

# IBM SECURITY STRATEGY

SECURING THE THREATS OF TOMORROW, TODAY



**Jasmina Zivanovic**

Security Channel Manager SEE & Central

October 2018





# Cybersecurity is a universal challenge

By 2020, there will be...

**20.8 billion**

“things” to secure

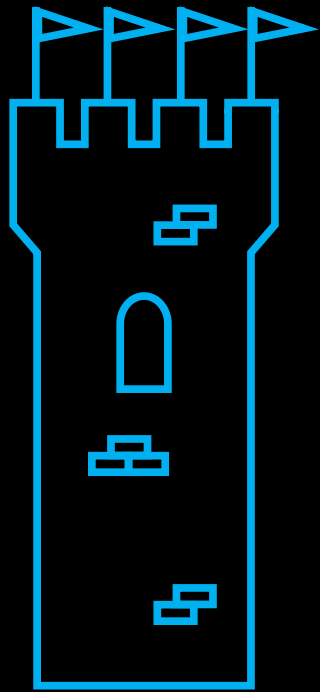
**5 billion**

personal data records stolen

**\$8 trillion**

lost to cybercrime

# How do you evolve your security program for the future?



**LAYERED  
DEFENSES**

**INTELLIGENCE  
and INTEGRATION**

**COGNITIVE, CLOUD,  
and COLLABORATION**

# The future of security is **Cognitive**

What if you could accelerate  
what analysts do each day?

## **Investigate threats faster**

Automatically triage incidents 60x faster  
with Watson for Cyber Security

## **Interpret unstructured data**

Draw from millions of security documents

## **Be more accurate**

Eliminate 98% of false positives





# The future of security is **Cloud**

Can you confidently say yes  
to digital transformation?

## **Accelerate innovation**

Access one of the largest cloud-based  
security portfolios in the world

## **Protect multiple clouds**

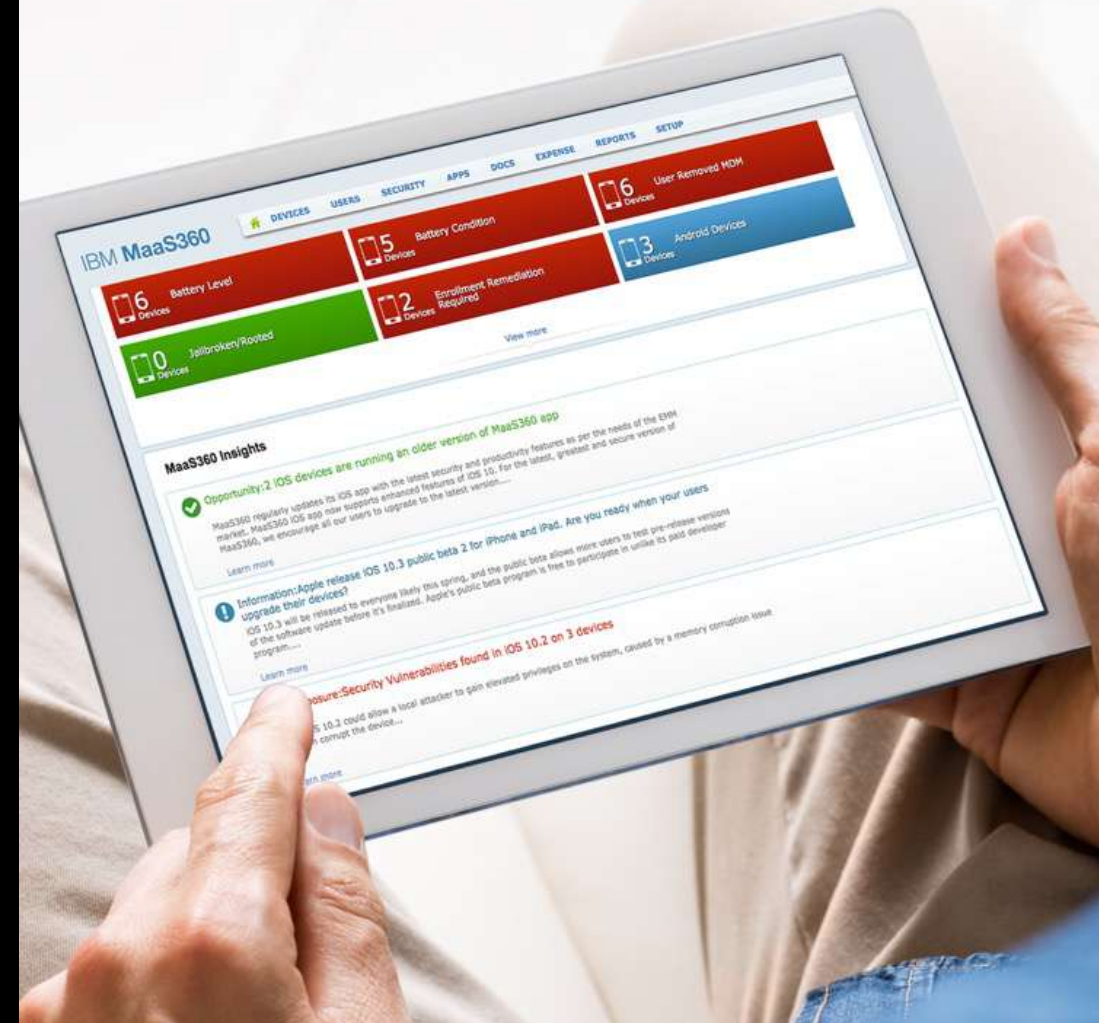
Use 25+ hybrid cloud security  
offerings, built for the enterprise

