

IBM Security Guardium
Protect data across
the hybrid cloud

Data is central to everything we protect in security

Workloads and Infrastructures

Workforce and Users (regardless of location)

Public Clouds

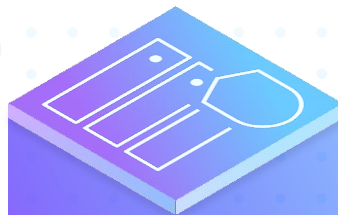
Mobile Devices and Apps

Private Clouds

Privacy and Compliance

Lines of Business

Software-as-a-Service



Monetizing Data

Data Governance

Data in Use

Data at Rest

Today's reality

Data is everywhere, security is not

Organizations need help to:

- Identify where critical data is stored, how it's accessed and how to best protect it
- Holistically uncover risk, create and enforce policies, and protect data in motion and at rest
- Simplify the process of meeting compliance and privacy requirements
- Automate data protection and remediation

Data is at rest and in-use across
on-prem and hybrid clouds

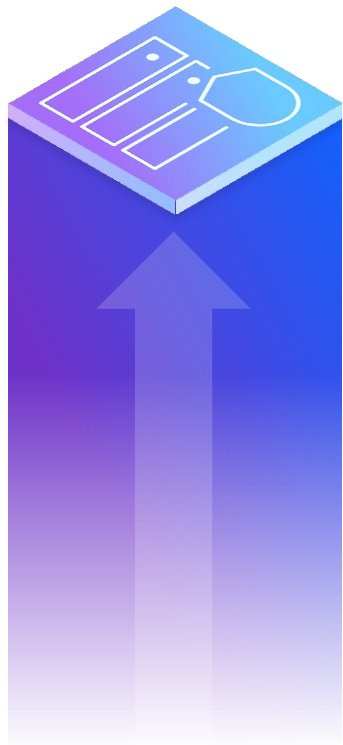


Data is accessed by siloed and distributed teams

Performing data security and compliance-driven activities using fragmented and disconnected tools



Protect data to accelerate business value



Reduce risk for cloud adoption

Implement a Zero Trust approach by centralizing data security and compliance across distributed hybrid cloud data sources

