaks as possible, from our institutions," he said

Dynamically Secure Your Data

IBM

Guardium®

What we'll cover next

How Guardium Data Protection can help in protecting your data

01 - Discover

Where is your sensitive data?

⚠ 53% Customer PII is the #1 target — compromised in 53% of breaches.

Discovery & Classify

02 - Monitor

Who is accessing it?

⚠ Malicious insider attacks are the costliest breaches — $4.92M

Monitoring & Least Privilege

03 - Comply

Can you show evidence to Auditors?

⚠ 1 in 3 breaches (32%) results in a regulatory fine

Automate Compliance

04 - Harden

Any back doors open in the database?

⚠ Vulnerability-led breaches cost $4.24M on average

Find & Fix Vulnerabilities

05 - Remediate

Can you auto block data exfiltration?

⚠ Ransomware costs $5.08M when the attacker discloses it

Detect & Remediate threats

Cost of Data Breach Report 2025 - https://www.ibm.com/forms/mkt-53830

Guardium Data Protection

The gold standard for real-time data activity monitoring and protection

Centralize visibility and control

Understand how users are accessing data, plus define and apply consistent security policies across hybrid cloud environments, reducing inconsistent governance

Dynamic data protection

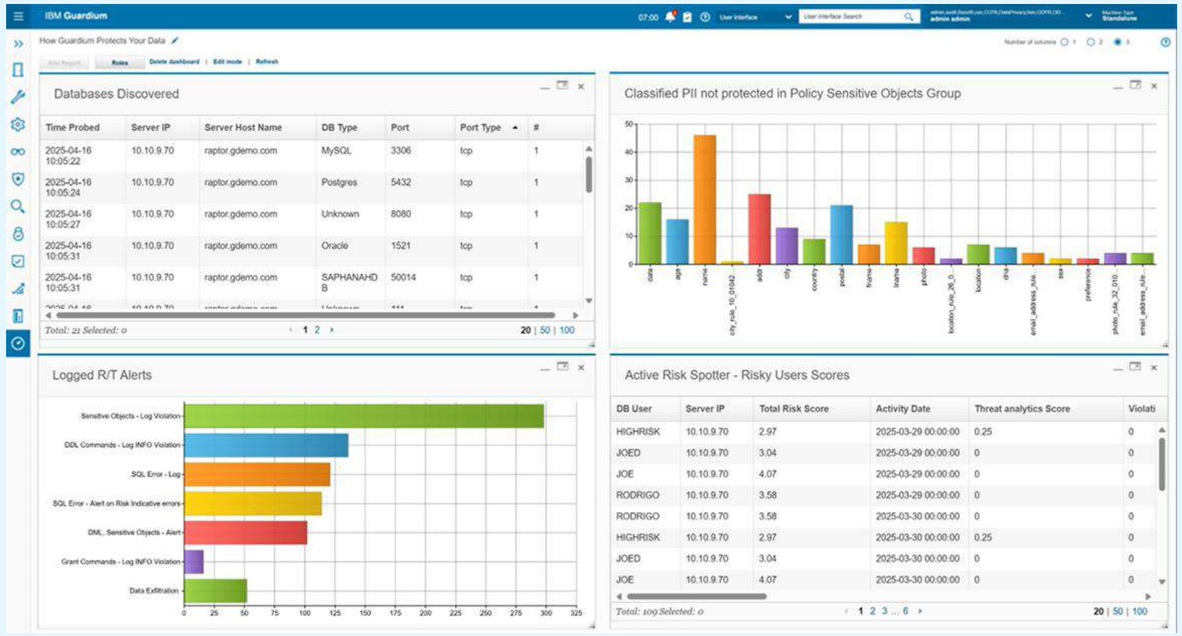
Protect sensitive data in real time with dynamic masking, redaction, quarantining and blocking – automatically triggered by suspicious user behavior or policy violations

Accelerate compliance

Streamline audit readiness with policies, automated workflows, and tamper-proof audit trails and reporting – significantly speeding up response to regulatory demands

Manage threats to data

Use AI and behavioral analysis to detect, prioritize and respond to insider threats, compromised accounts, and external actors to reduce dwell time and exposure of critical data



70%

reduction in time spent on responding to regulatory audits[1]

Large Utility Company, US

Meeting compliance obligations in the most efficient and effective way is not only an objective but a necessity while also measurably reducing risk and cost. This client used Guardium Data Protection's compliance templates to improve & simplify their compliance processes, decreasing the time and resources required to meet mandated corporate and government compliance regulations, reducing the initial generation of an audit request report from weeks to minutes.

Discover and Classify Data

Why it matters

Visibility Gap

Most breaches (53%) target **PII hidden** in locations you aren't even watching

Trust Deficit

Manual labels fail; you need **99%+ accuracy** to drive automated security

Exposure Window

80% of breaches involve data collection that **goes unnoticed** until it's too late

Why IBM

100+ Pre-Built Patterns

Accurately identify regulated data across hybrid environments with proven discovery templates

Auto-Discovery

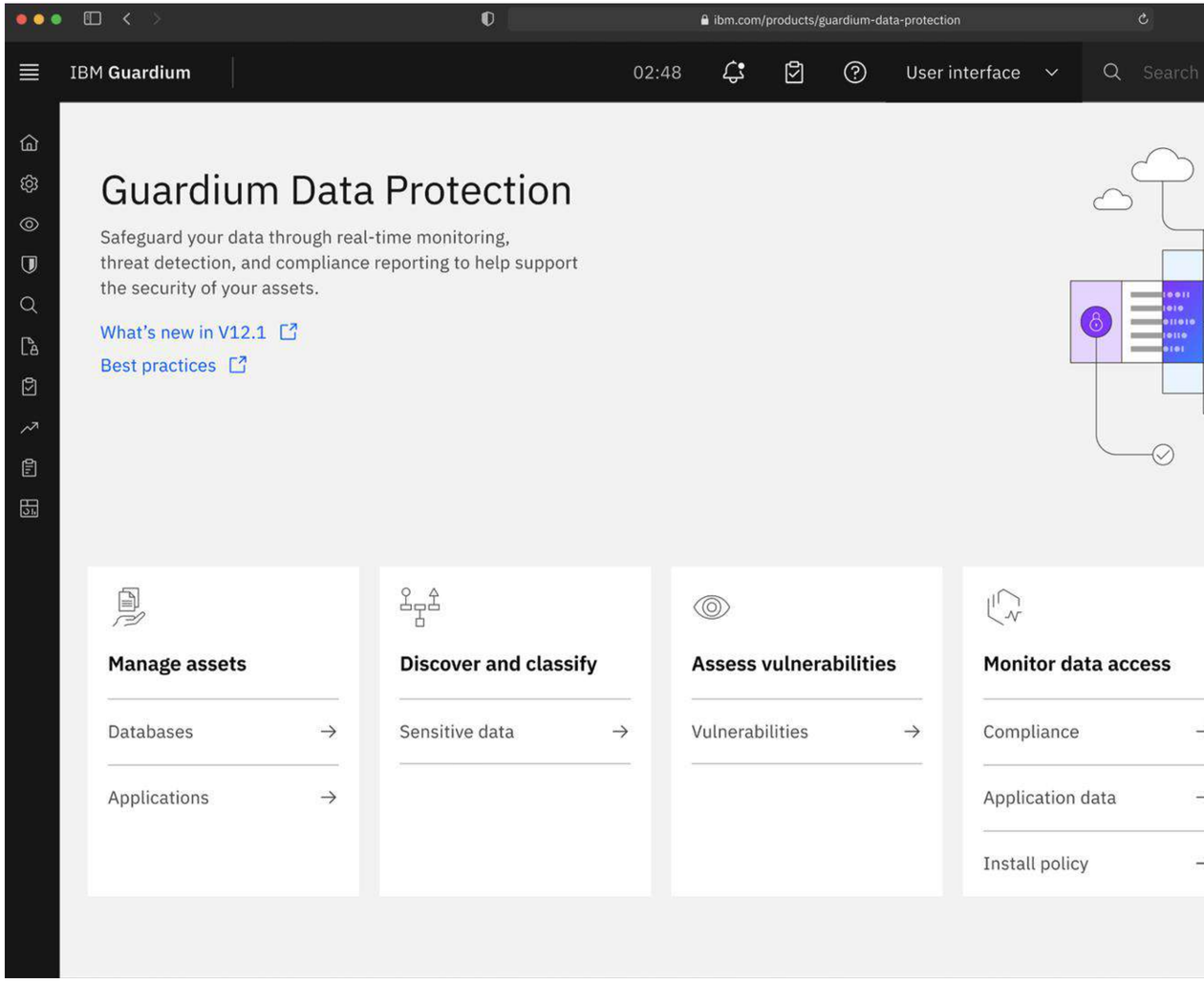
Database and port scanning reveals unmanaged and unexpected data sources automatically

High-Scale Scanning

Efficiently analyze hundreds of data sources with minimal performance impact

Centralized Control

Understand where sensitive data lives and apply the right protection policies from one console



Discover and classify regulated data

Leverage 100+ data discovery patterns to find regulated data

Hybrid Environment

Identify sensitive data like credit card numbers, personal financial data, or social security numbers across on-premises or the cloud.

Discover Sensitive Data Workflow Builder

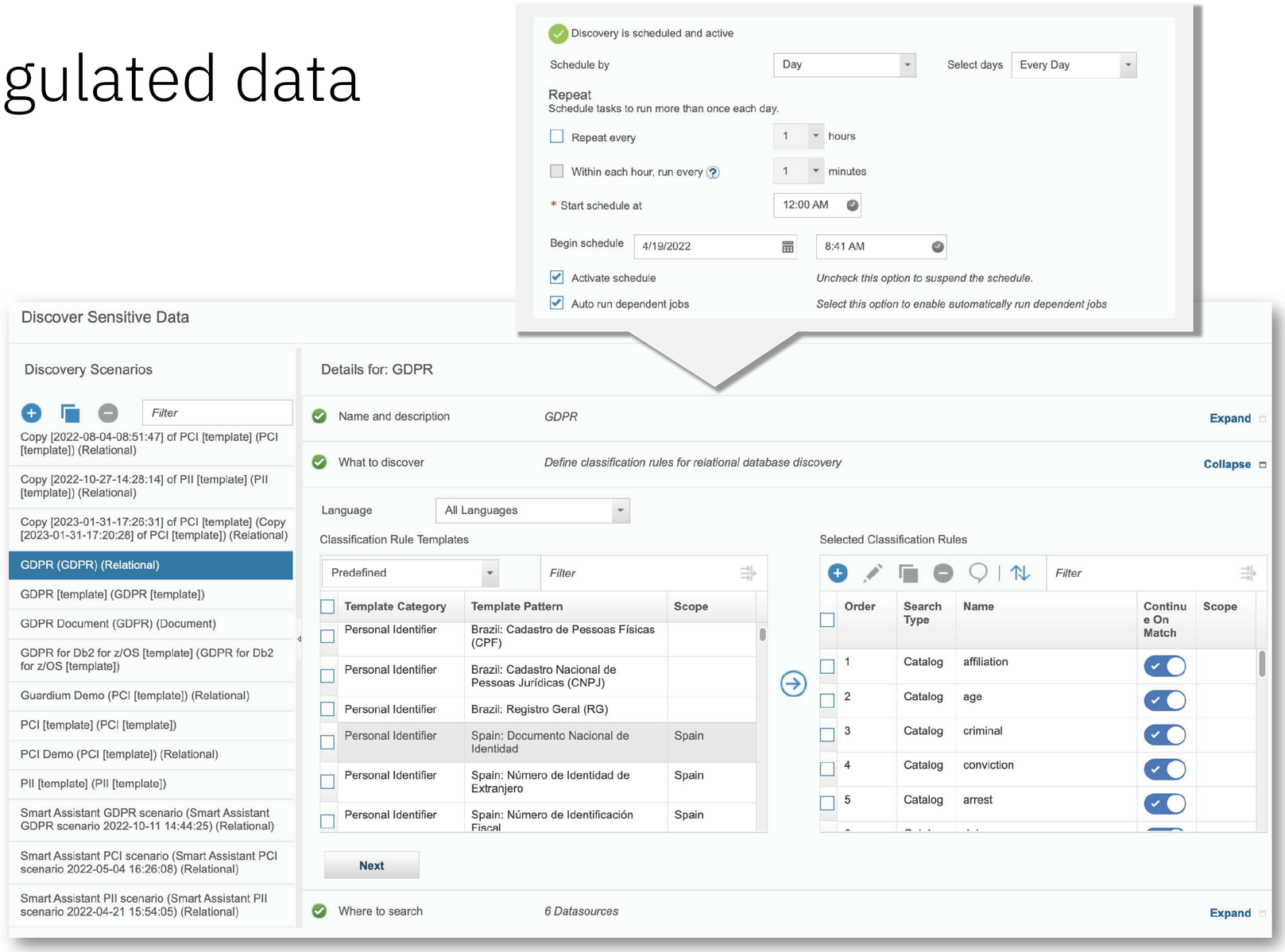
Specify rules for discovery, define actions to take on discovered data, specify which data sources to scan, distribute reports, and run the workflow on an automated schedule.

Database Auto-Discovery

Scans and probes servers for open ports to prevent unknown or unwanted connections to the network.

Run auto-discovery processes on demand or schedule the processes on a periodic basis.

Custom classification workflows for audit purposes



Manage Discovery Scenarios to define and map applications to their data sources

Monitor Data Activity and Enforce Least Privilege

Why it matters

Insider Threat

Malicious breaches average **$4.92M**; monitoring privileged access is the only way to stop high-cost misuse early

Dwell Time Gap

With attackers active for an average of **58 days**, real-time behavior visibility is critical to catching them before the data leaves

Analyst Fatigue

Manual reporting wastes **25%** of a team's time; centralized workflows are required to focus talent on high-value defense.

