

Smarter security for the modern data landscape.

IBM Security Guardium Data Protection

Digital transformation is accelerating



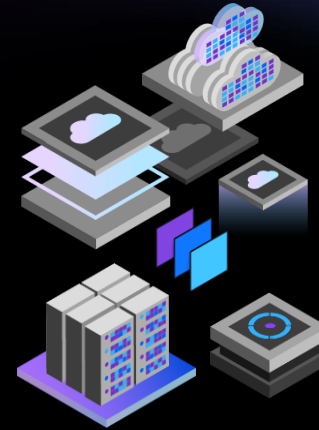
Applications

Modular, containerized,
and shifting to SaaS



Data

Shared resource for advanced
analytics and AI



Infrastructure

Distributed across hybrid
multicloud environments

Traditional security can't keep pace

Too much to do

- ❑ Meet with CIO and stakeholders
- ❑ Nail down third-party risk
- ❑ Manage GDPR program with privacy office
- ❑ Respond to questions from state auditors
- ❑ Update CEO for board meeting
- ❑ Update budget projections
- ❑ Write security language for vendor's contract
- ❑ Make progress on the never-ending identity project
- ❑ Review and updated project list
- ❑ Edit communication calendar
- ❑ Update risk rankings on security roadmap
- ❑ Clarify policies governing external storage devices
- ❑ Provide testing and encryption tool direction
- ❑ Provide data handling best practices
- ❑ Help with new acquisition
- ❑ Meet with senior project manager
- ❑ Send new best practices to development teams
- ❑ Review logs for fraud ongoing investigation
- ❑ Help with insider threat discovery
- ❑ Determine location of sensitive data in the cloud
- ❑ Investigate possible infection on legacy system
- ❑ Continue pen testing of new business mobile app
- ❑ Help architects understand zero-trust
- ❑ Answer security policy emails
- ❑ Format security status report for executives
- ❑ Meet with recruiter to discuss staffing
- ❑ Write test plan requirements for new products
- ❑ Meet regarding improving security of facilities

Too many vendors



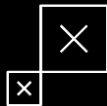
Too much complexity



Too many alerts



Hybrid cloud environments exacerbate key data security challenges for organizations



Stopping threats before they disrupt business

\$5.52 million

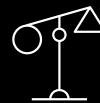
Average total cost of a breach at enterprises of more than 25,000 employees.



Keeping up with the sprawl of data

\$267,469

Average cost increase of a breach due to extensive cloud migration.



Achieving regulatory compliance

\$14.82 million

Average cost of a failed audit for compliance with data protection regulations.

A smarter, continuous approach for top data security challenges

Discover

Discover and classify your sensitive data across on premises and cloud data stores

Analyze

Analyze and assess risk with contextual insights and analytics

Protect

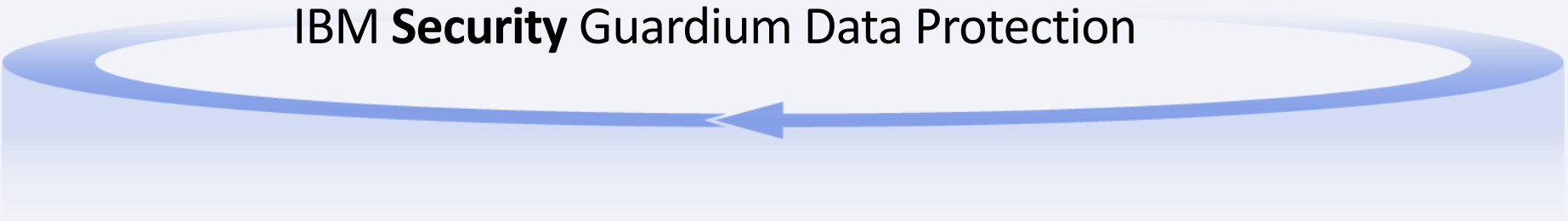
Protect sensitive data through data activity monitoring

Respond

Respond to threats in real time and send actionable alerts to security operations systems

