# Modernize your security operations center with connected security that advances Zero Trust

IBM Cloud Pak for Security

IBM Security Guardium Insights for Cloud Pak for Security

X-Force Threat Management

# Modernize the SOC Launch Messaging

# 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


# What we've heard from our customers

From thousands of engagements across the world, we've heard some common security concerns.

## Help me...

- ❑ Respond to the global security skills shortage
- ❑ Secure the journey to cloud and digital transformation
- ❑ Increase speed and provide consistent decisions on similar events
- ❑ Modernize, manage, optimize security frameworks and controls
- ❑ Mature my security posture pertaining to managing threats
- ❑ Provide end-to-end security visibility leveraging AI and orchestration

# Organizations are turning to zero trust to gain control over a rapidly changing environment

# 78%

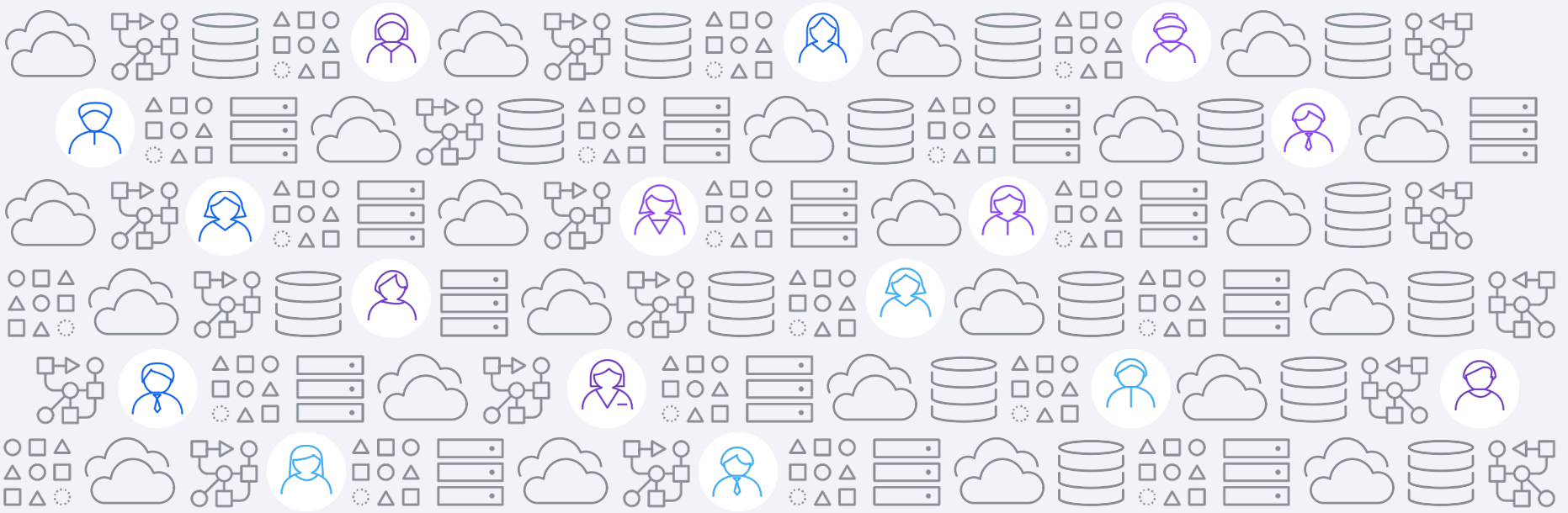
Of organizations plan to adopt a Zero Trust strategy.[1]

## Context is essential for zero trust:

Enabling the **right user** under the **right conditions** to have the **right access** to the **right data**

[1] 2019 Zero Trust Adoption Report, CybersecurityInsiders

# Better context requires a modern, unified approach to security



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

# An open multicloud platform to gain security insights, take action faster, and modernize your architecture

## Modular security capabilities

- Threat Management
- Data Security
- Identity & Access Management
- Open Security Ecosystem

