IBM Security Guardium 11.3:

What's New in December?

Functionality drives value

Enrique Gutiérrez Álvarez

Data Security Sales Leader

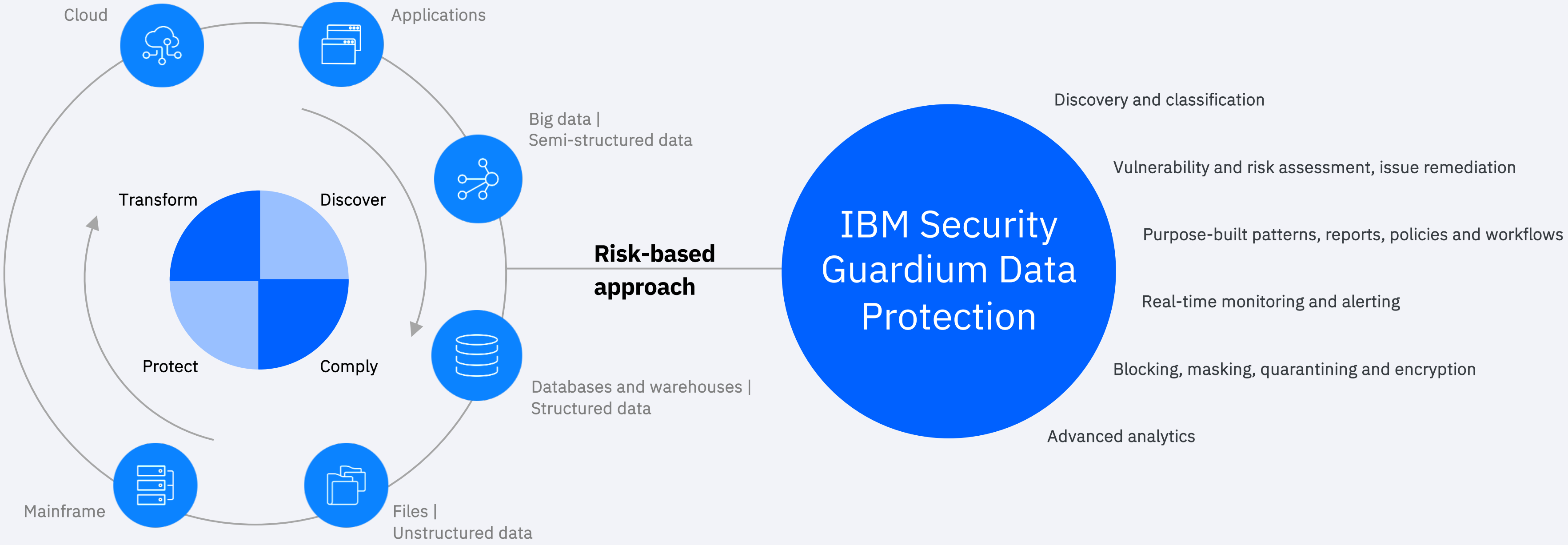
Public Sector, Federal, Healthcare Market

Enrique_Gutierrez@us.ibm.com

December 10th 2020

Guardium Data Protection empowers you to meet your critical data protection needs with smarter capabilities

Complete visibility — **Actionable insights** — **Real-time controls** — **Automated compliance**


Cloud
Applications
Big data |
Semi-structured data
Transform
Discover
Protect
Comply
Databases and warehouses |
Structured data
Mainframe
Files |
Unstructured data
Risk-based approach
IBM Security Guardium Data Protection
Discovery and classification
Vulnerability and risk assessment, issue remediation
Purpose-built patterns, reports, policies and workflows
Real-time monitoring and alerting
Blocking, masking, quarantining and encryption
Advanced analytics

The best of Data Security: Guardium Data Protection with Guardium Insights

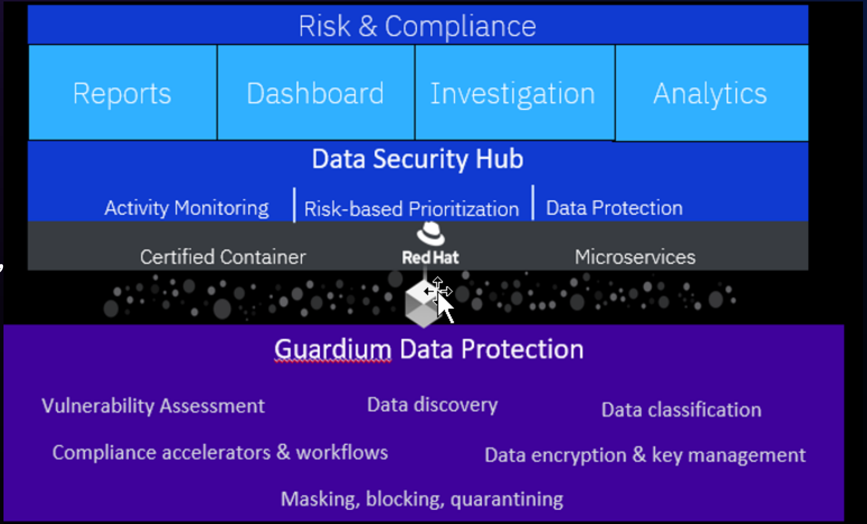
Guardium Data Protection ...

Simplifies compliance with monitoring, pre-built templates, policies & workflows

Deep capabilities with Discovery & classification, Real-time monitoring ,Dynamic data protection & separation of duties, Vulnerability assessment

Broad platform support across on-premises and cloud environments

Scales to support the largest environments



Guardium Insights ...

Retains collected data for years

Finds threats faster or as they happen

Makes it easy to prioritize response

Makes it easy to protect data across environments

Eliminates silos

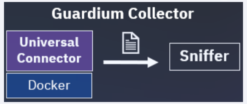
Delivers a modernized architecture

Deploys and scales flexibly – on premises or in public or private clouds

Guardium:
What’s new on 12/7?
MORE OF THE RIGHT STUFF!

Exciting capabilities GA in Guardium Data Protection 11.3!