Simplify

Simplify data privacy and security compliance



IBM Security Guardium Data Protection

Accelerates data discovery, improves accuracy and saves time

Discover

50%

increase in data
classification accuracy

Analyze

67%

increase discovering data
source vulnerabilities and
misconfigurations

Protect

43%

increase in data
threat detection
accuracy

Respond

42%

decreased time
remediating data
security issues

Simplify

89%

reduced time
spent preparing
for an audit

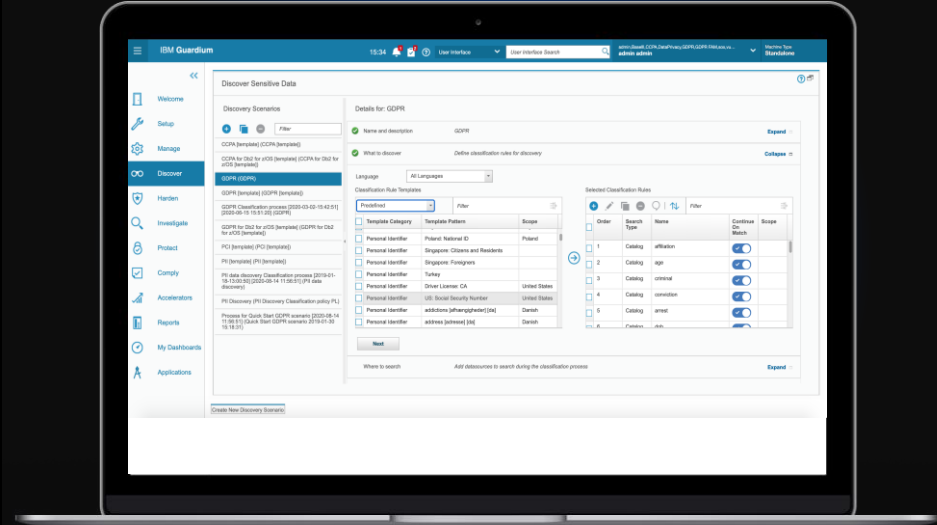
Guardium Data Protection

Discover and classify sensitive data across on-premises and hybrid multicloud environments

- Automatically discover databases or import assets manually. Define and map applications to their data sources
- More than 100 data discovery patterns identify regulated data in your environment

Analyze your environments for vulnerabilities

- Proactively scan for vulnerabilities using more than 3000 assessment tests across heterogeneous platforms
- Initiate remediation by integrated Security Operations solutions



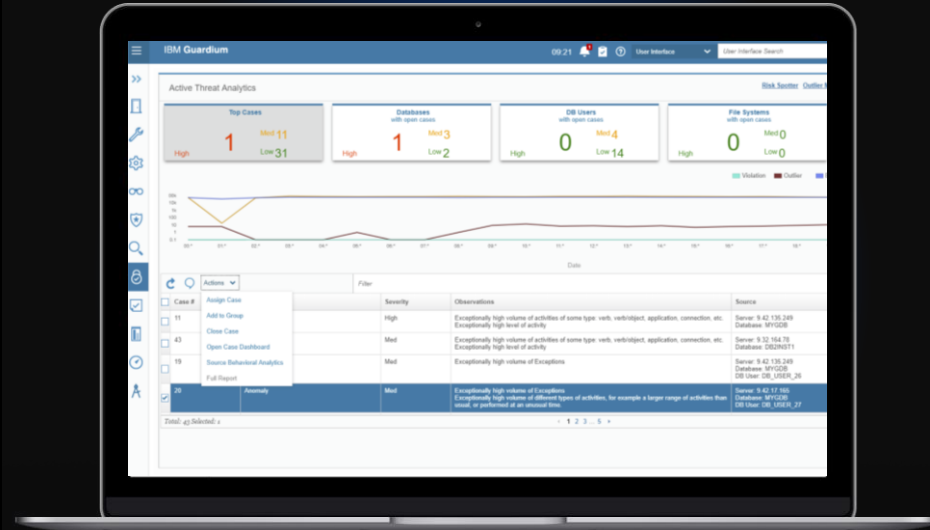
Guardium Data Protection

Protect sensitive assets with data activity monitoring

- Define rule-based policies to monitor, log, report and alert on unauthorized data access
- Predefined security policy templates can be customized based on your own audit requirements

