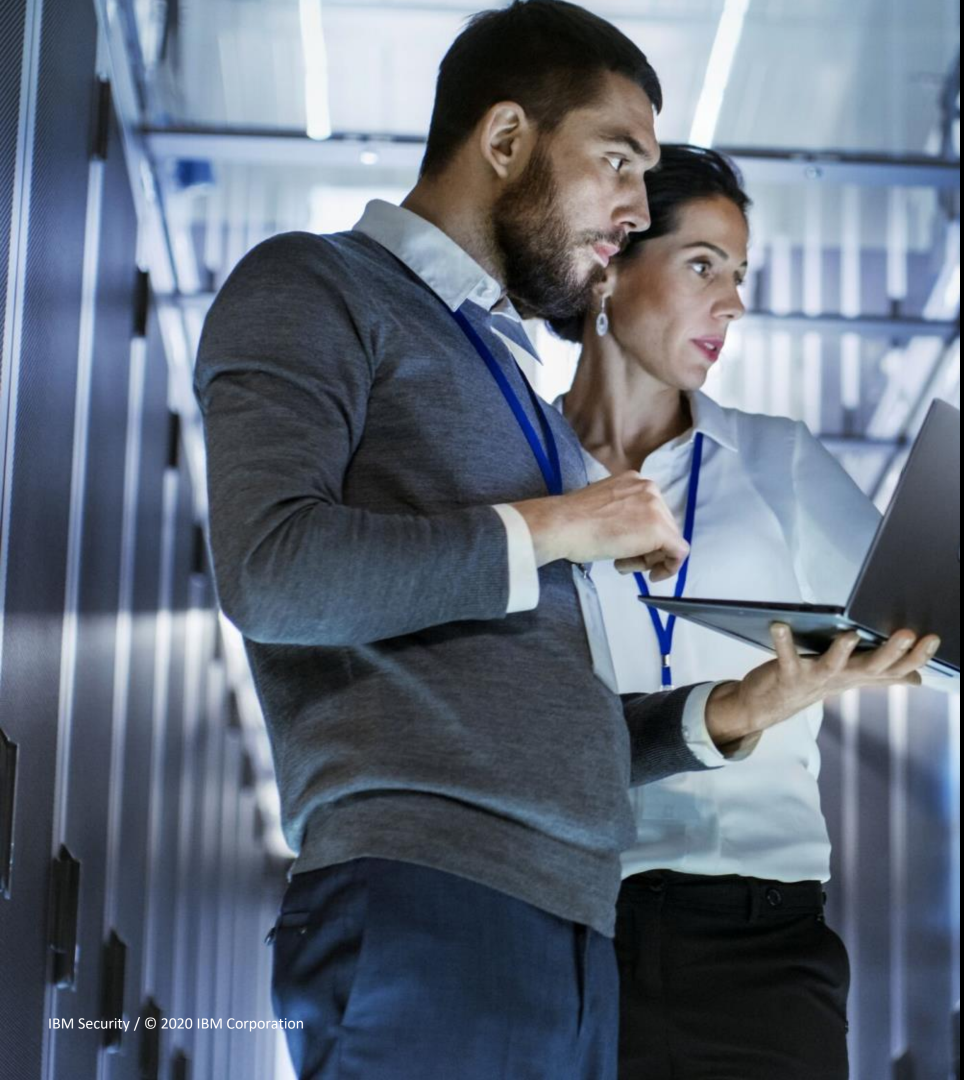
IBM Security Guardium

Smarter Data Security



Businesses are embracing hybrid multicloud to gain agility, competitive advantage and drive their organizations forward.

However, expanding the data footprint increases the organization’s attack surface, resulting in a host of new data security and compliance challenges.

