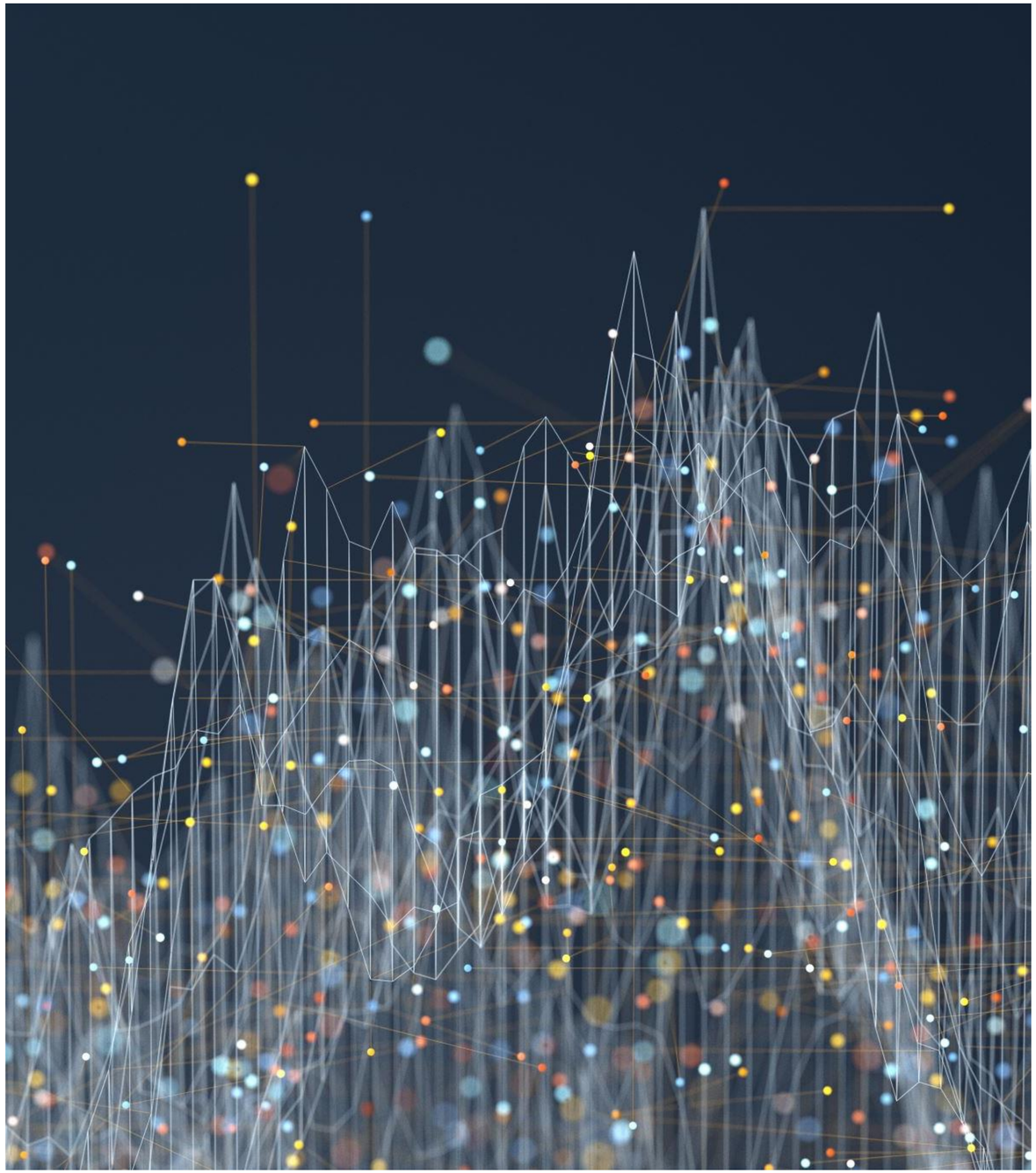
Guardium Data Security Center

Client Presentation



Domenick DeCarlo
WW Technology Sales Enablement
ddecarlo@us.ibm.com

IBM

Organizations are challenged with maturing their data security programs

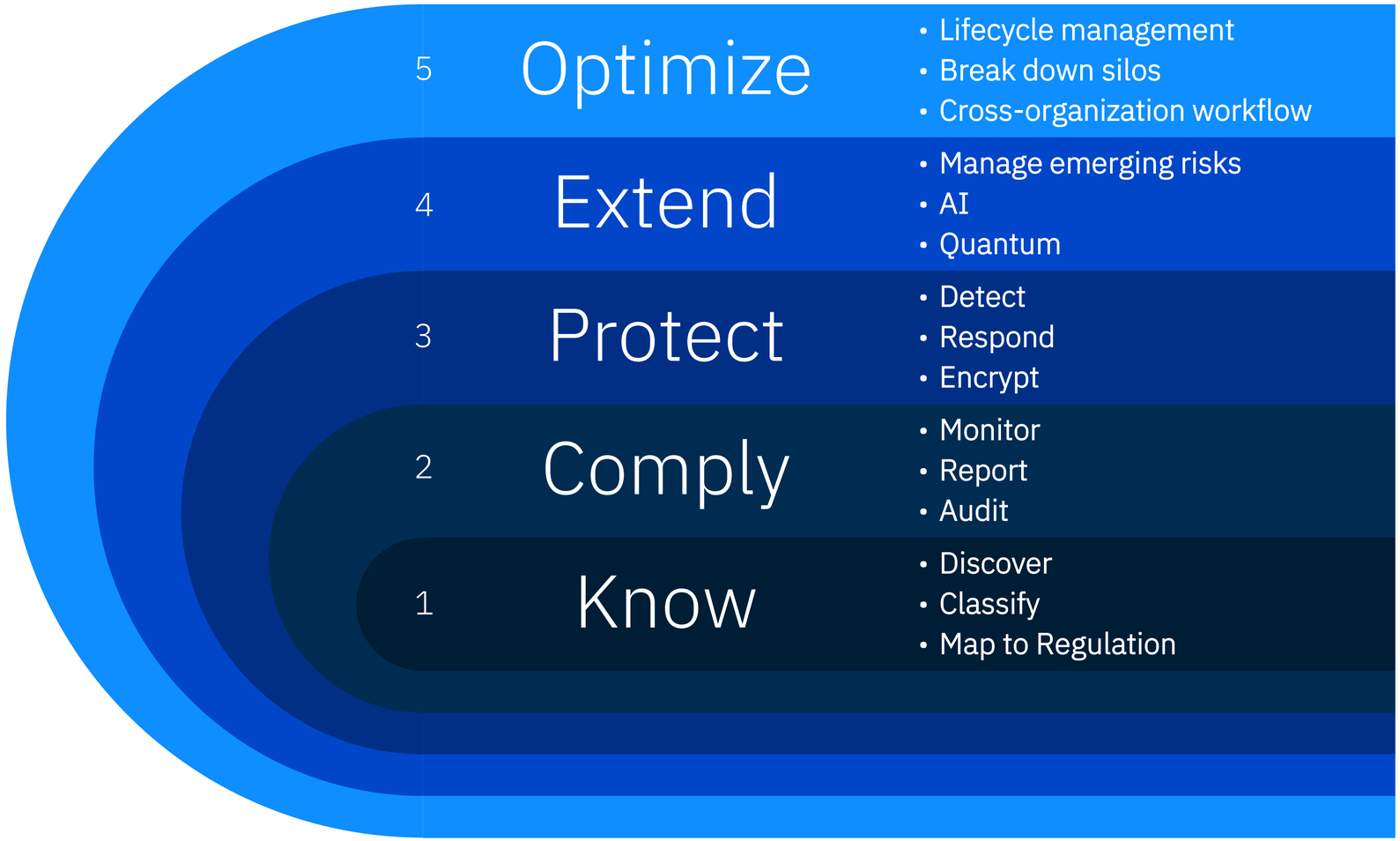
Data Security Maturity

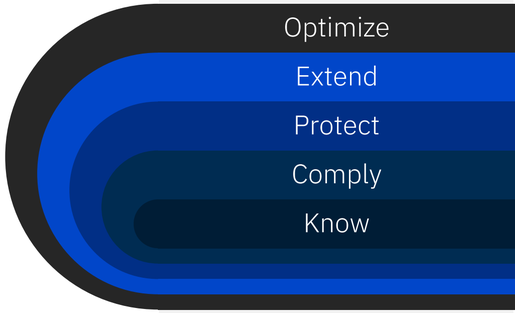
Maturing a data security program starts with the basics:

- Knowing where data resides, and
- Complying with regulations

The program matures as you:

- Proactively and reactively protect data,
- Extend to emerging use cases, and finally
- Optimize the program