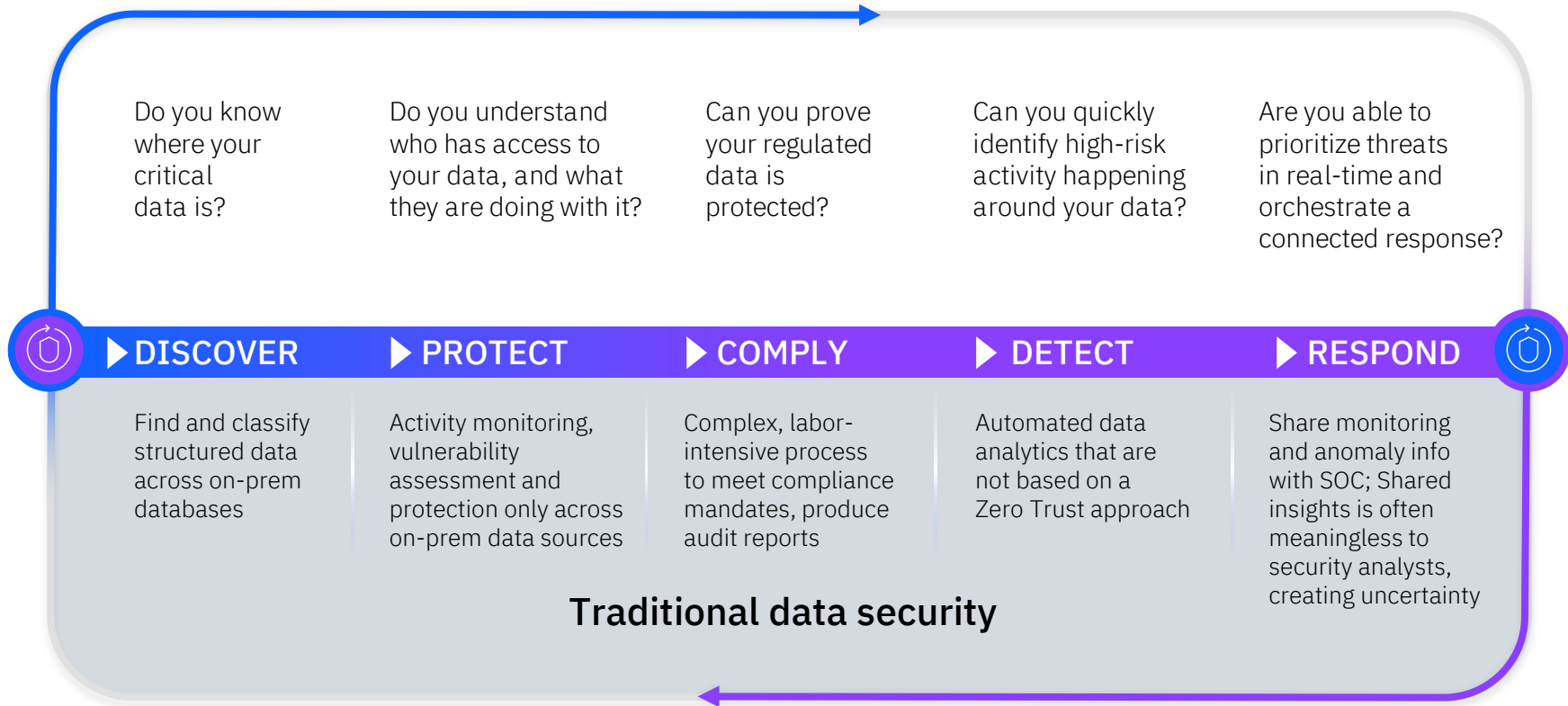
Proactively protect and respond

Enable teams to quickly visualize risk across disparate environments, automate processes, and respond quickly to suspicious activity

