

IBM Security Guardium Insights for IBM Cloud Pak for Security

Reed Shea

Offering Management

IBM Security Guardium Insights

Ryan Schwartz

Product Marketing

IBM Security Guardium Insights

Digital transformation is accelerating



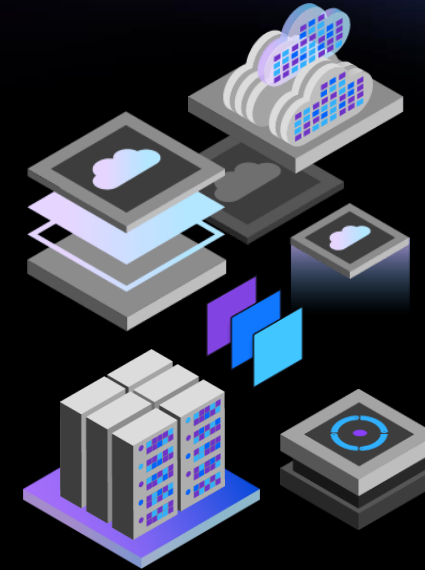
Applications

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



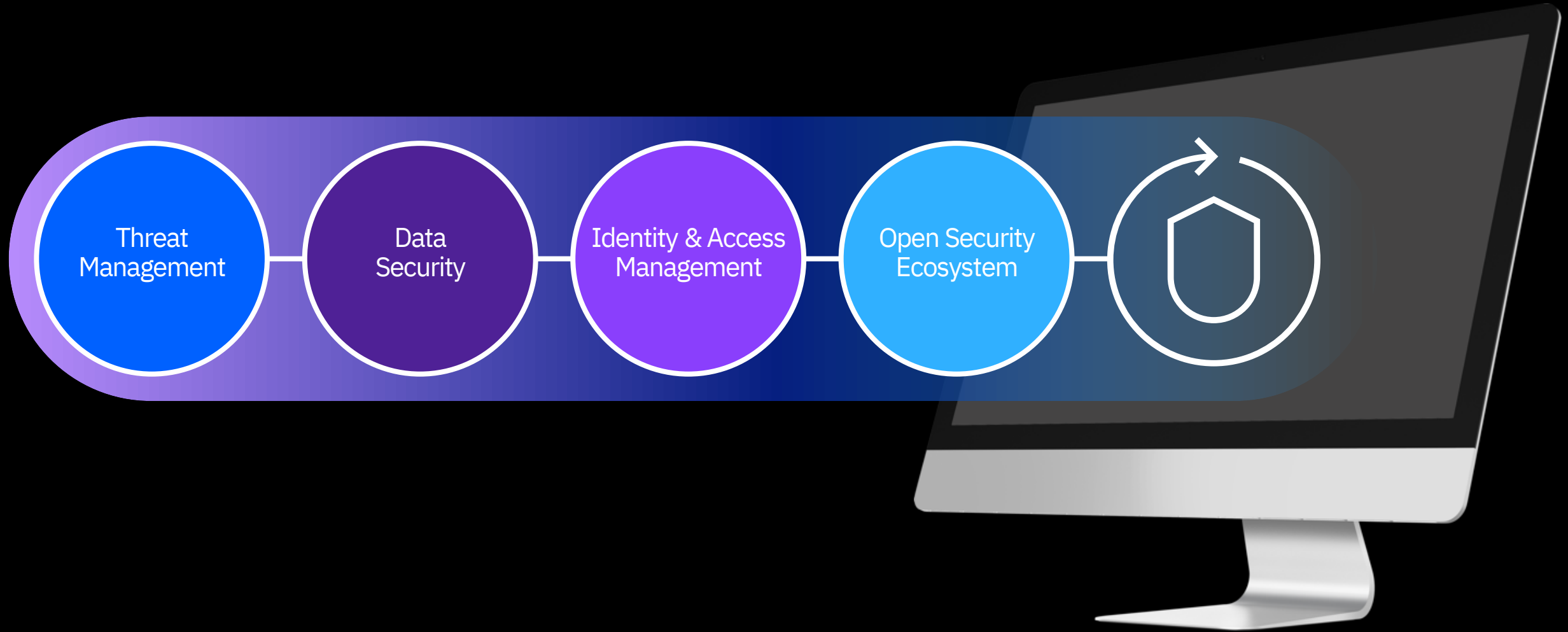
Too much complexity



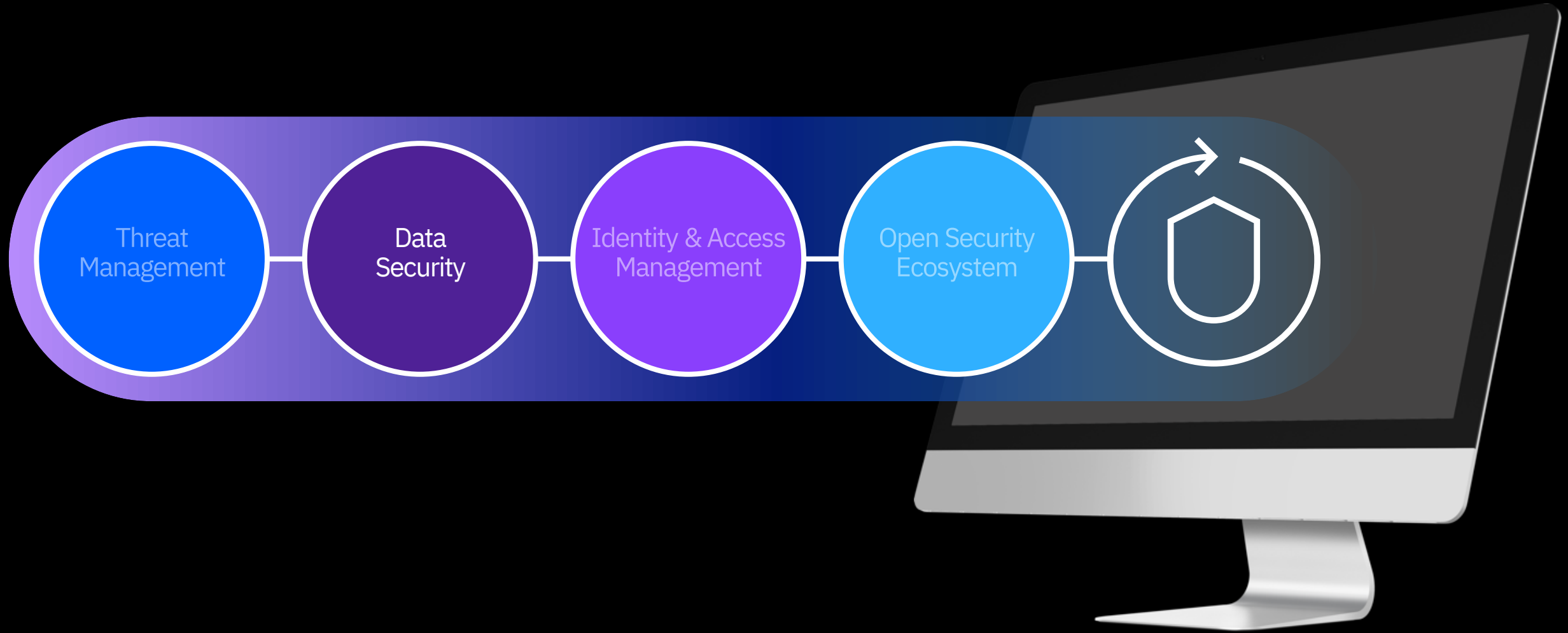
Too many alerts



