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

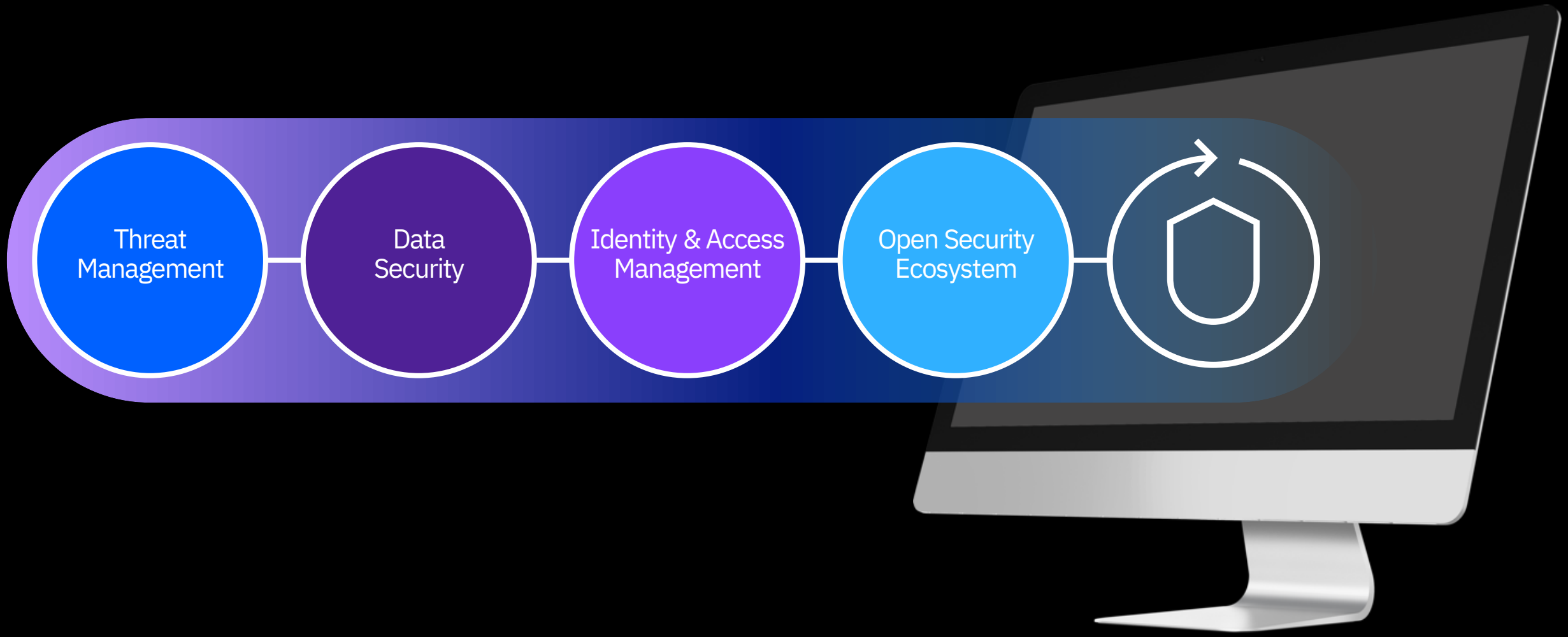
- Meet with CIO and stakeholders
- Nail down third-party risk
- Manage GDPR program with privacy office
- Respond to questions from state auditors
- Update CEO for board meeting
- Update budget projections
- Write security language for vendor's contract
- Make progress on the never-ending identity project
- 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