Why IBM

Flexible Monitoring

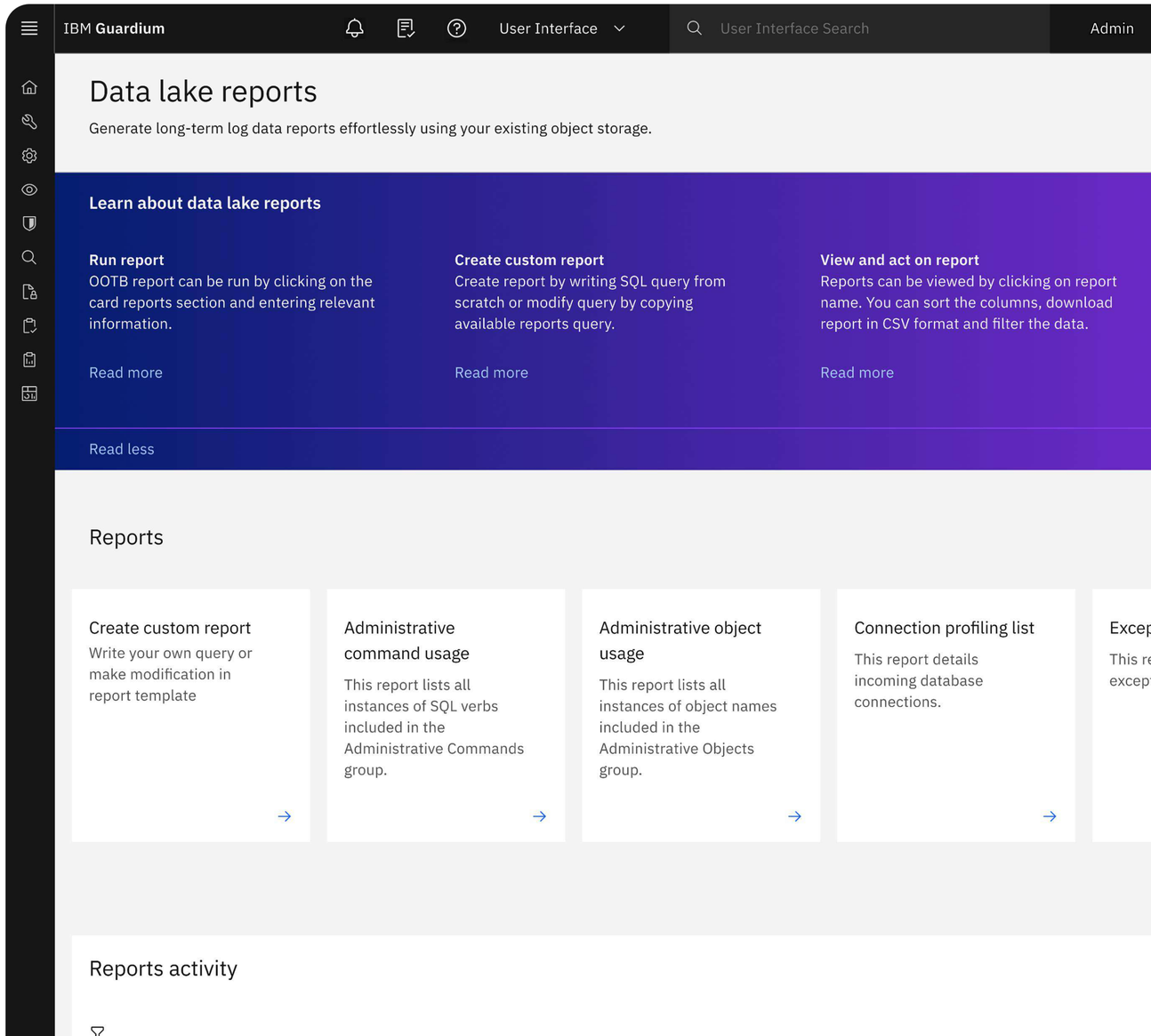
Agent-based and agentless options provide high-fidelity visibility across hybrid multi-cloud data environments

Unified Policy Enforcement

Automated audit workflows track compliance progress and streamline approvals across all data sources

Fine-Grained Controls

Rule-based policies enable monitoring, logging, reporting, alerting, and optional real-time blocking or redaction



Enable dynamic data protection

Protect sensitive data with real-time visibility into data-level access and activity

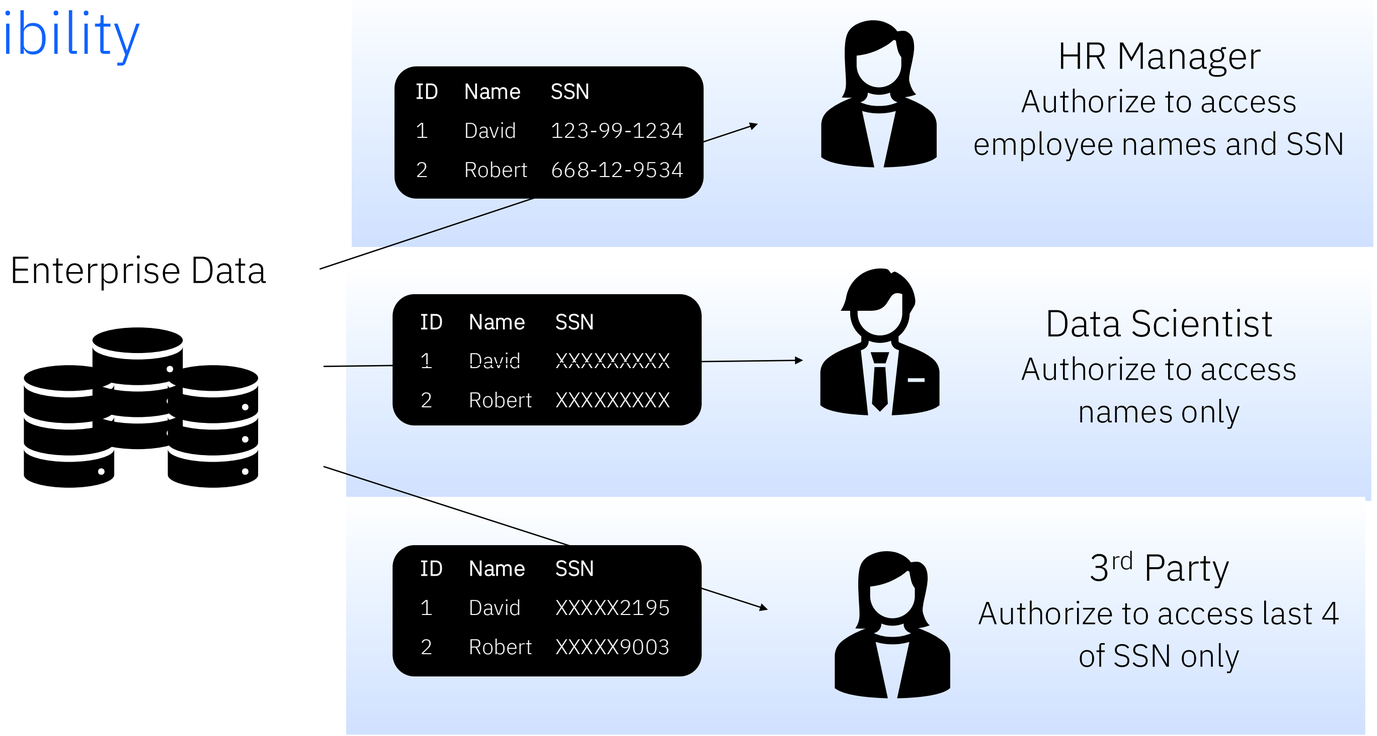
Centralize visibility
Collect monitoring data from hybrid multi-cloud data environments using flexible monitoring options.

Gain real-time visibility using agents and/or evaluate tradeoffs to go agentless for faster and lighter deployment.

Fine-grained access control
Enable basic or advanced security policies to gain deeper insights and strengthen posture.

Define rule-based policy actions to monitor, log, report and alert on unauthorized data access, and consider implementing real-time controls such as blocking and redaction.

Consistent policy enforcement
Ensure policies and rule actions are applied uniformly across hybrid data environment.



Ensure right users have access to right-level of data at a granular level.

*And for the **right purpose**, with Watson Knowledge integration.*

Automate Continuous Compliance

Why it matters

Audit Drag

With **28 audits per year**, teams spend 25% of their time in a constant cycle of manual preparation

Resource Drain

Compliance costs average **15,000+ hours** of effort; manual evidence gathering is a $2.3M budget sinkhole

Readiness Gap

Only 9% of teams can produce audit data in under two days; manual workflows cannot scale to modern audit demands

Why IBM

Guided Compliance Templates

Instantly map technical controls to global regulations like GDPR, SOX, and PCI DSS and more

Real-Time Control Monitoring

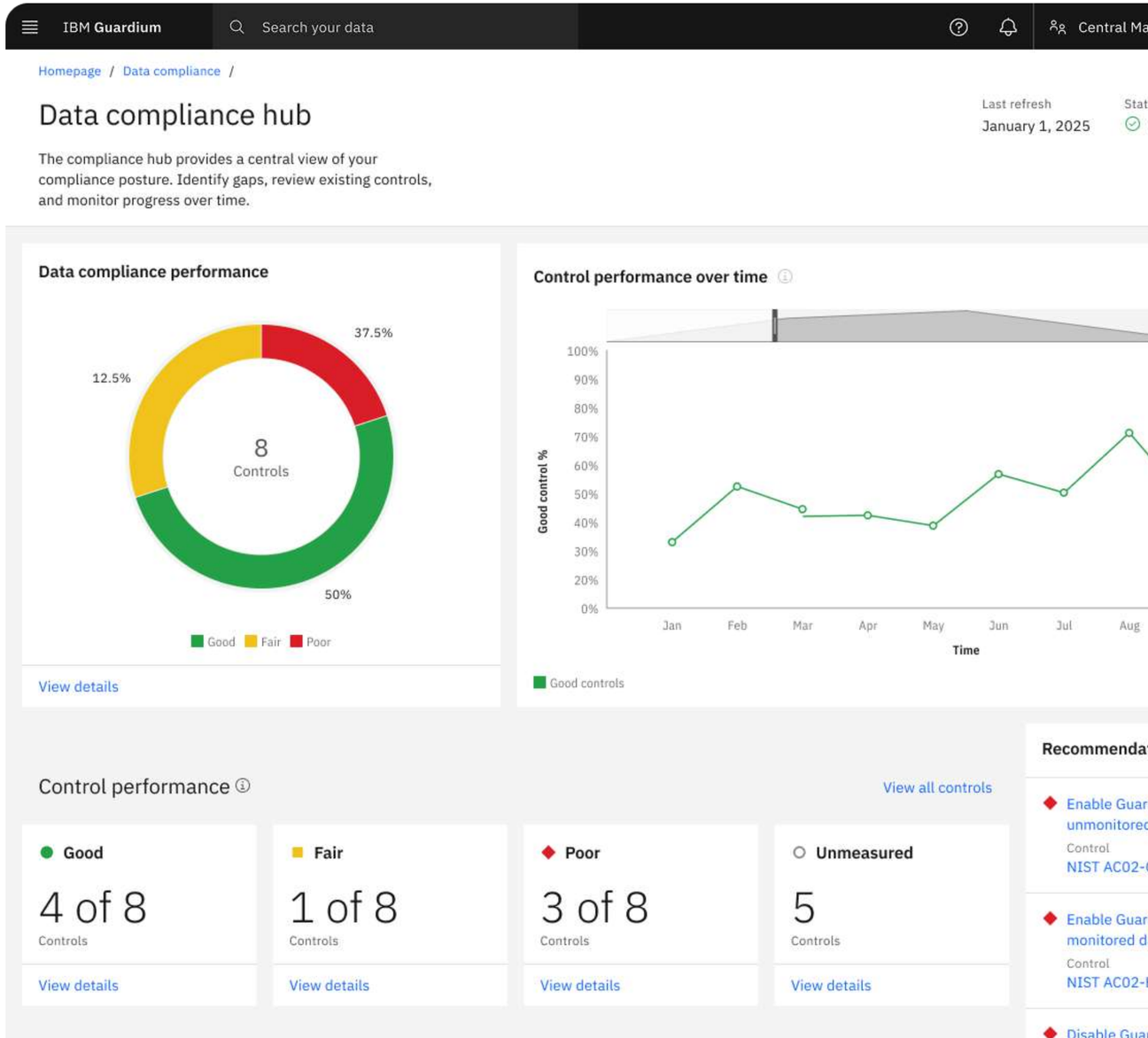
Move from "point-in-time" audits to 24/7 visibility with automated threshold alerts

Automated Audit Workflows

Schedule the collection and distribution of tamper-proof reports directly to stakeholders

Compliance Hub

A single, "scorecard" view to track audit readiness and control health across the entire hybrid estate



Unify. Simplify. Comply.

Create custom auditing policies and automate end-to-end reporting

Centralize policy management

Define new or customize audit rules from policy templates to get a head start.

Add compliance tags to map common requirements across regulations and avoid duplication of effort.

Ensure separation of duties

Conform to security first principles through continuous, fine-grained audit trails and ensure audit data is stored in tamper-proof repositories.

Enable compliance automation

Track progress towards compliance on all selected regulations from a single interface.

Setup and automate audit process workflow to share for review and signoff with key stakeholders.



Create new or customize audit policies quickly, and not from scratch

Compliance Controls

Map internal standards directly to Guardium controls, replacing spreadsheets. Use templates, attach evidence, and keep requirements, ownership, and status current—embedded in daily operations and audit-ready.

Compliance Thresholds

Define flexible KPIs and targets from Guardium data. Track aging tasks, SLA adherence, and trends to spotlight slipping performance, drive improvements, and demonstrate compliance.

The Hub

The Hub unifies control health, thresholds, and signals in a dashboard. See what's on track, pinpoint gaps, drill into owners and workflows and prioritize fixes.

Find and Fix Vulnerabilities

Why it matters

Vulnerability Exploitation

Vulnerability-led breaches are up **34% YoY**; finding database misconfigurations is now a race against time

Remediation Lag

With a **32-day median fix time**, half of all edge vulnerabilities remain exposed and unpatched

Cost of Inaction

Breaches triggered by unpatched exploits now average **$4.24M** in total losses

Why IBM

35+ Data Source Types

Support across hybrid cloud, including on-premises databases, cloud warehouses, and managed services with regular updates

2,000+ Vulnerability Tests

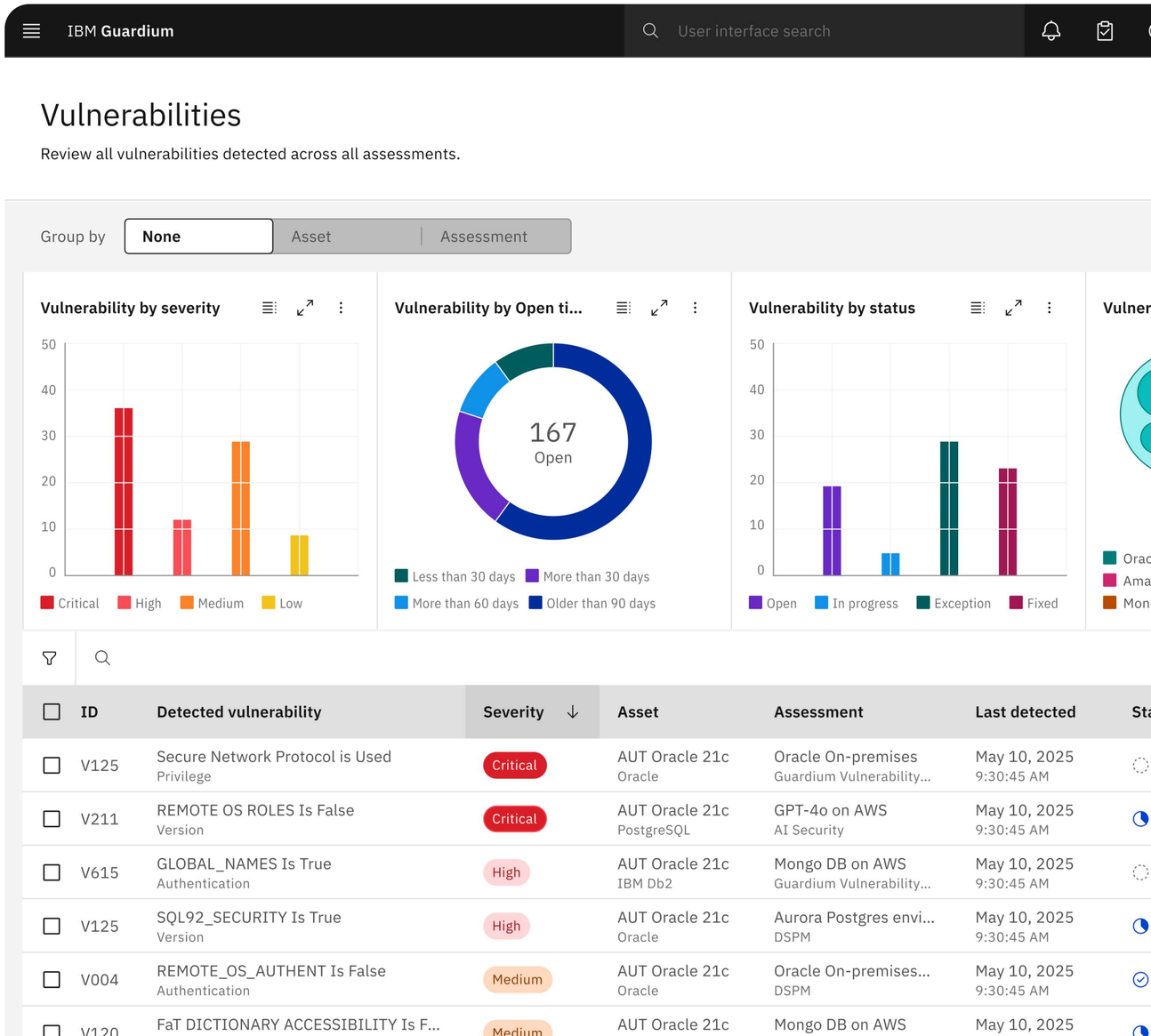
Deep scanning for misconfigurations, missing patches, and policy violations with zero performance impact