A unified and open approach for teams to connect data and workflows



A unified and open approach for teams to connect data and workflows



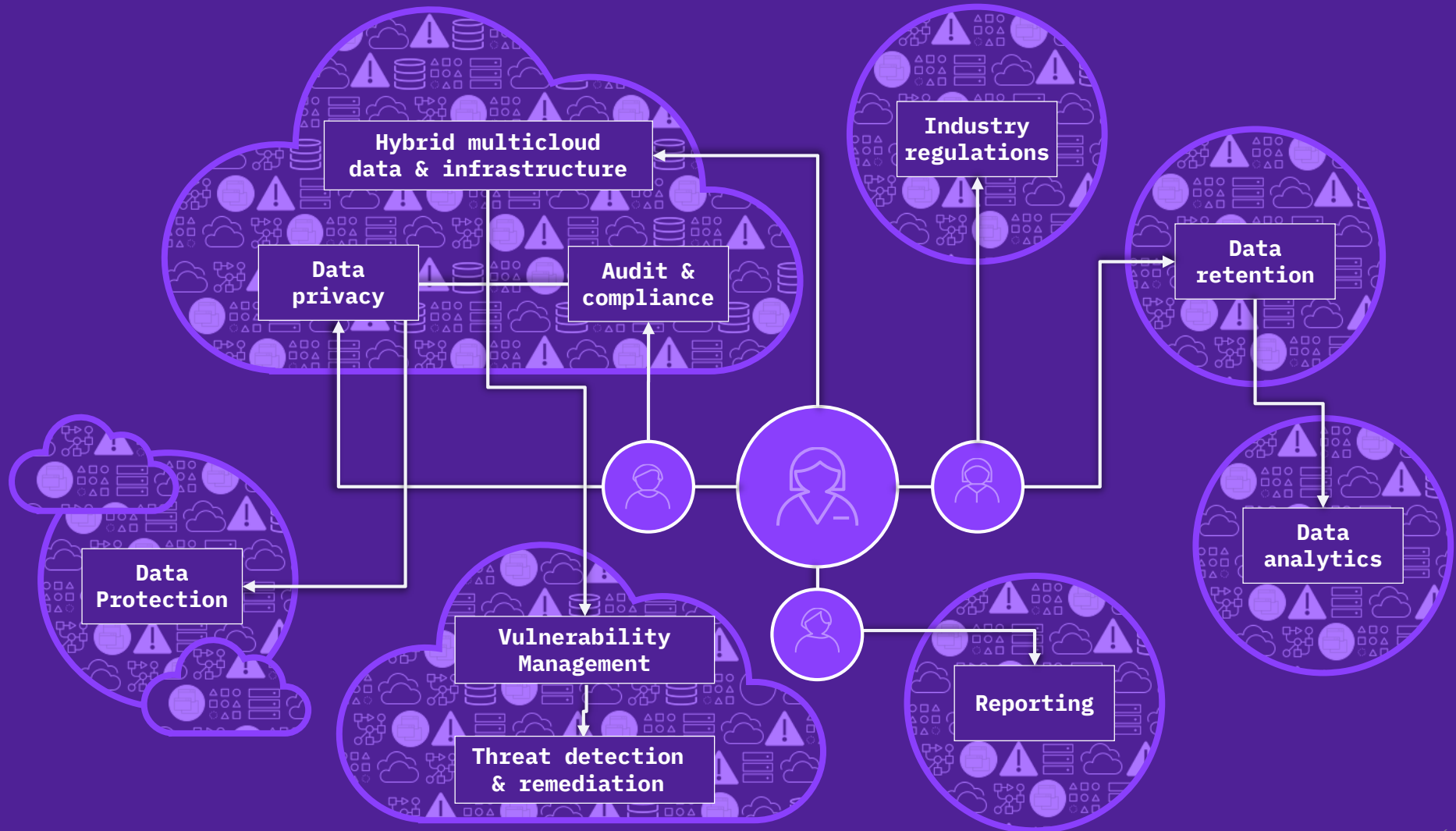
Data sprawl is fragmenting security policies and workflows

Data security teams need help...