Real world consequences

$11.45 million

Global average cost of an insider threat[1]

$3.92 million

Average cost of a data breach in 2019 for the organizations surveyed[2]

74%

Of organizations surveyed, 74 percent report being negatively impacted by a cybersecurity skills shortage.[3]

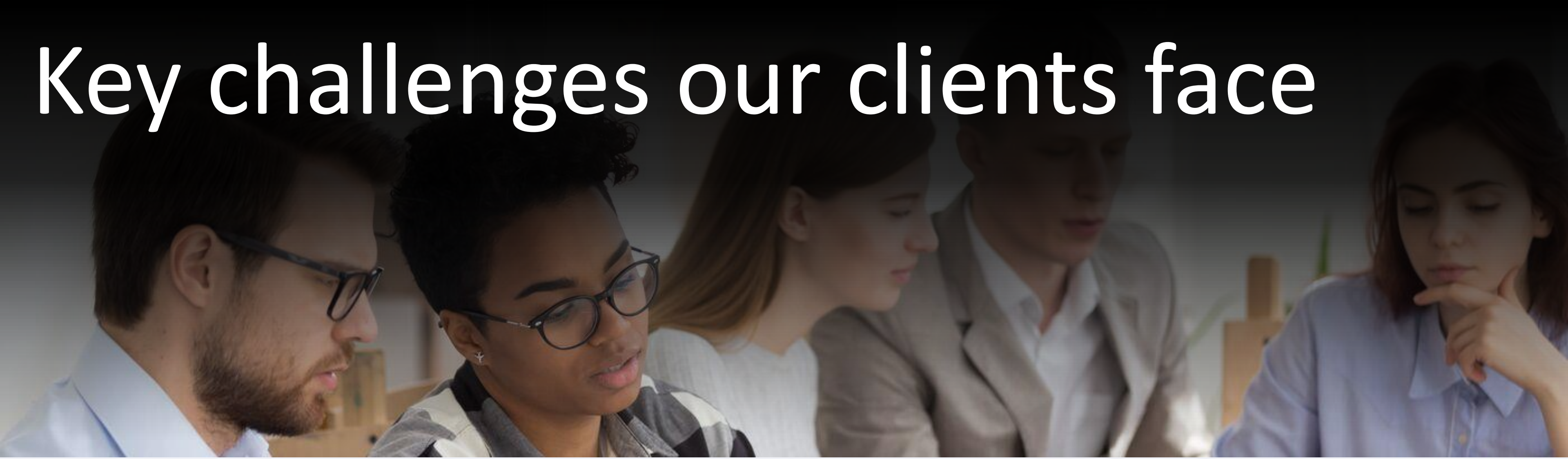
87%

87 percent of respondents stated that concerns around data security have adversely impacted usage of public cloud services.[4]

279 days

Average time to identify and contain a breach.[5]

Key challenges our clients face



Safeguarding against data breaches

Defending against insider threats

Protecting data across hybrid multicloud

Simplifying compliance

A smarter data security approach addresses key challenges across disparate IT environments

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

Assess risk with contextual insights and analytics

Protect sensitive data through encryption and flexible access policies

Monitor data access and usage patterns to quickly uncover suspicious activity

Respond to threats in real-time

Simplify compliance and its reporting

Environments & Data Sources

- Databases/Structured data
- Cloud
- Containers
- Big data/Semi-structured data
- Files/Unstructured data
- Mainframes
- Applications
- IoT

1. Discover and classify your sensitive data

- Find data on premises and in the cloud
- Classify data subject to specific regulations
- Identify data access and entitlement rights
- Visualize the flow of sensitive data

2. Assess risk with contextual insights and analytics

- Centralize security and compliance data
- Uncover patterns with predictive analytics
- Remediate, mitigate, and escalate issues

3. Protect sensitive data sources

- Encrypt, tokenize, and mask data
- Manage encryption keys
- Refine and implement entitlement policies
- Remove dormant accounts

4. Monitor data access to uncover suspicious activity

- See when, where, how, and who is accessing data
- Detect anomalous activity/unauthorized access
- Assess data risk and the business impact

5. Respond to threats in real-time

- Block and quarantine suspicious activity
- Suspend or shut down sessions
- Ensure workflows account for:
  - Data privacy and industry regulations
  - Span across data environments

6. Simplify compliance and audit reporting

- Ensure data security and compliance reporting covers regulatory mandates
- Confirm separation of duties through a continuous, fine-grained audit trail
- Integrate analytics from an open ecosystem of security products

We help clients get ahead of their challenges

Safeguard against data breaches

Centralize and correlate long-term security data from various tools and apply built-in advanced analytics to uncover, interpret and prioritize risk.