Benchmark-Aligned Guidance

Remediation recommendations based on STIG, CIS, CVE, and industry standards

Automated Integration

Scheduled scanning and automated integration with workflows like ServiceNow for streamlined triage and remediation



Guardium Vulnerability Assessment

Identify and remediate database vulnerabilities before they're exploited

Scanner modernization

Address scale and faster scans with a standalone client application that will run vulnerability assessments outside of Guardium Data Protection

Harden data infrastructure

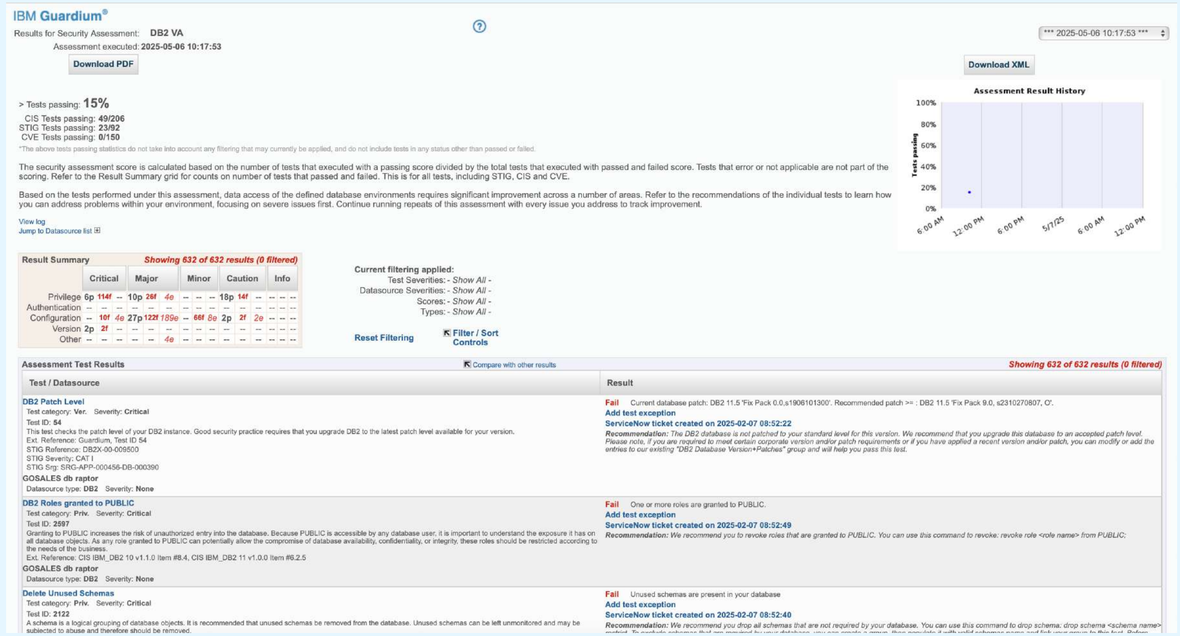
Implement automated scanning of databases, data warehouses, and big data environments across hybrid cloud to detect and remediate vulnerabilities based on benchmarks from STIG, CIS, CVE, and more

Risk-based prioritization

Apply asset classification context to prioritize the most critical vulnerabilities based on insights from metadata

Clear metrics and reports

Prove the effectiveness of the data infrastructure vulnerability management program by obtaining metrics and viewing trends over time to demonstrate progress



>30

data stores supported, executing more than 2,000 tests

Telecommunications Provider, US

To reduce cybersecurity risk, the client needed to assess over 10,000 databases across on-premises and Azure environments for vulnerabilities. Guardium Vulnerability Assessment was deployed to scan databases on a scheduled basis, with findings automatically routed to ServiceNow for triage and remediation. The result was tight integration into existing workflows, and improved visibility and control over database security posture.

Detect and Remediate Threats

Why it matters

Cost of Exposure

Whether via insiders (**$4.92M**) or phishing (**$4.8M**), initial access leads to multi-million dollar liabilities.

Ransomware Surge

Now appearing in **44% of breaches**, detecting abnormal data access is the only way to stop extortion before it starts

Disclosure Penalty

Incidents average **$5.08M** once attackers disclose a breach; rapid detection is the only lever to lower this cost.

Why IBM

Stop Breaches Early

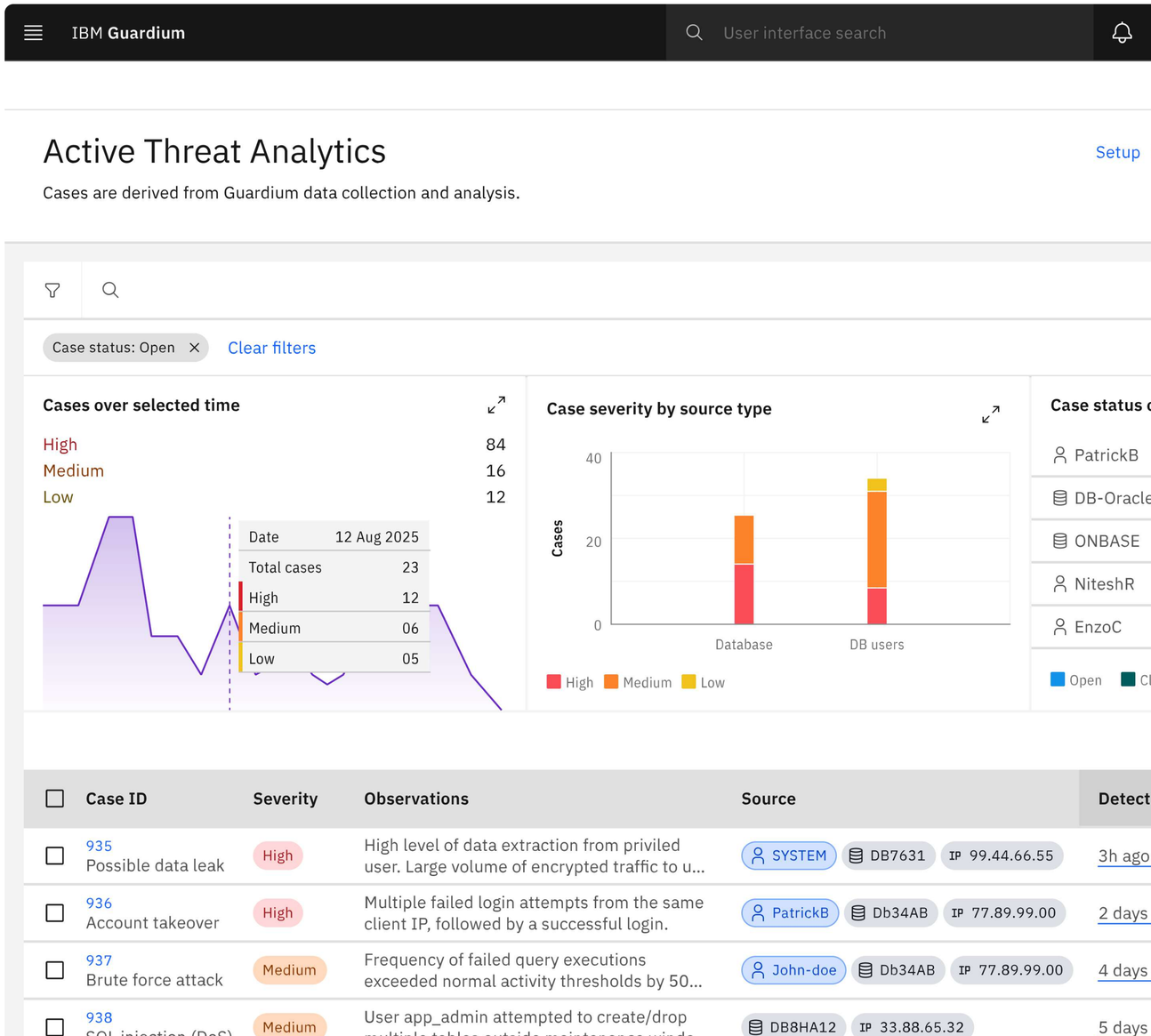
Multi-layer threat analytics combining outlier mining to surface potential breaches earlier than traditional rules-based monitoring

Expose Hidden Threats

Advanced outlier detection purpose-built for data-level threats, identifying abnormal behaviors

Unify Threat Signals

Consistent threat detection across hybrid cloud environments, correlating anomalies and attack indicators across distributed systems



Active Threat Analytics - Mechanisms

Outliers

- Data leak
- Denial of service
- Account take-over
- Schema tampering
- Data tampering
- Anomaly
- Massive grants

Threat Finder

+ custom policy-based ATA detection

- Cross-site scripting (XSS)
- OS command injection
- SQL injection – denial of service
- SQL injection – side channel
- SQL injection – tautology

Threat Diagnostics (aka Eagle Eye)

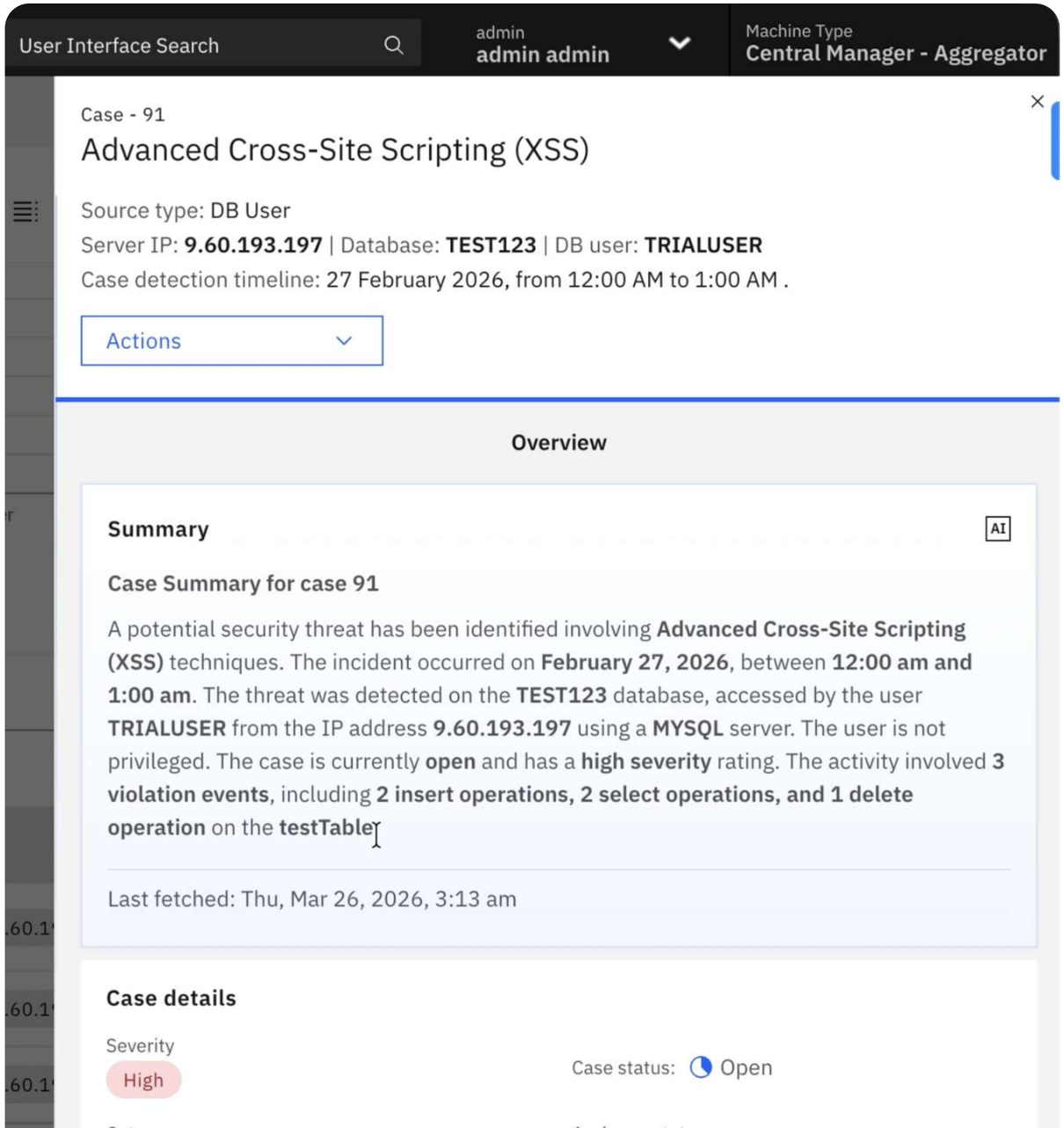
- SQL injection
- Malicious stored procedure
- Suspicious use of new grants
- Brute force attack

GenAI Case Summarization

Investigate Faster. Respond Smarter

AI-powered natural language summaries of Active Threat Analytics cases that distill complex security events into clear, actionable insights

- Reduce investigation time by 60% with AI-generated case summaries
- Enable faster decision-making with clear, natural language explanations
- Improve team efficiency by eliminating time spent parsing complex data



Flexible connections to data sources for active and passive monitoring



S-TAP: Agent-based for real-time monitoring of on-premise data sources



E-TAP: Agent-based, proxy solution for real-time monitoring of cloud data sources



Universal Connectors: Agentless passive monitoring for cloud and on-premise data sources



Streaming APIs: Agentless passive monitoring for cloud data sources

Examples of industry data sources and monitoring choices

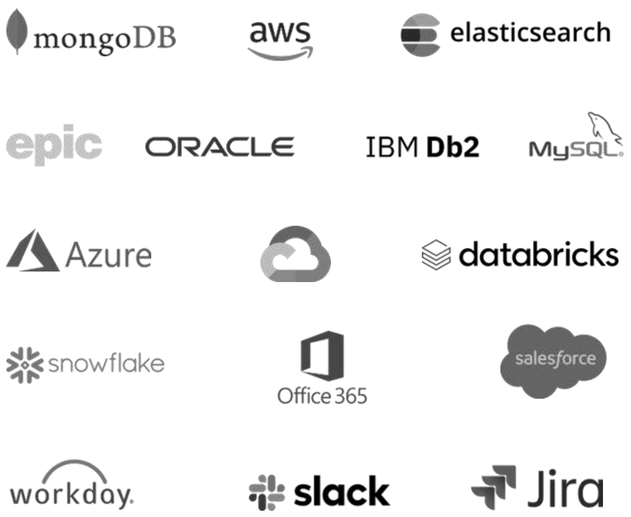
Industry	Data type	Monitoring approach
Financial	Bank account number	Agent, S-TAP, External S-TAP
Retail	Customer information (credit card)	Agent, S-TAP, External S-TAP
Healthcare	Health records (Non-PHI audit)	Agentless Native log files

Ecosystem

The Guardium ecosystem is designed for flexibility

Connectors

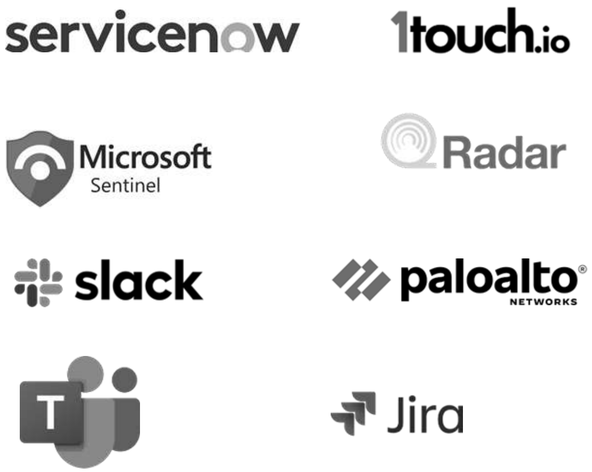
IBM Guardium secures databases, cloud data stores, and SaaS applications



And many more...