Announce 10/20, GA 12/7



1 **Game changer!! Introducing the Universal Connector: A lightweight new way to monitor**

→ Supports **agentless streaming** of audit logs & provides a common framework to quickly develop new connectors

→ **Unlike GDDI agentless streaming**, we normalize the data for reporting & analytics

→ For traditional & modern sources: MongoDB and AWS S3 support in v11.3

2 **More support for modern Cloud environments. Drives down TCO & helps with modernization.**

→ Support for AWS Secrets Manager (AWS's cloud-based cyber vault)

→ Backup/restore on Azure & AWS

3 **Easier compliance with policy rules tagging. Faster time to value, lower TCO.**

→ Accelerators … only better! **New flexible** way to apply rules & policies for multiple regulations

→ Out-of-the box and custom tags

4 **Enhanced Unified Health & Deployment Dashboard. Helps reduce TCO. Terrific client feedback!!**

→ More tiles provide more insight into STAP & GIM health, at-a-glance

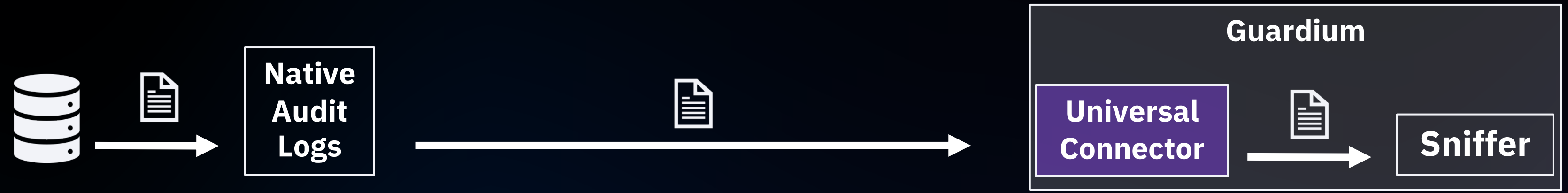
5 **Expanding 'connected Security'. Automation. Reduced TCO. Enhanced collaboration with SOC.**

→ Ticketing integration with IBM SOAR

→ Expanding integration with IBM Cloud Pak for Data to enforce governance policies

→ Classification support for MongoDB, vulnerability assessment for Couchbase

1 *Agentless* monitoring using the Guardium Universal Connector



Data source writes or pushes logs to storage

Pulls (or receives from Push) logs from data source

Captures: Session, Request, and Error info

Transforms logs into a universal format that the Sniffer understands

→ With the introduction of the Universal Connector, Guardium can support the most flexible options for monitoring and data collection:

- ✓ STAP for real-time monitoring of on-prem sources
- ✓ ETAP/Proxy for real-time monitoring of Cloud sources
- ✓ Agentless for passive monitoring for Cloud & on-prem sources
- ✓ API streaming for Cloud sources

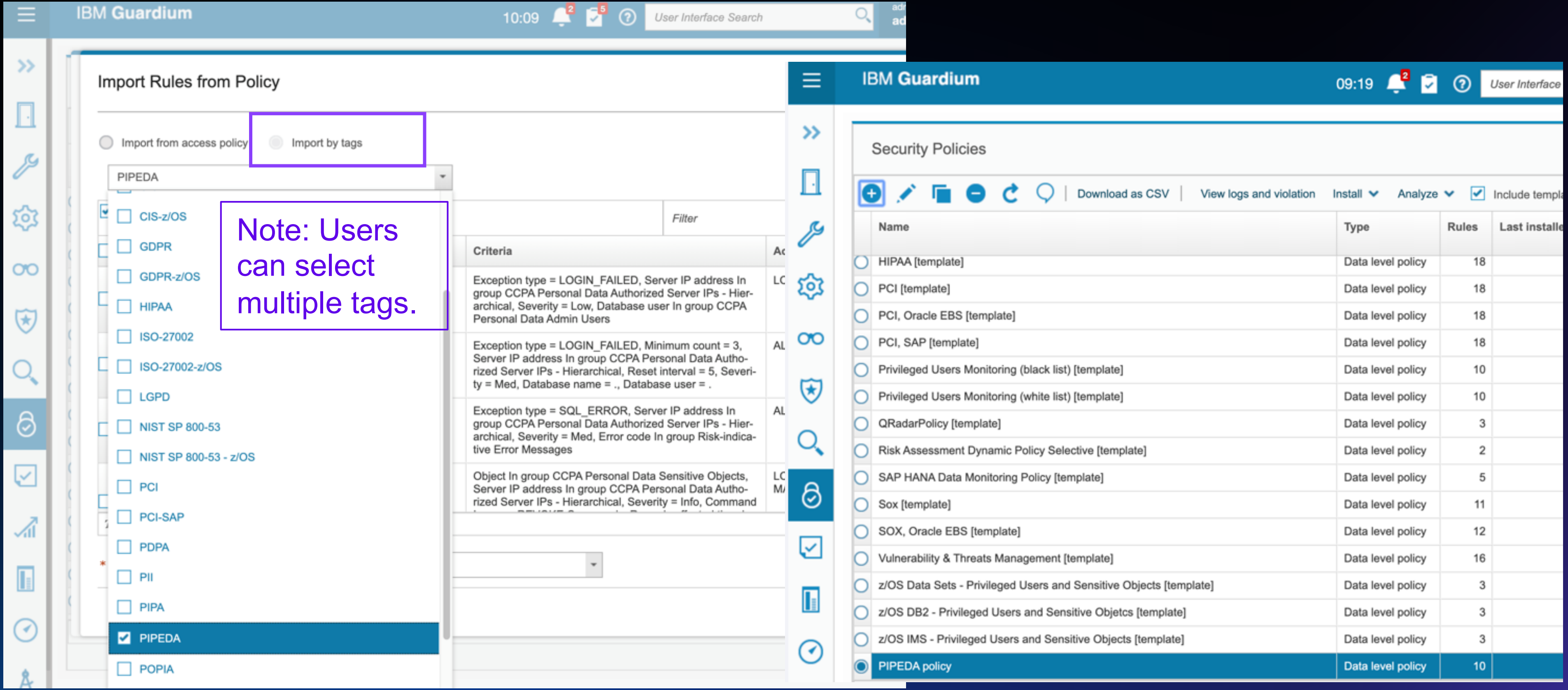
** Varies based on what is written to the native audit logs*

3 Next Gen Accelerators: Flexible tagging for faster, easier compliance

Supports two use cases

1) Create a new policy containing rules to support a regulation (PIPEDA) or multiple regulations

2) As a Guardium admin, I want to create a new policy containing rules to support PIPEDA.