Defend against insider threats

Get a broad view of your risk posture. Define and enforce entitlement policies. Detect suspicious behavior and remediate.

Protect data across hybrid multicloud

Monitor access, identify and remediate vulnerabilities and apply data security controls across on-premises and cloud data repositories.

Simplify compliance

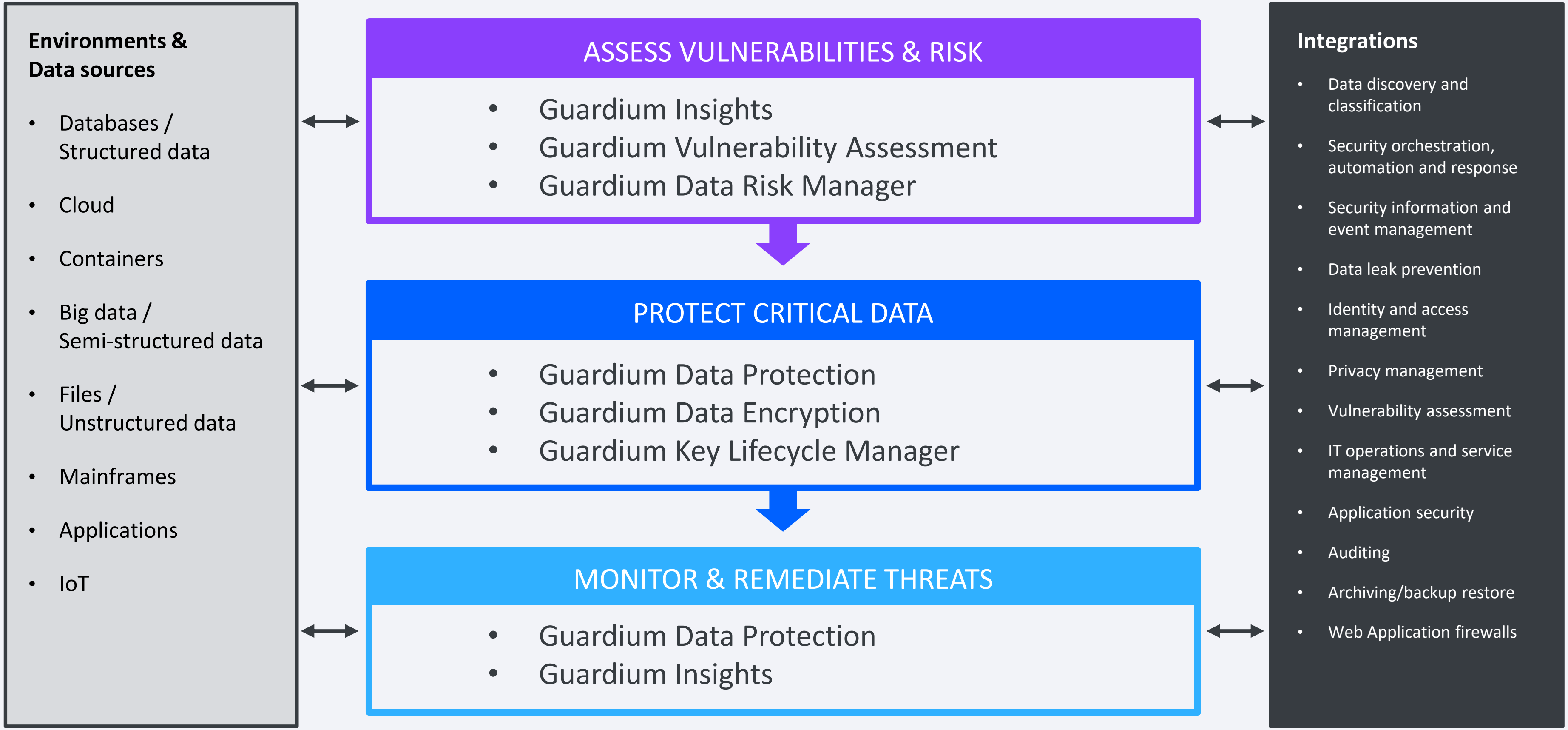
Identify sensitive data and uncover risks. Help simplify compliance through pre-built workflows and comprehensive reporting.