Respond to threats in real time

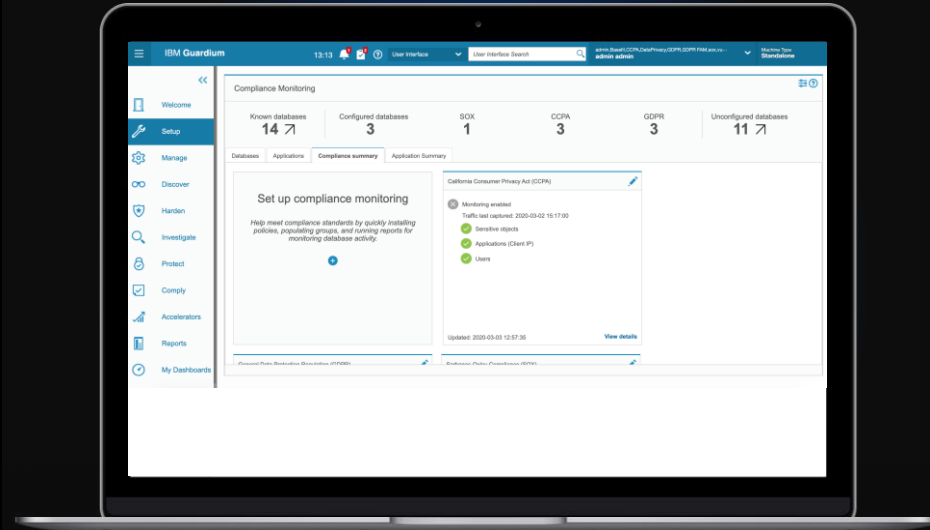
- Quickly uncover and respond to suspicious insider threats and external breach attempts
- Threat analytics tools allow you to investigate user risk details to determine “who,” “what,” “when,” and “where” of an event
- Block or quarantine suspicious users in real time



Guardium Data Protection

Simplify compliance auditing and reporting through automation

- Pre-built regulation templates can be used to automate tracking and reporting compliance
- Add tagging to multiple policies and rules to enable easier and faster policy management
- Track progress towards compliance on all selected regulations from single interface
- Accelerate audit activities and confirm separation of duties through a continuous, fine-grained audit trail



**Start taking a
smarter
approach to
data security**

IBM **Security** Guardium Data Protection

**Discover and
respond to
threats** before
they disrupt
business

**Successfully
migrate to the
cloud** while
securing your
sensitive data

**Comply with
privacy
regulations**
where the
business
operates

Built to protect data on premises, in the cloud, and everywhere in between.

Databases and data warehouses

Big Data

Files

Mainframe and z/OS

Cloud:

- AWS
- Azure
- Google Cloud
- IBM Cloud
- Oracle Cloud
- Database-as-a-Service



Getting specific

Securing hybrid multicloud environments with Guardium Data Protection

| Dynamic | Orchestrated | Modern |
|---|---|---|
| <p>Active & passive monitoring for 30+ cloud-native data sources</p> <ul style="list-style-type: none">– Agentless– Agent-based <p>Minimize security blind spots and take real-time action with blocking and redaction*</p> <p>Store data security and audit data to meet retention requirements and uncover unknown threats</p> | <p>Centralized policy enforcement and management across hybrid multi clouds</p> <p>Automate compliance workflows for audit reviews and approvals</p> <p>Orchestrate remediation and response with IT and SecOps tools</p> <ul style="list-style-type: none">– ServiceNow, Splunk, QRadar, Resilient, and more | <p>Uses cloud-native and containerized technology</p> <p>Simplify and streamline deployment with cloud management frameworks, such as Kubernetes and OpenShift</p> <p>Elastic, scalable and resilient</p> |