The rise of AI, quantum computing, and cloud will extend data security

Artificial Intelligence – Born of Data

As organizations are rapidly adopting AI, various challenges are arising around:

- Understanding the contents, location, classification, and details of training, tuning, and RAG data
- Determining if data and models are susceptible to vulnerabilities
- Folding these models and data into existing monitoring and data detection & response programs

Quantum Computing

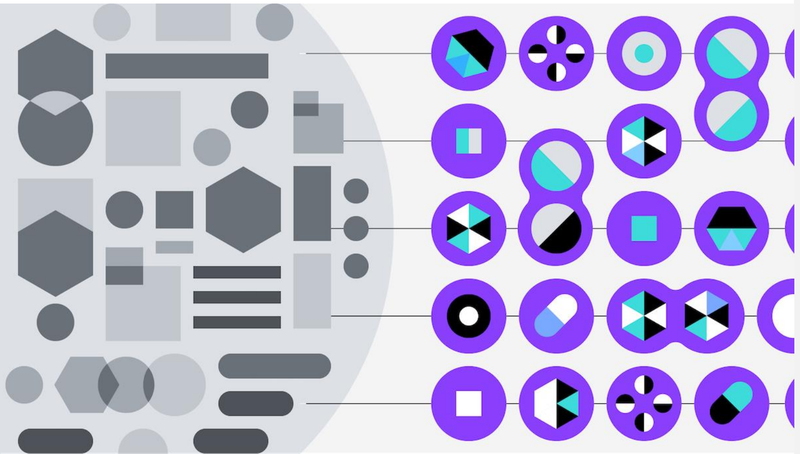
Quantum computing continues to accelerate, which means the clock continues to count-down for organizations to protect encrypted data that's susceptible to quantum attacks:

- Where is vulnerable crypto and data located?
- Which libraries and data should I be concerned with first?
- How do I formulate a remediation plan?

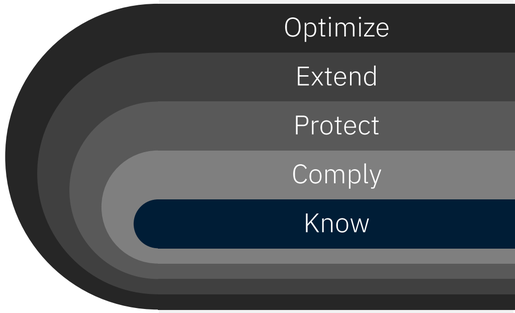
Cloud and SaaS

At this stage, organizations may have visibility to cloud and SaaS data if they've successfully built the discovery aspects of their data security program, but new challenges arise as they need to:

- Understand how data is moving between clouds
- Interrogate entitlements to cloud-resident data
- Determine if configuration and posture of cloud data stores creates risk

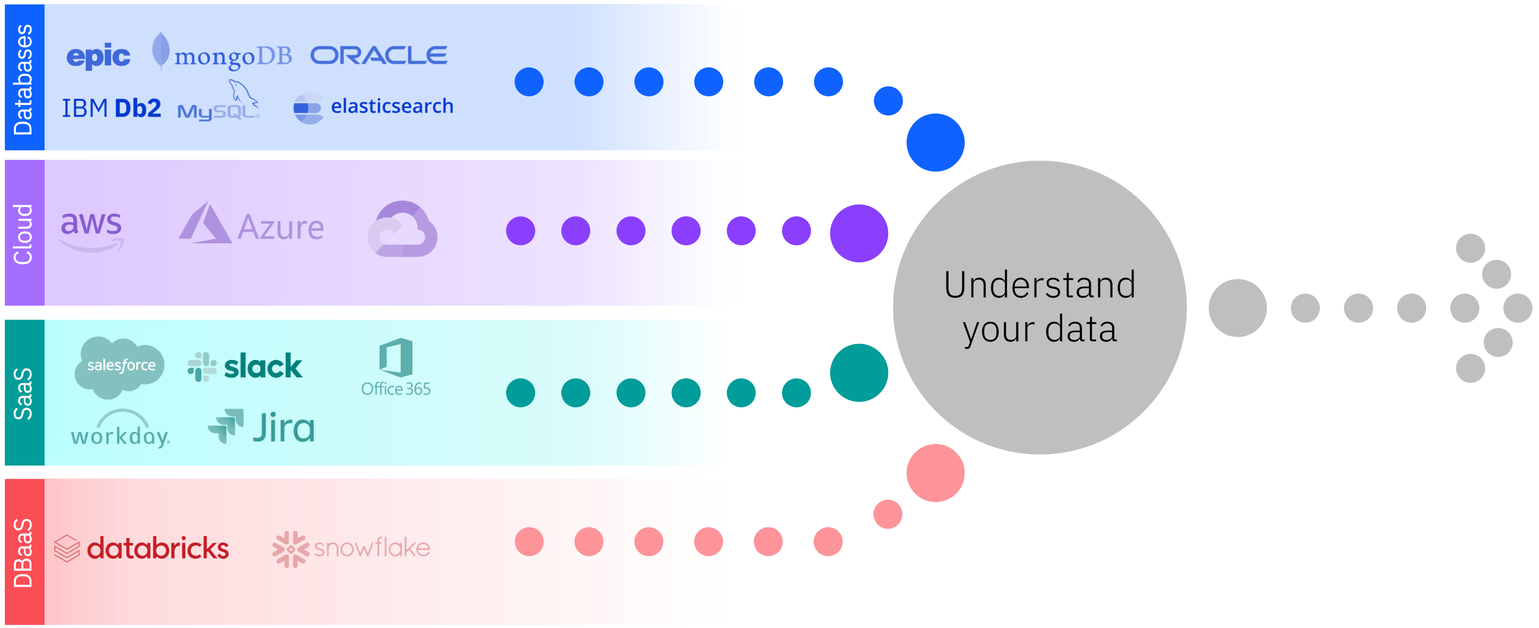


You can’t secure what you don’t know exists



Data security starts here

Data is sprawling across traditional data stores, such as relational databases, to non-traditional assets such as cloud, SaaS, and DBaaS

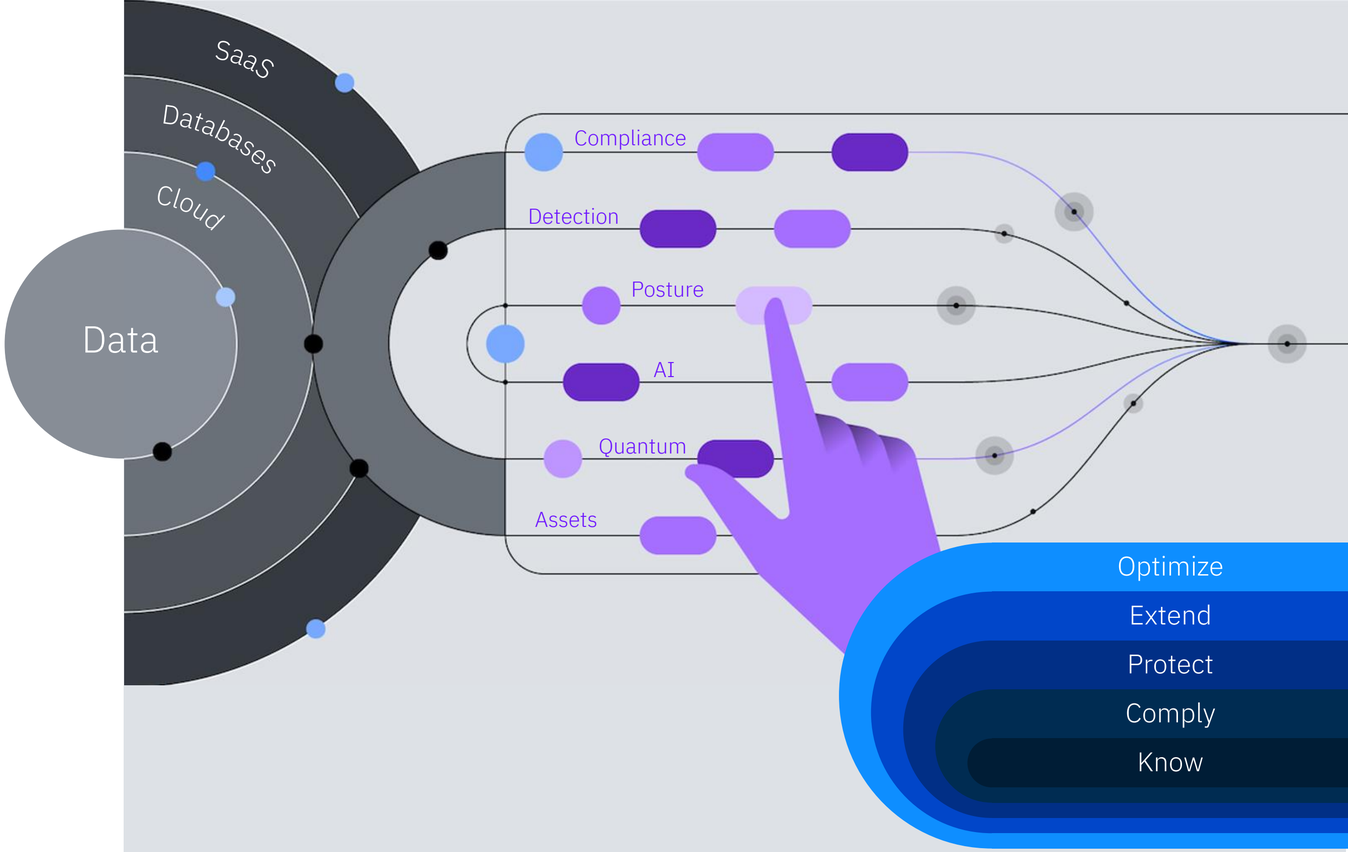


Asset Inventory

Successfully understanding your data results in a comprehensive asset inventory where you’ve:

- Discovered structured and unstructured data across the entire data estate
- Classified sensitivities, such as Personally Identifiable Information
- Mapped data to regulatory frameworks and policies pertinent to your business
- Compiled this information into a central asset inventory or catalog

Optimization requires the break-down of tool and organizational silos



Data Security Silos

You have one mission: **data security**. However, your teams are working in silos:

- Data Compliance
- Detection & Response
- Posture Management
- AI Security
- Quantum Readiness
- Discovery and Classification
- Vulnerability Management
- Etc.

Silo Challenges

When your data security program is fragmented into operational silos, it creates numerous challenges:

- Lack of visibility across functions
- Poor or non-existent communication between teams
- Limited intelligence or data sharing, masking “big picture” risks
- Inefficient and ineffective remediation
- Labor-intensive and manual workflows and task management that spans teams

Data Security Platforms

To address the challenges, enter the data security platform that provides:

- Efficiency of a common services platform
- Flexibility to turn on/off modules as needed
- Ability to address a range of data security challenges in a single place

Not all DSPs Created Equal

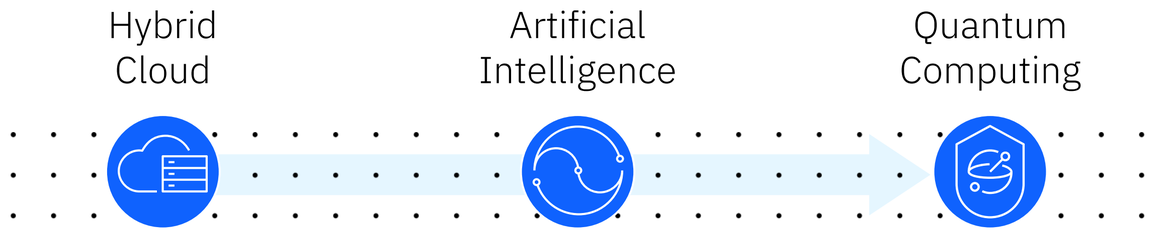
Beyond the basic objectives mentioned, organizational success with a DSP will also demand:

- Ability to address traditional and emerging use cases
- Bring together assets, workflows, and data to break down silos
- Protect hybrid assets, including databases, cloud storage, and SaaS, alike

Rapid business and technology innovation leaves critical data unprotected

Traditional methods of data protection must evolve to protect data in the cloud, in AI, and in the Quantum era

Technology innovations drive an expanded threat surface



To simplify data protection in the future, a shift from point products to a data security platform is happening

Compliance challenges

1000’s of hours preparing for audits with existing regulation complexity

New regulations are expected to address AI usage and eventually cryptographic risks posed by Quantum

Data exposure

Cloud and Generative AI adoption has created a loss in visibility of where data is stored, who has access, and how it is protected

Traditional encryption will be exposed enabling “Harvest now, decrypt later” strategy

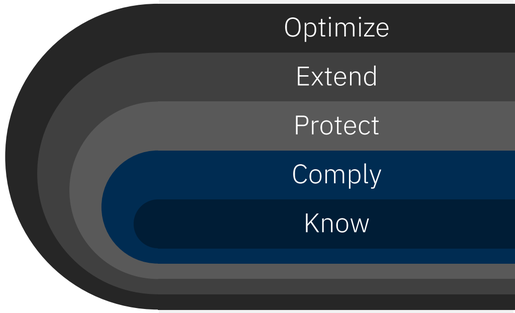
AI risks

Generative AI creates a new threat surface — training and fine-tuning data, models and applications — that must have a security and governance lifecycle to protect against risks (e.g., shadow AI, data poisoning, model evasions etc.)

Security posture

Organizations are struggling with visibility, a way to prioritize risks, and how to address security gaps across a spectrum of use cases — from shadow data, shadow AI to cryptographic posture — where data can be exposed; Siloed tools exacerbate this problem

Explaining your data is necessary for compliance



Situational awareness

After you've cataloged your data, now it's time to demonstrate that you understand key security controls through activity monitoring and reporting:

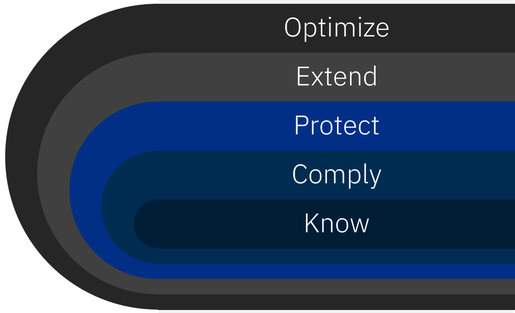
- Who's accessing your data
- What have they done and what *can* they do
- Who has privileged entitlements to sensitive data
- What controls are in place on a given data store
- When did a given change take place and by whom
- And so forth...

Compliance Reporting

Complying with internal policies, as well as external regulations, will demand that you can easily report upon your data, explaining the who, what, when, where, and why of data activity.

The ability to explain data activity is key to various regulations, such as SOX, HIPAA, GDPR, DORA, and CCPA.

Protecting data means getting proactive

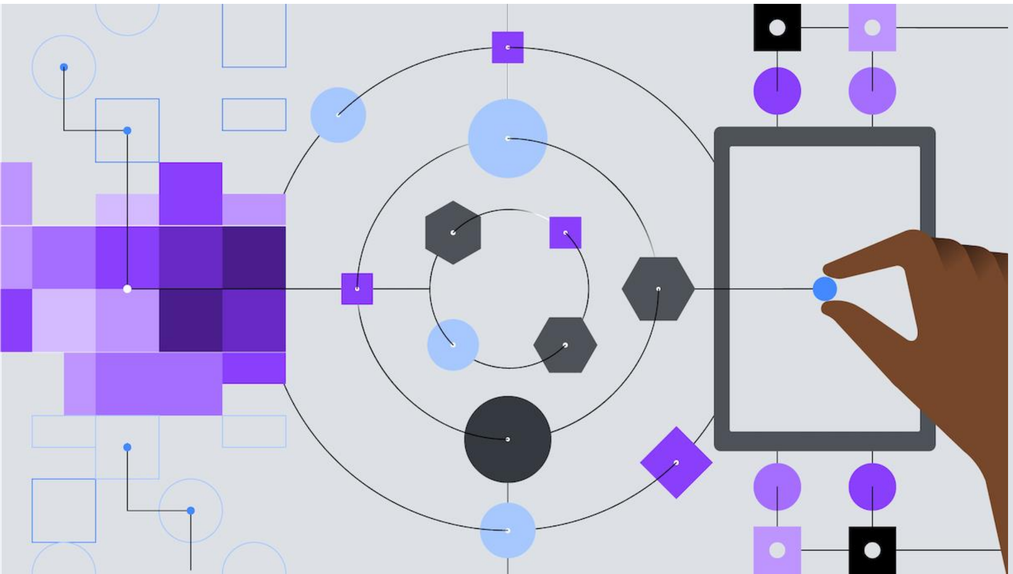


Data Detection and Response

Monitoring data activity is great – however, it's not a replacement for detection and response. Organizations will need to bridge the gap between large volumes of activity data and those small pieces that need to be bubbled to a SOC for action – this is where data detection and response (DDR) becomes key.

Encryption, Key, and Secrets Management

Proactively protecting data also means encrypting it with appropriately matched ciphers, all while keeping your keys and secrets properly managed.