Feel free to reach out to us!

Sally Fabian, Worldwide Data Security Technical Lead
sefabian@us.ibm.com

Jesse Sedler, Offering Manager, Data Security
Jesse.sedler@ibm.com

Smarter Data Security with IBM Security Guardium



Environments & Data sources

- Databases / Structured data
- Cloud
- Containers
- Big data / Semi-structured data
- Files / Unstructured data
- Mainframes
- Applications
- IoT

ASSESS VULNERABILITIES & RISK

- Guardium Insights
- Guardium Vulnerability Assessment
- Guardium Data Risk Manager

PROTECT CRITICAL DATA

- Guardium Data Protection
- Guardium Data Encryption
- Guardium Key Lifecycle Manager

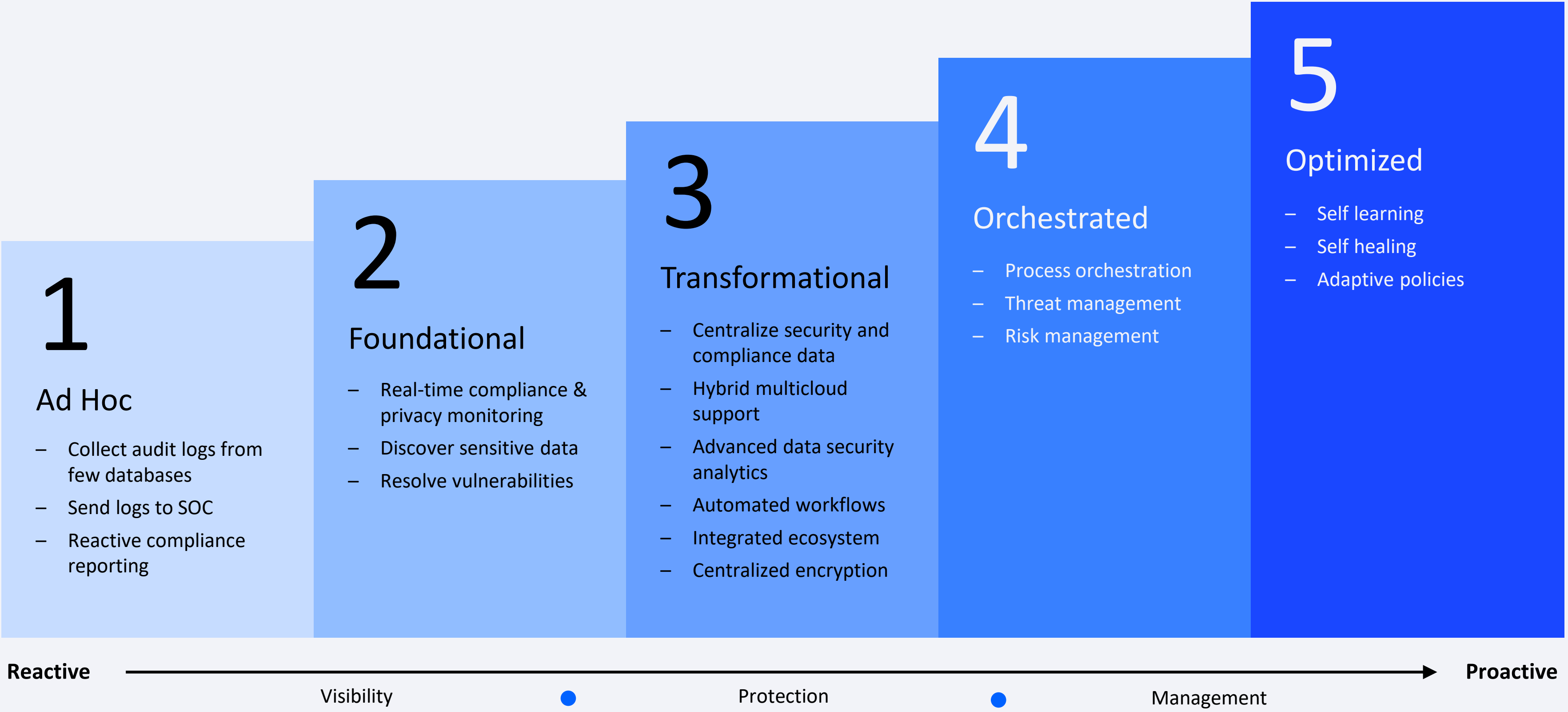
MONITOR & REMEDIATE THREATS

- Guardium Data Protection
- Guardium Insights

Integrations

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

Data security journey



1

Ad Hoc

- Collect audit logs from few databases
- Send logs to SOC
- Reactive compliance reporting