## Platform services

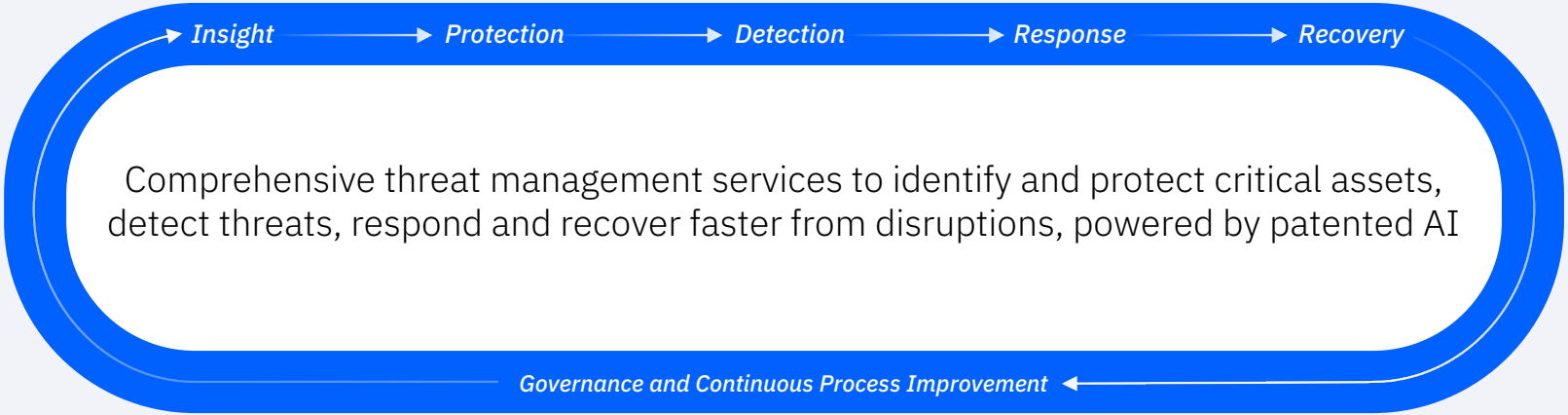
- Data connection
- Asset enrichment
- Case management
- Orchestration
- Automation
- Development tools

**Open and integrated hybrid multicloud platform**

SIEM tools | EDR tools | Cloud repositories | Data lakes | Database protection | Network protection | Additional point solutions