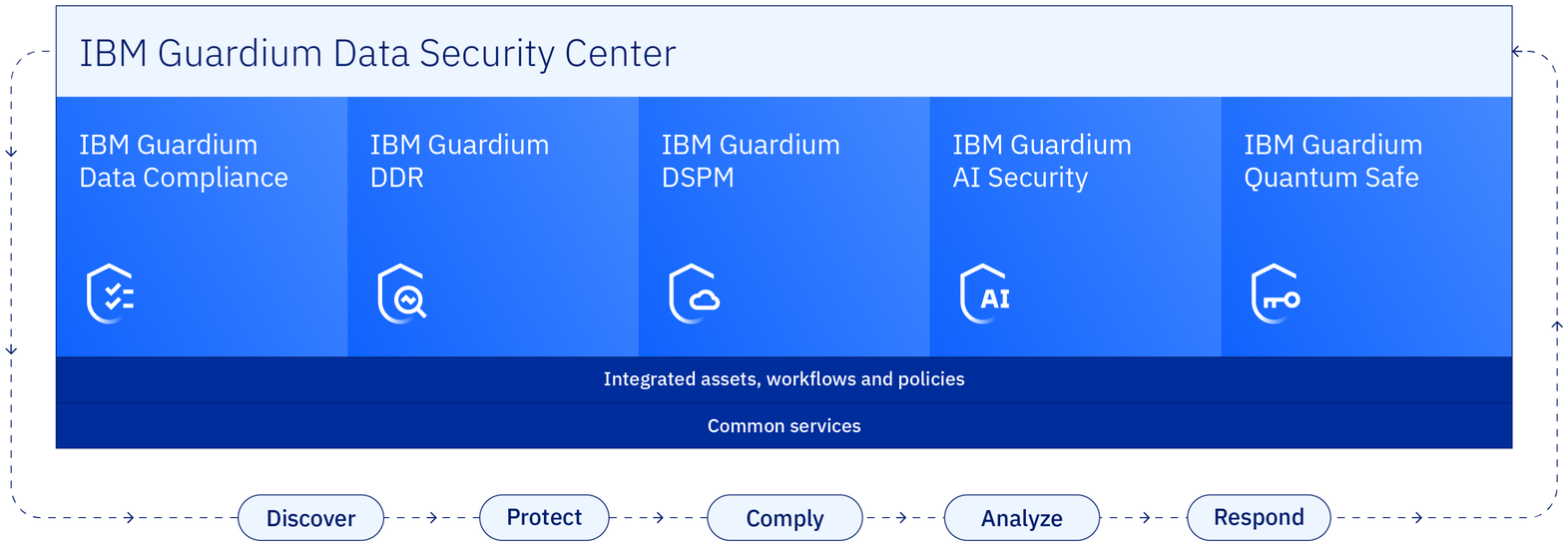
Getting to Actionable Intelligence

Simply feeding all your data activity to the SOC is too noisy. SOC analysts become overwhelmed and miss important events hidden in the noise.

Getting to actionable intelligence means utilizing smart approaches to detection, filtering, and explainability to ensure SOC analysts can respond effectively to the right events.

IBM Guardium Data Security Center

Single Product, Protect Data Everywhere, Throughout its Lifecycle



Unified Data Security Controls

One platform to manage the full data security lifecycle for all enterprise data

Protect Data Everywhere

Flexible and widest approach to apply data controls across current and emerging threat vectors

Empower Security Teams

Collaborate more effectively across multi-disciplinary teams with a common view of data assets, integrated workflows, analytics dashboards, centralized compliance policies ticketing, and reporting.

Flexible Deployments & Licensing

Reduce operational costs and efficiently scale, whether through SaaS or on-premise deployment with a modular platform and bi-directional ecosystem integrations.

Guardium Data Security Center is a powerful data security platform

Common Services

At the heart of our data security platform exists common services

- Identity and Access
- Risk Engine
- Policy Engine
- Data Ingestion & Warehouse
- API Gateway
- And more…

Shared Experiences

Shared Experiences bring intelligence and workflows together across modules

- Sharing data, events, and insights between modules
- Contributing and consuming data, events and insights between modules and the platform

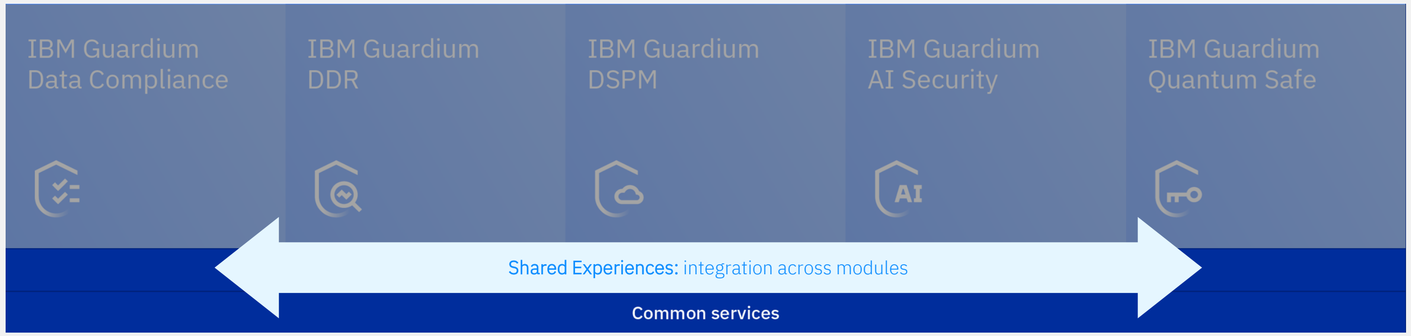
Common Standards

Standards, accessibility, and common design is at the heart

- Globalization Standards
- External Certifications
- Accessibility Standards
- Digital Marketplaces
- Trials and Demos
- Common Design Language

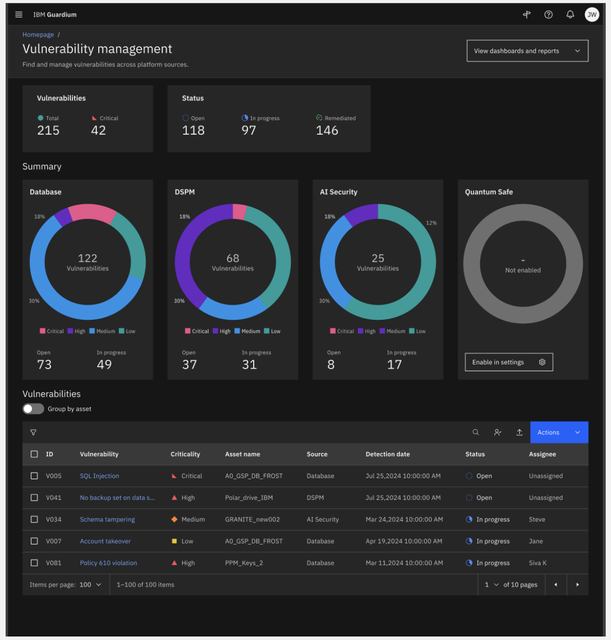
Shared Experiences

A data security platform truly becomes powerful once intelligence and workflows can traverse modules to create an outcome that's more than the sum of its parts

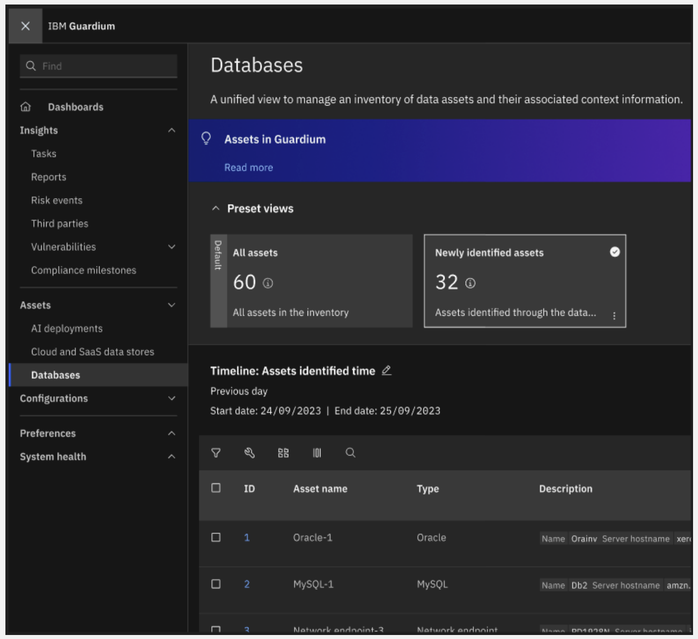


EXAMPLES

Vulnerability Management Hub



Common Asset View – Discover & Classification



Vulnerability Management Hub

Centralized vulnerability management enables customers to see and manage data security app vulnerabilities in a single hub[1]

Cross-App Vulnerabilities

Vulnerabilities may be surfaced to the hub by any application on the platform, including:

- Database Vulnerability Scanner
- Data Security Posture Management
- AI Security
- Quantum Safe
- Data Detection & Response