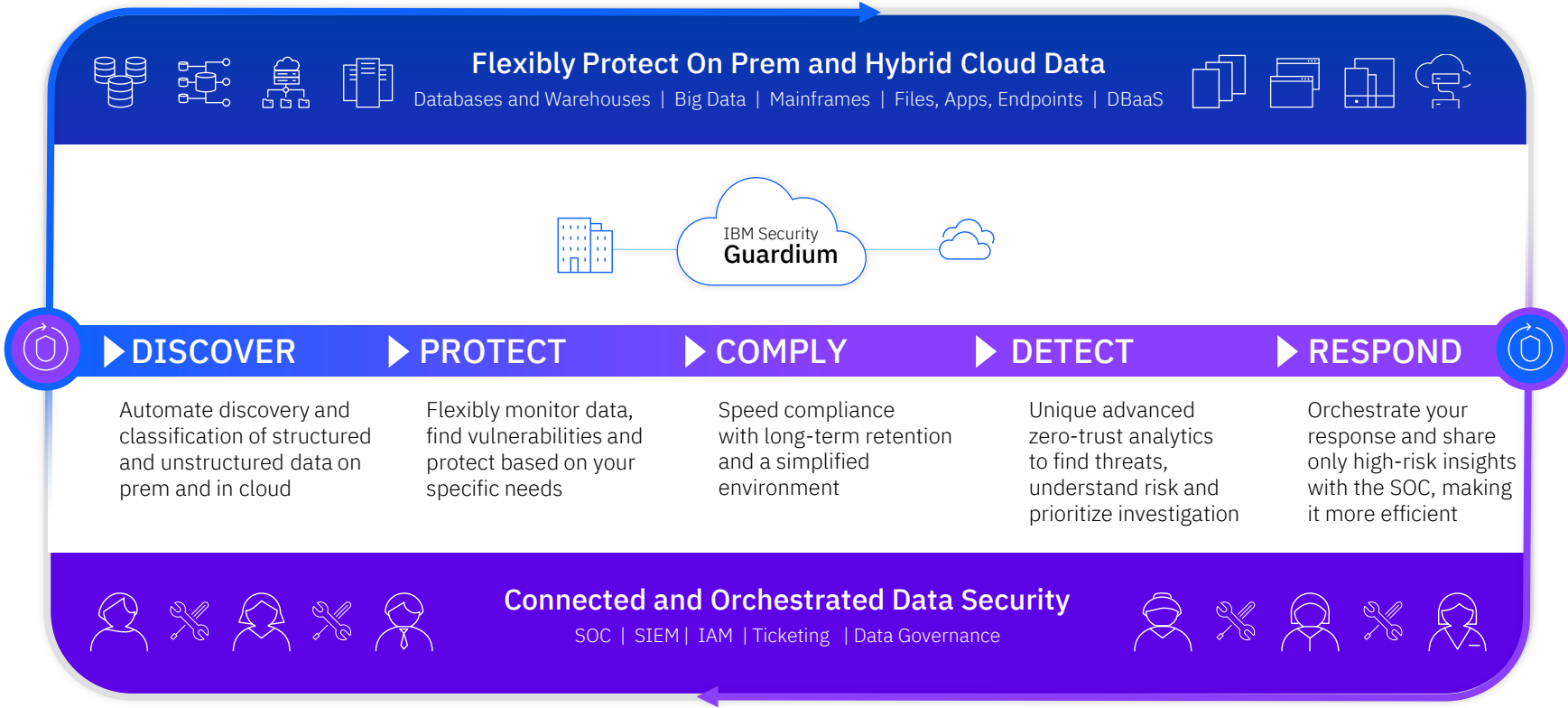
Safeguard data to build client trust

Help teams understand where sensitive data is, apply Zero Trust techniques to protect data in motion and at rest, and meet privacy requirements to create client trust

Where are you on your data security journey?



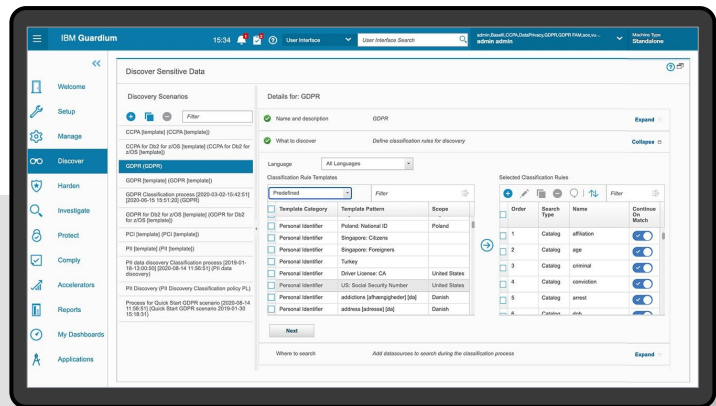
Protect data across the hybrid cloud



DISCOVER

Automate discovery and classification of on prem and cloud data and uncover vulnerabilities

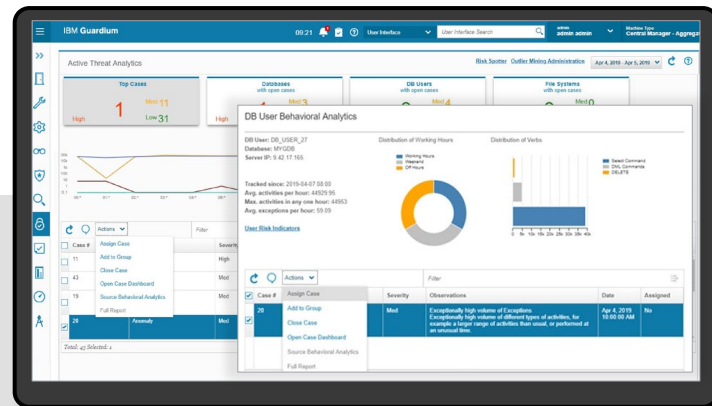
- Discover, classify, and catalog regulated structured and unstructured data
- Aggregate data for each data subject (individual) to help support DSRs
- Automate scanning to discover vulnerabilities, perform remedial actions, and track progress over time