- Wrangling the dramatic increase of data being created
- Understanding where data is being stored and how it is being accessed
- Identifying deviations that suggest risk
- Mitigating issues in a proactive fashion to avoid breaches

Structured and unstructured data across on premises, public, and private cloud

- Databases
- Applications
- Mainframes
- Files
- Containers
- Big data



A unified approach to data security



Protecting data with Cloud Pak for Security



Discover

Centrally store and visualize security and compliance data



Understand

Apply advanced analytics to uncover and analyze hidden risks



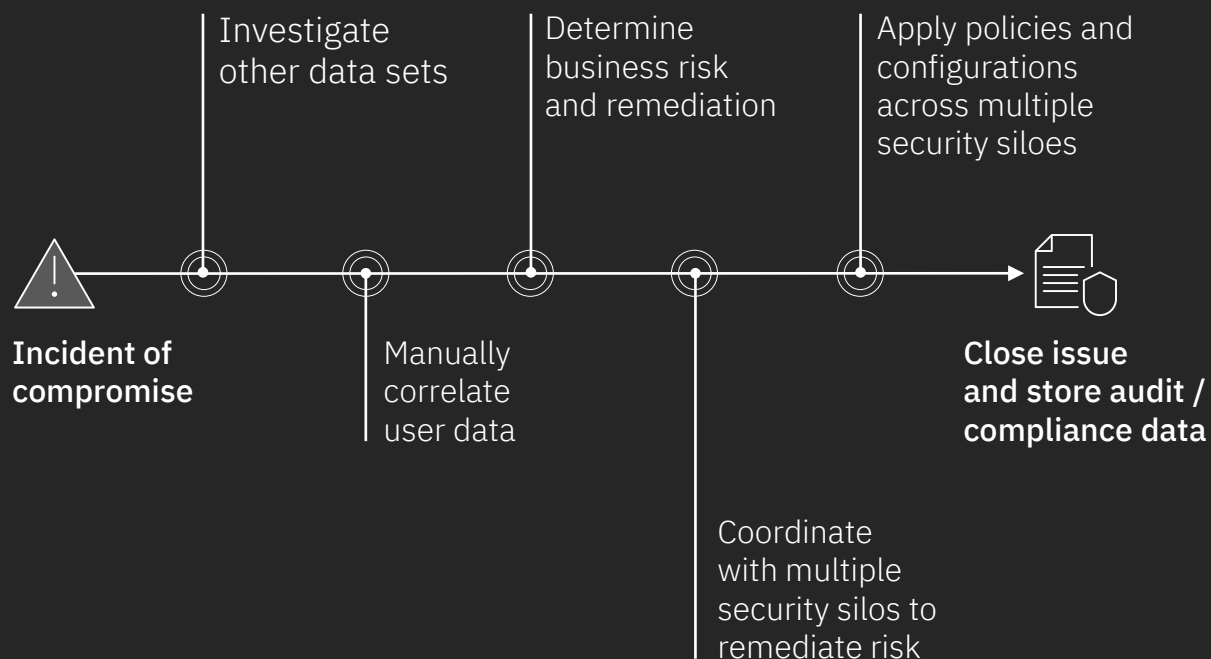
Respond

Orchestrate and automate policies and workflows across environments

A unified approach to stop insider threats

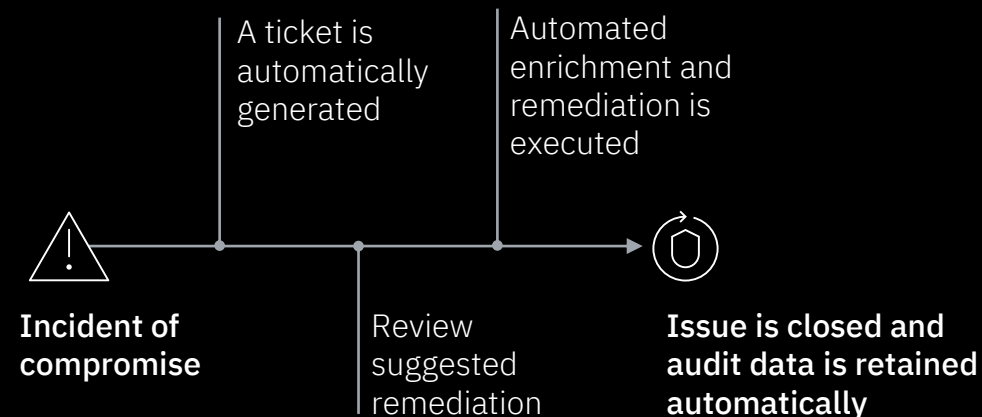
Traditional approach

Manual process across multiple siloed views
can take days to complete



IBM Cloud Pak for Security approach

An integrated and automated approach
can take just minutes to hours to complete



IBM Security Guardium Insights for IBM Cloud Pak for Security

Discover

Centrally store and visualize data security & compliance posture

Understand

Evaluate risk across hybrid multi-cloud data repositories

Respond

Centralize and accelerate responses

- Modernized deployment: on-premises, public cloud, or private cloud
- Orchestrated response and policy management
- Integrated Security Enrichment



Case Management Demo

On December 7th, Guardium Insights will be releasing:

- Integration with IBM Cloud Pak for Security “Cases” and IBM Resilient
 - Map a ticket in Guardium Insights to the “Cases” application and assign to a user
 - Allow SOC analyst to view and respond through the Cloud Pak for Security console

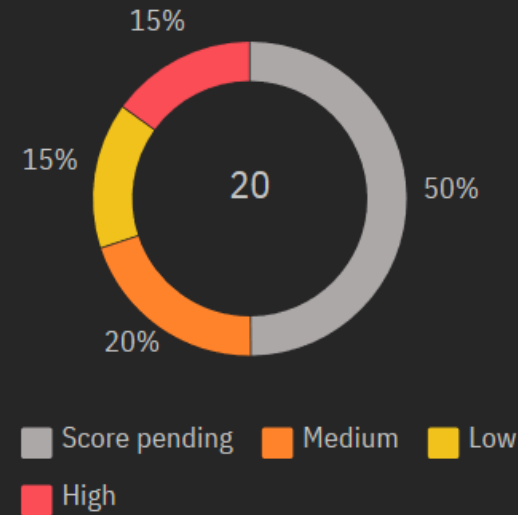
Discover

Centrally store and visualize security and compliance data

- Quickly visualize data activity across on-premises and cloud-hosted data sources
- Produce pre-defined and custom data security and compliance reports in seconds
- Track how data is being accessed, shared, and interacted with using agent and agentless based monitoring
- Discover hidden threats and potential risks

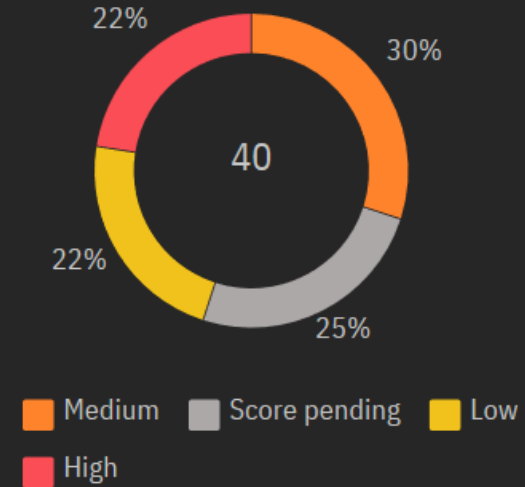
IBM Security Guardium Insights

Data source risk



[View all data sources](#) →

User risk



[View all users](#) →

Recent anomalies

Name	Confidence score(%)	Status
Data Modification January 10th 2020, 8:06:06 pm	99	Read
Data Extraction January 10th 2020, 8:06:00 pm	99	Unread

Understand

Apply advanced analytics to uncover and analyze risks

- Advanced analytics learn logical operations in a business – and spot anomalies at the first occurrence
- Excessive data modifications
- Business logic violations
- Examine suspicious activity triggers and alerts
- Detect potential fraud or threat activities faster

Data Extraction

2019-10-08 11:00:00

Summary

A HIGH data extraction violation has been triggered by on , which violates the normal extraction on asset USER.