Import Rules from Policy

○ Import from access policy ○ Import by tags

PIPEDA

- □ CIS-z/OS
- □ GDPR
- □ GDPR-z/OS
- □ HIPAA
- □ ISO-27002
- □ ISO-27002-z/OS
- □ LGPD
- □ NIST SP 800-53
- □ NIST SP 800-53 - z/OS
- □ PCI
- □ PCI-SAP
- □ PDPA
- □ PII
- □ PIPA
- ☑ PIPEDA
- □ POPIA

Note: Users can select multiple tags.

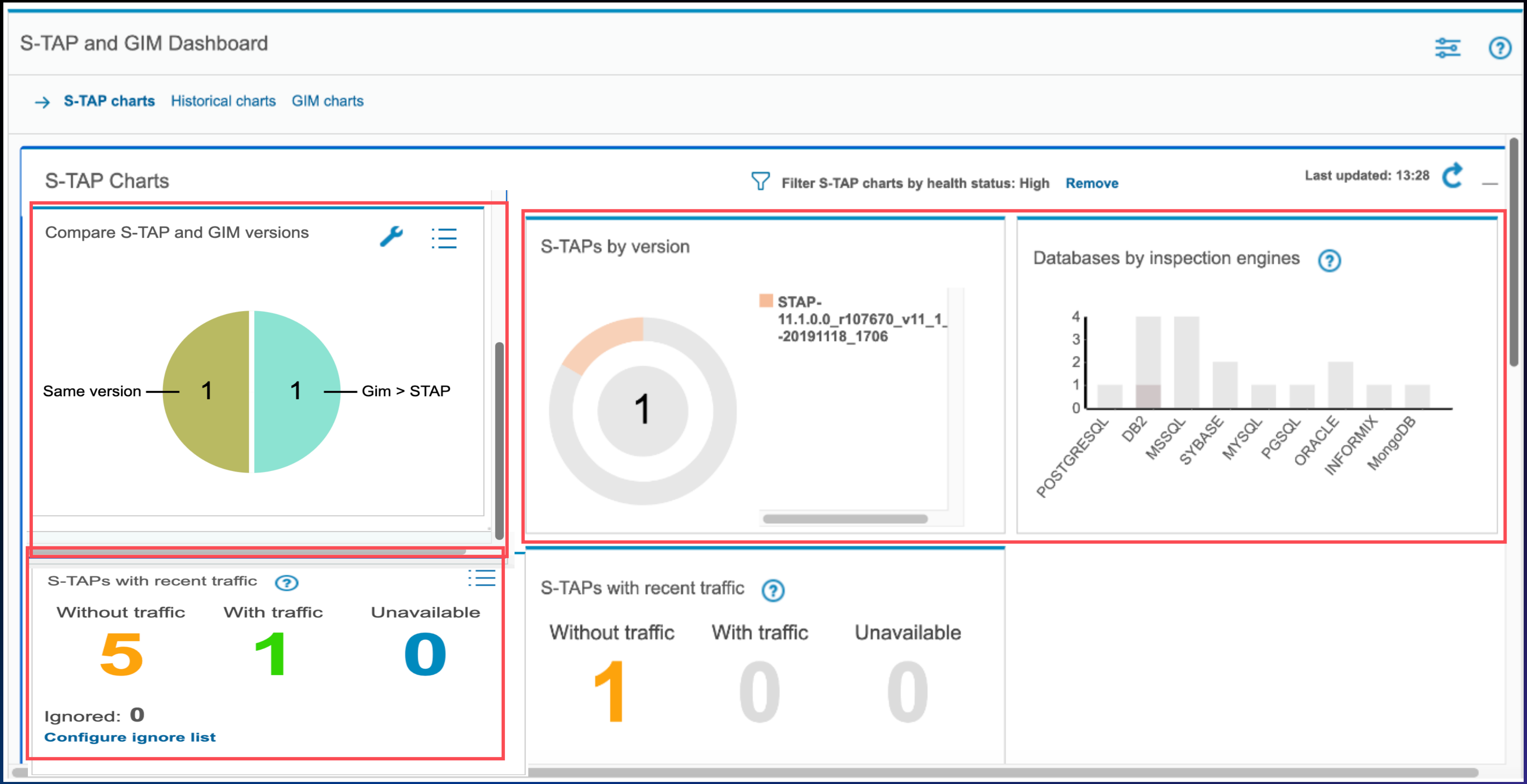
Filter

Criteria	Ac
Exception type = LOGIN_FAILED, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Low, Database user In group CCPA Personal Data Admin Users	LC
Exception type = LOGIN_FAILED, Minimum count = 3, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Reset interval = 5, Severity = Med, Database name = ., Database user = .	AL
Exception type = SQL_ERROR, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Med, Error code In group Risk-indicative Error Messages	AL
Object In group CCPA Personal Data Sensitive Objects, Server IP address In group CCPA Personal Data Authorized Server IPs - Hierarchical, Severity = Info, Command	LC M/

Security Policies

	Name	Type	Rules	Last installe
○	HIPAA [template]	Data level policy	18	
○	PCI [template]	Data level policy	18	
○	PCI, Oracle EBS [template]	Data level policy	18	
○	PCI, SAP [template]	Data level policy	18	
○	Privileged Users Monitoring (black list) [template]	Data level policy	10	
○	Privileged Users Monitoring (white list) [template]	Data level policy	10	
○	QRadarPolicy [template]	Data level policy	3	
○	Risk Assessment Dynamic Policy Selective [template]	Data level policy	2	
○	SAP HANA Data Monitoring Policy [template]	Data level policy	5	
○	Sox [template]	Data level policy	11	
○	SOX, Oracle EBS [template]	Data level policy	12	
○	Vulnerability & Threats Management [template]	Data level policy	16	
○	z/OS Data Sets - Privileged Users and Sensitive Objects [template]	Data level policy	3	
○	z/OS DB2 - Privileged Users and Sensitive Objetcs [template]	Data level policy	3	
○	z/OS IMS - Privileged Users and Sensitive Objects [template]	Data level policy	3	
●	PIPEDA policy	Data level policy	10	