PROTECT

Flexibly monitor data and protect based on your specific needs

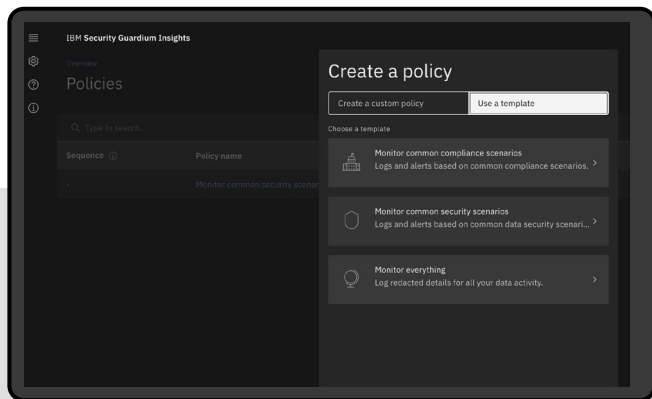
- Agent-based real-time monitoring across cloud and on-prem sources
- Automated Zero Trust analytics, active threat analytics, outlier detection, risk spotter help surface the 'needle in the haystack'
- Automate protective policy actions based on threats
- Flexibly protect with encryption, key management, real-time alerts, dynamic redaction, quarantining suspect IDs, and more



COMPLY

Speed compliance with long-term retention and a simplified environment

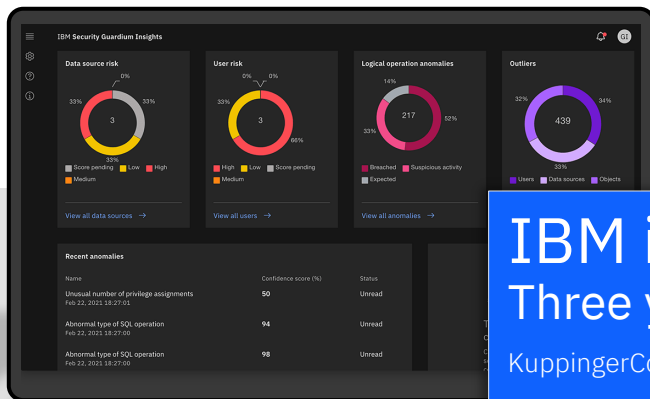
- Use out-of-the-box compliance policies, or easily create your own
- Reduce audit monitoring cost and complexity with agentless monitoring options to simplify the environment
- Long-term data retention helps enable faster, streamlined reporting and reduced TCO



DETECT & RESPOND

Unique advanced zero-trust analytics to find threats, understand risk and prioritize investigation

- Advanced analytics and risk scoring to identify unknown threats and take immediate action
 - Sequence-based predictive analytics to find unforeseen anomalies
 - Automated zero-trust analytics to reduce detection and response time
- Risk-based scoring to prioritize and orchestrate response in seconds across your SOC and ticketing systems