Integrations

IBM Guardium integrates to various products to enable workflow, task management, and more



Open framework

IBM Guardium is built to be open, supporting REST API standards for integrating the existing tools

Contributions

IBM participates in and supports various open communities to help shape the direction of security

NIST

AI Alliance

Post-Quantum Cryptography readiness

IBM

Guardium®

#1 Bring useful quantum computing to the world

#2 Make the world **quantum safe**

IBM is recognized as the current Company to Beat in a 2025 Gartner® report on Quantum Computing

Forbes Subscribe: Less than $1.50/wk Sign In

INNOVATION > CLOUD

IBM's Vision For A Large-Scale Fault-Tolerant Quantum Computer By 2029

By Paul Smith-Goodson, Contributor. Analyst-in-residence,... for Moor Insights and Strategy

Follow Author

Published Jun 10, 2025, 09:10am EDT, Updated Jun 10, 2025, 09:20am EDT

Share Save Comment 0



IBM's vision for its large-scale fault-tolerant Starling quantum computer
IBM

IBM has just made a major announcement about its plans to achieve large-scale quantum fault tolerance before the end of this decade. Based on the company's new quantum roadmap, by 2029 IBM expects to be able to run accurate quantum circuits with hundreds of logical qubits and hundreds of millions of gate operations. If all goes according to plan, this stands to be an accomplishment with sweeping effects across the quantum market — and potentially for computing as a whole.

Think Forward w3

September 12, 2025

WSJ's Bold Names podcast: IBM and quantum computing

Overview

WSJ's Bold Names podcast puts the spotlight on conversations with leaders of bold-named companies featured in the pages of The Wall Street Journal. Hosts Tim Higgins and Christopher Mims speak to CEOs and business leaders in interviews that challenge conventional wisdom and take the audience inside the decisions being made in the c-suite and beyond.

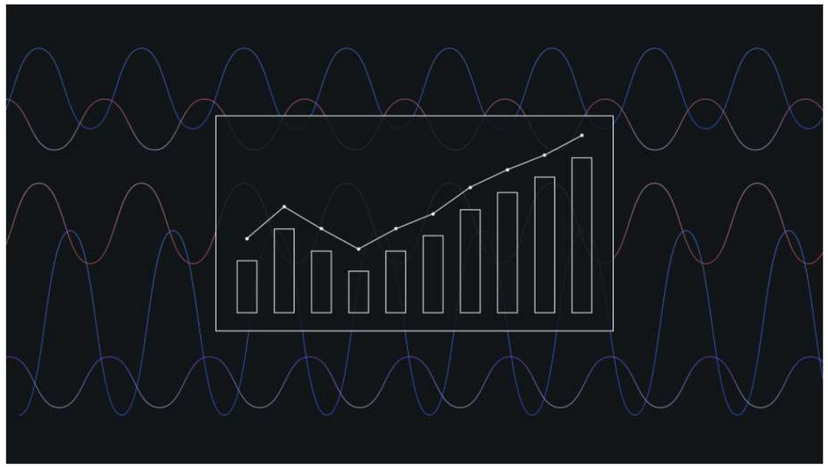
Arvind joined Tim and Christopher to talk about quantum computing, its applications and more.



IBM Sign in to Platform

IBM and Vanguard explore quantum optimization for portfolio construction

New research from IBM® and Vanguard investigates the use of variational quantum algorithms for portfolio optimization.



Date
29 Sep 2025

Authors
Roberto Lo Nardo
Gabriele Agliardi

Topics
Finance Algorithms Research Use Cases

Share this blog

Classical vs quantum bits

Classical bit (bit)

Only two possible states

0 and 1

Like the two faces of a coin

Heads or tails

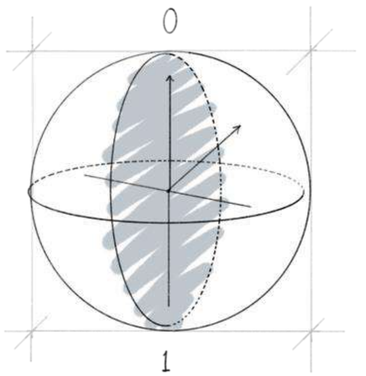


Quantum bit (qubit)

$|0\rangle$ or $|1\rangle$

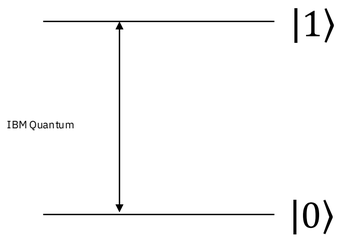
AND any linear combination of the two

e.g. 50% $|0\rangle$ & 50% $|1\rangle$

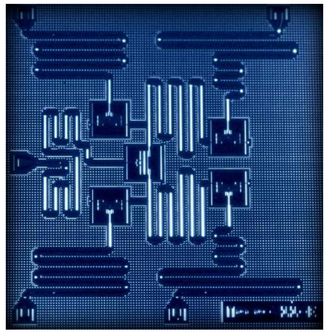


Qubit technology

Theoretically, any two-level quantum system can be used to make a qubit:

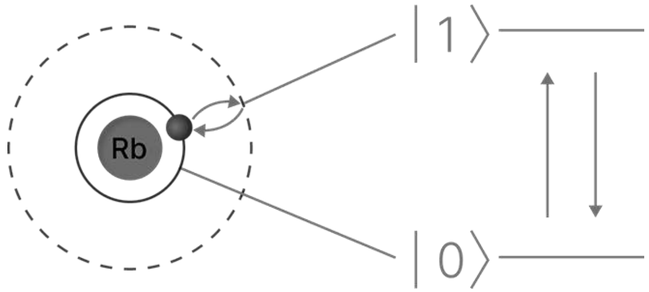


Superconducting qubits



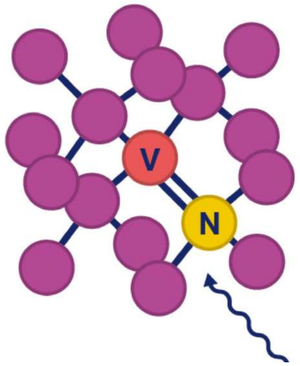
Source: IBM Quantum

Neutral atoms



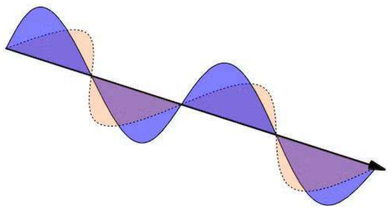
Source: QuEra

Nitrogen vacancy center qubits



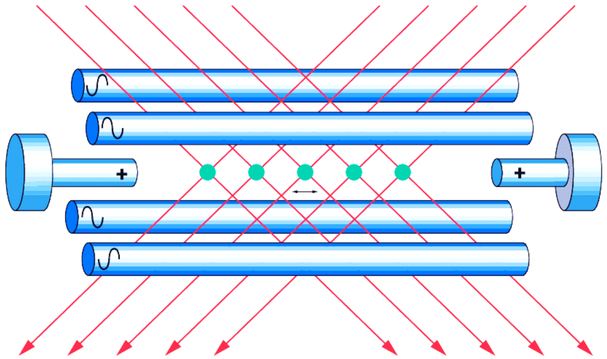
Source: IDTechEx

Photons



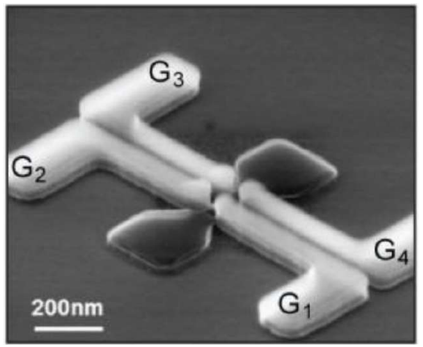
Source: University of Waterloo

Trapped ion qubits



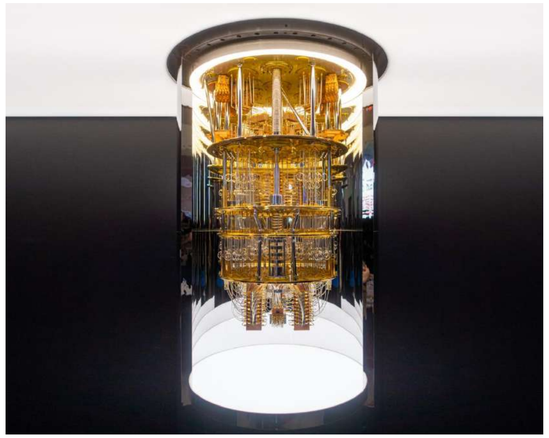
Source: Steane & Rieffel

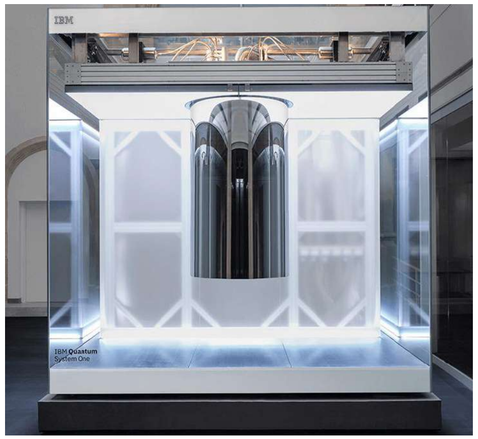
Quantum dot qubits

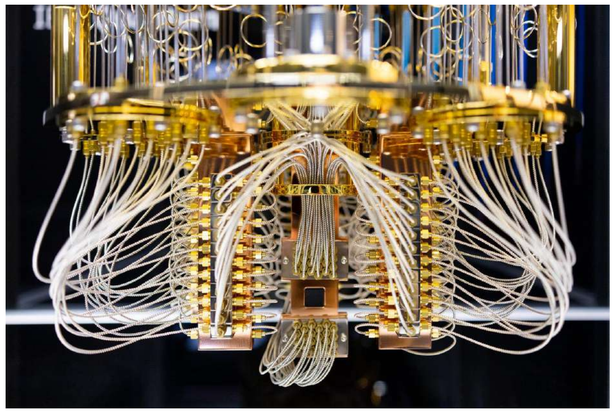


Source: Ansaloni, F

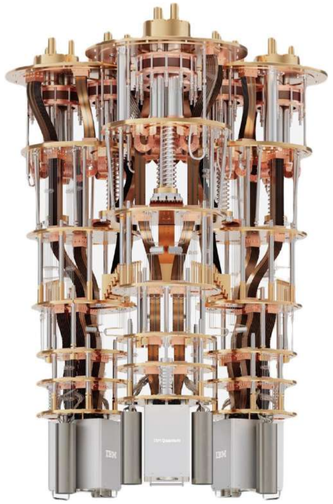
IBM Quantum System ONE







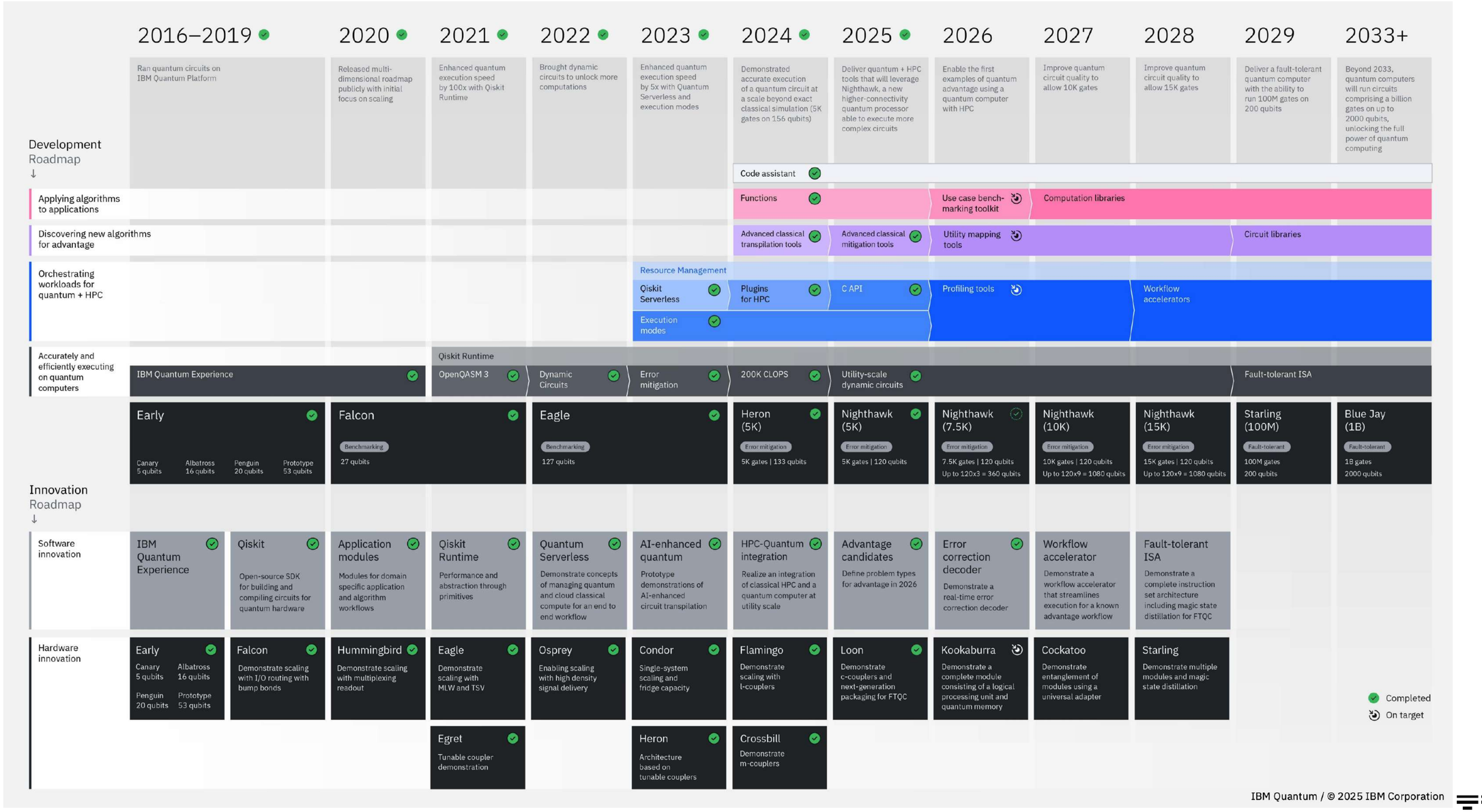
IBM Quantum System TWO







The IBM Quantum roadmap



IBM Quantum / © 2025 IBM Corporation

Quantum compute access

	Open Plan Sign up ↗	Pay-As-You-Go Plan Sign up ↗	Flex Plan Contact us ↗	Premium Plan Contact us ↗	On-Prem Plan Contact us ↗
Starting price	Free	$96 USD / minute	$72 USD / minute*	$48 USD / minute*	Contact for quote*
Minimum purchase	-	1 second	400 minutes	5200 minutes	-
IBM Quantum Platform	✓	✓	✓	✓	✓
Quantum computer access	✓	✓	✓	✓	✓
Technical support		✓	✓	✓	✓
Advanced tools & early access features*		✓	✓	✓	✓
IBM Quantum Network membership*			✓	✓	✓
IBM Quantum Accelerator offering*			✓	✓	✓
Full computer capacity as a service					✓
On-prem quantum system*					✓

Required actions for your organization

The path forward is concrete — six board-level decisions that simultaneously address the AI threat, the quantum threat, and all applicable regulatory obligations

1

Establish your CBOM — Now

Automated discovery of every algorithm, key, certificate, library, and protocol. Targeted by EU PQC Roadmap before end of 2026 and ZINFV-1. Typically takes 3–6 months to complete.