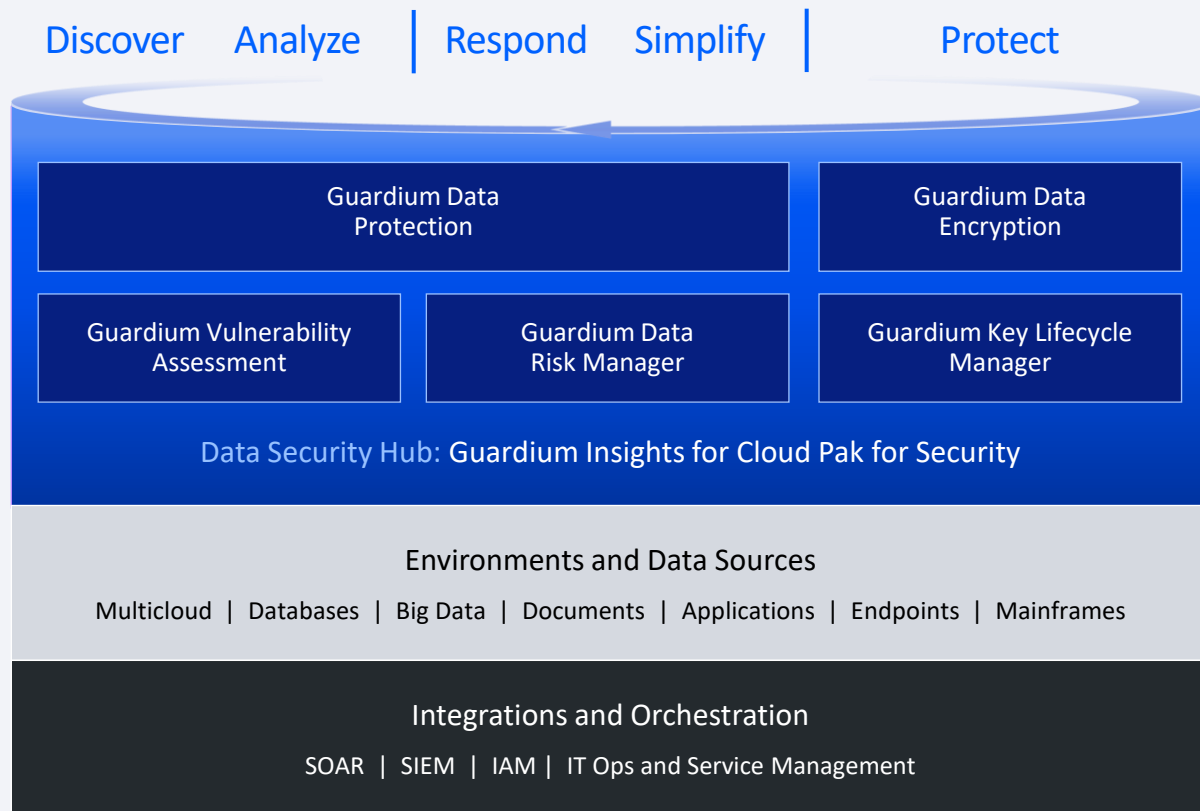
* Agent-based

Integration with the rest of the stack provides connected security for the enterprise

- Security orchestration, automation and response
- Security information and event management
- Identity and access management
- IT operations and service management
- Application security
- Archiving / backup restore
- Web Application firewalls
- Data security and data risk management
- Privacy auditing and compliance reporting



IBM Security Guardium product portfolio



Consulting, Systems
Integration and Managed
Security Services

Data Security Strategy

Data Discovery

Data Security Governance

Managed DAM

Managed Data Encryption

The best in the business put Guardium Data Protection to work

4 out of 5

top global **healthcare** organizations

7 out of 10

top global **telecom** organizations

3 out of 5

top US **retailers**

4 out of 5

top US **banks**

6 out of 10

top global **insurance** organizations

4 out of 5

top global **financial services** organizations

3 out of 5

largest US **government** agencies

Start taking a smarter approach to data security **today**

Schedule [a consultation](#)

Learn more about
[Guardium Data Protection](#)

See Guardium in action:
[launch the demo](#)

Guardium Data Protection

V11.3 – New features and enhancements

What's new in Guardium Data Protection v11.3?

Improved capabilities

- Improved efficiency and ease of use for compliance reporting tools
- Expanded scope and features of Unified Health and Deployment dashboard

Greater flexibility

- Universal Connectors import and normalize native logs
- S-Taps and External S-Taps allow real-time monitoring and response
- Updated APIs

Expanded support

- Integration with IBM Security Verify to support AWS Secrets Manager
- Expanded classification capabilities for MongoDB
- Support of PostgreSQL 12
- Couchbase database support for Vulnerability Assessment
- Expanded database support for Cloud Pak for Data: DB2, DB2 Warehouse, NPS* and BigSQL*
- Additional archive and backup support for Azure*