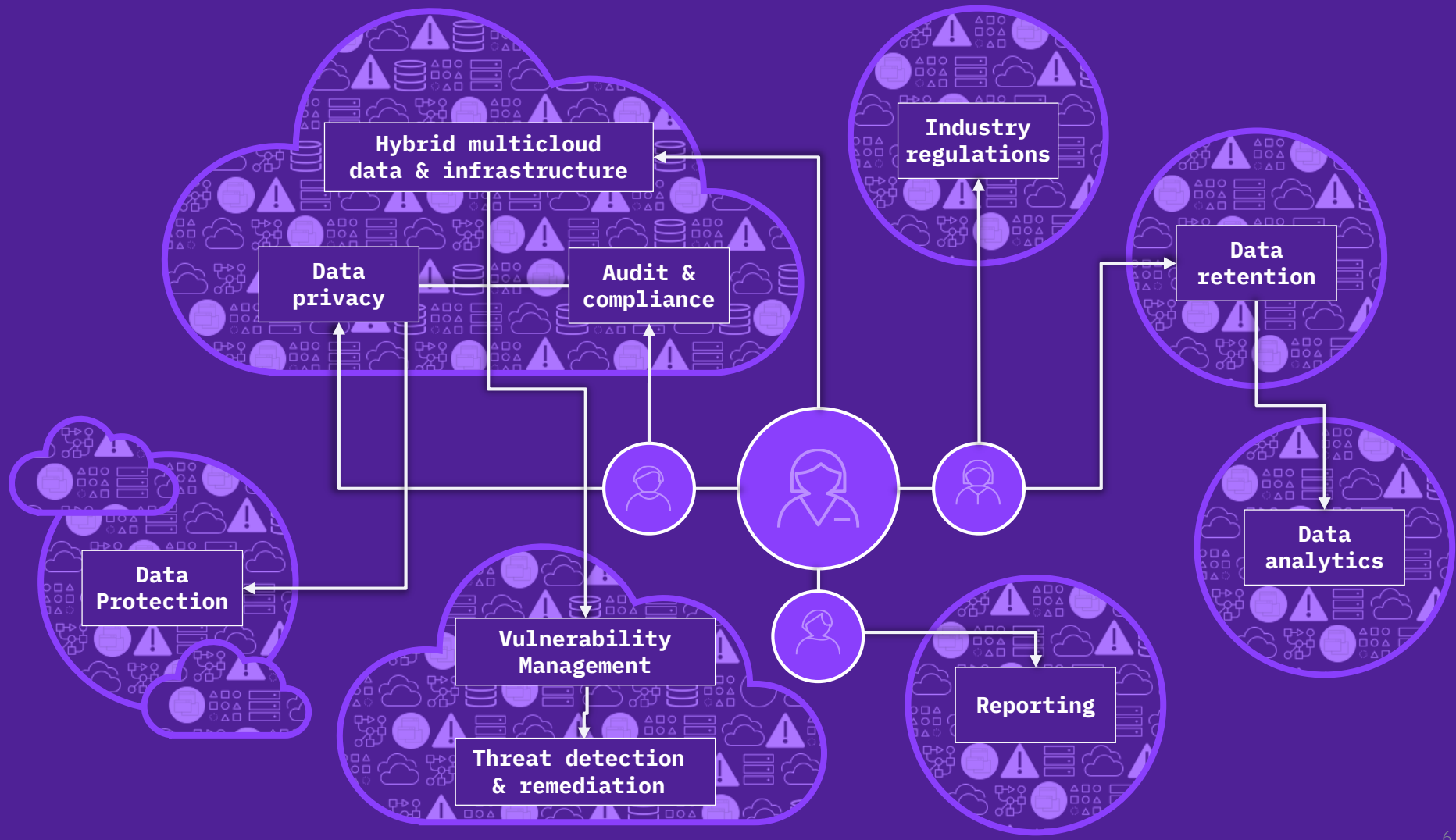
Data sprawl is fragmenting security policies and workflows