2

Foundational

- Real-time compliance & privacy monitoring
- Discover sensitive data
- Resolve vulnerabilities

3

Transformational

- Centralize security and compliance data
- Hybrid multicloud support
- Advanced data security analytics
- Automated workflows
- Integrated ecosystem
- Centralized encryption

4

Orchestrated

- Process orchestration
- Threat management
- Risk management

5

Optimized

- Self learning
- Self healing
- Adaptive policies

Reactive → **Proactive**

Visibility ● Protection ● Management

Client study finds Guardium improves efficiency and effectiveness in the protection of data:

65%

Following the deployment of Guardium Data Protection, 65% say their organizations recognized value in less than one month.

43%

Ability to accurately detect threats improved 43%

67%

Ability to detect data source vulnerabilities and misconfigurations increased by 67%

50%

Accuracy of data classification improved by 50%

42%

Time spent identifying and remediating data security issues decreased 42%

Source: “Ponemon Report: Client Insights on Data Protection with IBM Security Guardium,” Ponemon Institute, June 2019

Take the next step

Schedule

a consultation with one of our security experts to dive deeper into your challenges and use cases

Visit

IBM Security Guardium’s webpage for more information

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

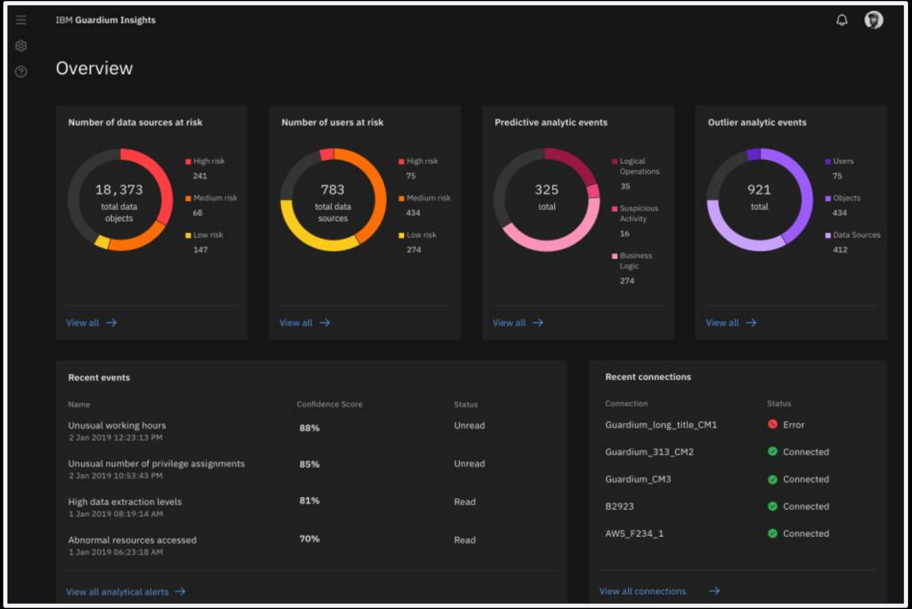
youtube.com/ibmsecurity

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.

IBM

IBM Security Guardium Insights

- Centralize, analyze and report on your data security and compliance data to uncover hidden threats.
- Analyze, apply advanced analytics across your on-premises and cloud hosted data stores security products so you can act on connected insights.
- Detect and respond, connect workflows in a centralized interface to respond to risks faster and orchestrate data security and compliance tasks using the same user experience.