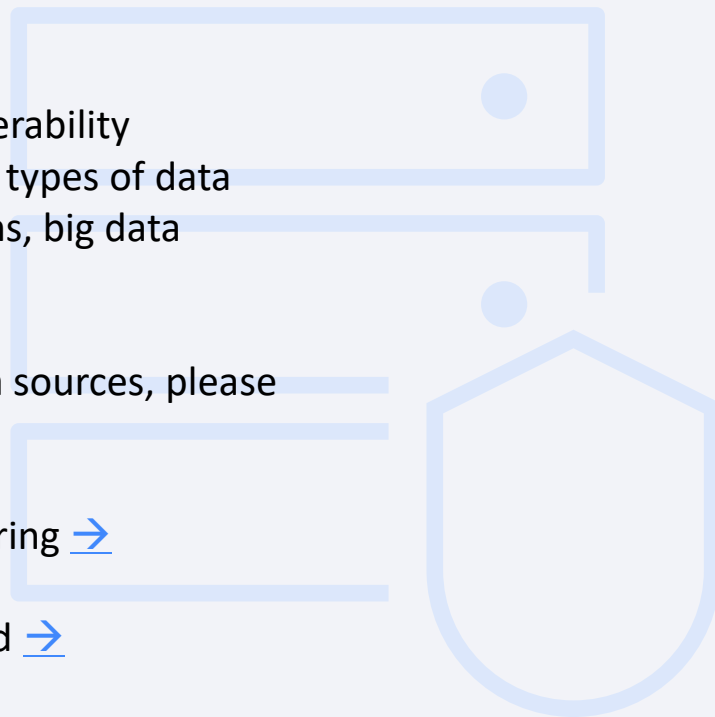
*Available Q1 2021

Guardium Data Protection supports a wide range of platforms and data sources.

Guardium Data Protection offers activity monitoring, vulnerability assessment, and compliance reporting support for several types of data sources, including databases, data warehouses, file systems, big data platforms, and z/OS.

For a comprehensive lists of supported platforms and data sources, please visit:

- [Supported Platform Database for Data Activity Monitoring](#) ➔
- [Detailed system requirements and platforms supported](#) ➔



Get started today:

Schedule a consultation [here](#).

Learn more about [IBM Security Guardium Data Protection](#)

Explore the interactive demo: [Guardium Data Protection](#)





IBM Security Guardium Value Assessment

A 3-hour engagement to review how the security and privacy of your critical data may be improved:

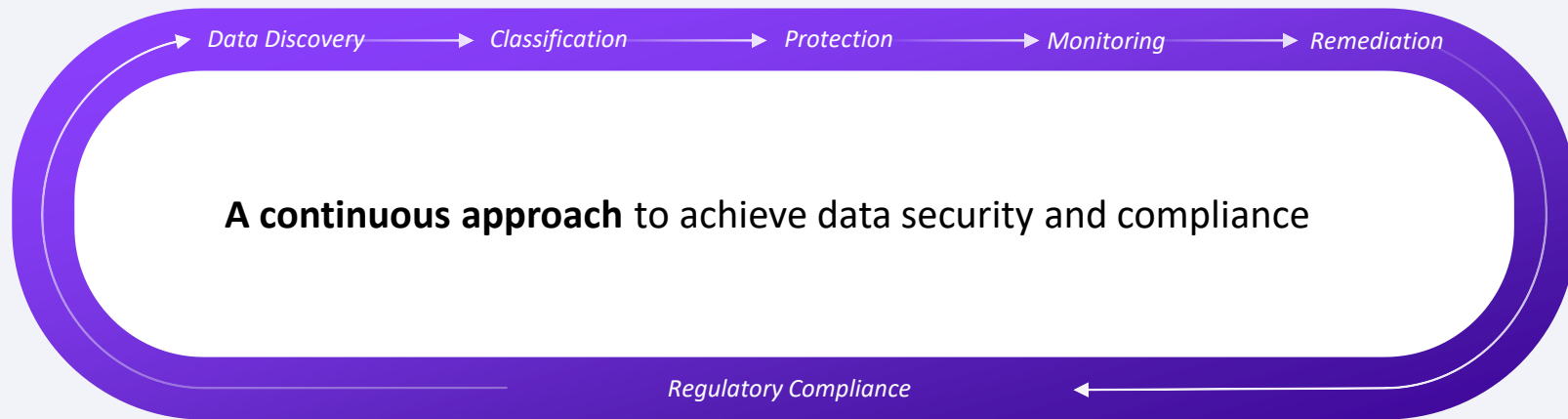
- **Outline your desired end state**, including any developments or changes in strategy or environment since initial implementation
- **Gain actionable recommendations** to move from current to desired state
- **Update your team on the evolution** of your solution set (there are often surprises here!)
- **Demonstrate how Guardium is an enabler** for your business and its ability to innovate
- **Prioritize recommendations** that will be delivered within the first week

As your environment and data security needs evolve, are you realizing as much value as possible from your investment?

The **Guardium Value Assessment** is a free customized report that describes your current deployment and delivers a clear action plan to achieve your desired goals.