On premise | Hybrid Cloud | Multicloud

# The range of expertise to build a holistic end-to-end threat management strategy




### Business Framing

Identify critical needs and how to get value, fast

### Managed Security Services

Extend your coverage with 24x7 security expertise

### Offensive Security

Hacking anything to secure everything

### Incident Response & Intelligence

Gain the expertise needed to deal with *"Right of Boom"*

Offering Focus

# Cloud Pak for Security

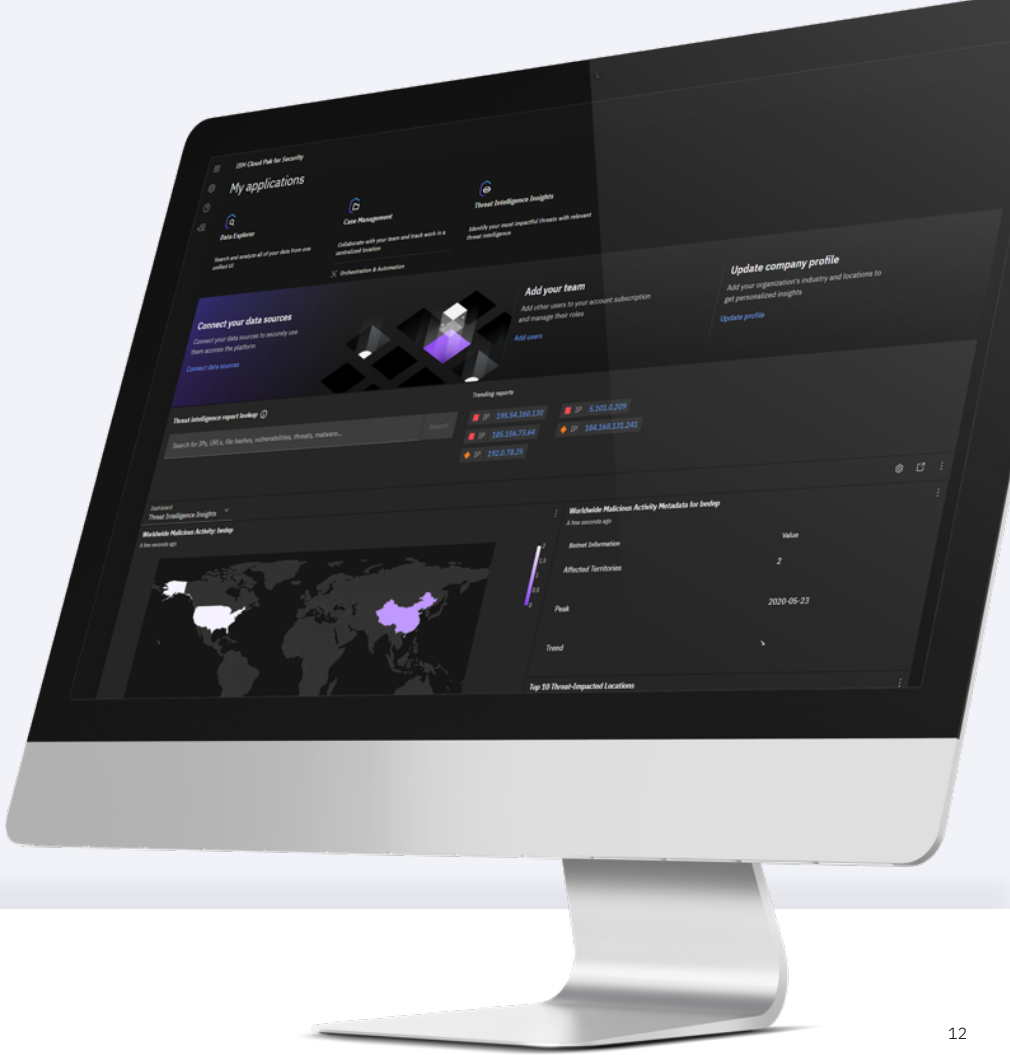