IBM is a LEADER
Three years in a row

KuppingerCole's Data Security Leadership Compass

Let IBM help you transform your business and manage risk with trusted advisors

Consulting Services

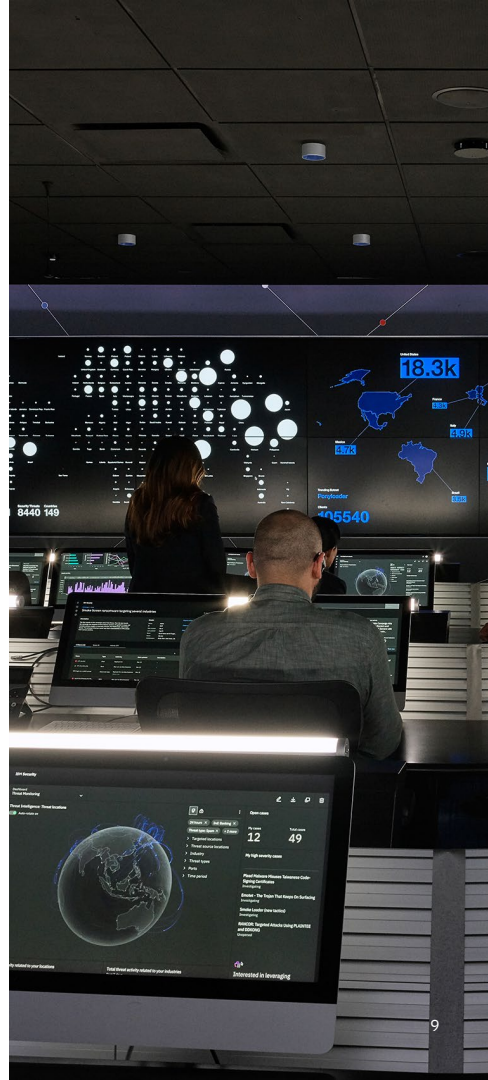
- Leverage our team of 5,500+ global security experts in 130 countries with deep industry and security domain expertise to help you understand, define, and execute your security program
- Expert technical guidance—with 1,200+ certifications in security and cloud solutions and platforms—to help implement, execute, and integrate new and existing technologies across your security architecture

Managed Services

- Trusted advisors available 24x7x365 to help augment your security program with tailored services, including threat, cloud, infrastructure, data, identity and response management
- 8 global security operations centers, 5 regional SOC locations, and local delivery capability
- Threat monitoring of more than 3 trillion MBs of data for 15K+ customers

IBM Security X-Force

- World-renowned team of hackers, responders, researchers, and analysts
- **X-Force Red**: Uncover high risk vulnerabilities and remediate them quickly
- **X-Force IR**: Reduce the impact of a breach and improve resiliency to attacks
- **X-Force Threat Intelligence**: Stay current on today's threat actors and indicators
- **Command Centers**: Hone your incident response and security leadership skills



Client success with IBM Security Guardium

360° visibility

“Prior to using Guardium, there was a lot of mystery around what was happening with our data. We’ve gained a view into where our data’s going and what it’s being used for.”

IT Security Domain Architect
Progressive Insurance

All-inclusive

“We can take advantage of that built-in functionality to give us a faster start, without having to build up things from scratch.”

Senior Governance Specialist
Insurance company

Effortless scalability

“Our old solution did not scale as well. Now we add more databases, and the same size team can absorb that into their daily workload, without having to hire new people.”

VP of Cyber Security Management,
Financial Services Institution

Peace of mind

“Because we are using Guardium and it’s monitoring 24x7, I sleep a lot better at night—and so does my management team.”

Data Security Engineer
Westfield Insurance

The Total Economic Impact of IBM Security Guardium

Through customer interviews and data aggregation, Forrester concludes IBM Security Guardium has the following three-year financial impact