4 New tiles on the Health Dashboard share more health insights



S-TAP and GIM Dashboard

→ **S-TAP charts** Historical charts GIM charts

S-TAP Charts

Filter S-TAP charts by health status: High **Remove**

Last updated: 13:28

Compare S-TAP and GIM versions

S-TAPs by version

Databases by inspection engines

S-TAPs with recent traffic

Without traffic	With traffic	Unavailable
5	1	0

Ignored: 0

Configure ignore list

S-TAPs with recent traffic

Without traffic	With traffic	Unavailable
1	0	0

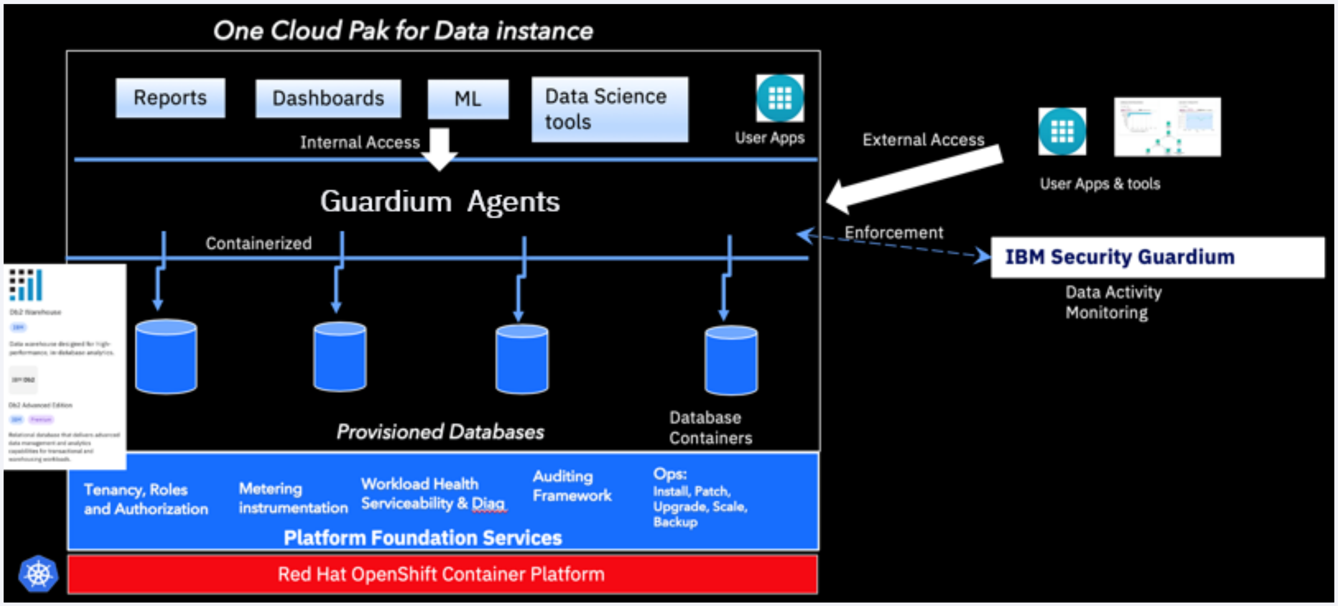
5 Connected Security Example: Guardium DP & CP4D: Help CP4D customers easily enforce their governance policies

Value

- ✓ Simplified out-of-box config in CP4D to secure data sources
- ✓ Monitor access and protect data
- ✓ Simplify security and compliance reporting
- ✓ Detect anomalous data usage & block suspicious activity

Competitive Differentiation

- ✓ CP4D + Guardium provides unique value – no competitors match up
- ✓ Tighter integration w/ IBM & Open Source DBs vs. competitors
- ✓ Improved total cost of ownership with integrated common platform
- ✓ End-to-end visibility & protection, which competitors lack in breadth



CP4D 3.0.1 data sources supported by GDP:

- ✓ DB2
- ✓ DB2 Warehouse
- ✓ Netezza Performance Server
- ✓ Big SQL
- Data Virtualization (1Q20)
- PostgreSQL (1Q21)
- Cockroach DB (1Q21)
- Mongo DB (1Q21)

Guardium Insights v2.5

Announce Oct. 10th, GA Dec. 7th

1

Help Guardium Data Protection clients reduce TCO by reducing reliance on aggregators and collectors. New in Guardium Insights v2.5:
— Customizable reports for power users
— Schedule and send reports to support audit workflows
— Create & manage groups in Guardium Insights

2

Integrate **vulnerability assessment** results in Guardium Insights for greater context and more efficient reporting

3

Simplify maintenance and enhance ease of use with streamlined installation & deployment, consolidated Guardium health APIs
— Improve Guardium operational maintenance with **agent health info**

4

Enable security analysts to **respond faster to data-related threats** with a seamless integration with the security operations center (SOC)
— Automated ticketing with SOAR in Cloud Pak for Security