# IBM Cloud Pak for Security

A platform to more quickly integrate your existing security teams and tools to generate deeper insights into threats and risks, orchestrate actions and automate responses—all while leaving your data where it is.

- **Gain security insights**
  With a unified console that provides visibility and analytics across IBM and 3rd party security tools, data, and clouds

- **Take action faster**
  With AI and automation, simplify operations and streamline response, to save time and lower risk

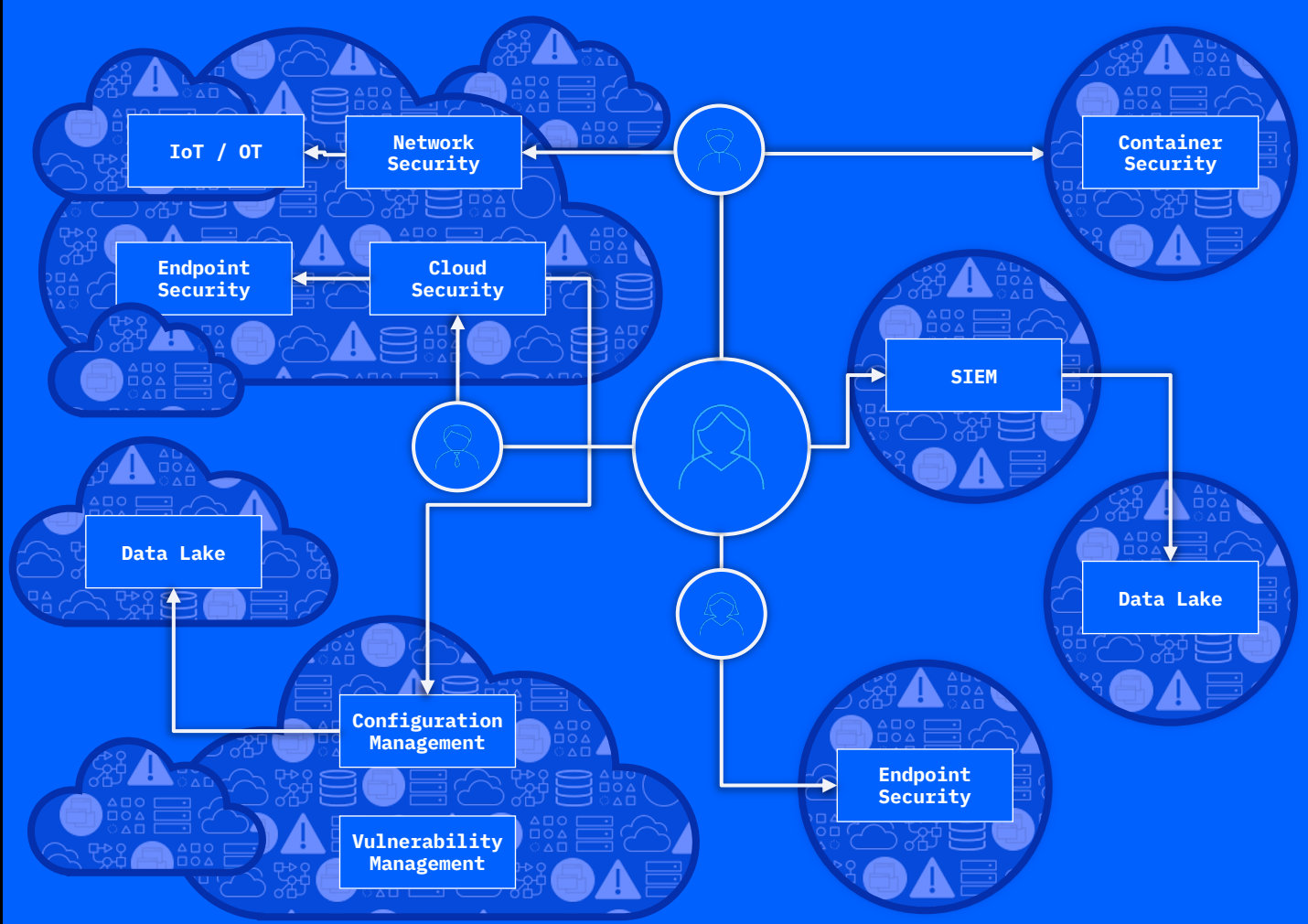
- **Modernize your architecture**
  Run anywhere with an open, multicloud platform that gives you flexibility, extensibility and avoids lock-in