How end-to-end data security services accelerate steps towards smarter data security



1

Seamless global delivery and support team

50+

Global team of advisors across fifty countries from a security-certified talent pool

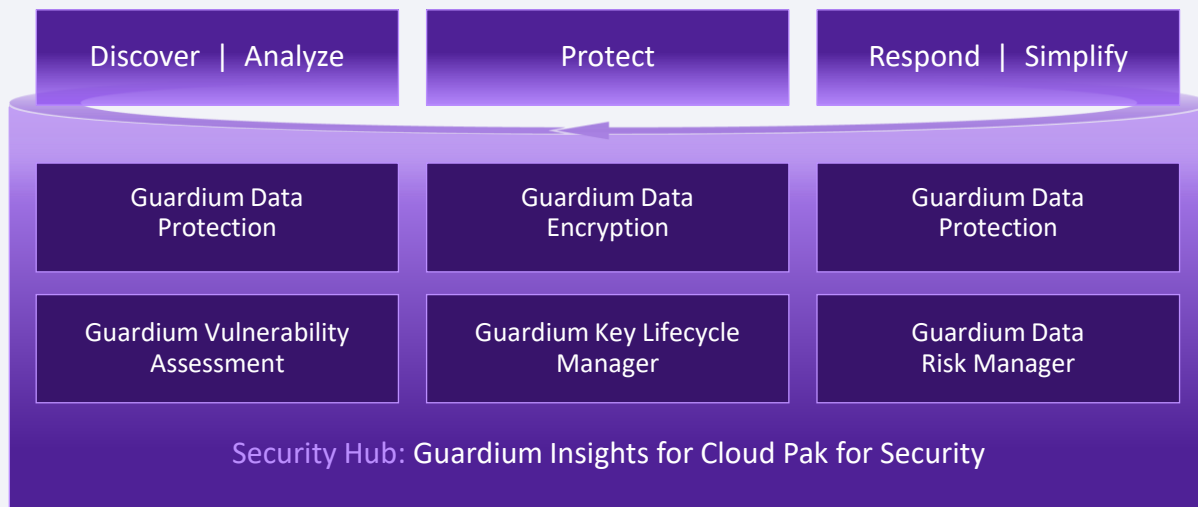
50+

Certifications with strategic advisors for consultancy services

2800

WW MSS experts with 400+ T1 triage and T2 investigation analysts

Smarter Data Security Integrations with IBM Security Guardium



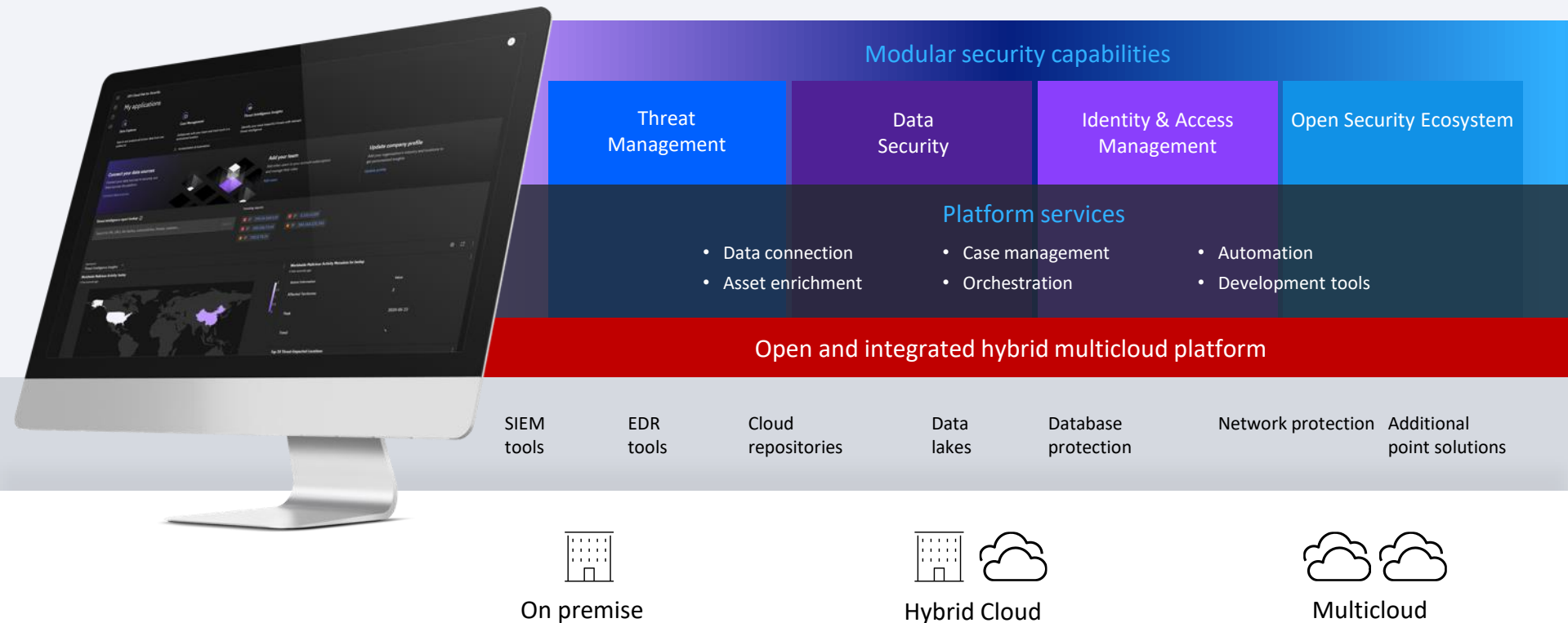
Integrations

- Data discovery and classification
- Security orchestration, automation and response
- Security information and event management
- Data leak prevention
- Identity and access management
- Privacy management, auditing