Prerequisite

2

Classify exposure by risk tier

Use the CBOM to identify systems using RSA/ECC (quantum-vulnerable public-key) and legacy symmetric ciphers protecting long-lived data.

3

Deploy AES-256 for all Long-Lived data

The fastest security improvement available. Replace AES-128 in data-at-rest and data-in-transit pipelines for any data with a confidentiality requirement exceeding 5 years.

Fastest win

4

Adopt a written PQC migration plan

Required by EU PQC Roadmap (end of 2026) and ZINFV-1 security documentation obligations. Migration targets must be NIST-finalized standards only — no unvalidated candidates.

Regulatory obligation

5

Launch a hybrid PQC pilot on critical systems

Implement ML-KEM / ML-DSA alongside existing RSA/ECC on one or two high-risk systems. Validates readiness and satisfies EU PQC Roadmap pilot requirement for 2026.

Satisfies 2026 pilot req.

6

Centralize key management & cryptographic intelligence

Policy-driven automated issuance through a dedicated platform. Designate a function to track NIST updates, ENISA/NCSC advisories, and CVEs. AI-driven cryptanalysis will continue — respond in hours, not years.

Why PQC migration takes 5–8 years

PQC migration is not a software update — it is a multi-year programme of discovery, dependency mapping, testing, and phased replacement that requires board-level commitment and funding to start today

Total migration duration: 5 – 8 years minimum[1]

1

Cryptographic Discovery & CBOM

Months 1-6

Every cryptographic dependency across infrastructure, applications, APIs, and source code must be found and catalogued. Most enterprises have tens of thousands — many unknown. Without a complete inventory, migration cannot begin.

2

Risk Classification & Prioritization

Months 4-9

Long-lived data systems (medical, financial, defense) migrate first. Dependency mapping reveals which systems are coupled — a single library update can cascade to hundreds of applications.

3

Algorithm Selection & Hybrid Testing

Months 6-18

ML-KEM and ML-DSA tested for performance impact. Hybrid deployments (classical + PQC in parallel) validated for compatibility with partners, vendors, cloud providers, and hardware (HSMs, TPMs).

4

Supply Chain & Vendor Alignment

Months 12-30

Suppliers, cloud providers, payment processors, and software vendors must also support PQC. OpenSSL — used by approximately two-thirds of web servers — must be updated and redeployed across every dependent server.

5

Phased Production Rollout

Years 2-5

System-by-system migration across the full estate — replacing certificates, keys, protocols, and libraries. Each system requires testing, rollback planning, and sign-off. Large enterprises manage hundreds of simultaneous workstreams.

6

Validation, Audit & Compliance

Ongoing from year 3

CBOM currency maintained, migration progress documented, incident response for newly discovered vulnerabilities. EU PQC Roadmap targets documented progress by 2026; full migration for critical sectors by 2030.

IBM Guardium Cryptography Manager & IBM Vault

1. OpenSSL migration prediction

Cryptographic Agility — Strategic requirement

With certificates shrinking to 47 days and AI accelerating cryptographic risk, cryptographic agility is now a board-level survival requirement

What is Crypto Agility?

The organisational and technical ability to **replace cryptographic algorithms and rotate certificates** across all systems rapidly — without disrupting services, without touching individual application code — whether the trigger is a new threat or a new industry deadline.

What is CBOM?

A living, **structured inventory** of every **cryptographic algorithm, key, certificate, library, and protocol** in use across your infrastructure and code. The cryptographic equivalent of a Software Bill of Materials (SBOM).

TLS certificate lifetime reduction (Binding on publicly trusted TLS server certificates — Web PKI)

Today	Mar 15, 2026	Mar 15, 2027	Mar 15, 2029
398 days	**200 days**	**100 days**	**47 days**
Current maximum ~13 months	First mandatory reduction	Renewals now quarterly	8× renewals/year DCV2 reuse: 10 days

Without Crypto Agility
Current state of most organizations

Replacing cryptography requires changes across **hundreds of applications**, demanding **years of engineering effort** and coordination

A new AI-discovered vulnerability leaves the organisation **exposed for an extended and legally dangerous period** while teams work through manual remediation

Certificate renewals at **47-day cycles overwhelm manual processes** — at 10,000 certificates, 80,000 renewals per year. Outages become routine, not exceptional

No single inventory means **no automated monitoring** — teams discover expiries only when services fail

With Crypto Agility
The target state

Algorithm selection is **centralised in policy** — a single policy change propagates automatically to all new key and certificate issuances across the entire organisation

When the next breakthrough occurs — AI-driven cryptanalysis guarantees there will be one — the organisation **responds in hours, not years**

Automated certificate lifecycle (issuance, rotation, revocation) handles **47-day cycles without human intervention** — eliminating outage risk at any scale

Cryptographic inventory (CBOM) enables **real-time visibility** across all certificates, algorithms, and expiry dates

IBM: "A new era for certificate management" — ibm.com/think/insights/certificate-management, 2. Domain Control Validation

IBM currently leads the world in quantum computing and quantum-safe research

3

NIST approved post-quantum cryptography algorithms were co-developed by IBMers[1]

ML-KEM

ML-DSA

SLH-DSA

4

IBM-supported schemes for quantum-safe digital signatures are under NIST evaluation for future adoption[2]

SQIsign

UOV

MAYO

FAEST

1. IBM-Developed Algorithms Announced as NIST's First Published Post-Quantum Cryptography Standards, IBM Newsroom, 2024
2. IBM's quantum-safe signature schemes advance in NIST's PQC process, IBM Research, 2025

IBM © 2025 IBM Corporation

Algorithms landscape: Cryptosovereignty requires Cryptoagility

Country / Region (regulator)	PQC Alignment	Primary Algorithms	Strategic Focus & Nuance
United States (NIST / CISA / NSA)	Pure NIST Baseline	KEM: ML-KEM Signature: ML-DSA, SLH-DSA Stateful Hash: XMSS, LMS	Fastest mover: mandatory federal migration, pure PQC preferred
United Kingdom (NCSC)	NIST-Aligned	KEM: ML-KEM-768 Signature: ML-DSA-65, SLH-DSA	Follows US baseline; hybrid allowed only as interim safety net
EU (BSI Germany, ANSSI France, NCSC-NL)	NIST + Conservative Hybrid	NIST Baseline plus: KEM: FrodoKEM, Classic McEliece	Lattice-skeptic: permanent hybrid with non-lattice backups
South Korea (MSIT / KPQC)	Sovereign Suite	KEM: SMAUG-T, NTRU+ Signature: AIMer, HAETAE	Fully independent national standards track (KPQC)
China (ICCS)	Sovereign Suite	China-specific commercial and state cryptographic standards	Closed, native portfolio; no Western alignment with NIST/ETSI standards bodies
India (DST / National Quantum Mission)	Dual-Track / Sovereign Preference	NIST Baseline for global use; Indigenous variants for CII	NIST for enterprise, indigenous variants mandated for critical infra
Malaysia	Sovereign Development	Domestically developed algorithms in progress	Building a national PQC program and certification pipeline

IBM Quantum-safe technologies

IBM Guardium **Quantum** Safe Explorer

Discover cryptography and vulnerabilities in custom applications.

Obtain insights on code-level risks to guide remediation efforts.

Remediate at-risk cryptography by pinpointing precise location in code.

IBM **Guardium** Cryptography Manager

Gain visibility into cryptography use across the enterprise network and applications.

Enable faster compliance by applying internal and regulatory policies.

Prioritize vulnerabilities, based on policies, to accelerate remediation actions and track progress.

IBM Guardium **Quantum** Safe Remediator

Protect application and network endpoints today without any application changes.

Evaluate the performance of quantum-safe cryptographic algorithms

Mitigate “Harvest Now, Decrypt Later” scenarios

© 2025 IBM Corporation

Accelerate crypto-agility with IBM Quantum Safe Explorer

Findings

- 5,815 code repos scanned
- 440,000 files scanned
- 47,000,000 lines of code scanned
- 2,499 Crypto Assets identified
- 3,900+ Vulnerabilities identified
- Numerous legacy components using deprecated key sizes
- Hardcoded cryptographic parameters used in Java and Python
- Unsafe defaults and missing crypto-agility patterns

Read IBM Client Zero Story here

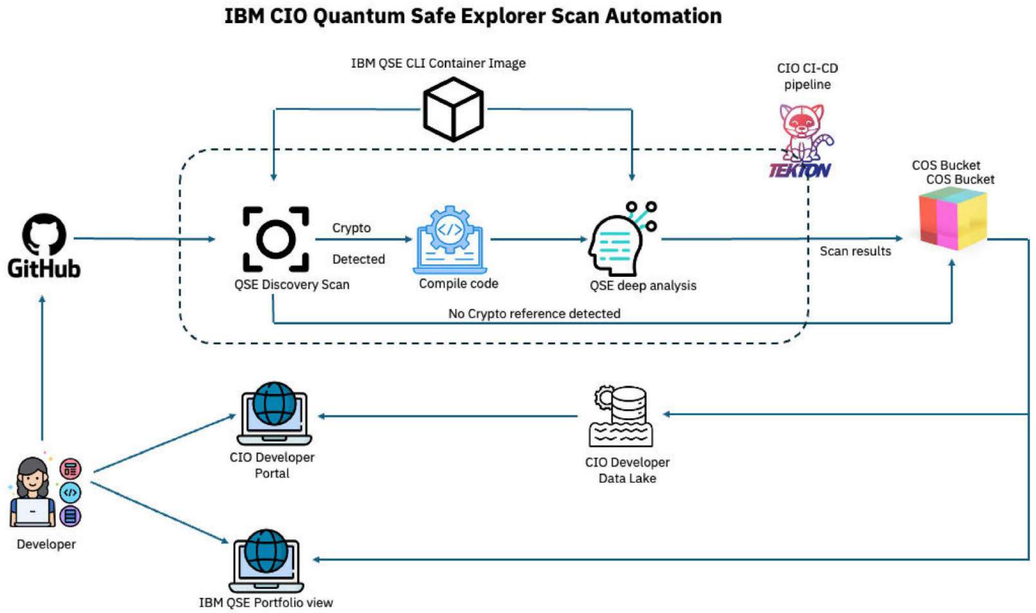
IBM Quantum Safe / © 2025 IBM Corporation

Objectives

1. Discover cryptographic artifacts
2. Generate an actionable Cryptography Bill of Materials (CBOM) for full visibility
3. Identify and remediate crypto-agility anti-patterns before they reach production
4. Proactively manage quantum-era cryptographic risk with measurable outcomes.

Challenges

- Cryptography is embedded deep in code across multiple libraries (each with 100s of APIs).
- Manual discovery impractical across thousands of homegrown applications and scattered codebases
- Lack centralized up-to-date visibility of cryptography across applications
- Non-compliance with Regulations (NIST)



Outcomes

- Automated scans, integrated with application's build pipeline, became part of regular DevSecOps routines (near-zero manual effort)
- Produced a Cryptography Bill of Materials (CBOM) for each repository scanned
- Minimal-friction pipeline integration ensures each build generates fresh CBOMs, consolidated into IBM's CIO Office's Developer Data Lake
- Translate technical findings to actionable business risks and help meet NIST 2035 inventory requirements



Achieve Crypto-Agility

Guardium Cryptography Manager

The solution to embrace crypto-agility: protect data today, and prepare for tomorrow’s threats

Discovery and Inventory

Build a live inventory of cryptographic objects and protocols across hybrid environments, mapped to systems and owners with expiry and strength context.

Assess and Comply

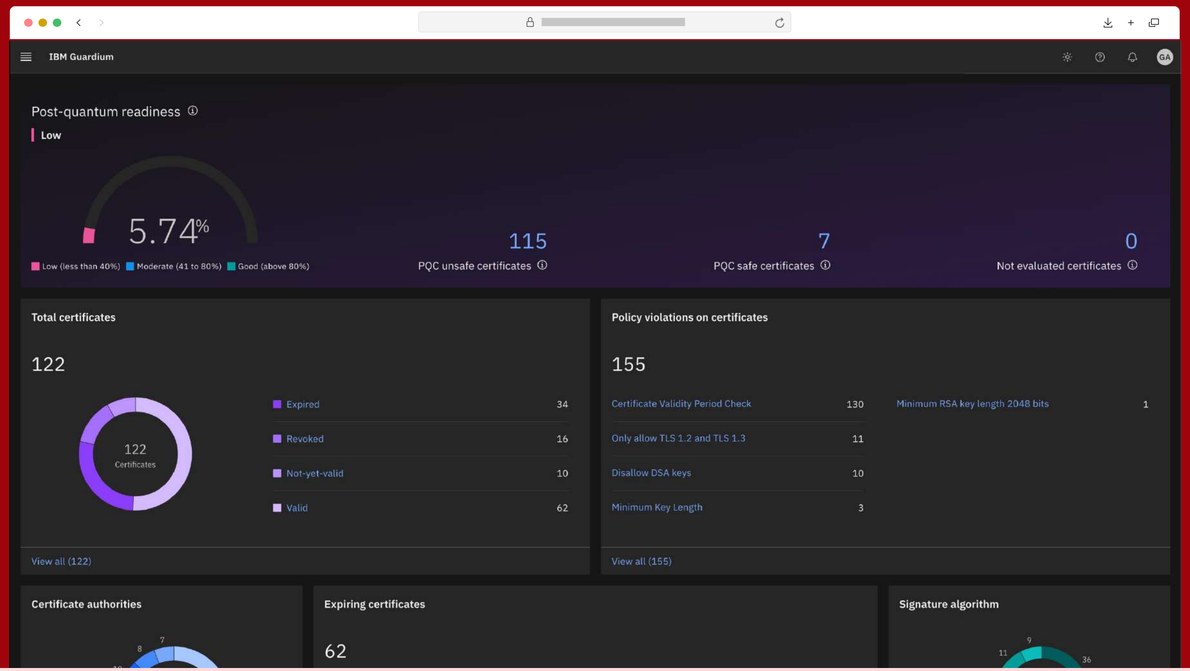
Assess post-quantum readiness across your environment, flag outdated or vulnerable algorithms, and generate audit-ready reports to expedite compliance.