# Growing threats, tools and data are inhibiting security operations

## SOC analysts need help...

- Prioritizing the increasing amount of events, alerts and intelligence they have
- Quickly navigating multiple tools and data sources to investigate threats
- Reducing manual processes and even more tools to resolve security incidents



# A unified approach to managing threats

Managing threats with Cloud Pak for Security

## Detect

Gain prioritized threat intelligence and apply real-time detection across hundreds of use cases and multicloud environments

## Investigate

Automate alert investigation with AI and federate search across any data source, on-premise or in the cloud, without moving data

## Respond

Respond to incidents faster with dynamic playbooks, automation, and orchestration across all teams

# Detect, investigate and respond efficiently and effectively

## Detect

**51%**

increase in ability to detect attacks

## Investigate

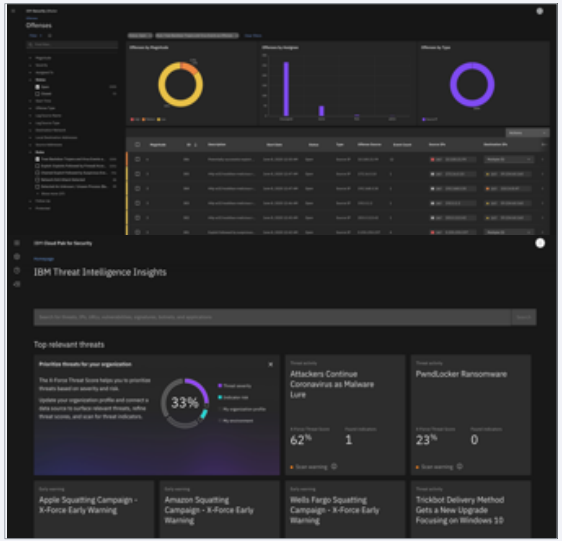
**60x**

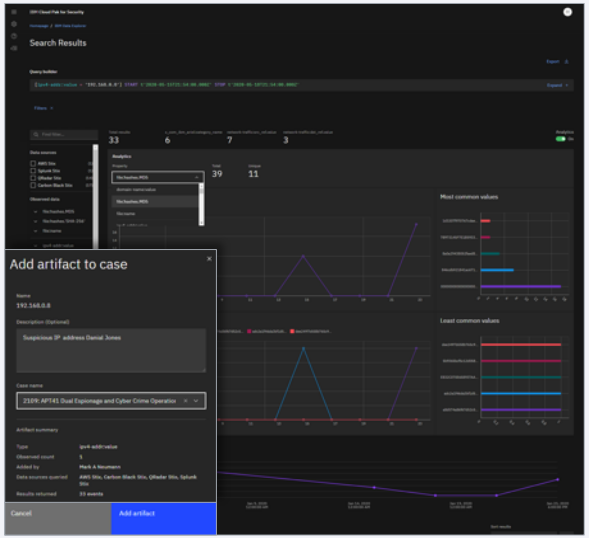
improvement in investigation time

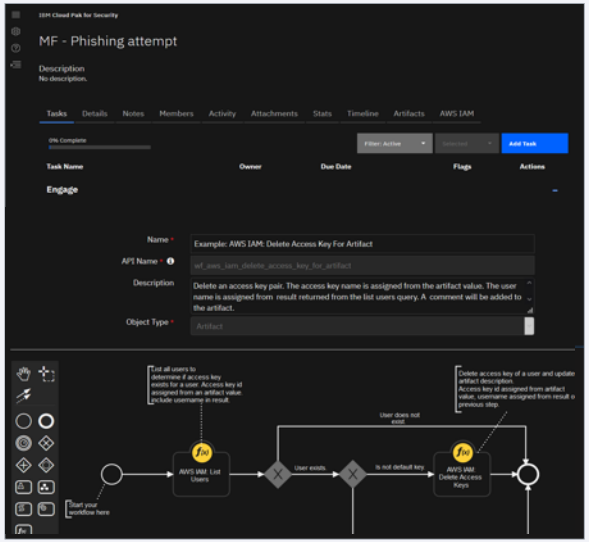
## Respond

**8x**

increase in speed to respond to security incidents



# A unified console to detect threats and view incidents, tied together with simple, visual case management

## Enhance threat management workflows

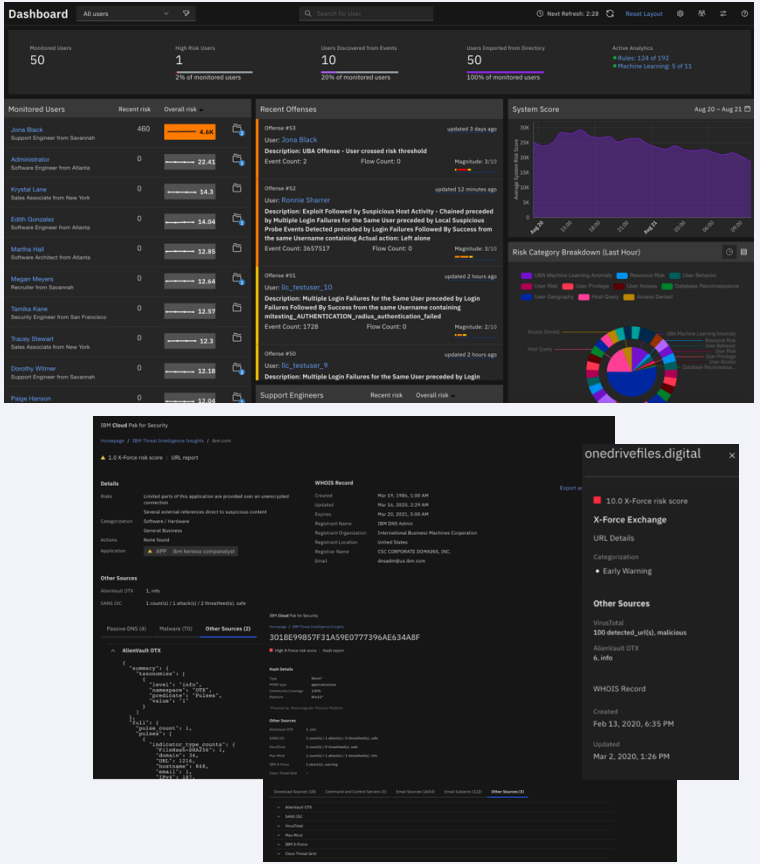
- Seamlessly view and access **QRadar offenses** in Cloud Pak for Security case management
- Extend search capabilities with support for **QRadar AQL searches** from within Cloud Pak for Security
- Increase visibility by migrating existing **QRadar dashboards** to Cloud Pak for Security

## Identify insider threats

- Quickly identify risky users associated with insider threats from within Cloud Pak for Security by leveraging **QRadar's User Behavior Analytics** as part of an end-to-end threat management workflow

## Infuse third-party threat intelligence feeds

- Reuse investment in **3rd party threat intelligence** through simple single configuration screen
- Augment existing integrated workflow between Threat Intelligence Insights, SOAR and Data Explorer with 3rd party threat intelligence in context of an investigation or incident