- Vulnerability assessment
- IT operations and service management
- Application security
- Archiving / backup restore
- Web Application firewalls

Consulting, Systems Integration and Managed Security Services

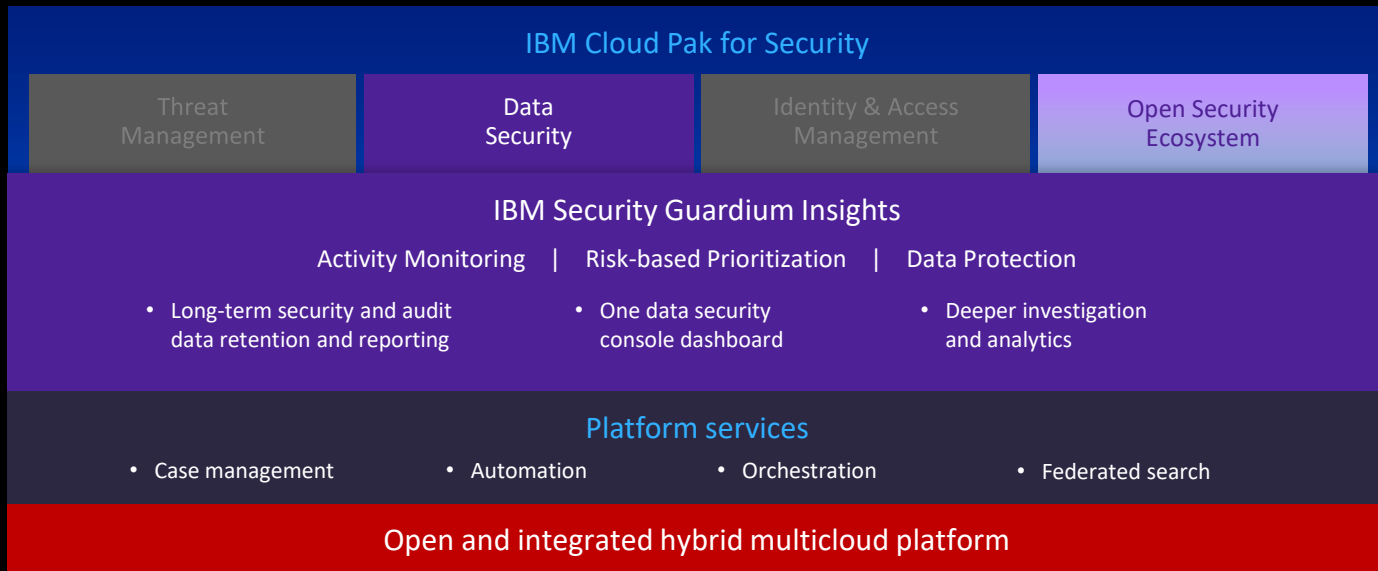
IBM Cloud Pak for Security

An open multicloud platform to gain security insights, take action faster, and modernize your architecture



IBM Security Guardium Insights for IBM Cloud Pak for Security

Collect, analyze and act on years of data security and audit data in the Guardium Insights for Cloud Pak for Security data security hub — whether that data comes from Guardium Data Protection via collectors or is streamed directly into the hub from Cloud sources in an agentless way.