Manage Lifecycle

Centralize cryptographic object lifecycle operations, detect weak or expired certificates, automate certificate renewals and manage revocation to streamline management.

Protect and Adapt

Orchestrate agentless transparent database encryption to protect sensitive data and support migration to NIST-approved quantum safe algorithms.



Only 30%

of organizations have their apps, data, and services inventoried to understand how cryptography is used across the organization[1]

Vodafone, UK/Global

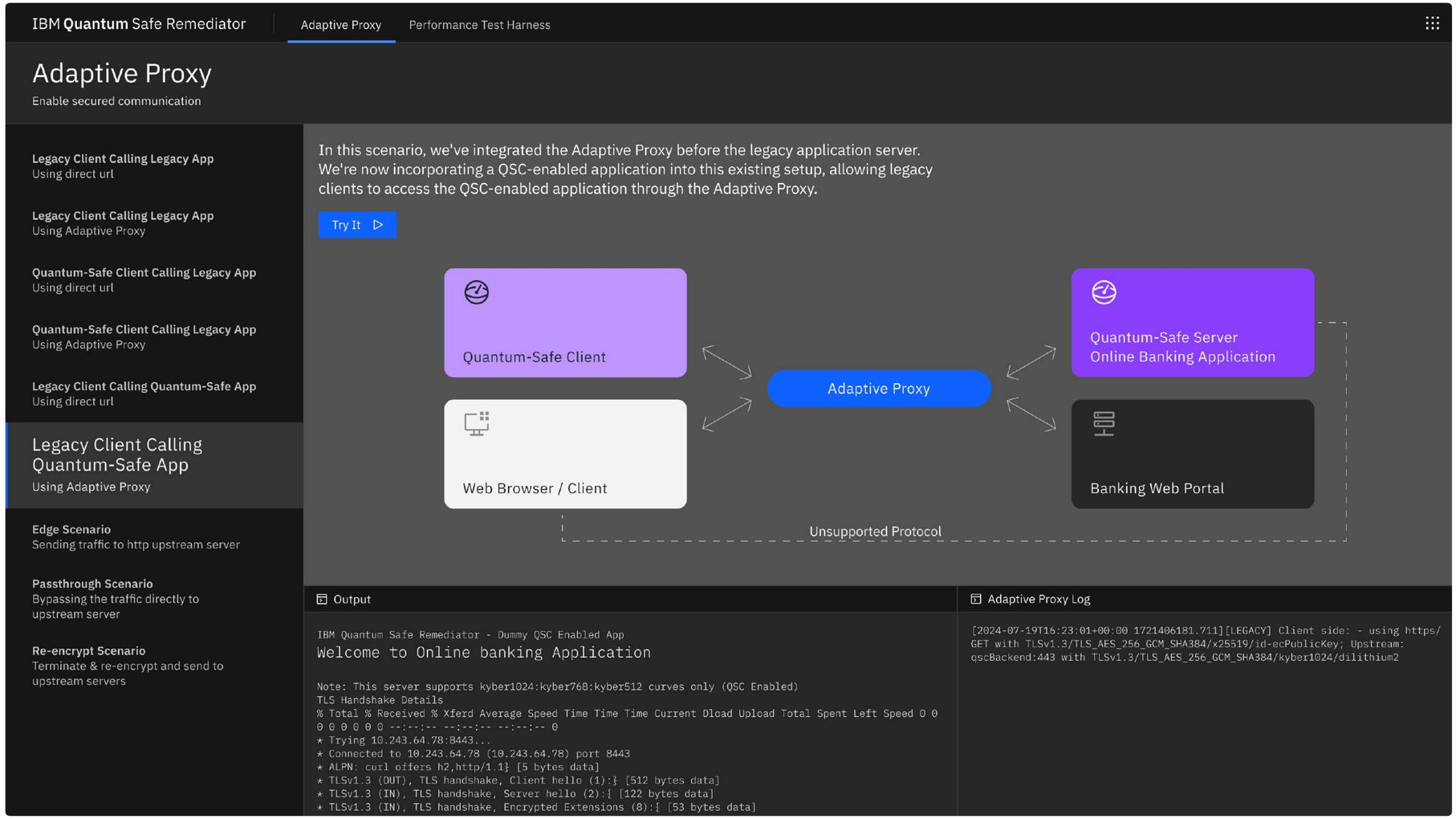
Vodafone aimed to protect their mobile customers from future quantum threats. They partnered with IBM to pilot post-quantum cryptography in Vodafone Secure Net, their digital security service used by millions of customers to protect against phishing, malware and identity theft. This POC demonstrated how new cryptography standards could be integrated into existing customer-facing services, and protect against existing risks of “harvest now, decrypt later”.[2]

1. Quantum-Safe Readiness, IBM Institute for Business Value, 2025

IBM Quantum Safe Remediator

Adaptive Proxy

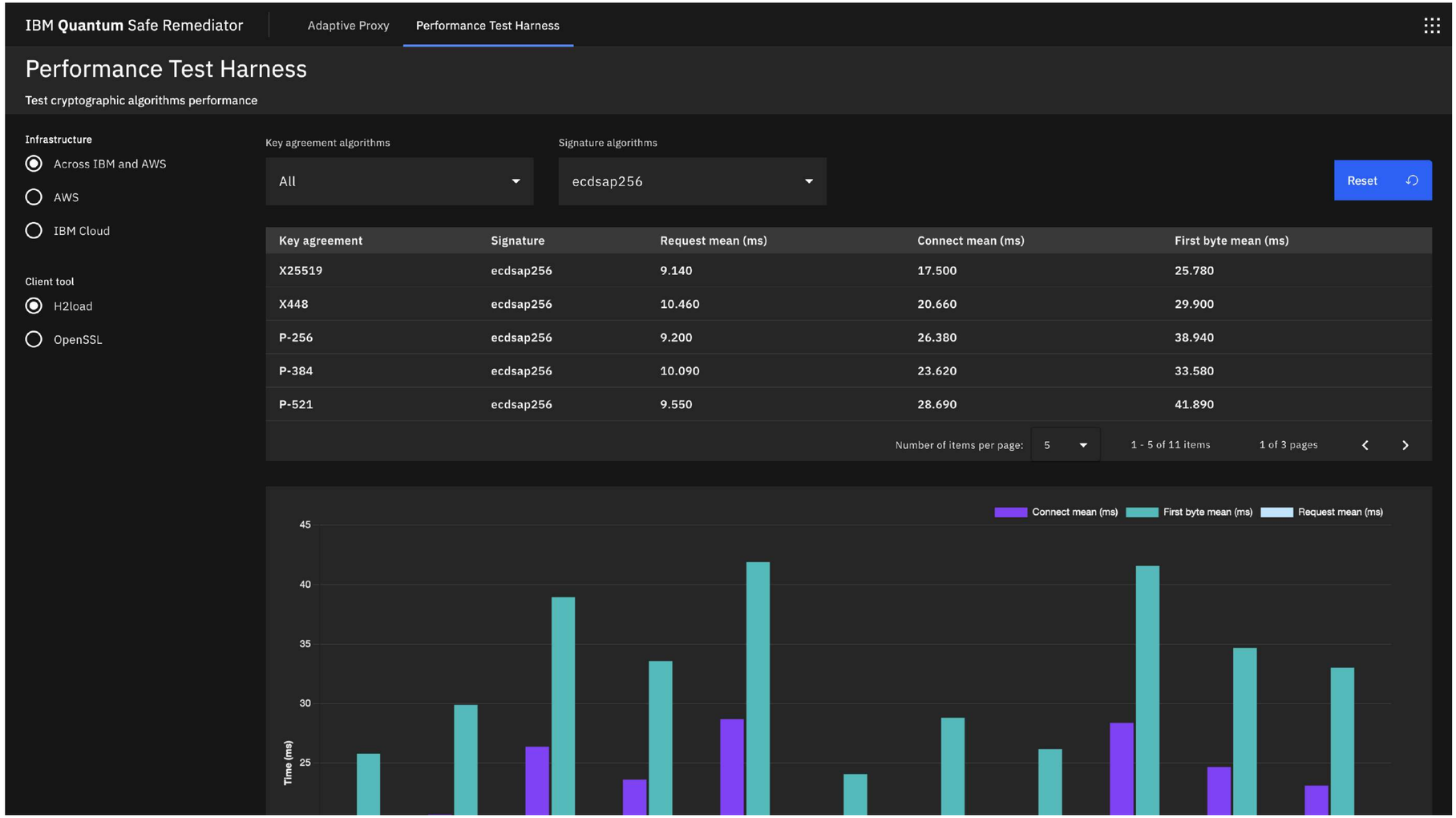
- Designed to seamlessly handle both legacy and post-quantum ready clients and servers by enabling backward compatibility and smooth interoperability to ensure communication without changing code in applications.
- Offers centralized control over TLS protocols and policies, hence streamlining the management of complex environments.



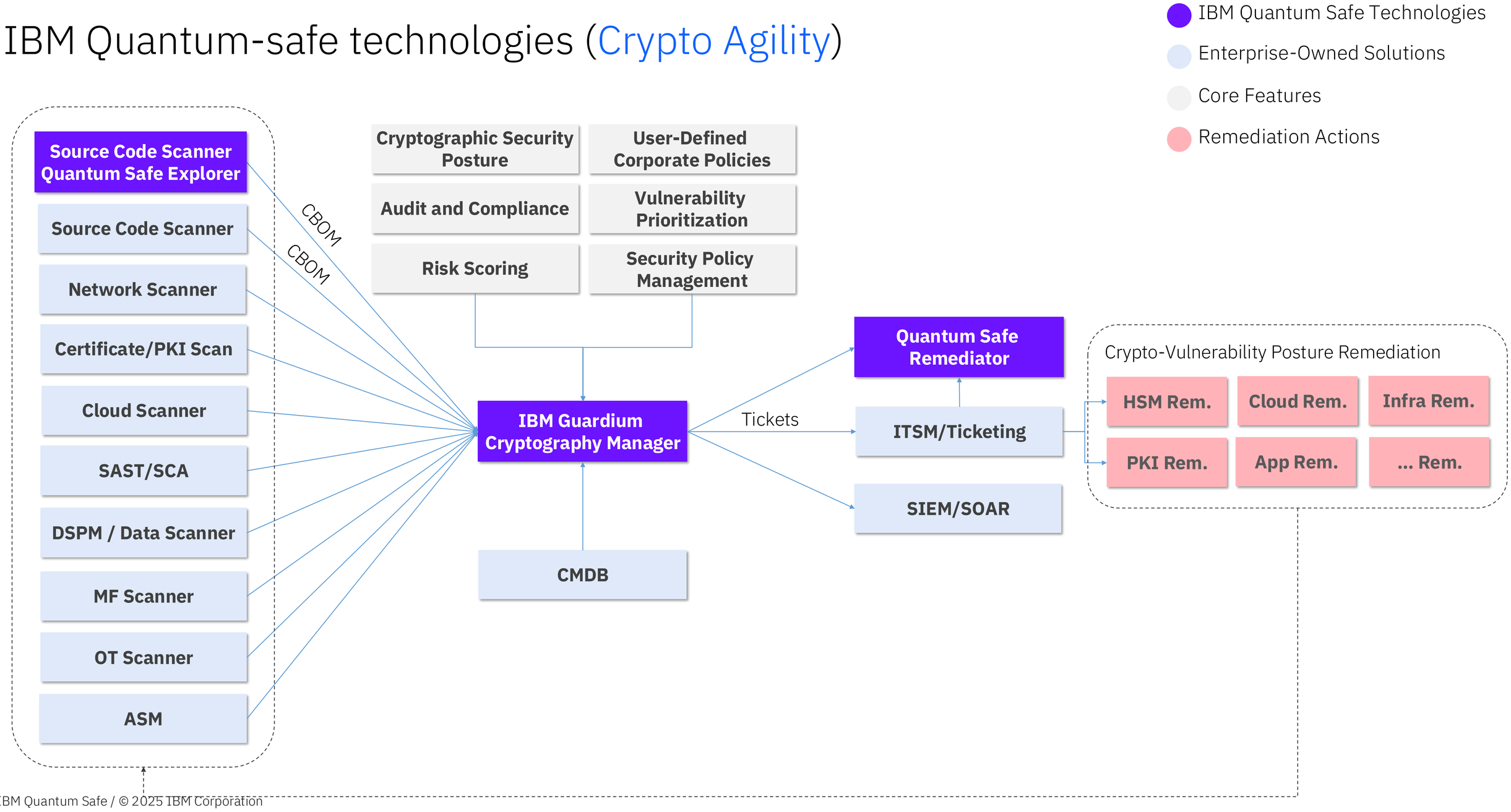
IBM Quantum Safe Remediator

Performance test harness

- Measure HTTP traffic and understand how the algorithms are impacting behaviors.
- View benchmark data, understand impact on infrastructure performance, and make informed remediation recommendations.
- Understand the potential impact of recommended upgrades to the applications prior to making changes.



IBM Quantum-safe technologies (Crypto Agility)



IBM Quantum Safe / © 2025 IBM Corporation

Quantum-safe today. Secure tomorrow.