## **Use a proven platform**

270M+ endpoints connected to our cloud

IBM MaaS360  
IBM QRadar on Cloud  
IBM Trusteer  
IBM AppSec on Cloud

IBM Security App Exchange  
IBM X-Force Exchange  
IBM IDaaS  
Data Security on Cloud



# The future of security is **Collaboration**

Are you part of the bigger picture?

## **Orchestrate responses**

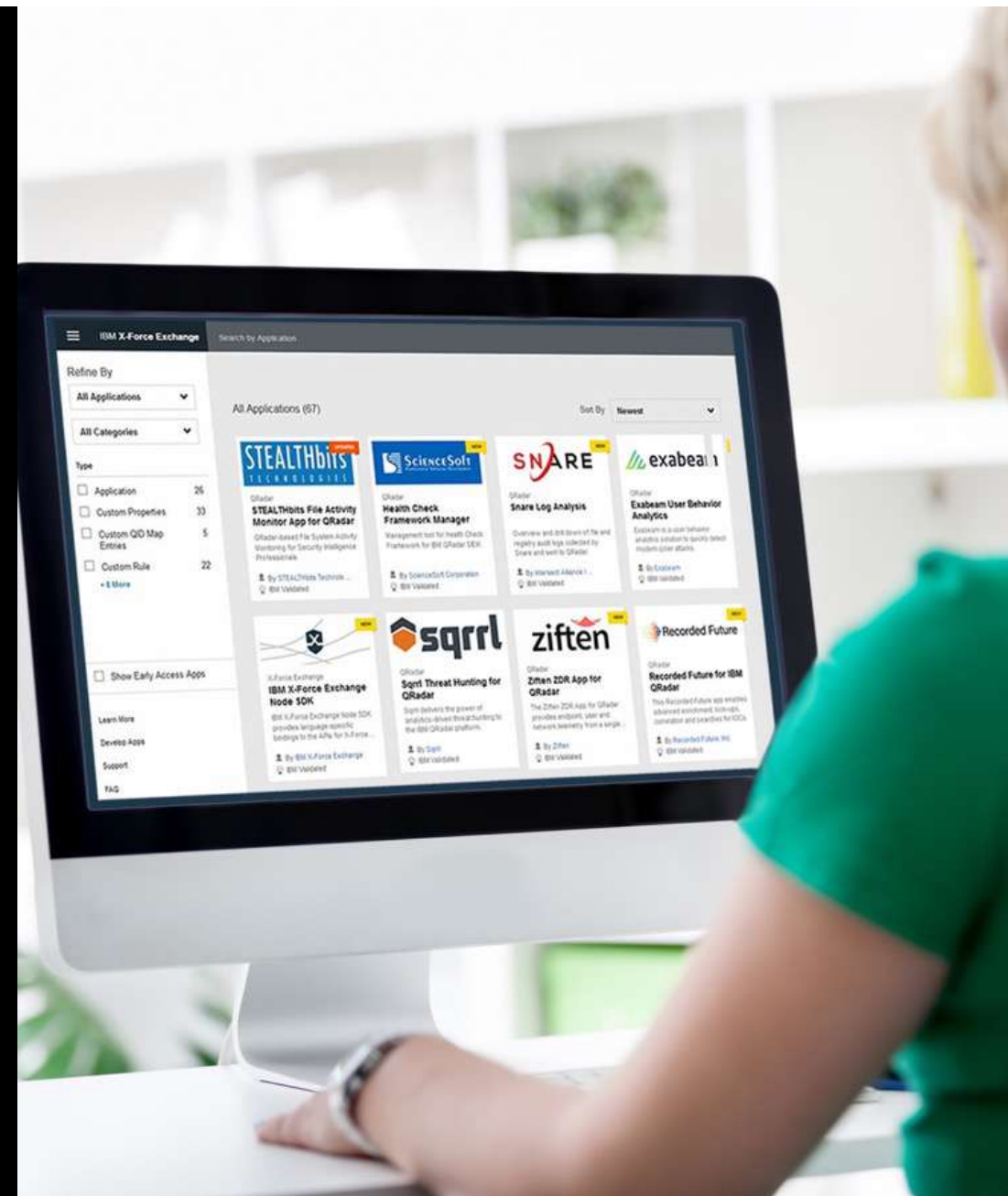
Respond to threats in minutes  
instead of hours with IBM Resilient