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

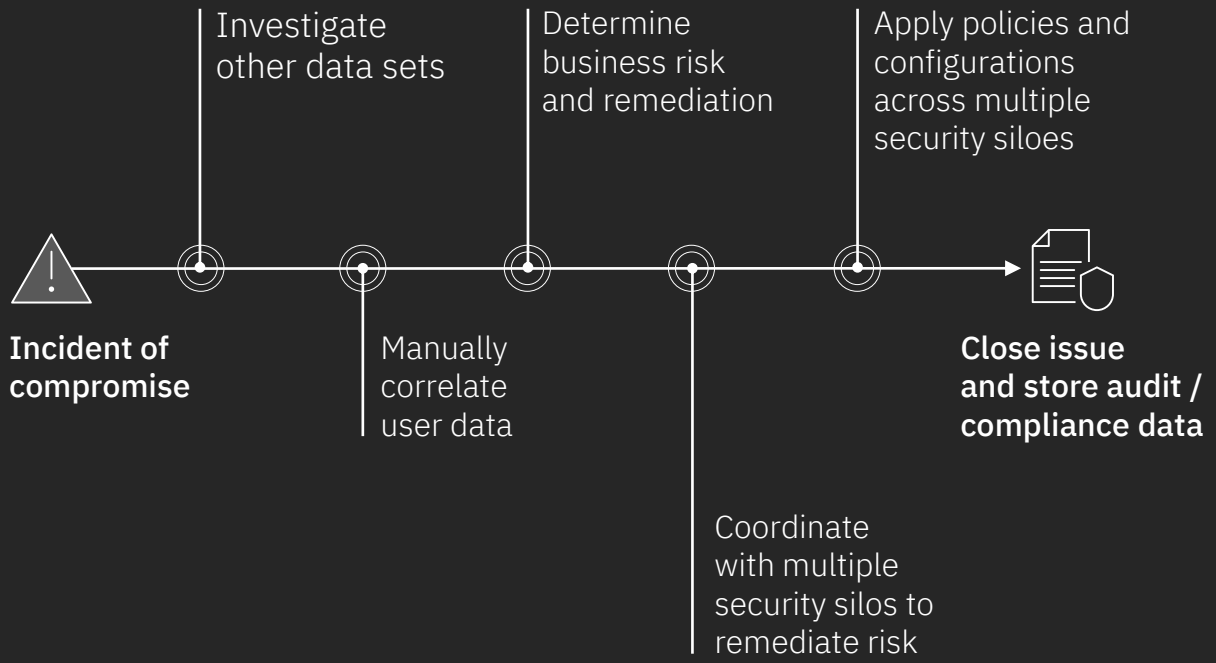
Respond

Orchestrate and automate policies and workflows across environments

A unified approach to stop insider threats