Post-quantum cryptography built into IBM infrastructure hardware

2026 hardware portfolio

FIPS 203 ML-KEM = CRYSTALS-Kyber **FIPS 204 ML-DSA** = CRYSTALS-Dilithium **FIPS 205 SLH-DSA** = SPHINCS+



IBM z17

- Dual signature scheme protects firmware
- Crypto Express 8S HSM with PQC APIs
- zCDI builds the crypto inventory
- Pervasive Encryption, hybrid key exchange

MECHANISMS

- ML-KEM FIPS 203
- ML-DSA FIPS 204
- Kyber + ECDH hybrid KEX
- Dilithium + ECC dual signing
- LMS / XMSS



IBM LinuxONE

- Quantum-safe firmware and secure boot
- Crypto Express 8S quantum-safe APIs
- libica / openCryptoki usage counters
- zCDI not available — plan tooling

MECHANISMS

- ML-KEM FIPS 203
- ML-DSA FIPS 204
- SLH-DSA FIPS 205
- Kyber + ECDH hybrid KEX
- Protected-key AES-256



IBM Power11

- Hybrid Secure Boot blocks tampering
- LPM traffic encrypted quantum-safe
- Crypto Express 4770, FIPS 140-2 L4
- PowerSC 2.2 one-click crypto inventory

MECHANISMS

- ML-KEM FIPS 203
- ML-DSA FIPS 204
- SLH-DSA FIPS 205
- ECC + ML-DSA hybrid signing
- OpenSSH ML-KEM



IBM DataPower

- Gateway X4 quantum-safe out of the box
- PQC KEM in TLS profiles from 10.6.4
- ML-DSA private key generation, 10.6.6
- FIPS 140-3 and SafeNet Luna HSM 10.9

MECHANISMS

- ML-KEM-512 / 768 / 1024
- X25519MLKEM768
- SecP256r1MLKEM768
- SecP384r1MLKEM1024
- ML-DSA FIPS 204



IBM FlashSystem

- FCM5 hybrid PQC key transport
- ML-DSA verifies firmware authenticity
- XTS-AES-256 engine, no performance cost
- Integration with IBM Key management infrastructure

MECHANISMS

- ML-KEM FIPS 203
- ML-DSA FIPS 204
- Hybrid classical + PQC
- XTS-AES-256
- SHA-2 integrity



IBM SAN Gen 8

- Quantum-safe SAN in Fabric OS v10.0.0
- PQC in SSH, TLS and IKEv2
- AES-256 in-flight, 384 Gbps per ASIC
- Root of Trust and SPDM attestation

MECHANISMS

- ML-KEM-1024
- ML-DSA-87
- LMS SHA256/192
- XMSS
- AES-256 in-flight

2016–2022
IBM co-develops Kyber and Dilithium

Aug 2024
FIPS 203 / 204 / 205 published

Sept 2025
Quantum-safe SAN in Fabric OS 10

2026
Portfolio ships quantum-safe

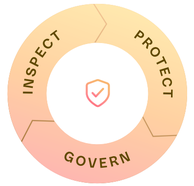
2030–2035
CNSA 2.0 mandatory

Dynamically Manage Your Secrets





Building continuous trust through discovery, automation, and agility



	DAY 0	DAY 1	DAY 2	DAY N
	DISCOVER	AUTOMATE	GOVERN	MODERNIZE
PLATFORM	Build a trusted inventory of certificates, machine identities, and CAs	Automate certificate issuance, renewal, rotation, and workflows	Standardize PKI operations and lifecycle management at scale	Support evolving trust requirements, shorter certificate lifetimes, and cryptographic agility
DEV	Inventory application dependencies on certificates, PKI, and cryptographic services	Integrate certificate lifecycle and signing workflows into CI/CD and application delivery processes	Adopt standardized APIs, policies, and approved services	Modernize applications for crypto agility and future PQC migration initiatives
SECURITY	Identify cryptographic assets, algorithms, PQC exposure, and policy gaps	Automate policy enforcement, risk remediation, and controls	Monitor certificate posture, compliance, cryptographic and risk	Enable PQC readiness, governance, and continuous adaptation

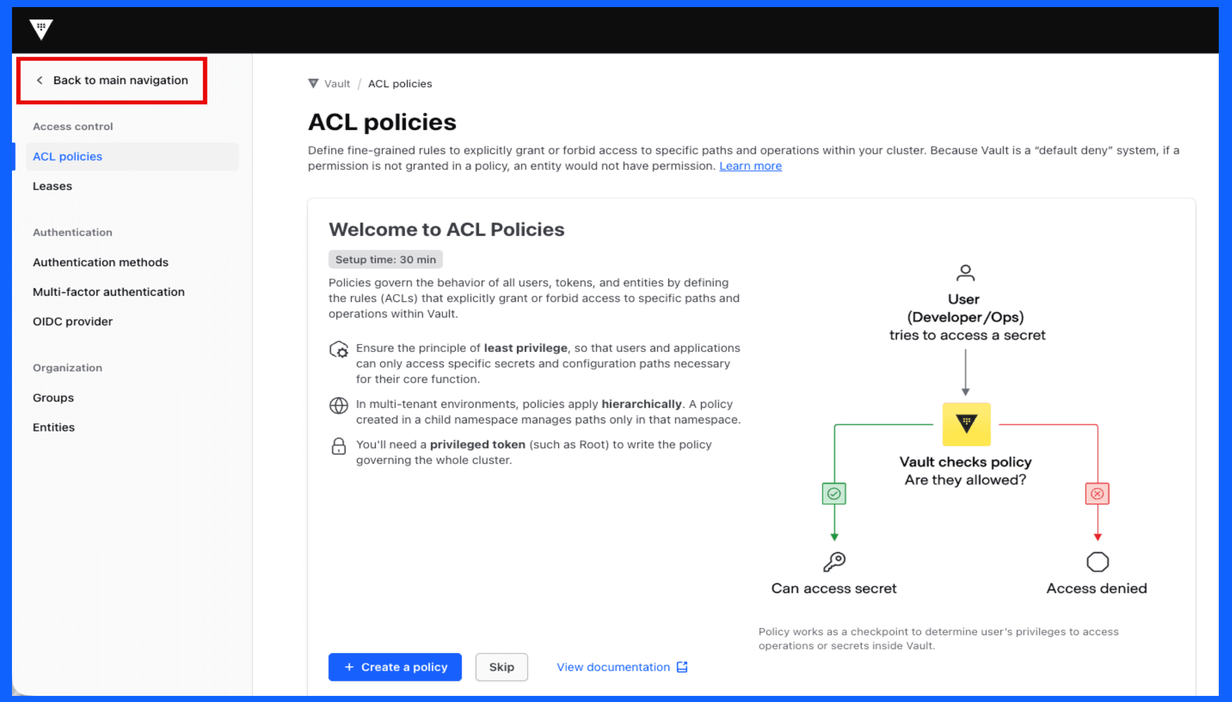
Disclaimer / © 2026 IBM Corporation

Secrets management with HashiCorp Vault

Centrally store, access, and distribute secrets

Vault centrally manages and enforces access to secrets and systems based on trusted sources of application and user identity.

- Identity-based security uses trusted identities to automate access to secrets, data, and applications
- Security system of record to centrally store and protect secrets across clouds and applications
- Lifecycle management of your credentials to ensure proper oversight, rotation, and expiry



~1 in 10

breaches are caused by stolen or compromised credentials

Detection is inherently hard:

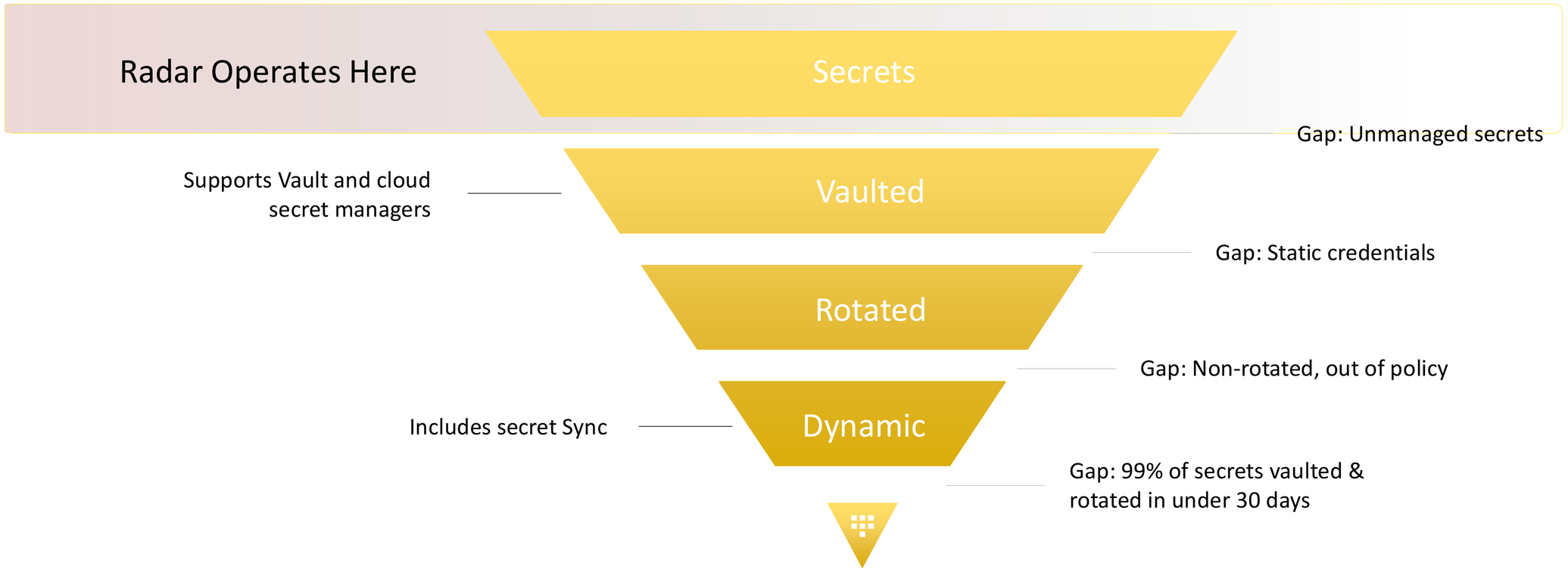
IBM's 2026 report frames it as "malicious activity can begin with successful authentication" — once an attacker has a valid credential, they look like a legitimate user to most monitoring tools, which is why these breaches take ~243 days on average to catch and shut down.

Duration drives cost:

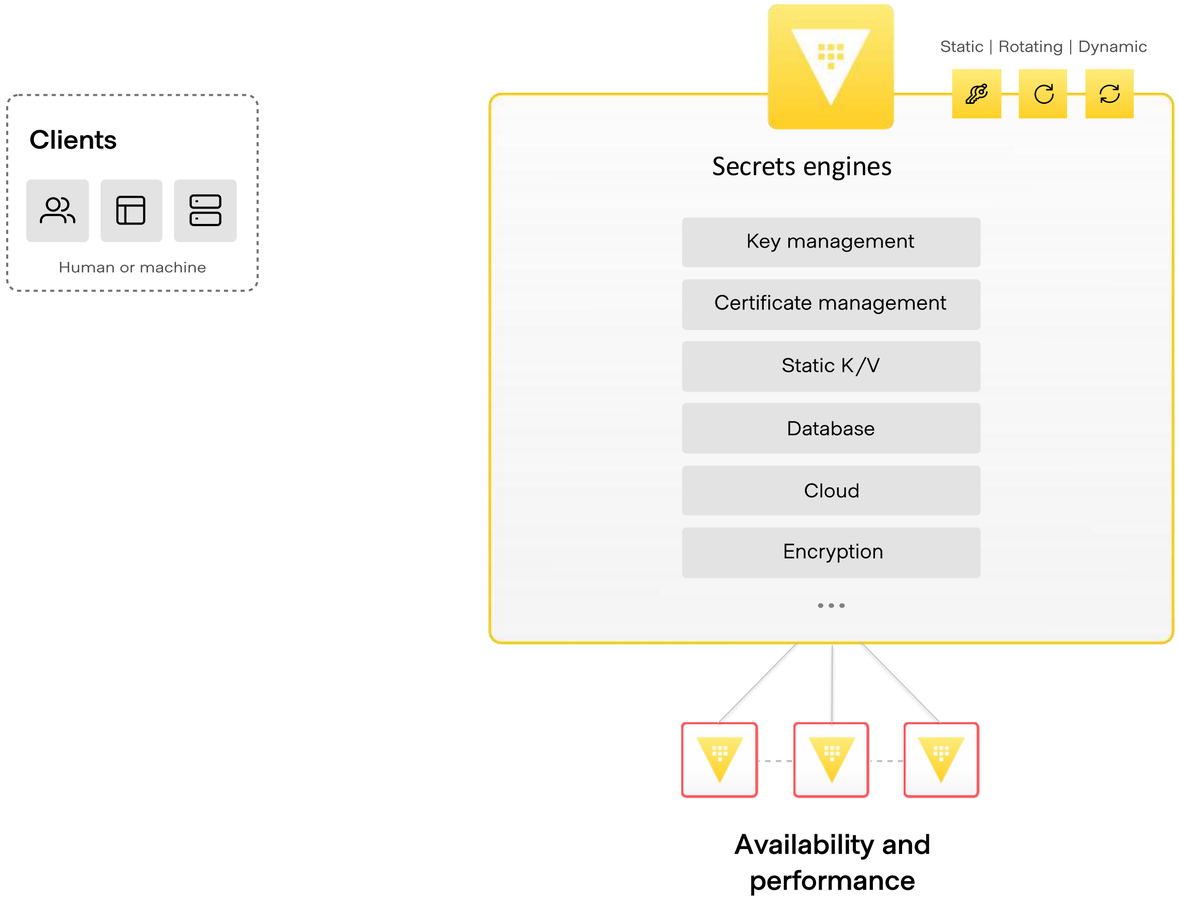
breaches that run longer than 200 days average $5.65M, versus $4.32M for ones caught faster — a >$1.3M gap. Credential-based intrusions are disproportionately represented in the "long-running" category because they don't trip normal alerts.

Secrets lifecycle management

Secrets Inventory Categories



Architecture

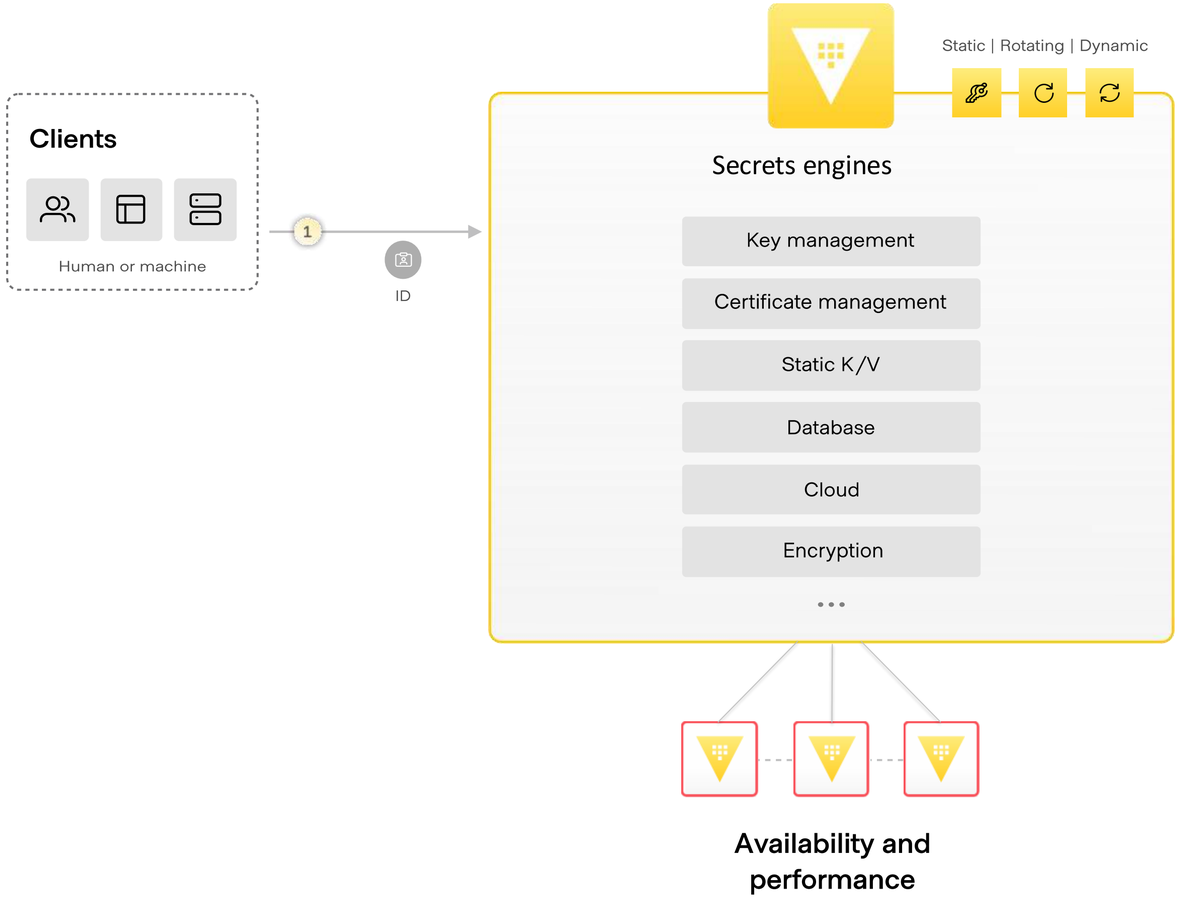


Architecture

How Vault works

1

A client provides credentials (ID) to Vault requesting access.