Guardium Data Protection

Sources supported via:

STAPs
ATAPs
ETAPs

Native Audit Logs
(i.e., Oracle)

AWS Aurora via Kinesis for:
PostgreSQL

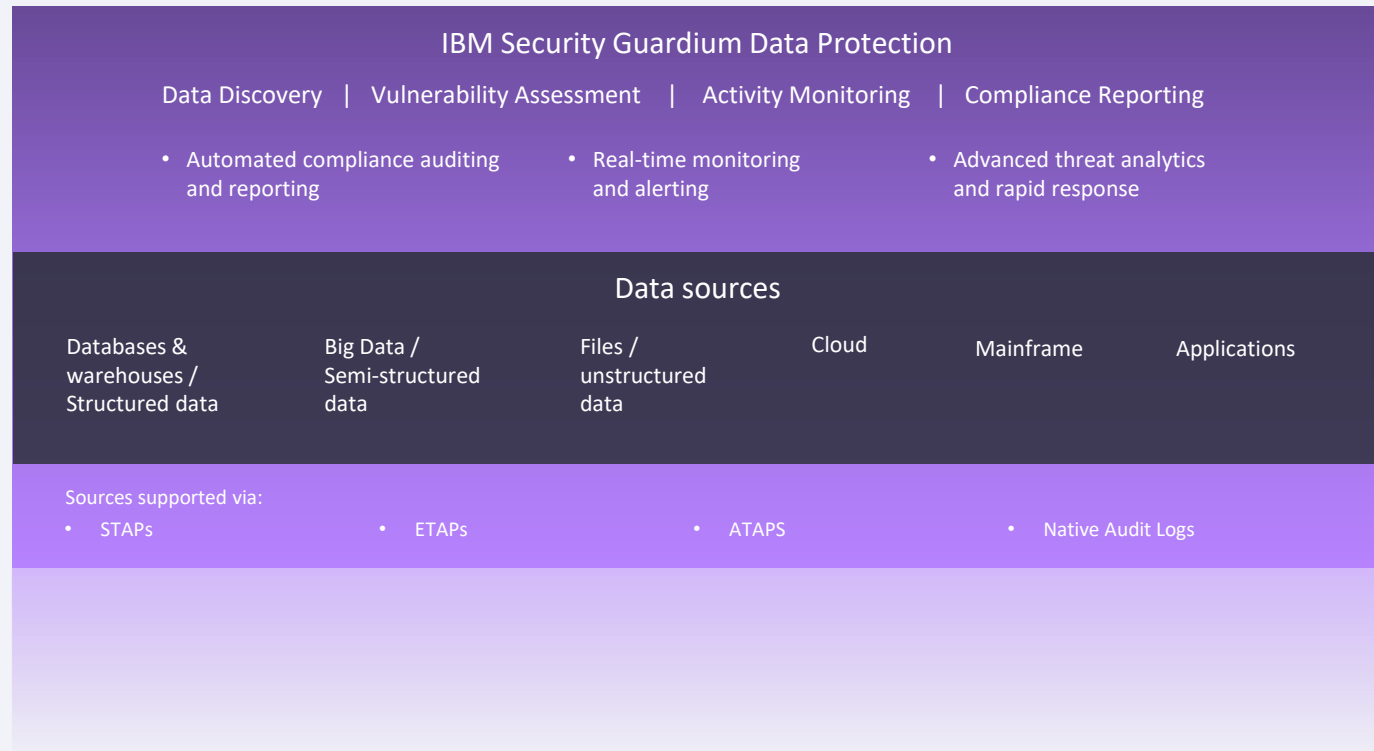
Microsoft Azure Event Hubs for:

Azure SQL
Cosmos SQL
Cosmos MongoDB

Cosmos Cassandra
Cosmos Gremlin
Cosmos Table

IBM Security Guardium Data Protection

- Discover and classify sensitive data, regardless of whether its stored on-premises or in hybrid multicloud
- Harden your infrastructure with vulnerability scans
- Discover and respond to threats in real time
- Use pre-built templates to simplify and accelerate your compliance journey



Smarter data security with Guardium

Data Protection and Guardium Insights for Cloud Pak for Security