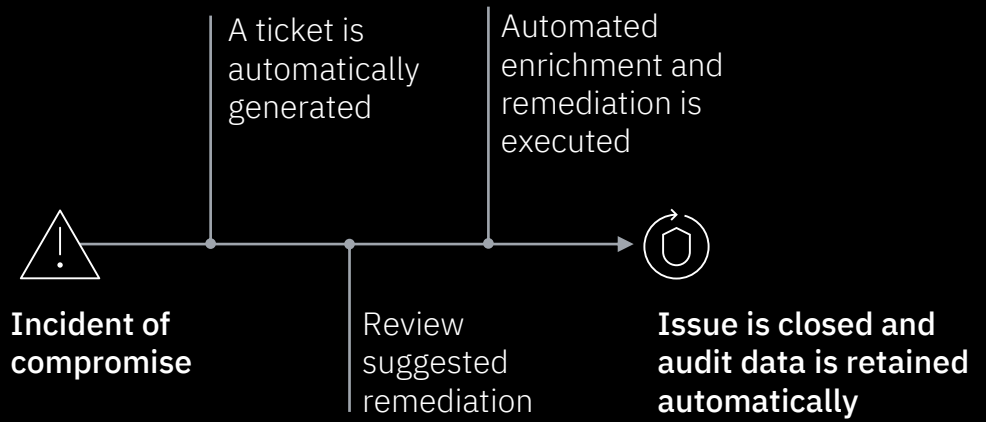
Traditional approach

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

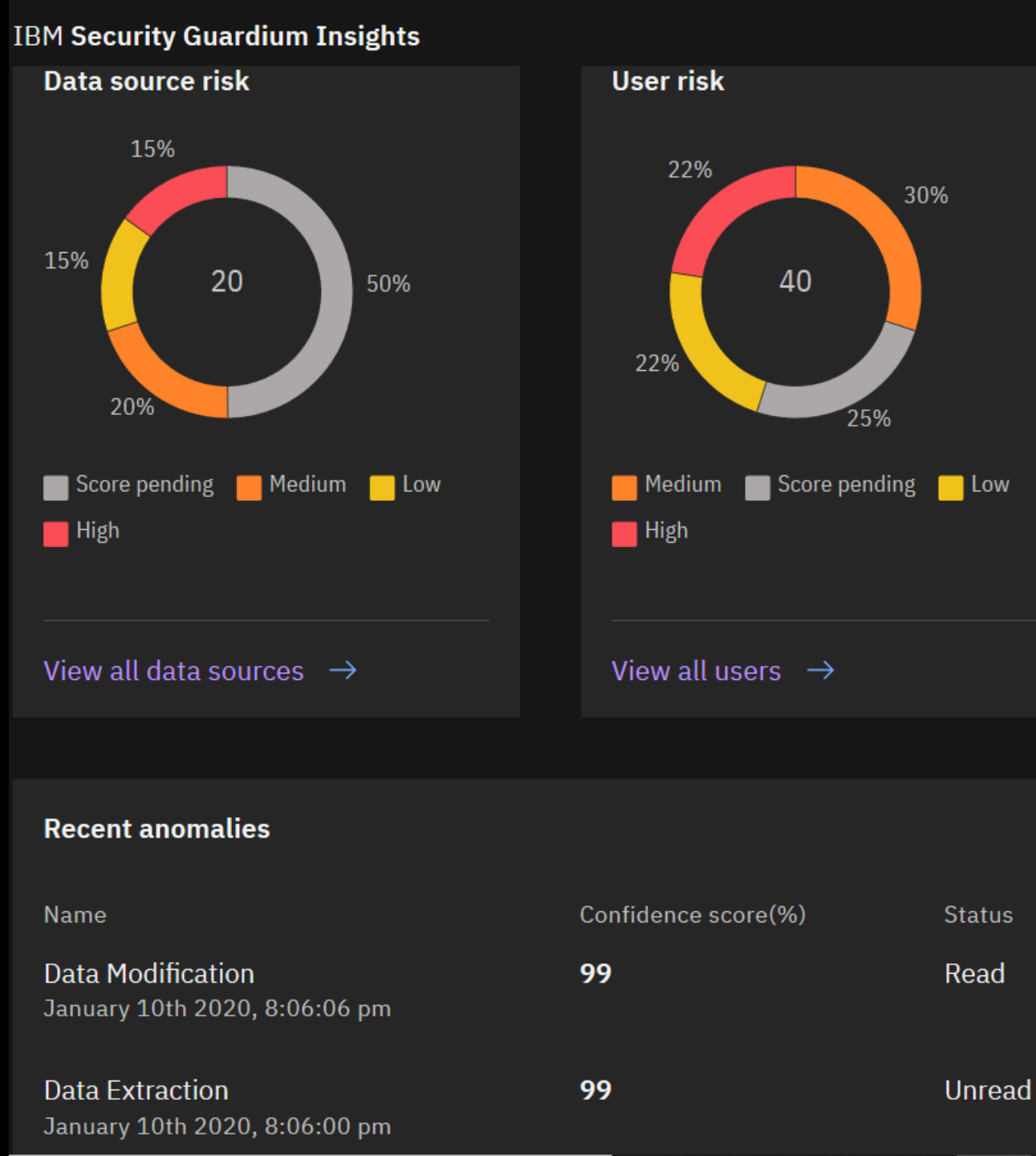
On December 7th, Guardium Insights will be releasing:

- 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

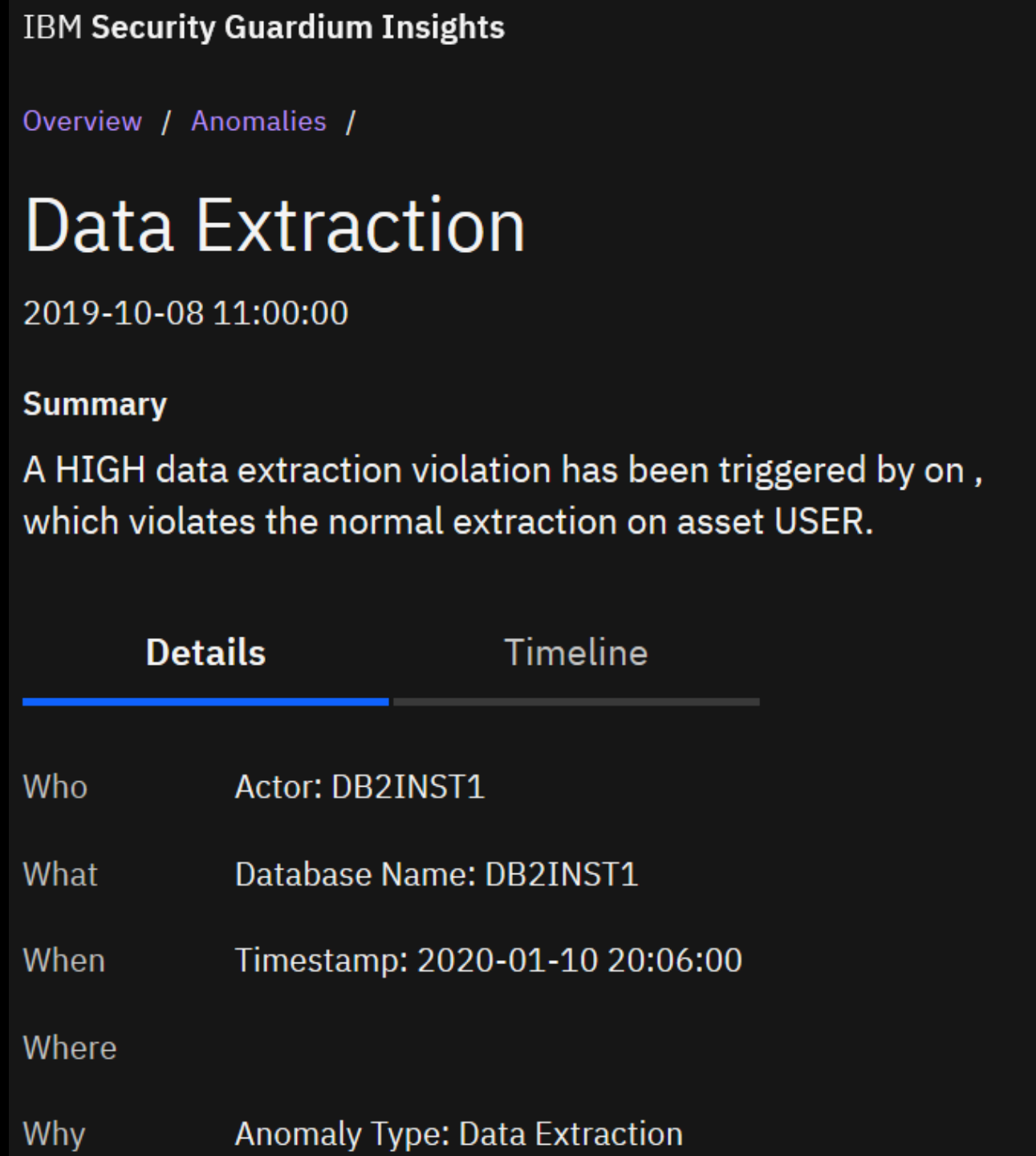
- Quickly visualize data activity across on-premises and cloud-hosted data sources
- Produce pre-defined and custom data security and compliance reports in seconds
- Track how data is being accessed, shared, and interacted with using agent and agentless based monitoring
- Discover hidden threats and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



Understand

Apply advanced analytics to uncover and analyze risks

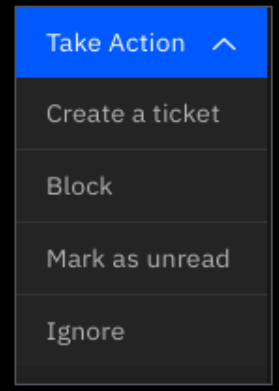
- Advanced analytics learn logical operations in a business – and spot anomalies at the first occurrence
  - Excessive data modifications
  - Business logic violations
- Examine suspicious activity triggers and alerts
- Detect potential fraud or threat activities faster