Vulnerability Correlation

Vulnerabilities can be correlated across data security apps on the platform to create composite vulnerabilities:

- A database vulnerability affecting compliance;
- A cloud repository vulnerability potentially incorporated in a breach attempt;
- An encryption library vulnerability associated with regulated data

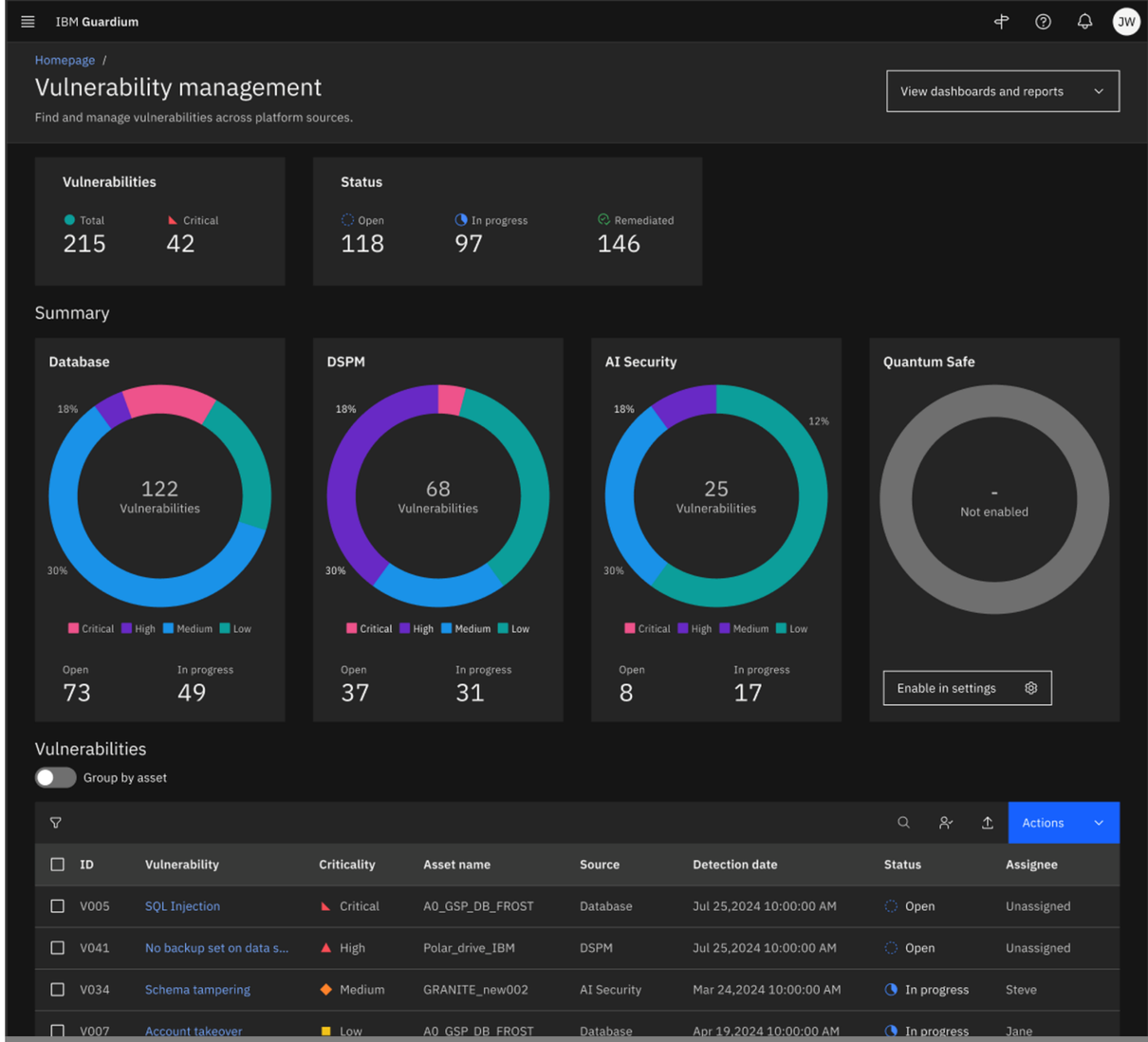
Manage Open Vulnerabilities

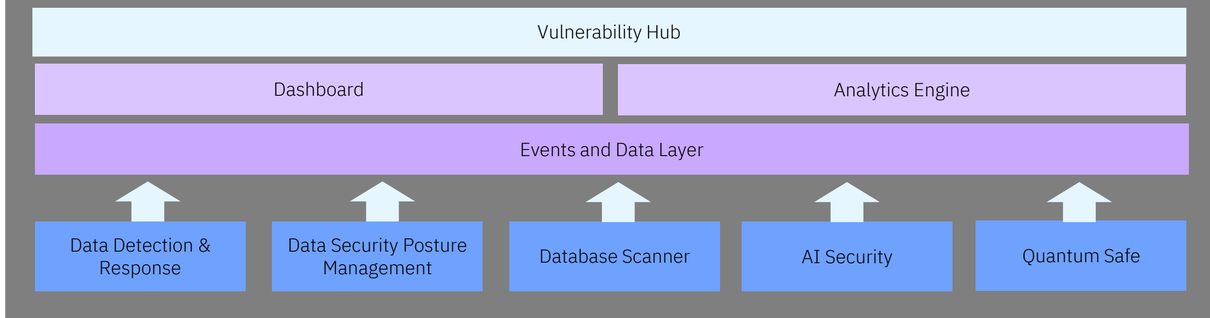
Track, assign, and close-out vulnerabilities using the platform's workflow engine and integrations to ServiceNow.

Drill Down by Asset

Asset views provide insight into how composite vulnerabilities may be impacting any given data store, along with the array of vulnerabilities associated with it.

[1] Coming Q1 2025





Discovery & Classification

Centralized D&C underpins the applications on the platform to provide consistent asset information[1]

Hybrid Discovery

Discovery is supported across a hybrid set of data sources covering:

- Cloud infrastructure data stores
- SaaS applications
- On-premise data stores
- DB-as-a-Service
- Structured and unstructured

Open Framework

A heterogenous approach to D&C is necessary to synthesize findings in complex environments

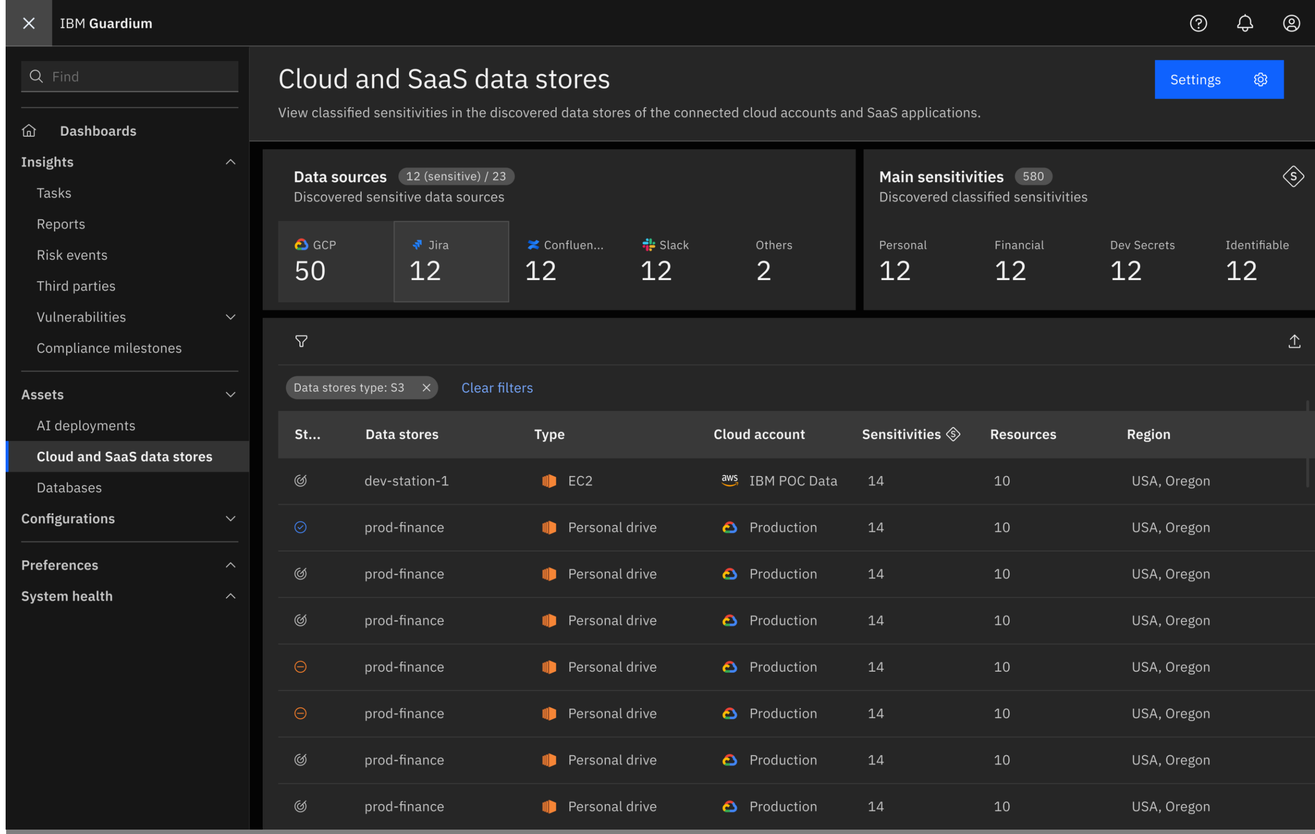
- Synthesized technologies
- Open APIs
- Integration with data governance (catalogs, observability, etc.)