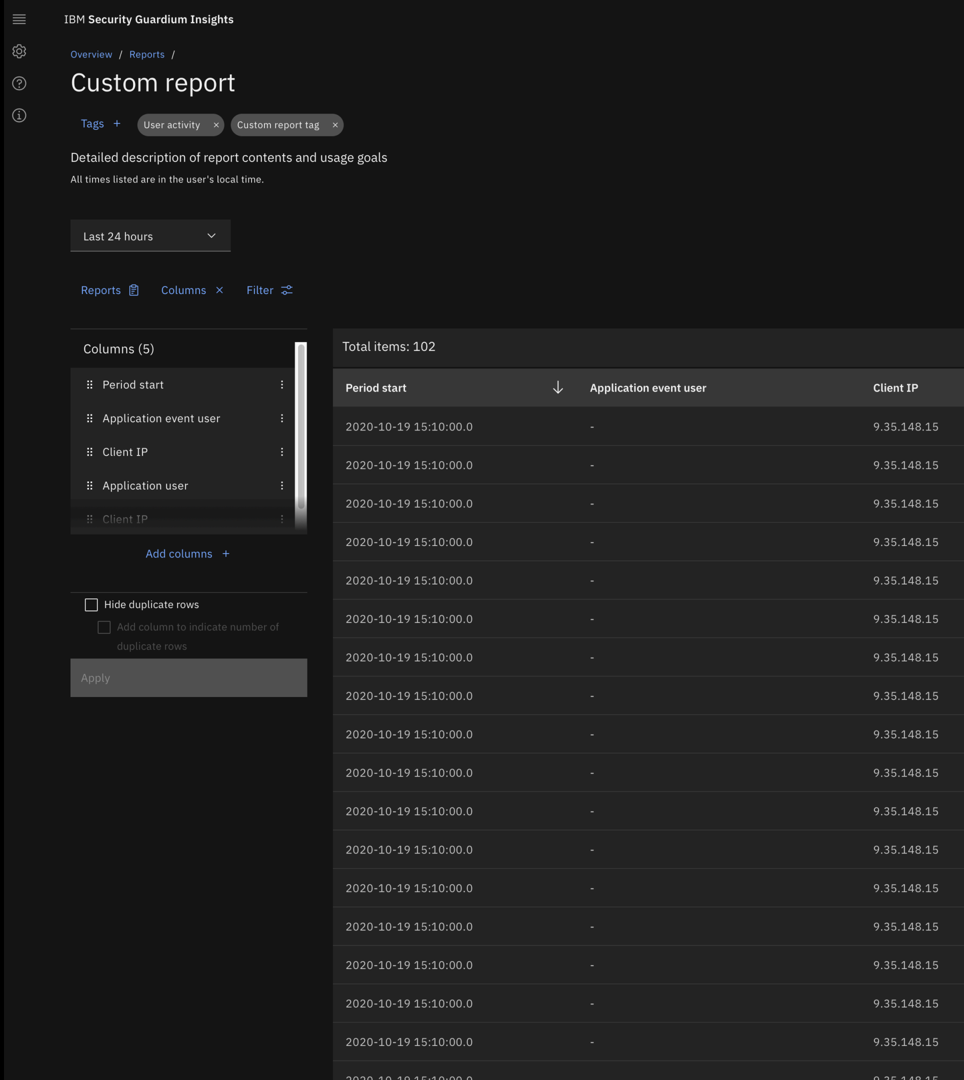
1 Reduce the need for GDP aggregators, improve TCO

Meet compliance standards faster and more easily with flexible, **customizable & repeatable reports** – built from scratch

Support automated audit processes with **scheduled reporting**

Create and manage groups in Guardium Insights, consolidated vulnerability assessment directly in Insights

Bottom line: Customers can phase out aggregators & collectors to streamline their legacy costs



IBM **Security Guardium Insights**

Overview / Reports /

Custom report

Detailed description of report contents and usage goals

All times listed are in the user's local time.

Columns (5)

- Period start
- Application event user
- Client IP
- Application user
- Client IP

☐ Hide duplicate rows

☐ Add column to indicate number of duplicate rows

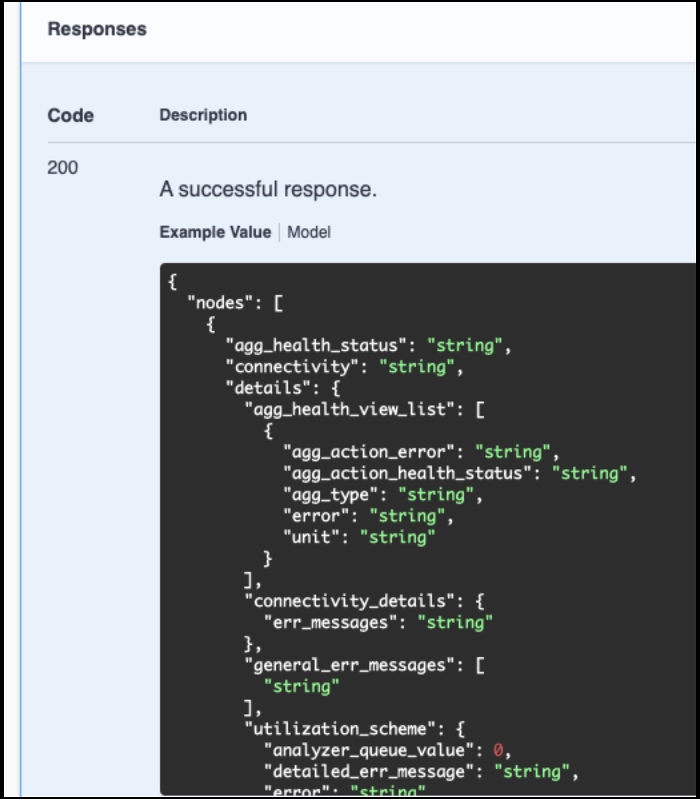
Total items: 102

Period start ↓	Application event user	Client IP
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0	-	9.35.148.15
2020-10-19 15:10:00.0		9.35.148.15

3 Simplified maintenance & deployment

Dramatically **streamlined installation** and deployment – ½ as many steps, get started faster

Simplify maintenance of Guardium infrastructure with consolidated **Guardium health APIs** – clients can feed their operational dashboards directly



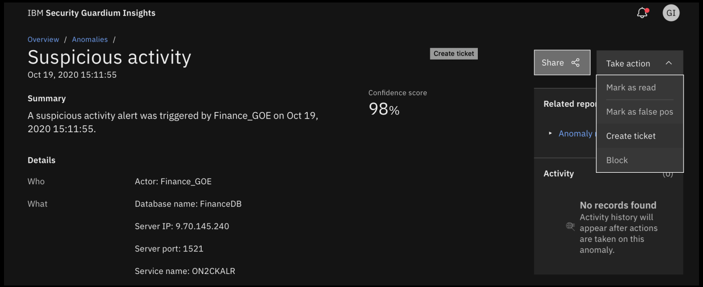
Responses

Code	Description
200	A successful response.