# A unified console to detect threats and view incidents, tied together with simple, visual case management

## Anchor workflow with robust SOAR

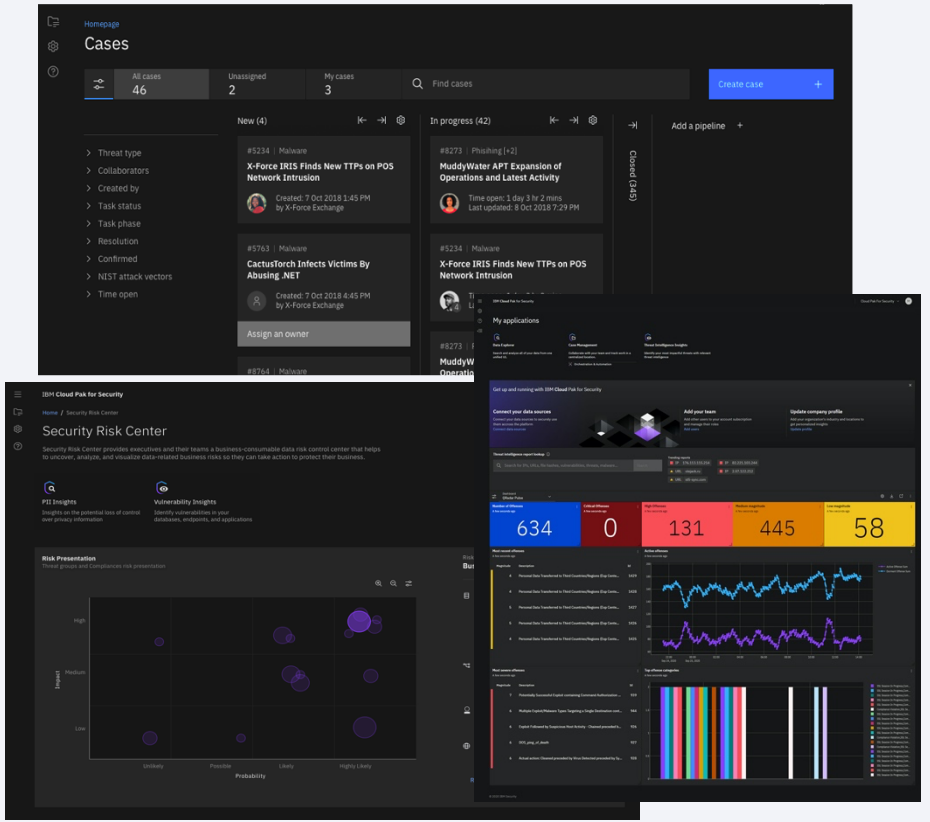
- Use visual process techniques utilized in **lean manufacturing (Kanban)** to manage and coordinate security responses
- Easily identify leverage points used by attackers, track IOCs over time and classify attributes using **improved artifact management capabilities**
- Meet compliance regulatory requirements with **Privacy add-on**

## Gain more insight into risk

- Get early visibility into potential security risks by correlating insights across risk vectors and personally identifiable (PI) data with **Risk Manager**

## Unify SOC dashboards *(available today in v1.4)*

- View and customize **unified threat management dashboards with operational metrics from Threat Intelligence, SIEM and SOAR systems**
- Build your own dashboard canvases to visualize security data and drill into different views



Offering Focus

# Guardium Insights for Cloud Pak for Security

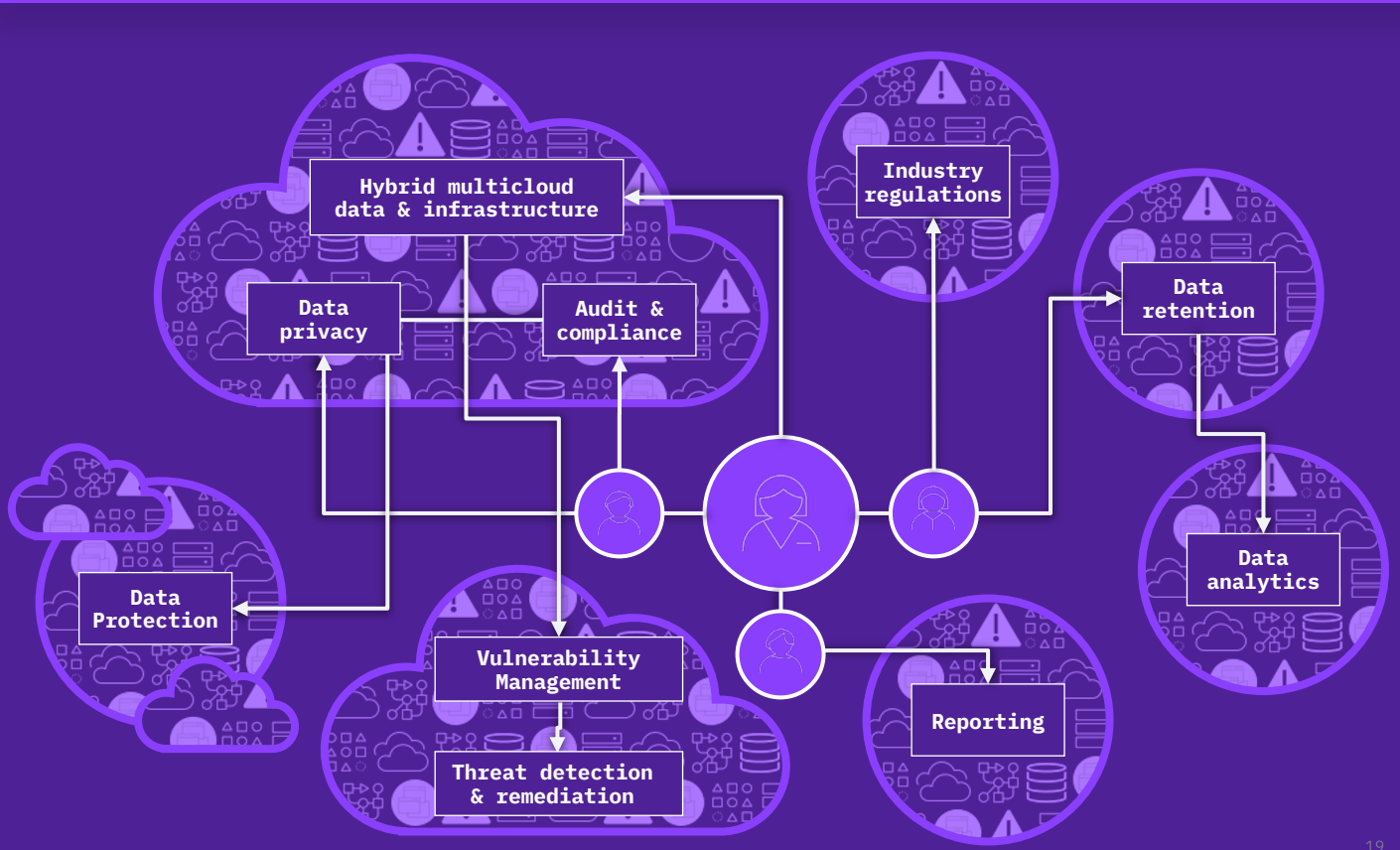
# Data sprawl is fragmenting security policies and workflows