	Details	Timeline
Who	Actor: DB2INST1	
What	Database Name: DB2INST1	
When	Timestamp: 2020-01-10 20:06:00	
Where		
Why	Anomaly Type: Data Extraction	

Respond

Orchestrate and automate policies and workflows across environments

- Standardized remediation workflows across hybrid multicloud environments
- Block unauthorized and suspicious users from accessing data
- Automatically create tickets, enrich cases, and escalate issues
- Share alerts and reports across teams

Take Action ^

Create a ticket

Block

Mark as unread

Ignore

Create a ticket

Open an incident report ticket in Service Now

Brief description

Add a short description

Assign ticket

Choose an individual or group to assign

Detailed description

Include all necessary details here

Homepage /

Select a Report

User Activity

Client IP Activity

Data points

Client IP
Source Program
SQL Verb
Object Name

View Description

User Activity

Full SQL by DB User Name

Data points

Client IP
Source Program
SQL Verb
Object Name
Depth (in SQL command)

View Description

User Activity

Sensitive Objects Usage

Data points

Client IP
Source Program

View Description

User Activity

Sessions by Client IP

Data points

Count of Client IP

View Description

User Activity

DML Execution on Sensitive Objects

Data points

Access Period
Client IP
Source Program

View Description

User Activity

DDL Commands

Data points

Client IP
Server IP
Server Type
SQL Verb
Count of Commands

View Description

User Activity

Policy Violations

Data points

Access Rule Description
Client IP
Server IP
DB Username
Full SQ String
Severity Description