Example Value | Model

```
{
  "nodes": [
    {
      "agg_health_status": "string",
      "connectivity": "string",
      "details": {
        "agg_health_view_list": [
          {
            "agg_action_error": "string",
            "agg_action_health_status": "string",
            "agg_type": "string",
            "error": "string",
            "unit": "string"
          }
        ],
        "connectivity_details": {
          "err_messages": "string"
        },
        "general_err_messages": [
          "string"
        ],
        "utilization_scheme": {
          "analyzer_queue_value": 0,
          "detailed_err_message": "string",
          "error": "string"
```

4 Reminder! Clients can leverage data insights as they modernize their SOC



Suspicious activity

Oct 19, 2020 15:11:55

Confidence score

98%

Summary

A suspicious activity alert was triggered by Finance_GOE on Oct 19, 2020 15:11:55.

Details

Who Actor: Finance_GOE

What Database name: FinanceDB

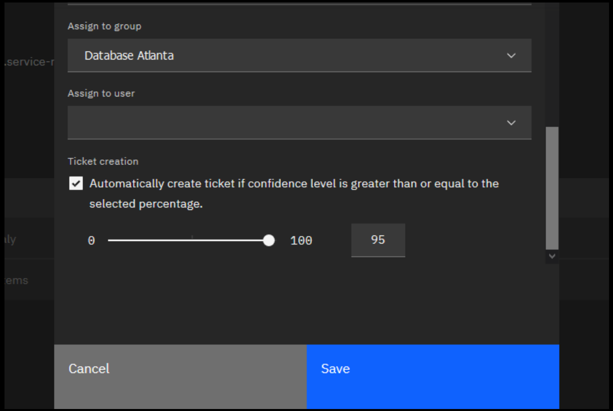
Server IP: 9.70.145.240

Server port: 1521

Service name: ON2CKALR

No records found

Activity history will appear after actions are taken on this anomaly.



Assign to group: Database Atlanta

Assign to user:

Ticket creation

☑ Automatically create ticket if confidence level is greater than or equal to the selected percentage.

0 100 95

Clients can now:

Simplify their IT architecture by using the same OpenShift environment for IBM Cloud Pak for Security and Guardium Insights

Enable their security operations center to **respond faster to data-related threats**

- **3 clicks** to open a ticket in cases or SOAR
- Ticket may be auto-populated with asset & risk info for the SOC team

IBM **Security**

THANK YOU

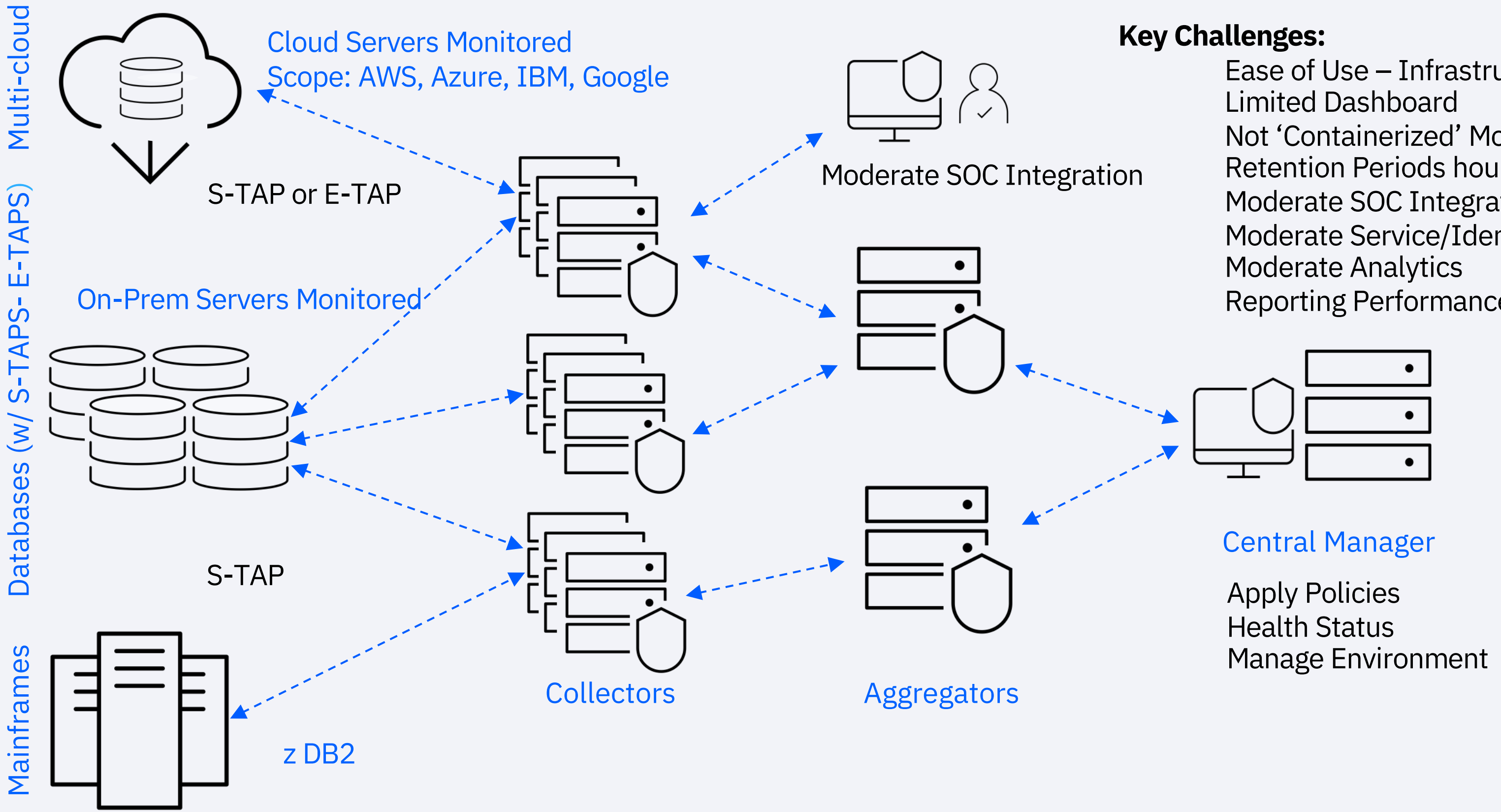
FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

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.