Recent events

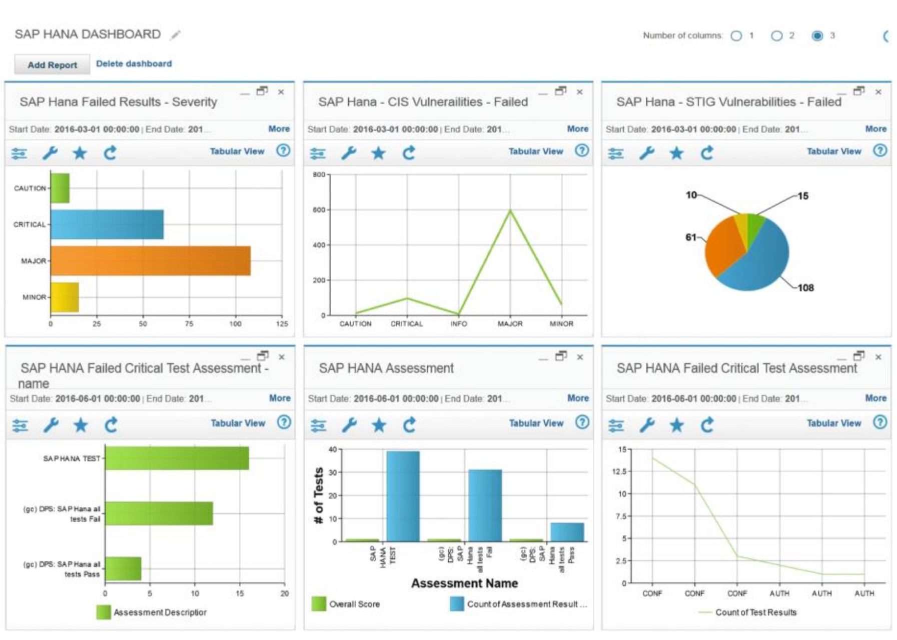
Name	Confidence Score	Status
Unusual working hours 2 Jan 2019 12:23:13 PM	88%	Unread
Unusual number of privilege assignments 2 Jan 2019 10:53:43 PM	85%	Unread
High data extraction levels 1 Jan 2019 08:19:14 AM	81%	Read
Abnormal resources accessed 1 Jan 2019 06:23:18 AM	70%	Read

Recent connections

Connection	Status
Guardium_long_title_CM1	Error
Guardium_313_CM2	Connected
Guardium_CM3	Connected
B2923	Connected
AWS_F234_1	Connected

IBM Security Guardium Vulnerability Assessment

- Scan-the entire data source infrastructure and provide platform-specific static tests, preconfigured vulnerability tests, and dynamic tests for behavioral vulnerabilities
- View and share detailed reports-and escalate to improve efficiency
- Remediate issues using detailed recommendation plans with simple, actionable steps to harden data sources
- Available reports include summary security evaluations, deep dives, sign-off, and scheduled assessments with automatic report distribution



SAP HANA DASHBOARD

Number of columns: ○ 1 ○ 2 ● 3

SAP Hana Failed Results - Severity

Start Date: **2016-03-01 00:00:00** | End Date: **201**...

SAP Hana - CIS Vulnerailities - Failed

Start Date: **2016-03-01 00:00:00** | End Date: **201**...

SAP Hana - STIG Vulnerabilities - Failed

Start Date: **2016-03-01 00:00:00** | End Date: **201**...

SAP HANA Failed Critical Test Assessment - name

Start Date: **2016-06-01 00:00:00** | End Date: **201**...