View Description

User Activity

Policy Violations

Data points

Total Exceptions Logged

View Description

Improve your data security efficiency

Discover
67%

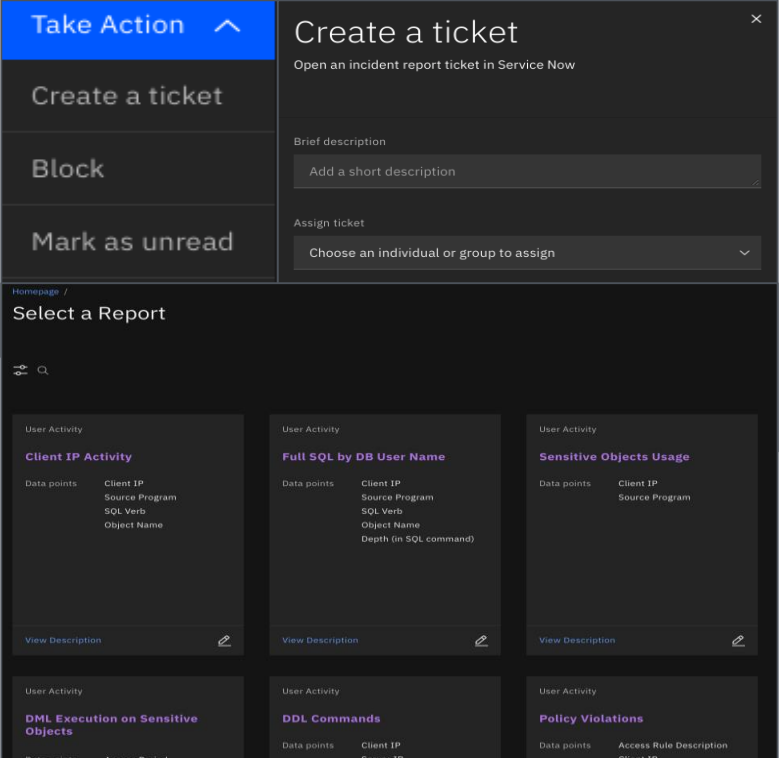
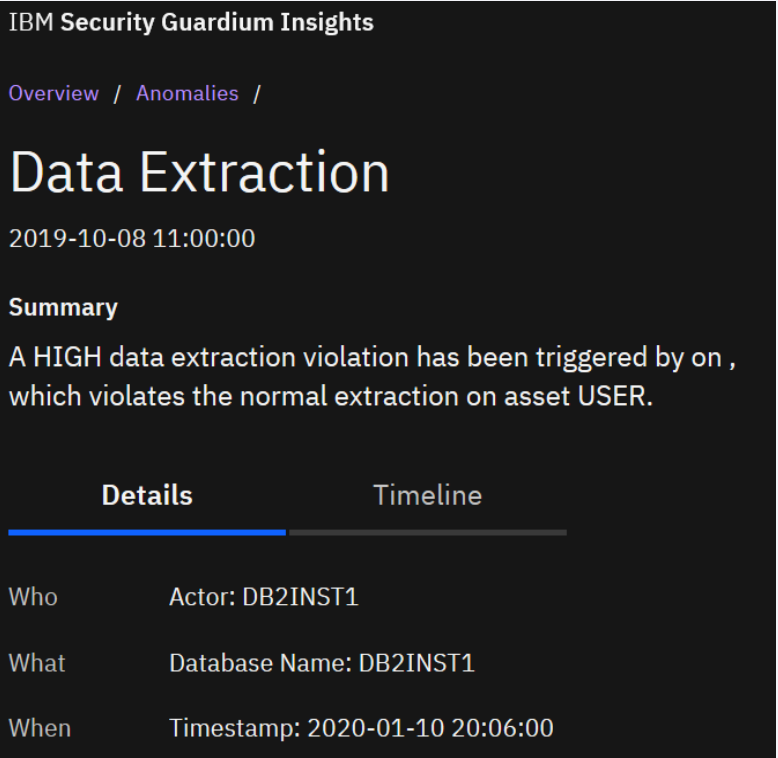
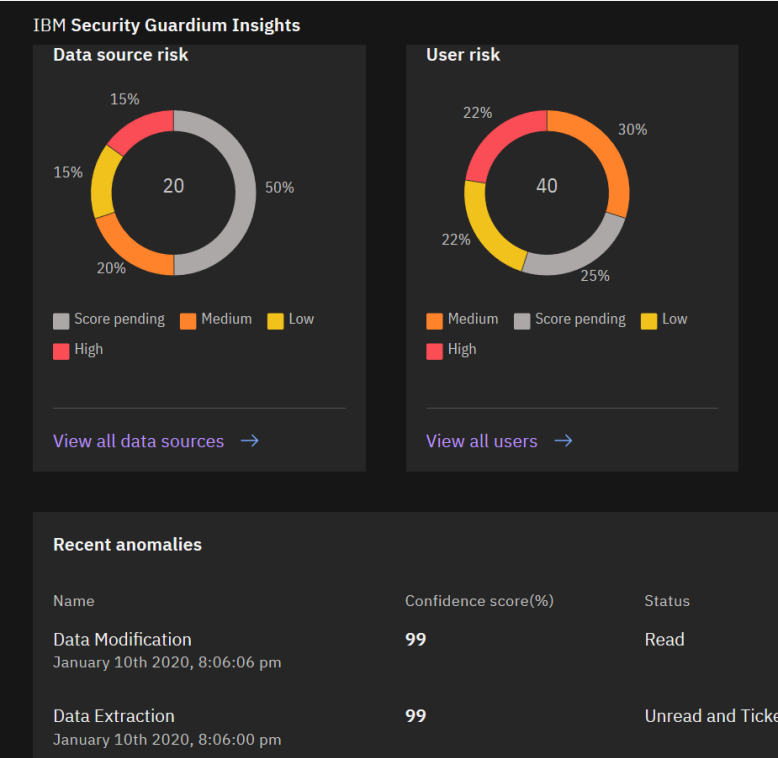
increase in discovering data source vulnerabilities and misconfigurations

Understand
50%

increase in accuracy of data classification

Respond
42%

decreased time spent remediating data security issues



What's next?

Learn more about Guardium Insights at:

<https://www.ibm.com/products/guardium-insights>

Explore the interactive Guardium Insights demo:

<https://www.ibm.com/security/digital-assets/guardium/insights-demo/>

Learn more about Cloud Pak for Security:

<https://www.ibm.com/products/cloud-pak-for-security>



Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. 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.