V8, V9, V10 –Guardium Implementation Architecture

Client Server Tiered Monitoring: S-TAP & E-TAP – Immediate Action, Regulatory Compliance

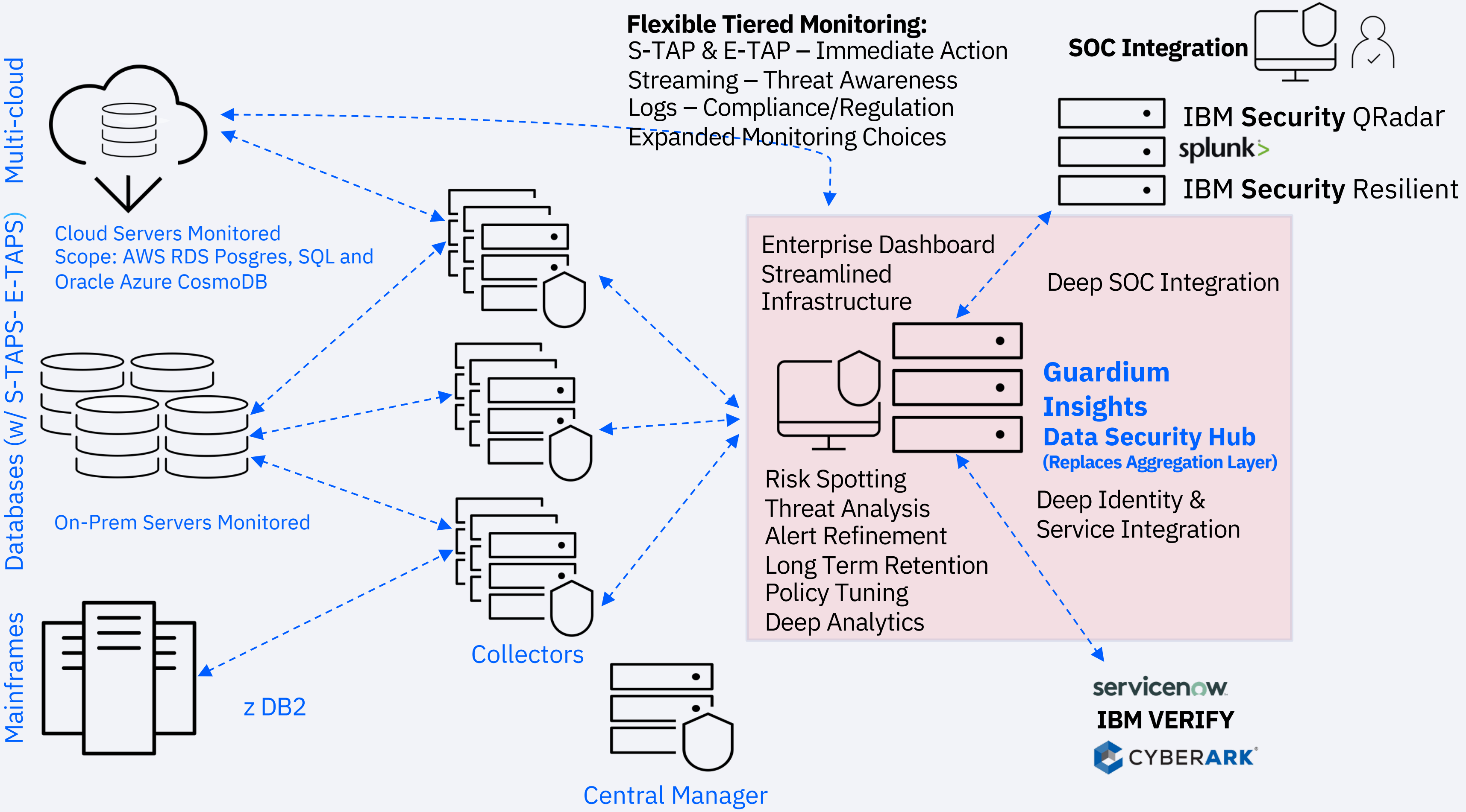


Apply Policies
Health Status
Manage Environment

Key Challenges:

Ease of Use – Infrastructure Management, Limited Dashboard
Not 'Containerized' Modern Architecture
Retention Periods hours/days
Moderate SOC Integration
Moderate Service/Identity Integration
Moderate Analytics
Reporting Performance Varies

Guardium v11 with Insights – Next Generation Architecture



Flexible Tiered Monitoring:
S-TAP & E-TAP – Immediate Action
Streaming – Threat Awareness
Logs – Compliance/Regulation
Expanded Monitoring Choices

SOC Integration

IBM **Security** QRadar
splunk>
IBM **Security** Resilient

Multi-cloud

Databases (w/ S-TAPS- E-TAPS)

Mainframes

Cloud Servers Monitored
Scope: AWS RDS Posgres, SQL and Oracle Azure CosmoDB

On-Prem Servers Monitored

z DB2

Collectors

Central Manager

Enterprise Dashboard
Streamlined Infrastructure

Deep SOC Integration

Guardium Insights
Data Security Hub
(Replaces Aggregation Layer)

Risk Spotting
Threat Analysis
Alert Refinement
Long Term Retention
Policy Tuning
Deep Analytics

Deep Identity & Service Integration

servicenow
IBM VERIFY
CYBERARK

IBM Security Guardium Insights Differentiators

Our Guardium Platform is purpose-built to accelerate Data Security Programs to Identify, Classify, and Protect sensitive data across the enterprise

Enterprise Data Security Hub and Dashboard

Cloud-Ready, Micro-Services, Enterprise Data Security Hub and Dashboard leveraging flexible data source monitoring, Machine Learning and Advanced Analytics for Outlier Detection, Risk Spotting and Privileged User Access Control.

Risk-Based Normalized Analytics Engine

Use Machine-Learning to identify Data Security Risks. Establish effective granular policies and rules to alert on potential data security hot spots. Surface exposures based on weighted data sensitivity.

Contextual Integration with SIEM/SOC

Pre-built Integrations to SIEM/SOC tooling with advanced contextual alerting to reduce false-positives and provide easy ‘drill-down’ functionality for SOC Analysts. Intuitive GUI for enriched investigations.