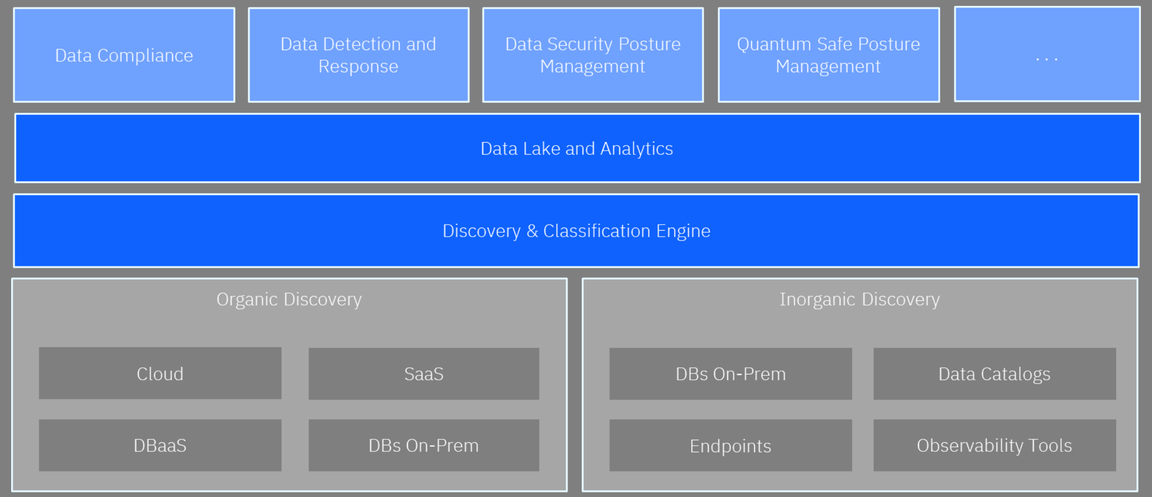
Foundational

D&C is a foundational technology that must be accessible and shared by core data compliance and security applications on a common platform

Contextual

D&C, in and of itself, is far less useful unless contextualized with intelligence within compliance and operational security use cases





[1] Coming Q1 2025

Data Compliance

IBM Guardium Data Compliance

Run your data compliance program effectively and at-scale while minimizing cost and risk

Programmatic

Manage the lifecycle of your data compliance with programmatic reports, workflows, tasks, schedules, and notifications

Compliance Journeys

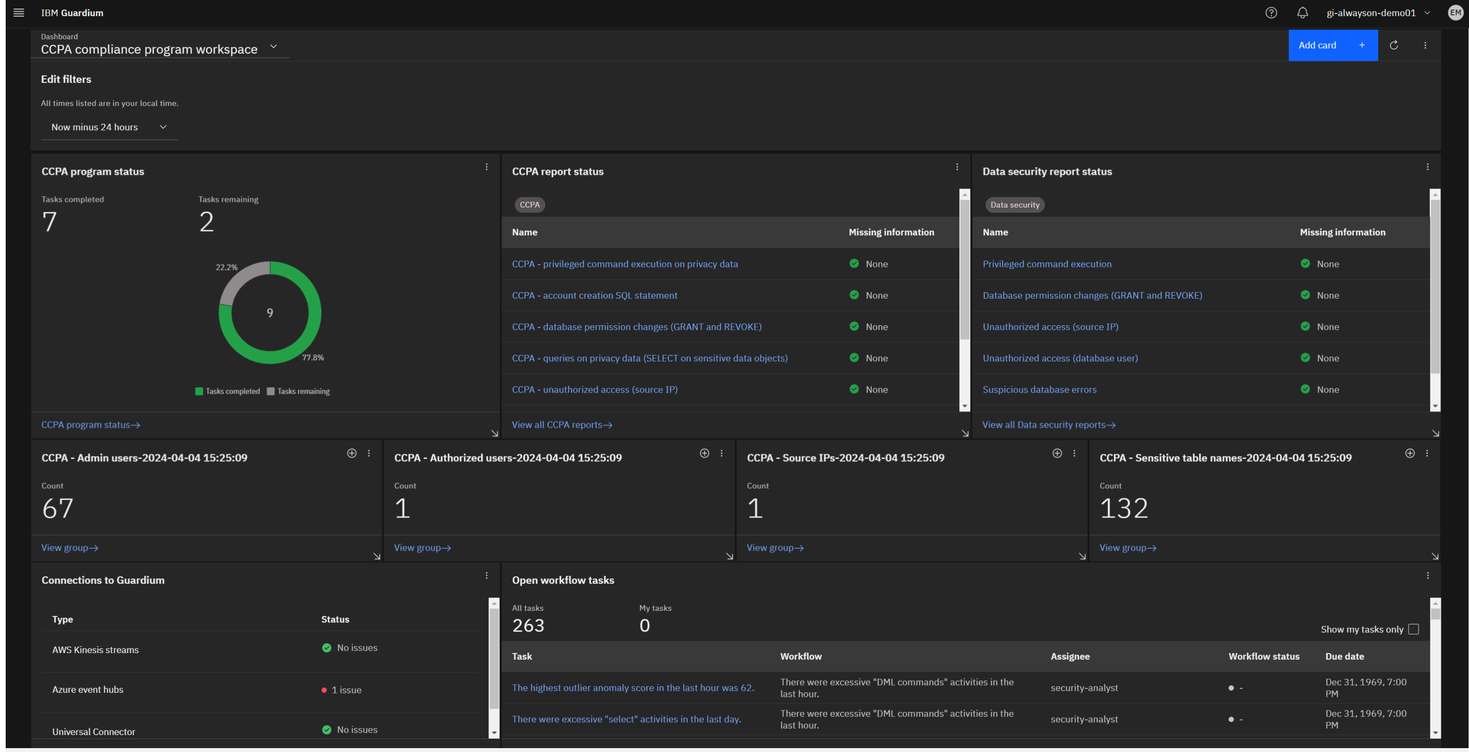
Quickly configure your program with the use of Compliance Journeys that help automate SOX, GDPR, HIPAA, and other regulatory requirements

Activity Monitoring

Monitor privileged activity to on-prem and cloud data stores, collecting necessary information to raise violations, provide evidence, and produce auditor reports

Cross-Platform

Manage data compliance across existing instances of Guardium Data Protection (GDP), modules within Data Security Center (DSC), or both



1000s

Of hours spent a year by organizations to help facilitate audits[1]

A complex web of regulations – DORA, GDPR, CCPA, SOX, PCI, HIPAA, etc. – means more than ticking boxes, it means diving deep into unauthorized access, data lineage, and movement.

Meeting these obligations in the most efficient and effective way possible is not only an objective but a necessity for organizations that strive to meet obligations while also measurably reducing risk and cost.