SAP HANA Assessment

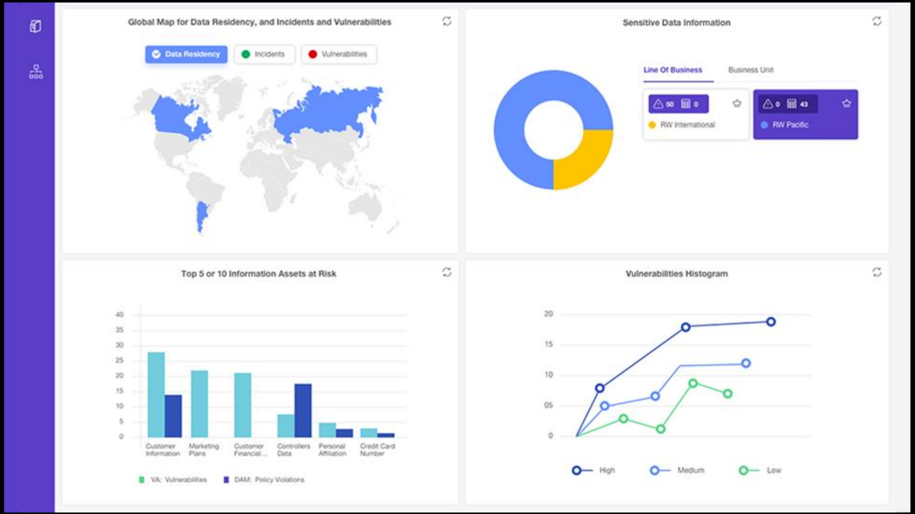
Start Date: **2016-06-01 00:00:00** | End Date: **201**...

SAP HANA Failed Critical Test Assessment

Start Date: **2016-06-01 00:00:00** | End Date: **201**...

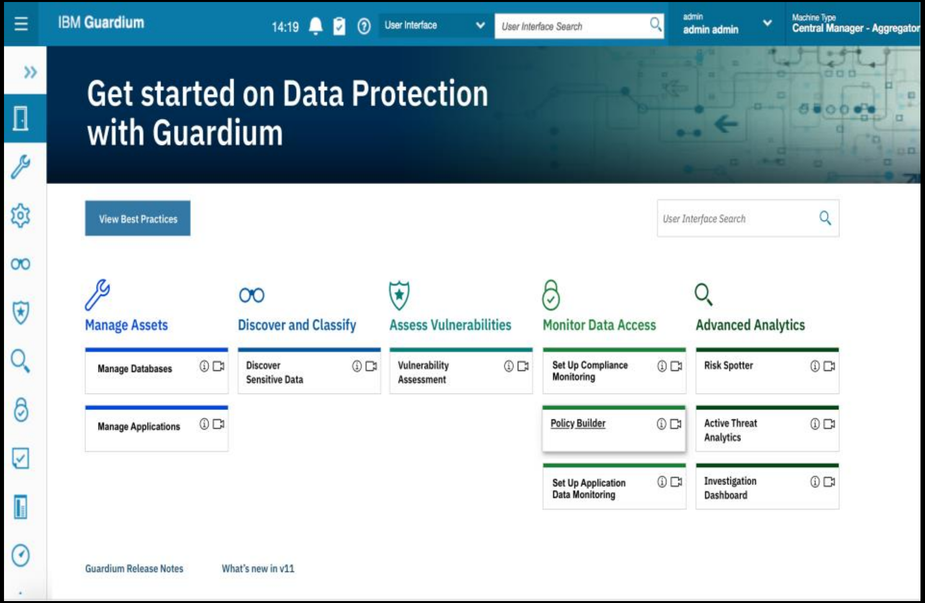
IBM Security Guardium Data Risk Manager

- Identify high-value, business-sensitive assets at risk from internal and external threats with interactive data risk control center
- Visualize potential business risks and provide remediation recommendations
- Communicate data-risk information across teams, business units and technologies to your board of directors with an executive-ready dashboard and reports



IBM Security Guardium Data Protection

- Identify and classify sensitive data across hybrid multi-cloud environments
- Visualize and understand risk holistically, and drill down to understand the root cause
- Quickly uncover and respond to suspicious insider threats and external breach attempts
- Simplify compliance through pre-built custom workflows
- Accelerate audit activities and get a tamper-proof audit trail
- Integrate with data security and IT service management tools