## 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

# Improve your data security efficiency

## Discover

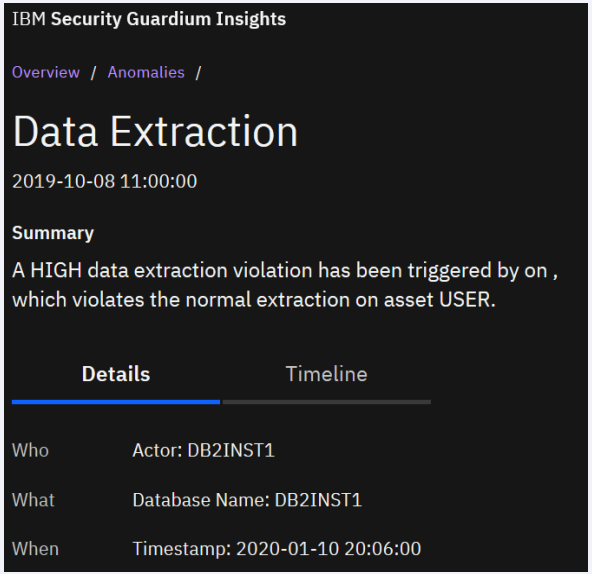
**67%**

increase in discovering data source vulnerabilities and misconfigurations


## Understand

**50%**

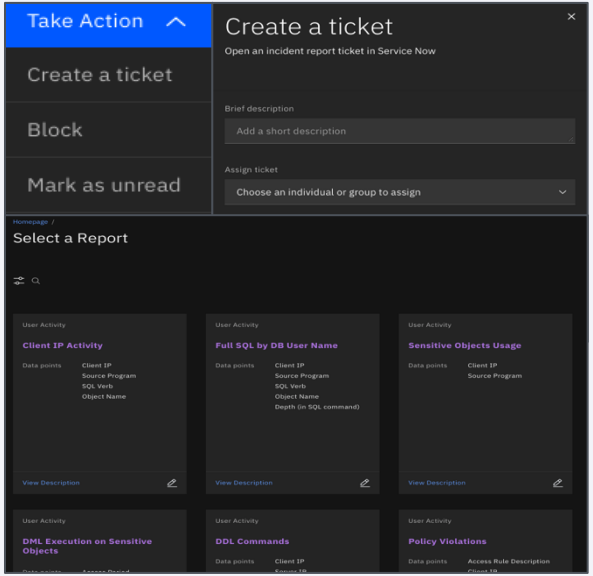
increase in accuracy of data classification