Reduced probability of a breach by 40%




Increased automation saves 79 hours during database analysis

Effort required to complete an audit decreased by 75%

IBM Guardium is a
LEADER

KuppingerCole’s Leadership Compass
Database and Big Data Security

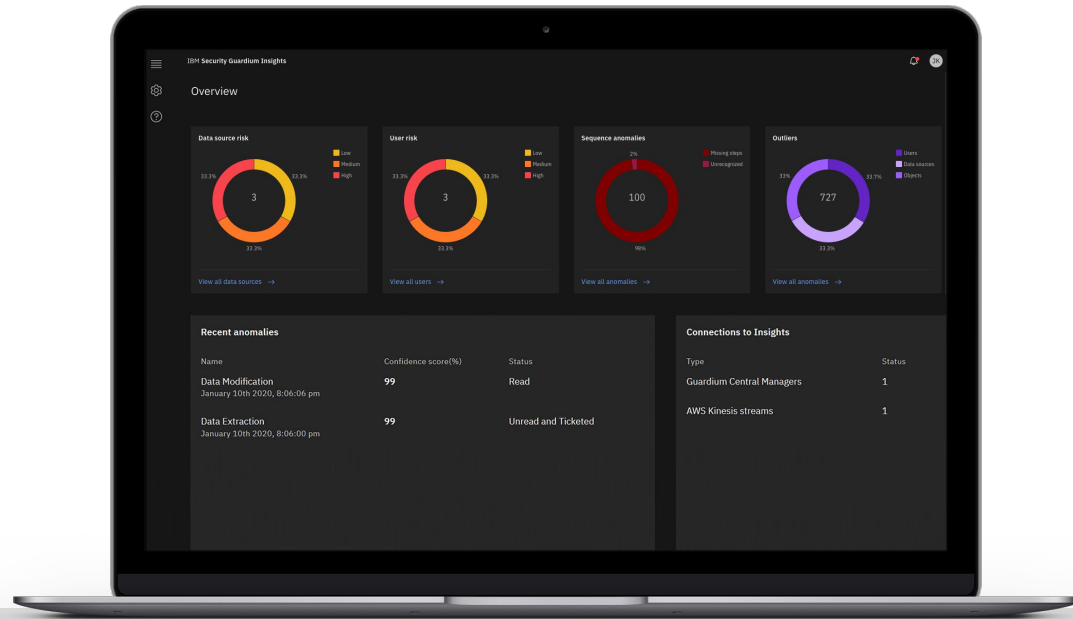
IBM Security solutions to deliver Zero Trust outcomes

	 Protect data across the hybrid cloud	 Secure the remote workforce	 Reduce the risk of advanced threats
Continuously verify	<ul style="list-style-type: none"> • Verify Access 	<ul style="list-style-type: none"> • Verify Access 	<ul style="list-style-type: none"> • Verify Access
Least privilege	<ul style="list-style-type: none"> • Verify Governance • Verify Privilege • Guardium Insights and Data Protection 	<ul style="list-style-type: none"> • Verify Governance • Verify Privilege • MaaS360 	<ul style="list-style-type: none"> • Verify Governance • Verify Privilege • MaaS360 • Guardium Insights and Data Protection
Assume breach	<ul style="list-style-type: none"> • QRadar XDR • IBM Security Discover and Classify • Guardium Insights and Data Protection 	<ul style="list-style-type: none"> • QRadar XDR • Guardium Insights • MaaS360 	<ul style="list-style-type: none"> • QRadar XDR • IBM Security Discover and Classify • Guardium Insights and Data Protection • MaaS360
IBM Security Services*	<ul style="list-style-type: none"> • Security Services for Cloud • X-Force Threat Management 	<ul style="list-style-type: none"> • Security Services for SASE • X-Force Threat Management 	<ul style="list-style-type: none"> • X-Force Threat Management
IBM Zero Trust Partners	Zscaler, Illumio	Zscaler, Illumio	Zscaler, Illumio Thycotic / Delinea

Manage your complete data security lifecycle with one integrated suite

IBM Security Guardium

- Adopt cloud with confidence
- Proactive protection and response
- Safeguard data to build client trust



DISCOVER

Automate discovery and classification of on prem and cloud data and uncover vulnerabilities

PROTECT

Flexibly monitor data and protect based on your specific needs

COMPLY

Speed compliance with long-term retention and a simplified environment

DETECT

Unique advanced zero-trust analytics to find threats, understand risk and prioritize investigation

RESPOND

Orchestrate your response and share only high-risk insights with the SOC, making it more efficient



Next steps towards modernizing your data security maturity

01

Schedule a Guardium consultation

ibm.biz/GuardiumConsult

02

View Guardium Insights in action

ibm.biz/GuardiumInsightsDemo

03

Learn more about Data Security Services

ibm.biz/DataSecServices

04

Quickly evaluate your current security practices


[Zero Trust Maturity Assessment](#)


Cybersecurity threat resources related to the Russia-Ukraine war

IBM Security resources to help support your organization with crisis management

[Book a one-on-one consultation to build a plan](#)

If you are experiencing cybersecurity issues or an incident, contact X-Force to help.