DDR

IBM Guardium DDR

Detect and respond to data security events effectively while reducing noise in your SOC

Hybrid Monitoring

Monitor critical data stores across your hybrid asset estate – including traditional databases on-prem to cloud data services running across AWS, Azure, and GCP

Detection

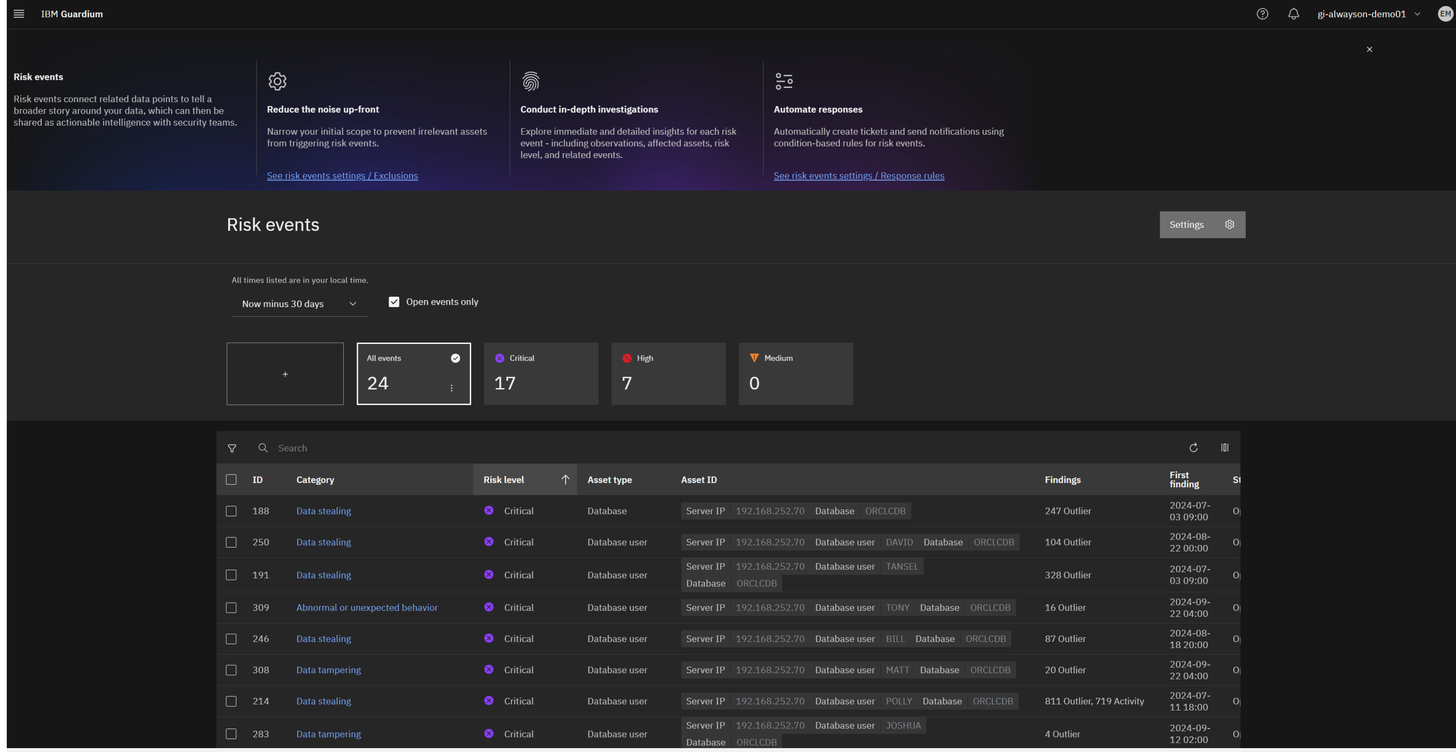
Detect threats, including singular events through complex orchestrated events, utilizing configurable rules and AI that reduces noise for your SOC

GenAI

Generative AI helps improve the DDR experience by summarizing risks and dissecting data, such as SQL commands, into natural language to expedite the analyst's response

SOC Integration

Pushing just the actionable intelligence into your SOC not only reduces noise and improves the likelihood of a rapid analyst response, but it also reduces costs for SIEM and SOAR licenses



$4.88M

Average cost of a data breach, up 9.2% from 2023[1]

Data breaches are on the rise, and they're costly in more ways than one. Direct financial implications can be staggering, but indirect fall-out, such as reputational damage, can be difficult to repair.

Staying ahead of data breaches means employing sophisticated data detection and response (DDR) technologies to monitor, analyze, and respond to threats in real-time.

[1] IBM Cost of a Data Breach 2024

DSPM

IBM Guardium DSPM

Uncover vulnerabilities across the hybrid cloud, while remediating issues quickly

Shadow Data

Rapidly find structured and unstructured data that's resident across cloud, SaaS, and DBaaS environments that may be sensitive and regulated in nature

Data Movement

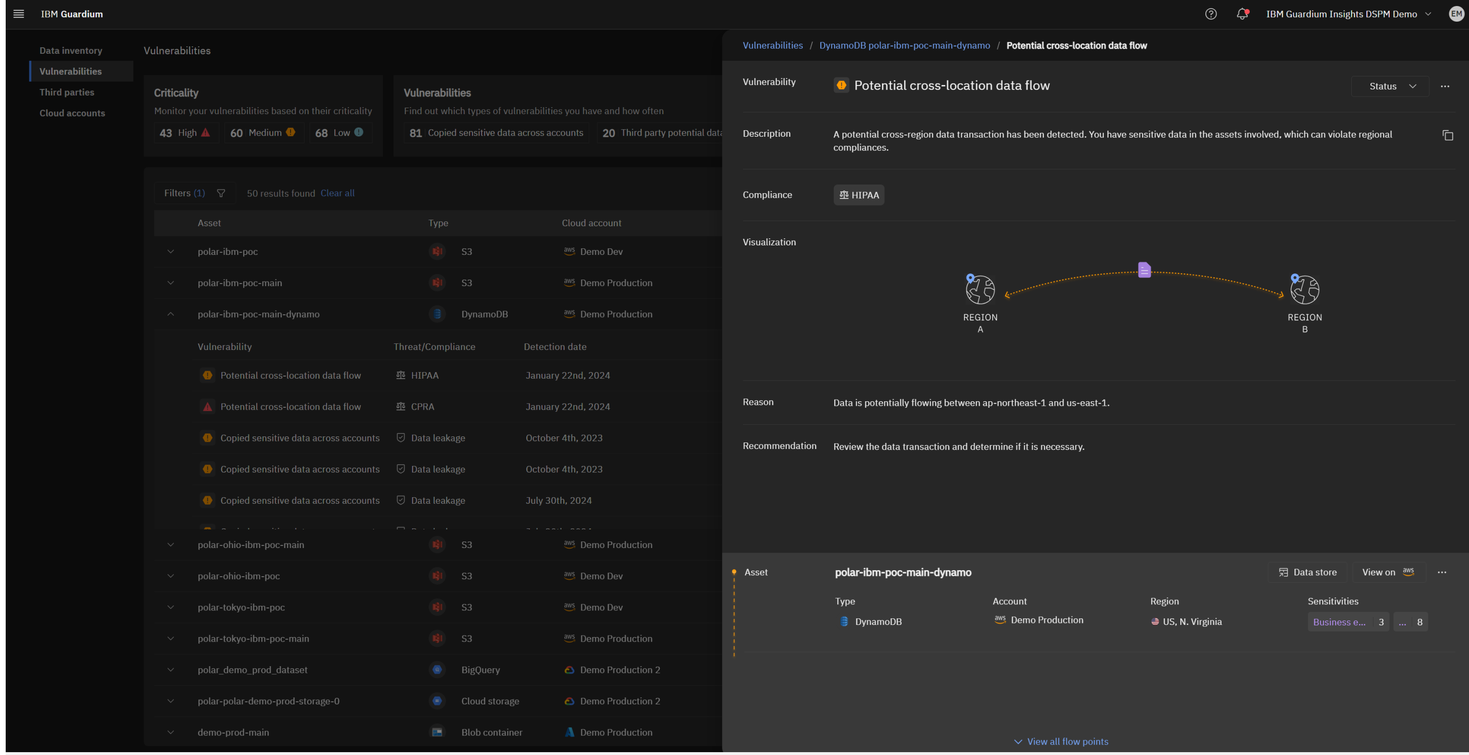
Interrogating entitlements and audit logs, alike, see where your data *can* move and where it's *actually* moving, to understand proliferation risks

Vulnerabilities

Whether an S3 bucket open to the Internet, PCI regulated data in a log file, or 3rd parties with access to PII, vulnerabilities are raised for action

Remediation

Remediating issues is made simple thanks to automated Terraform and console scripts that give you ready-to-execute fixes for many types of vulnerabilities



1 in 3

Breaches found to involve elements of shadow data

[1] IBM Cost of a Data Breach 2024

Thanks for ongoing cloud and SaaS adoption, data continues to shift into these domains at an accelerating pace. However, most conventional data security programs are blind to the risks given only traditional tooling.

DSPM allows your organization to bring shadow data back into the light – discovering this data, analyzing critical entitlements, raising vulnerabilities, and providing remediation strategies.