## Respond

**42%**

decreased time spent remediating data security issues



# 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 |

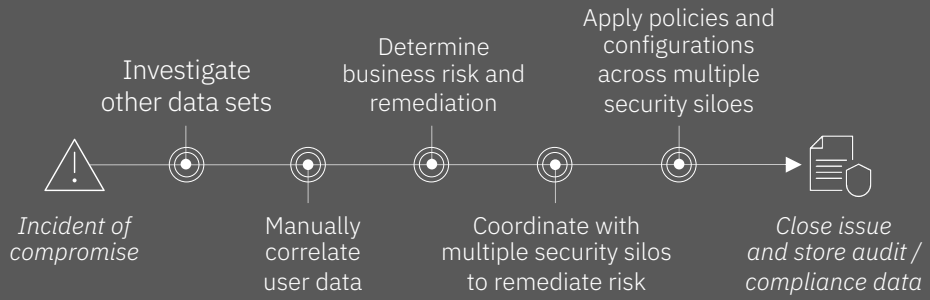
- ✓ Modernized deployment: on-premises, public cloud, or private cloud
- ✓ Orchestrated response and policy management
- ✓ Integrated Security Enrichment

Use case across data security and SOC teams

# Mitigate against insider threats

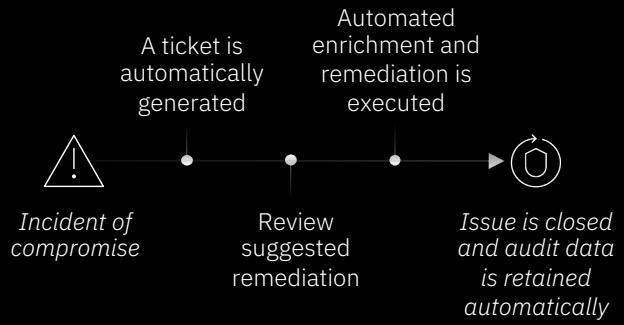
## Traditional approach

Manual process across multiple siloed views can take days to complete




## IBM Cloud Pak for Security approach

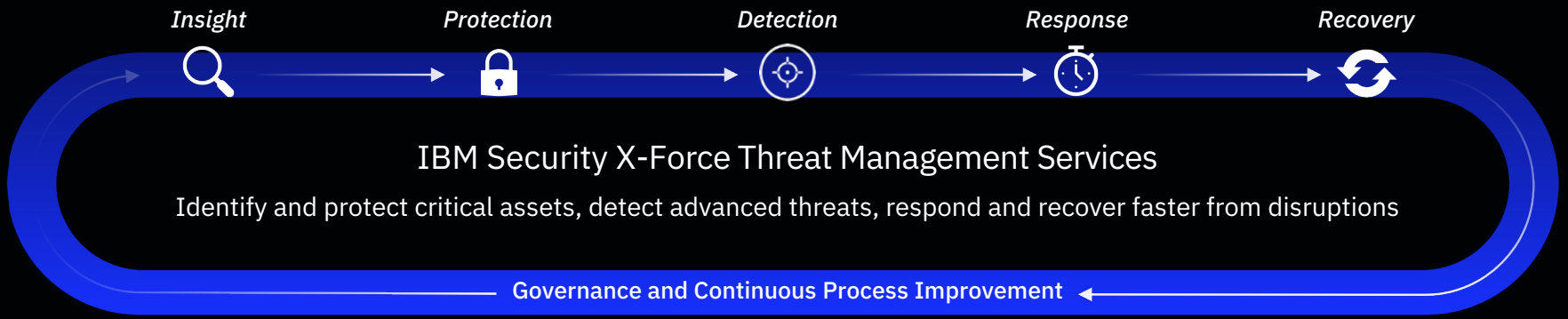
An integrated and automated approach can take just minutes to hours to complete



Offering Focus

# X-Force Threat Management

# Defend your business with end-to-end threat management




## Seamlessly combining leading SIEM technologies and Threat Management expertise

IBM Security QRadar

#1 SIEM for advanced threat defense

Hack anything to secure everything

170 Renowned veteran hackers and experts

Gain the expertise needed to deal with “Right of Boom”

$1M+ Savings when a breach is contained within 30 days

Extend your coverage with 24x7 security expertise

20+ Years of experience through thousands of engagements

# X-Force Threat Management and Cloud Pak for Security

*Expertise and tools to modernize Security Operations and address the end-to-end threat management lifecycle*

## X-Force Advise

Advisory services to assess, design and implement an end-to-end threat management strategy to improve your SOC operations with CP4S

## XFTM SOAR Bridge

Synchronize XFTM CP4S playbooks and cases to facilitate close collaboration between IBM and your security operations team, while keeping your company's unique playbooks private

## X-Force Respond

In collaboration with your team, IBM experts leverage CPS4 SOAR native integrations and/or Ansible to take action to respond to and contain threats

## IBM Management of CP4S

Policy management, connector configuration, log source integration, user administration, patching and infrastructure monitoring, and integration with IBM Virtual Security Operations Center, to ensure Cloud Pak is operational and up to date