US hotline 1-888-241-9812 

Global hotline (+001)
312-212-8034 

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

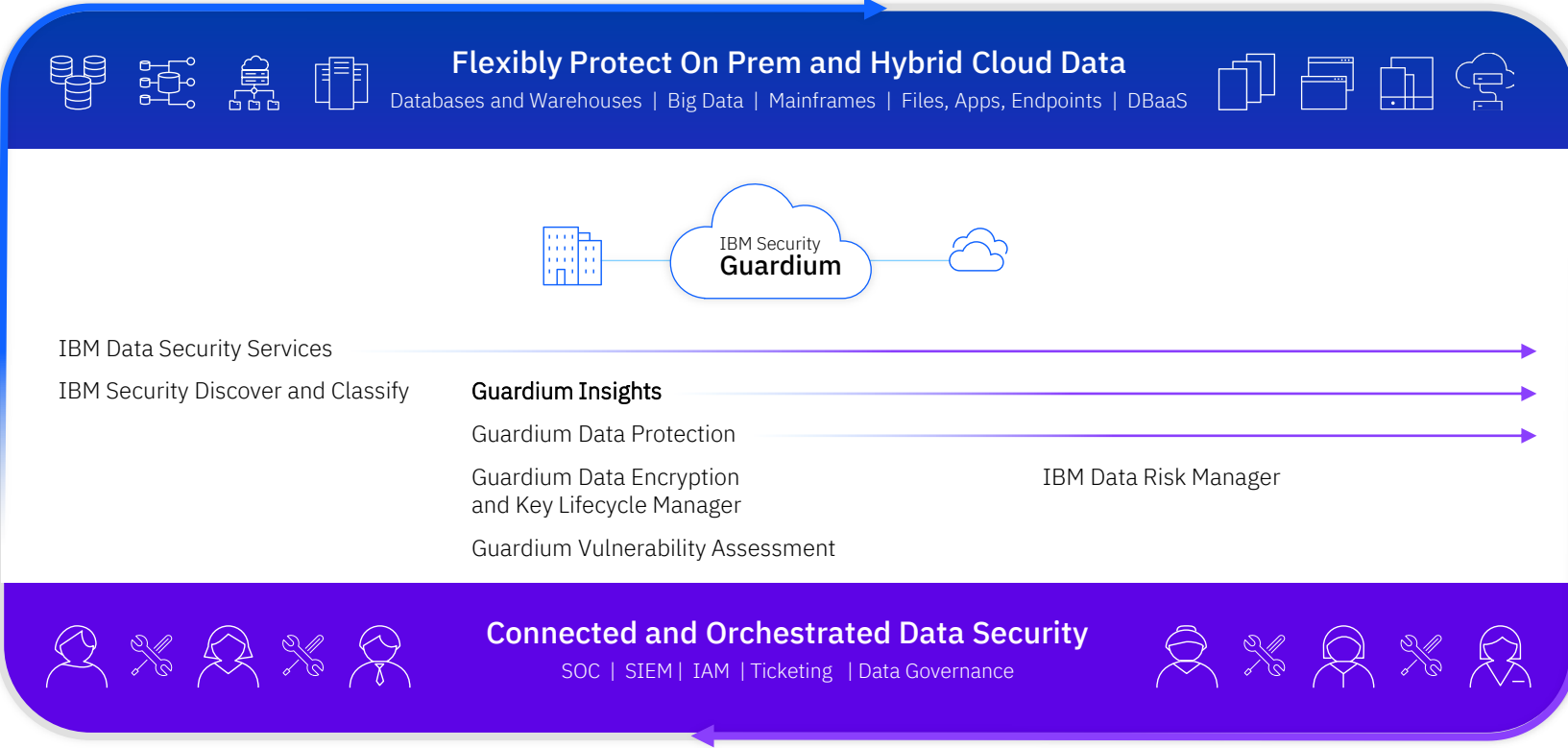
@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2022. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