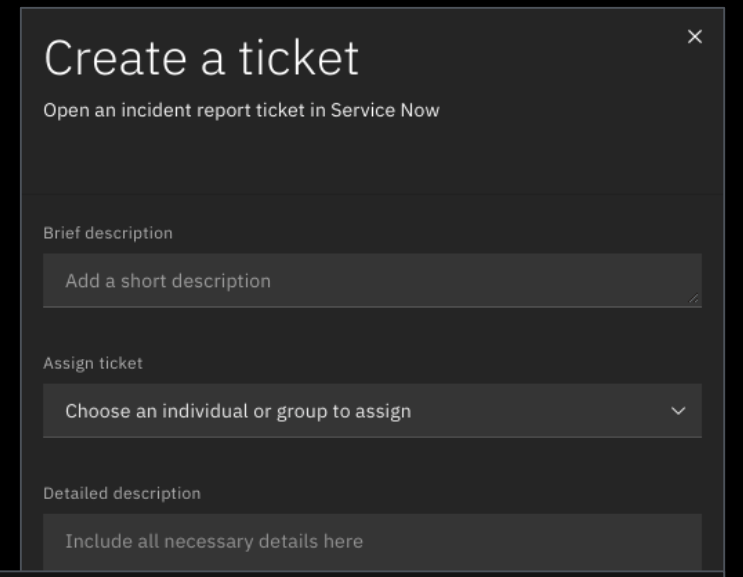


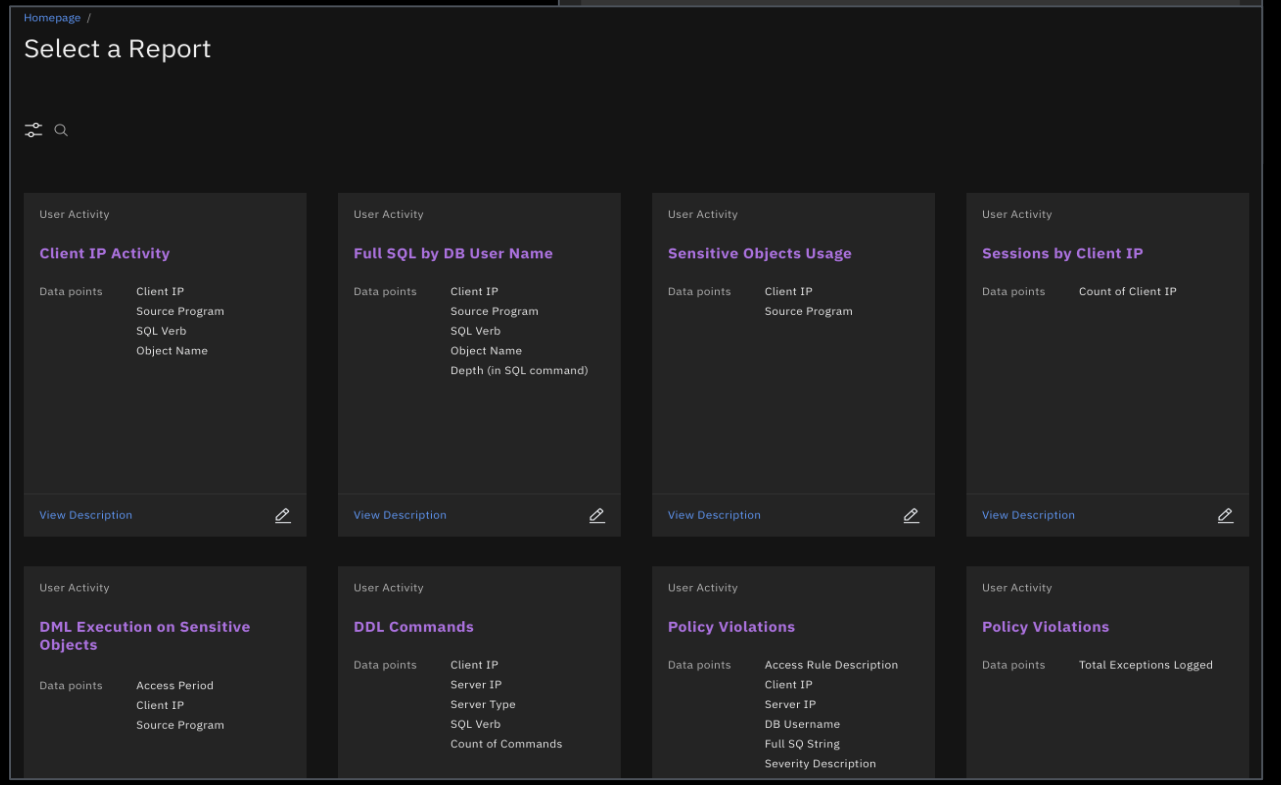
Respond

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







Improve your data security efficiency

Discover

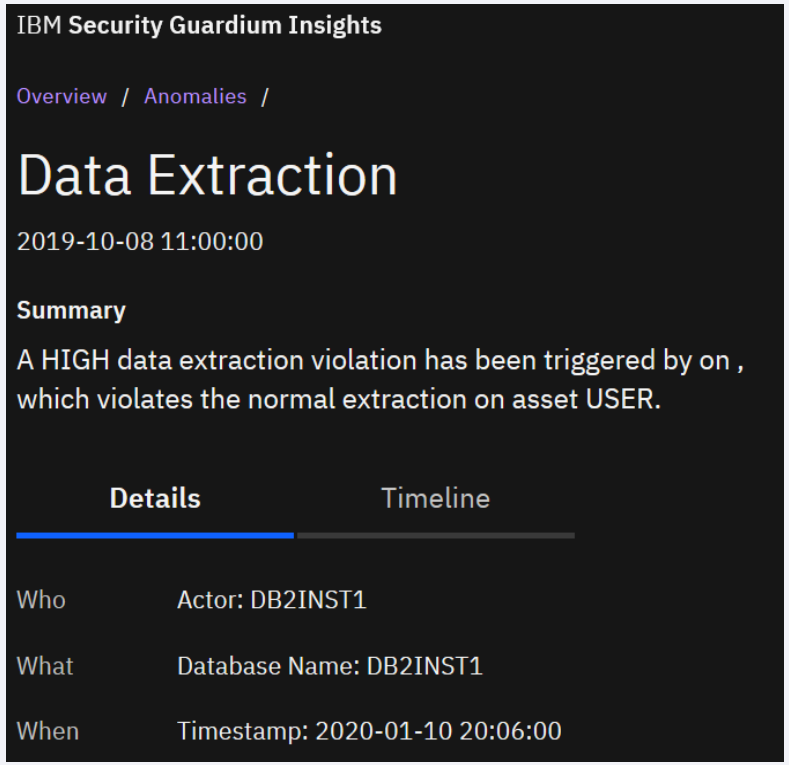