Long-Term Retention

Retain years of Data Security Data in a normalized Data Lake. Perform advanced user behavior and threshold analytics across time. Capture and retain critical Privacy data.

Advanced Cloud-Ready Data Security

Advanced relationships with Cloud Providers enables timely flexible pre-built high-performance normalized Cloud Data Security Protection and Monitoring for both IaaS and DBaaS Cloud environments.

Compliance Reporting Accelerators

Tried and tested Pre-Built Identification and Classification algorithms to speed time to value. Pre-Built Accelerators for critical regulatory reporting and audit response.

Guardium Insights customer-facing assets

Blog: Slowing Data Security Tool Sprawl in a Hybrid Multicloud World

Marketplace page: IBM Security Guardium Insights

Data Sheet: IBM Guardium Insights Data Sheet

Explainer Video: Exploring Guardium Insights

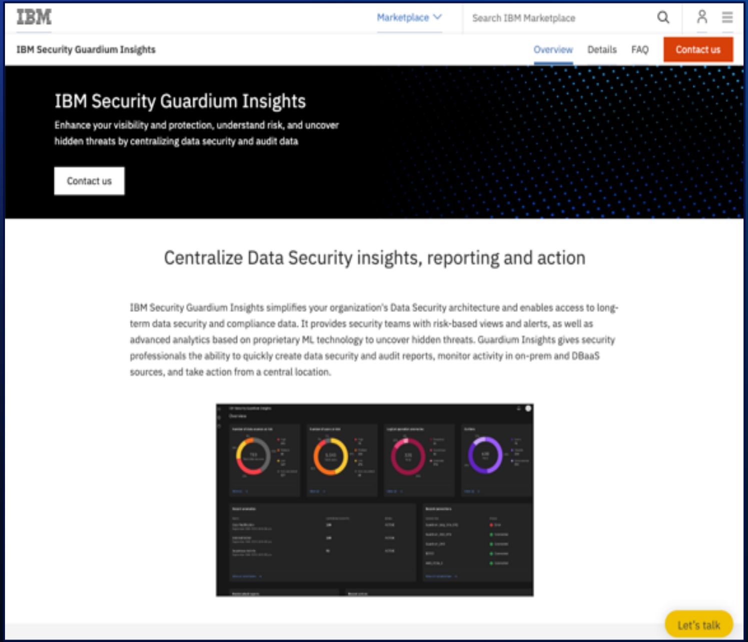
Demo: Product tour

Infographic: Unifying Data Security with IBM Security Guardium Insights

FAQs: Frequently Asked Questions

IDC Next Gen Data Security Assets: White paper, Webcast, Blog

Ebooks: 5 Pitfalls of Data Security & Overcoming data security challenges in a hybrid multicloud world



IBM Security Guardium Insights

Enhance your visibility and protection, understand risk, and uncover hidden threats by centralizing data security and audit data

Centralize Data Security insights, reporting and action

IBM Security Guardium Insights simplifies your organization's Data Security architecture and enables access to long-term data security and compliance data. It provides security teams with risk-based views and alerts, as well as advanced analytics based on proprietary ML technology to uncover hidden threats. Guardium Insights gives security professionals the ability to quickly create data security and audit reports, monitor activity in on-prem and DBaaS sources, and take action from a central location.

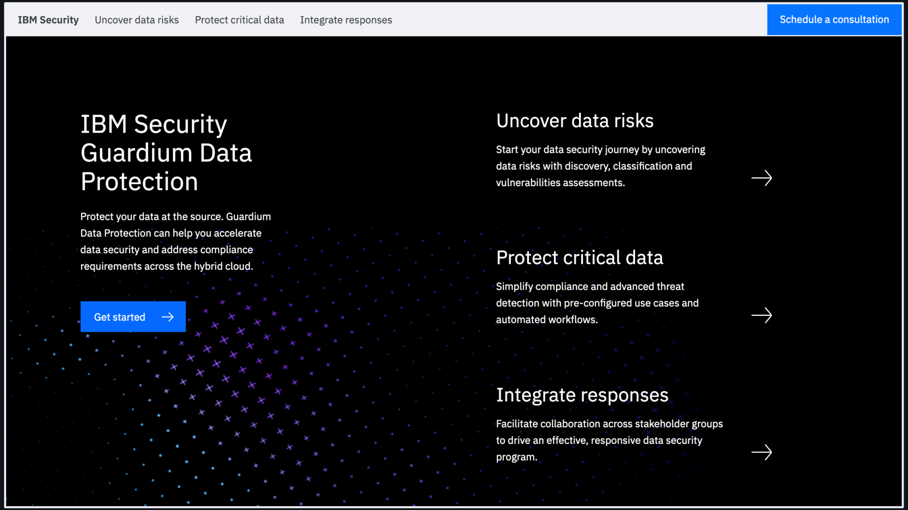
Public-facing assets for Guardium Data Protection

Marketing assets:

- Smarter Data Security ebook and PDF
- 5 Common Data Security Pitfalls to Avoid e-book
- Overcoming data security challenges… e-book
- Guardium Data Protection solution brief
- Guardium Data Protection for SAP HANA data sheet

Webinars and tech talks:

- Webinar: "Containers and Data Security: What You Need to Know"
- Webinar: "End-to-end data activity monitoring services and solution provide smarter data security"
- Tech Talks:
  - Hybrid multi-cloud data protection with IBM Security Guardium
  - Securing SAP Hana deployments with IBM Security Guardium
  - How CSOs can leverage their security infrastructure to comply with privacy mandates



IBM Security Uncover data risks Protect critical data Integrate responses Schedule a consultation

IBM Security Guardium Data Protection

Protect your data at the source. Guardium Data Protection can help you accelerate data security and address compliance requirements across the hybrid cloud.

Get started →

Uncover data risks

Start your data security journey by uncovering data risks with discovery, classification and vulnerabilities assessments. →

Protect critical data

Simplify compliance and advanced threat detection with pre-configured use cases and automated workflows. →

Integrate responses

Facilitate collaboration across stakeholder groups to drive an effective, responsive data security program. →

Product tours and demos:

- Guardium Data Protection Product Tour (Qwik Tour)
- Guardium Data Protection interactive demo