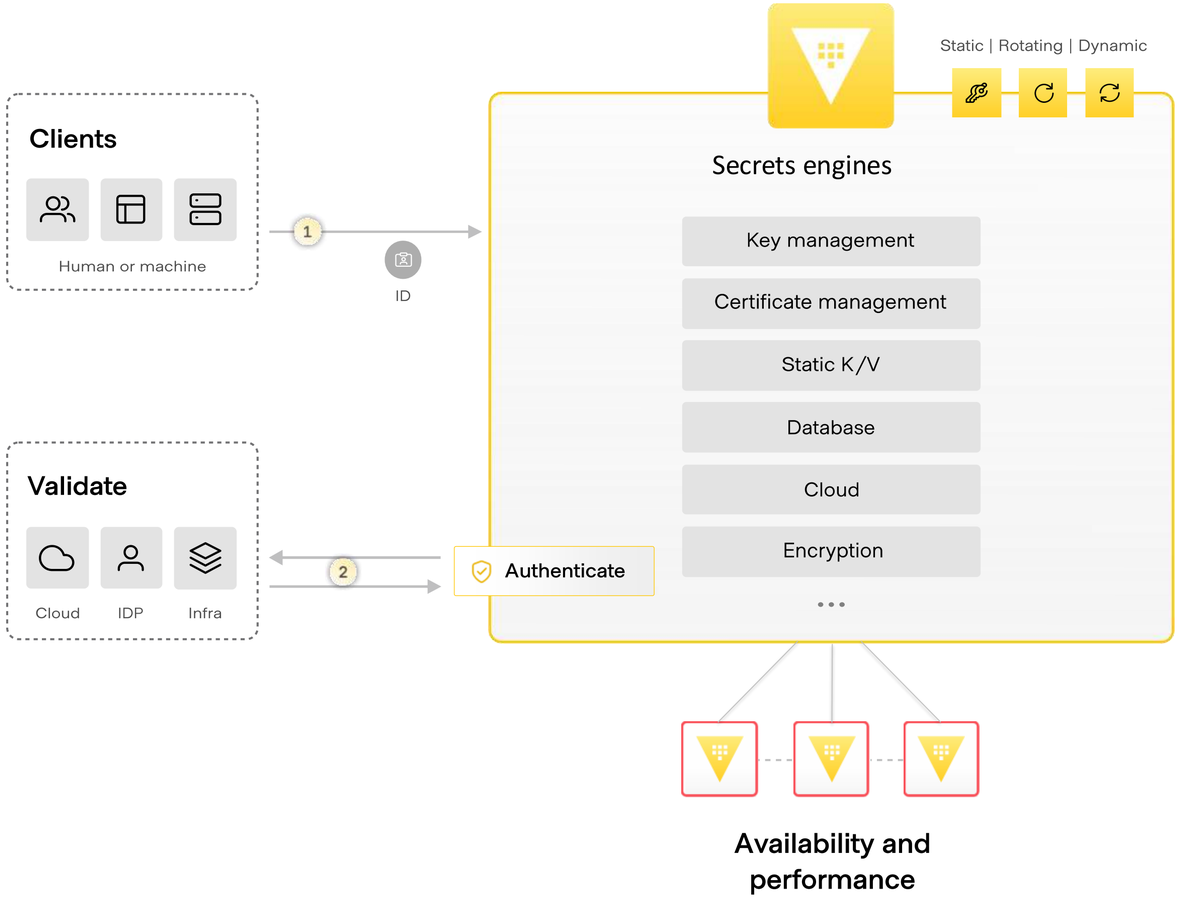


Architecture

How Vault works

2

Vault uses authentication plugins to validate the client against the appropriate trusted third-party resource, such as GitHub, LDAP, CSP, or others.

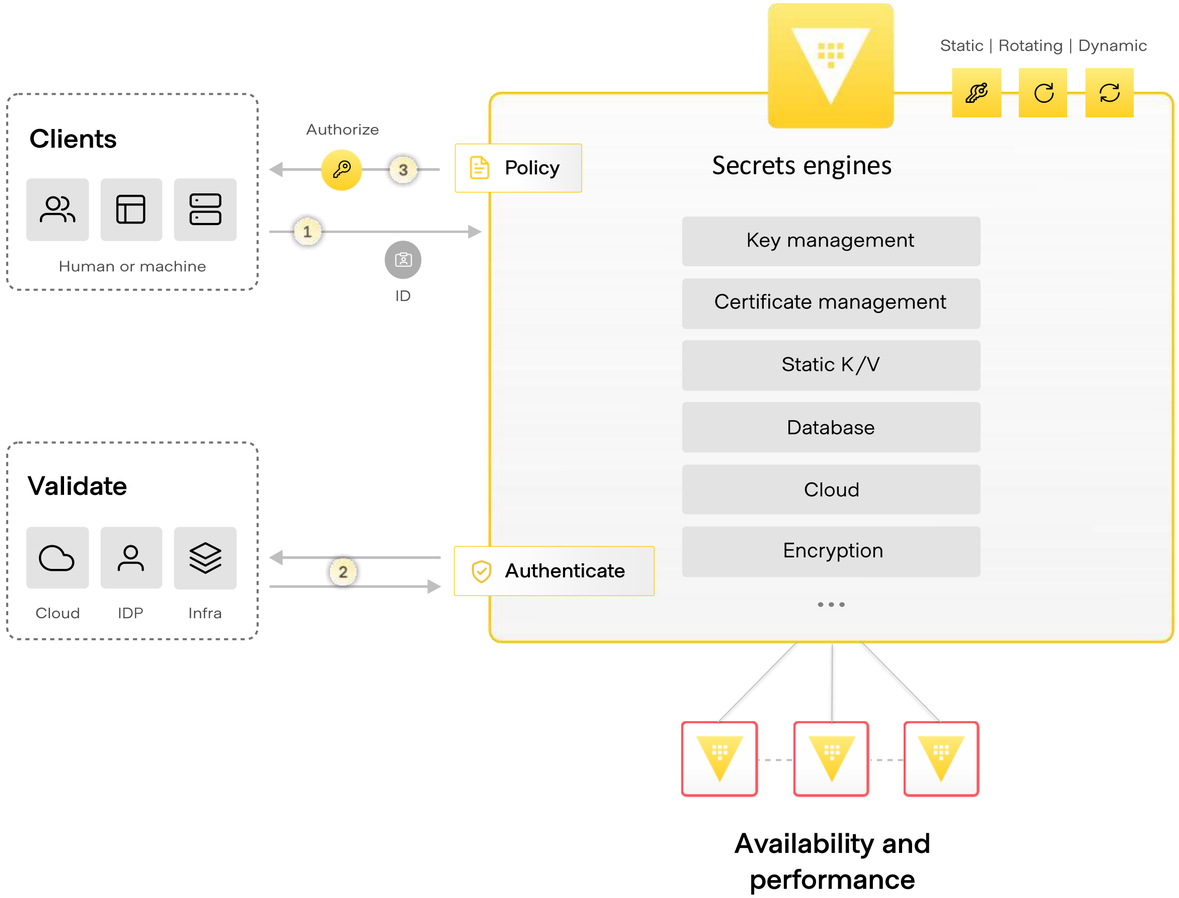


Architecture

How Vault works

3

Vault grants access to secrets and encryption capabilities by issuing
a token tied to policies associated
with the client's identity.

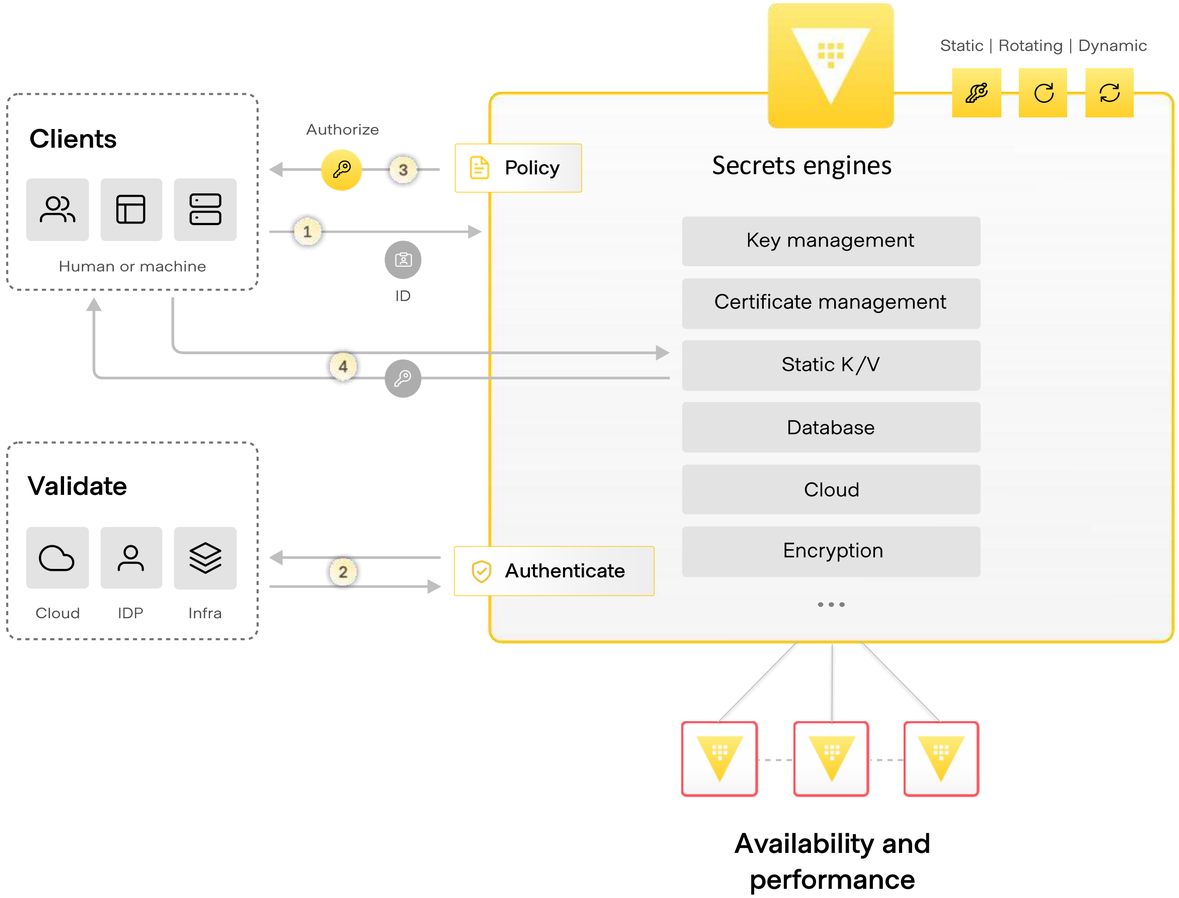


Architecture

How Vault works

4

Client uses policy-based access
to retrieve secrets, keys, and certificates,
and to perform other operations, like data
encryption.

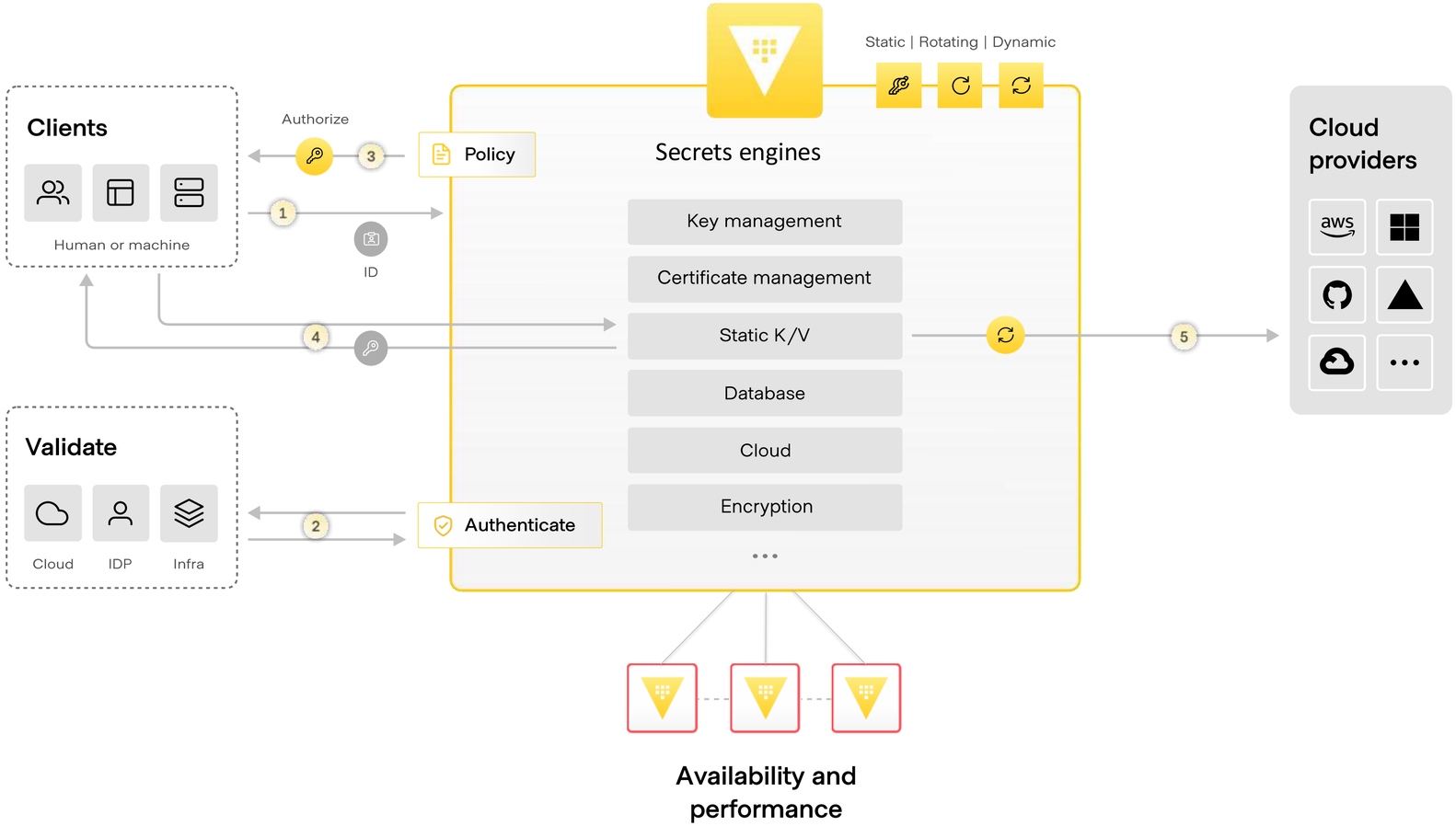


Architecture

How Vault works

5

Static secrets can be centrally managed and automatically synced to destination sources.



Integration diagram of Guardium, Quantum Safe and HashiCorp Vault