67%

increase in discovering data source vulnerabilities and misconfigurations

Understand

50%

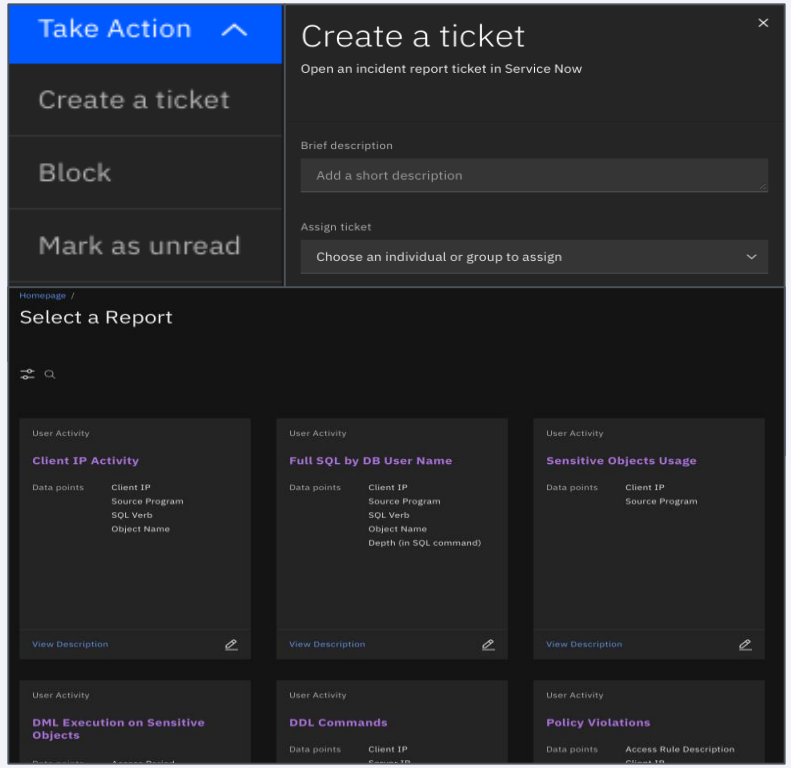
increase in accuracy of data classification



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