AI Security

IBM Guardium
AI Security

Protect AI data, models, and applications across multiple deployment platforms

Shadow AI

Discover your AI deployments, including training and RAG data, models, and the applications that are utilizing these models

Uncover Vulnerabilities

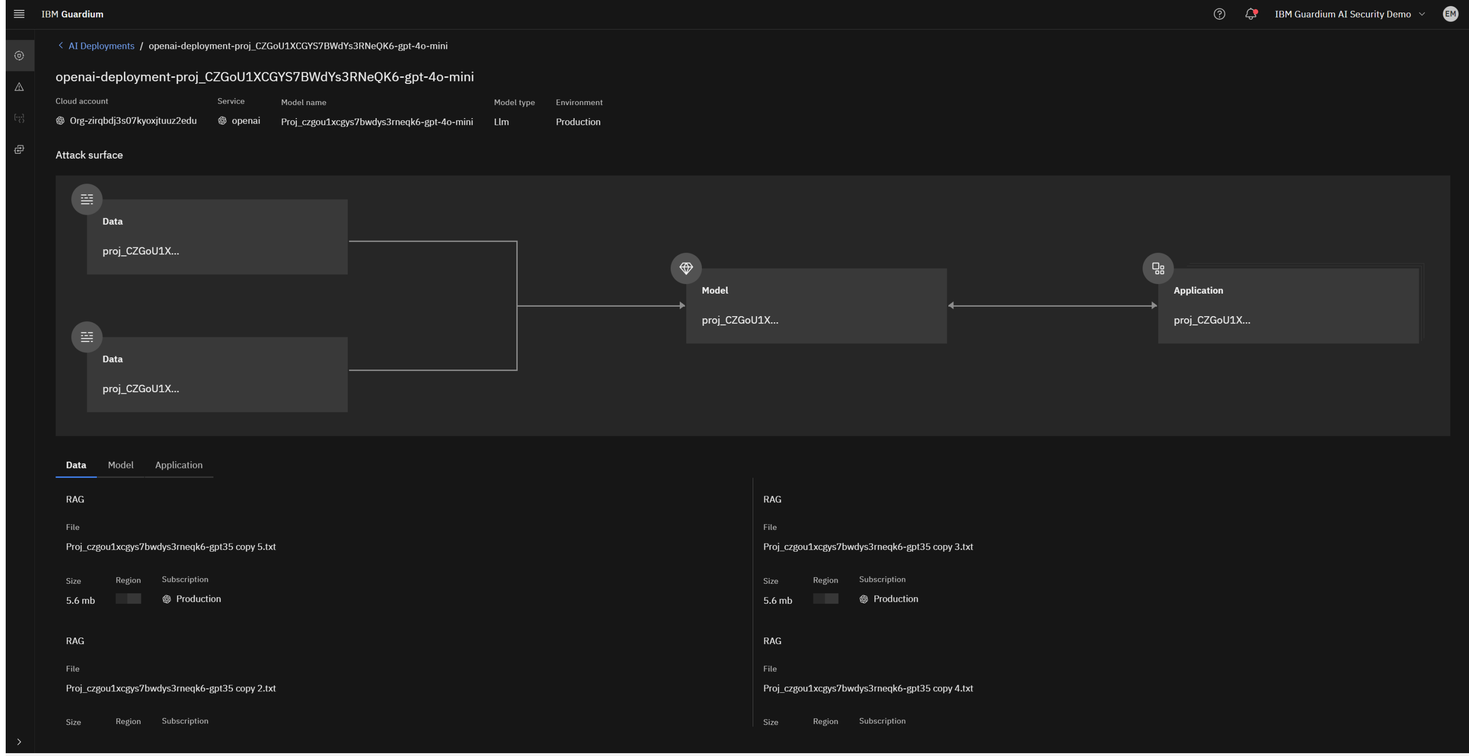
Quickly determine if data and models are vulnerable to attack, poisoning, exfiltration, and manipulation, including mapping to OWASP

Drill Down and Monitor

Drill down into training data, understand classification and sensitivities, and monitor ongoing access and entitlements to data supporting models[2]

Govern with WatsonX

Import discovered AI inventories into WatsonX.Governance to fully manage the lifecycle of the model, including bias, drift, tolerance, and more



61%

Of IT leaders have recognized shadow AI as a significant threat[1]

AI is quickly being adopted and deployed at-pace. With that comes significant risk, much of which today lives in the shadows.

Managing AI risk means first uncovering AI models, data, and applications, followed by detailing their vulnerabilities and establishing on-going governance and monitoring.

[1] Cloud Security Alliance

[2] Utilizing Data Security Center capabilities and modules

Quantum Safe

IBM Guardium Quantum Safe

Prepare your organization to be Quantum Safe – addressing vulnerable cryptography

Crypto Inventory

Build a cryptographic inventory by comprehensively scanning and ingesting data such as source repositories and vulnerability scanners

Evaluate Posture

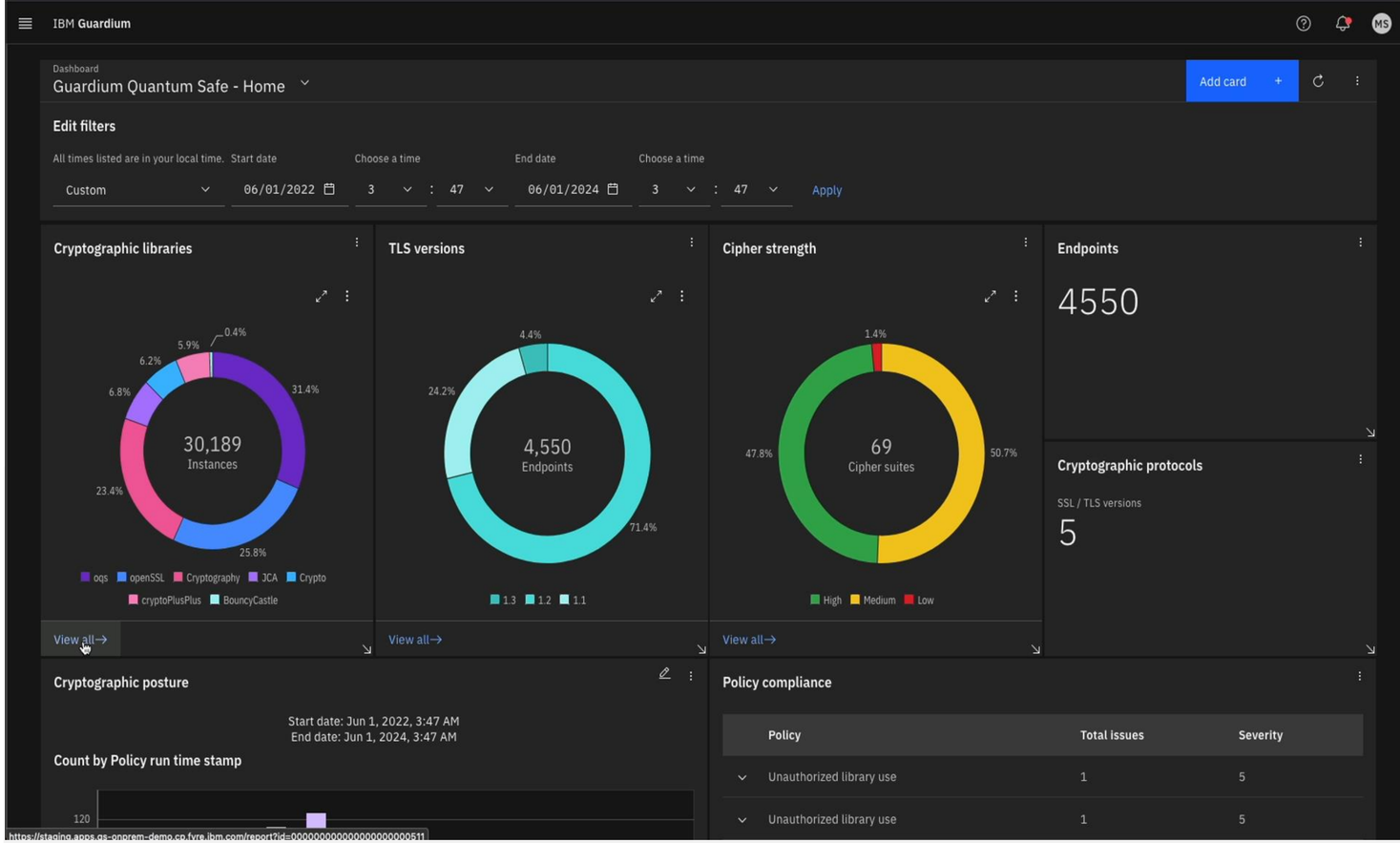
Evaluate your organization's posture based upon findings, such as library types, versions, cipher strengths, endpoints, and protocols employed

Policy & Vulnerabilities

Drill down into specific vulnerabilities, including remediation recommendations, opening tickets to put fixes into motion

Track Progress

Track the organization's posture over time by tracking progress of open vulnerabilities and policy violations



2024

First set of PQC standards are published[1]

[1] NIST

The advancement in quantum computing has given rise to a new threat – the ability for quantum computers to easily break conventional asymmetric encryption.

While quantum computers cannot yet break encryption today, adversaries are employing techniques like harvest-now decrypt-later in preparation, posing an immediate and concerning risk.