Protect data across the hybrid cloud

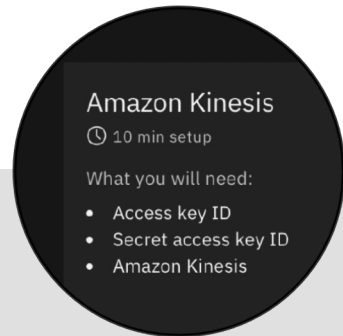


Protect data across the hybrid cloud

IBM Security Guardium: Data security for Zero Trust and modern environments

Monitor data across clouds

Built on Red Hat OpenShift and compatible with cloud data sources, including AWS Kinesis and Microsoft Azure Event Hubs



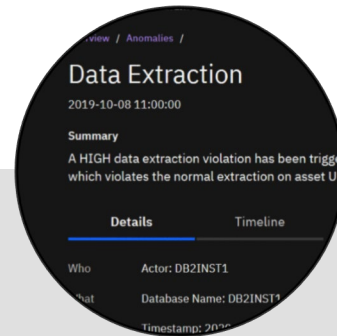
Discover and classify data

Automate discovery and classification of on premises and cloud data and uncover critical vulnerabilities



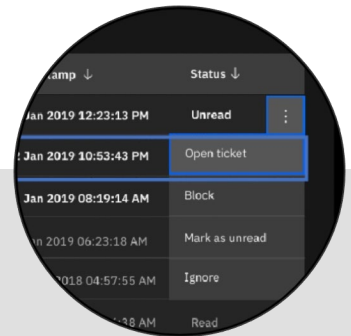
Help automate compliance

Generate reports and automate notification on long-term data activity within seconds, across the audit lifecycle



Detect Threats and Respond

Identify and respond to compliance and data security risks, across environments and teams, from one place



“Guardium is a huge product for us... prior to using it, there was a lot of mystery around what was happening with our data. What we’ve gained is a view into where our data’s going and what it’s being used for.”

Guardium can help reduce risk by unifying data security and data governance

Address compliance with industry and government regulations

Data Security IBM Security Guardium

- Real-time data access monitoring
- Enforce data governance policies
- Detect and remediate insider threats
- Protect workloads across hybrid cloud deployments

Data Governance IBM Cloud Pak for Data

- Document policies and privacy rules for governance and enforcement
- Discover and classify sensitive or regulated data stored across hybrid cloud
- Define user access rights to sensitive data

IBM Data Security Platform Vision

Deliver a single control point to visualize, prioritize and remediate risk

Governance, Risk and Compliance

Data (Access) Governance

Data Privacy

IBM Security
Guardium

- Ingest data security telemetry
- Create risk-based views and prioritization
- Push orchestrated policies
- Enforce everywhere

DISCOVER

PROTECT

COMPLY

DETECT

RESPOND

DLP

CASB

DLM

Other...

IBM Data Security Platform Vision, continued

How Guardium Insights becomes the centralized data security platform



Centralized risk views and response

- Pull in telemetry from data-related tools (vulnerabilities, classification, crypto-risk results, DLM issues, etc.)
- Manage role-based access and data access governance across structured and unstructured data
- Accelerate proactive data protection
- Context-based risk scoring enables faster prioritization and investigation
- Uncover threats faster with a range of machine learning and AI-driven analytics
- Guided, simplified experience

Efficient and connected protection

- Centrally create and manage policies and enforce across the data ecosystem
- Long-term retention for faster reporting
- Easy-to-use, automated audit workflows
- Flexible monitoring options to support audit and data security use cases
- Share only high-risk insights with SOC/SIEM to reduce labor and cost
- Centrally trigger encryption, check on key management, manage and remediate crypto-vulnerabilities, and more
- Streaming from agents, edge processor

Modernize GDP capabilities

- Risk-spotter, real-time trust evaluator, threat detection analytics, etc.
- Policy analyzer
- Mature custom reports
- Fine-grained data protection
- Next-generation vulnerability assessment