Get started on Data Protection with Guardium

Manage Assets
- Manage Databases
- Manage Applications

Discover and Classify
- Discover Sensitive Data

Assess Vulnerabilities
- Vulnerability Assessment

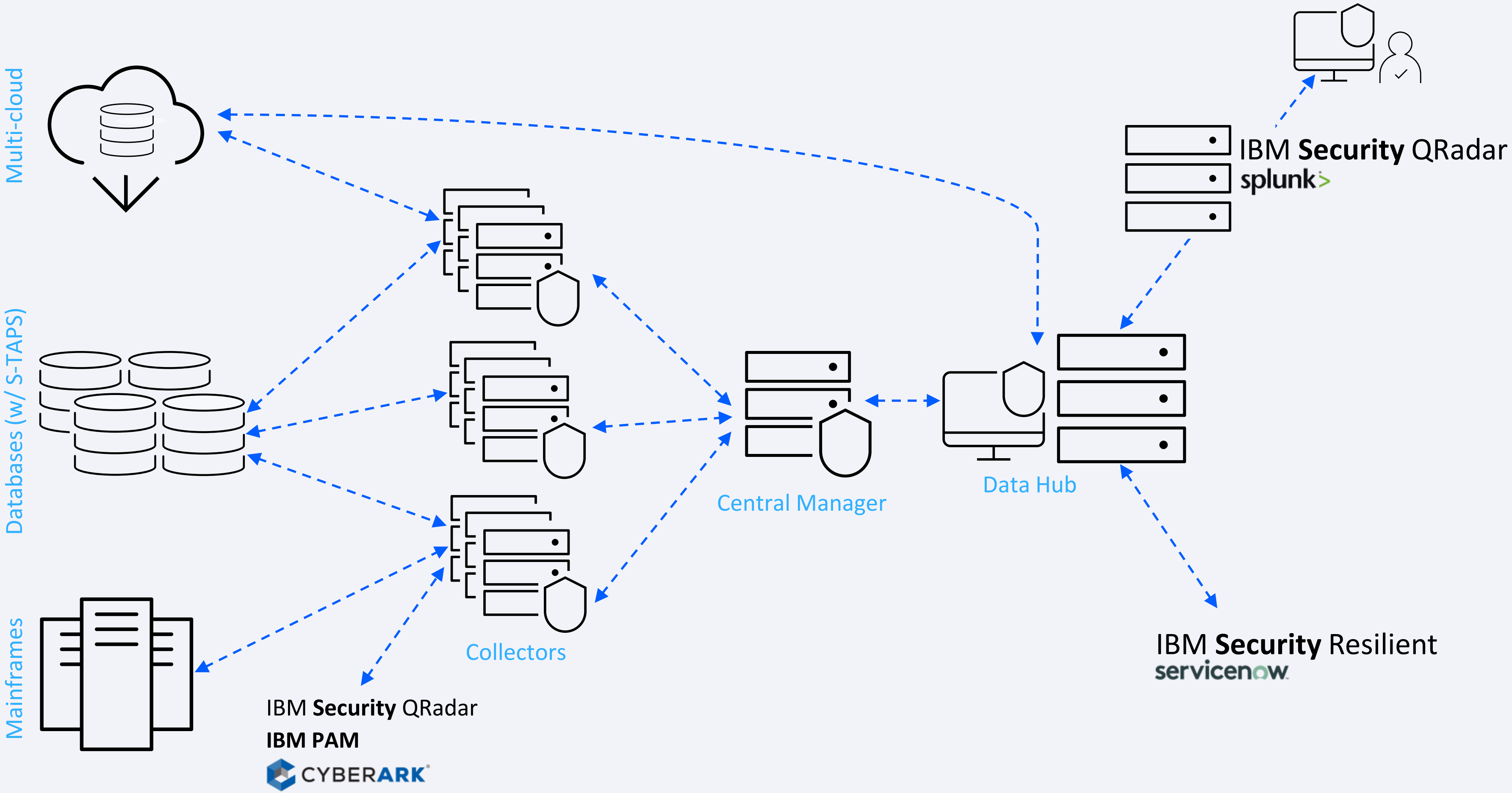
Monitor Data Access
- Set Up Compliance Monitoring
- Policy Builder
- Set Up Application Data Monitoring

Advanced Analytics
- Risk Spotter
- Active Threat Analytics
- Investigation Dashboard

Guardium Release Notes

What's new in v11

Guardium Federated, Interconnected System


Multi-cloud
Databases (w/ S-TAPS)
Mainframes
Collectors
Central Manager
Data Hub
IBM **Security** QRadar
splunk>
IBM **Security** Resilient
servicenow
IBM **Security** QRadar
IBM PAM
CYBERARK