## **Share knowledge**

Interact with 41K+ X-Force Exchange  
users and 800+ TB of threat intelligence

## **Tailor your defenses**

Customize security with 100+ apps  
on the IBM Security App Exchange



# What our customers are facing



## COMPLIANCE MANDATES

GDPR fines can cost  
**billions**  
for large global  
companies



## SKILLS SHORTAGE

By 2022, there will be  
**1.8 million**  
unfulfilled cybersecurity  
positions



## TOO MANY TOOLS

Organizations are using  
**too many**  
tools from too many  
vendors

# Look familiar?

Security analytics

Privileged user management

Access management

User behavior analytics

Data access control

Incident response

Data protection

Endpoint patching  
and management

Fraud protection

Identity governance and administration

Network visibility and segmentation

Mainframe security

Network forensics and threat management

Vulnerability management

Firewalls

IdaaS

Malware protection

Application  
scanning

Application  
security management

Device management

Transaction protection

Sandboxing

Virtual patching

Indicators of compromise

Criminal detection

Content security

Endpoint detection  
and response

Malware analysis

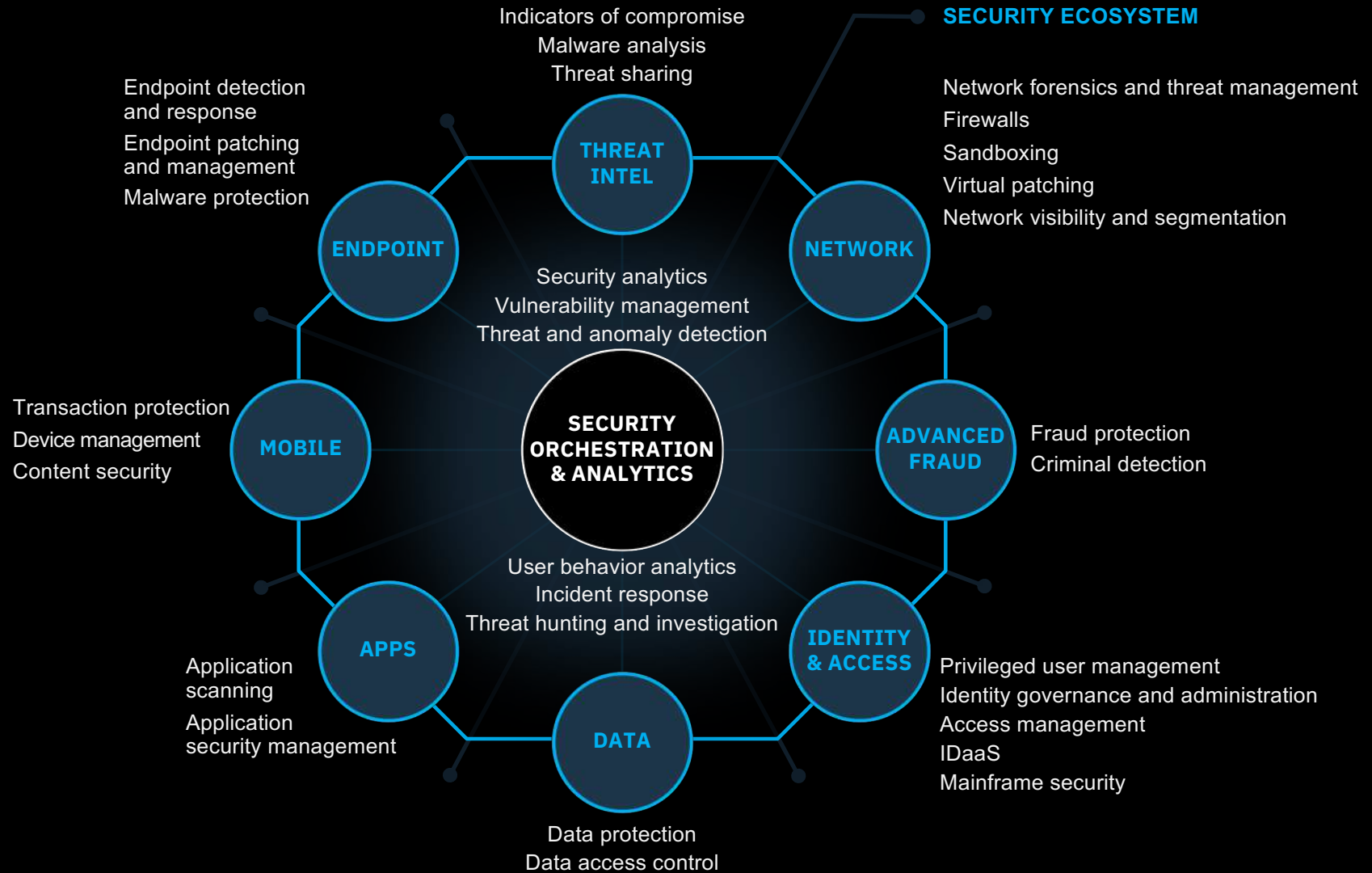
Threat and anomaly detection

Threat sharing

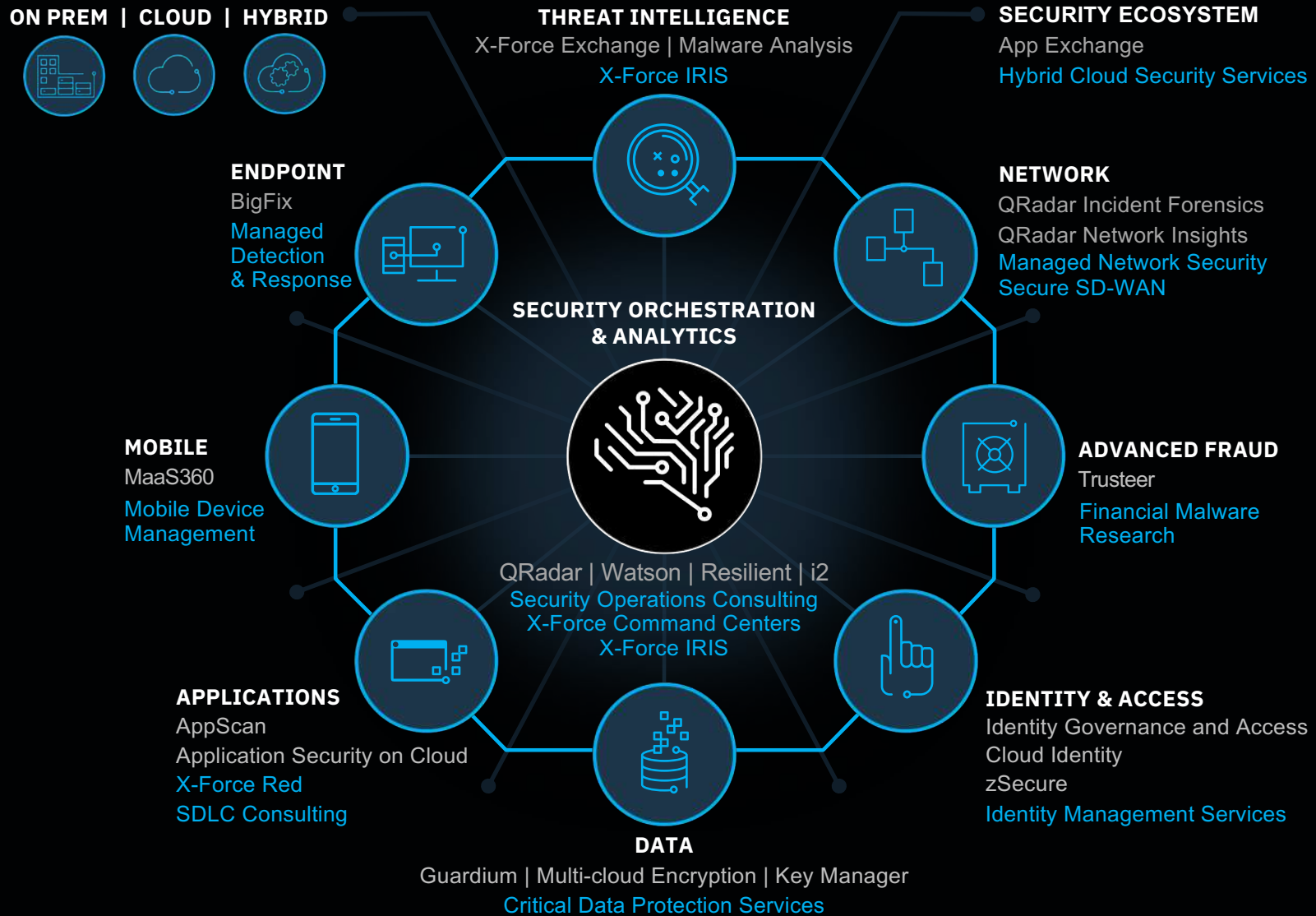
Threat hunting and investigation



# An integrated and intelligent security immune system



# IBM Security Immune System

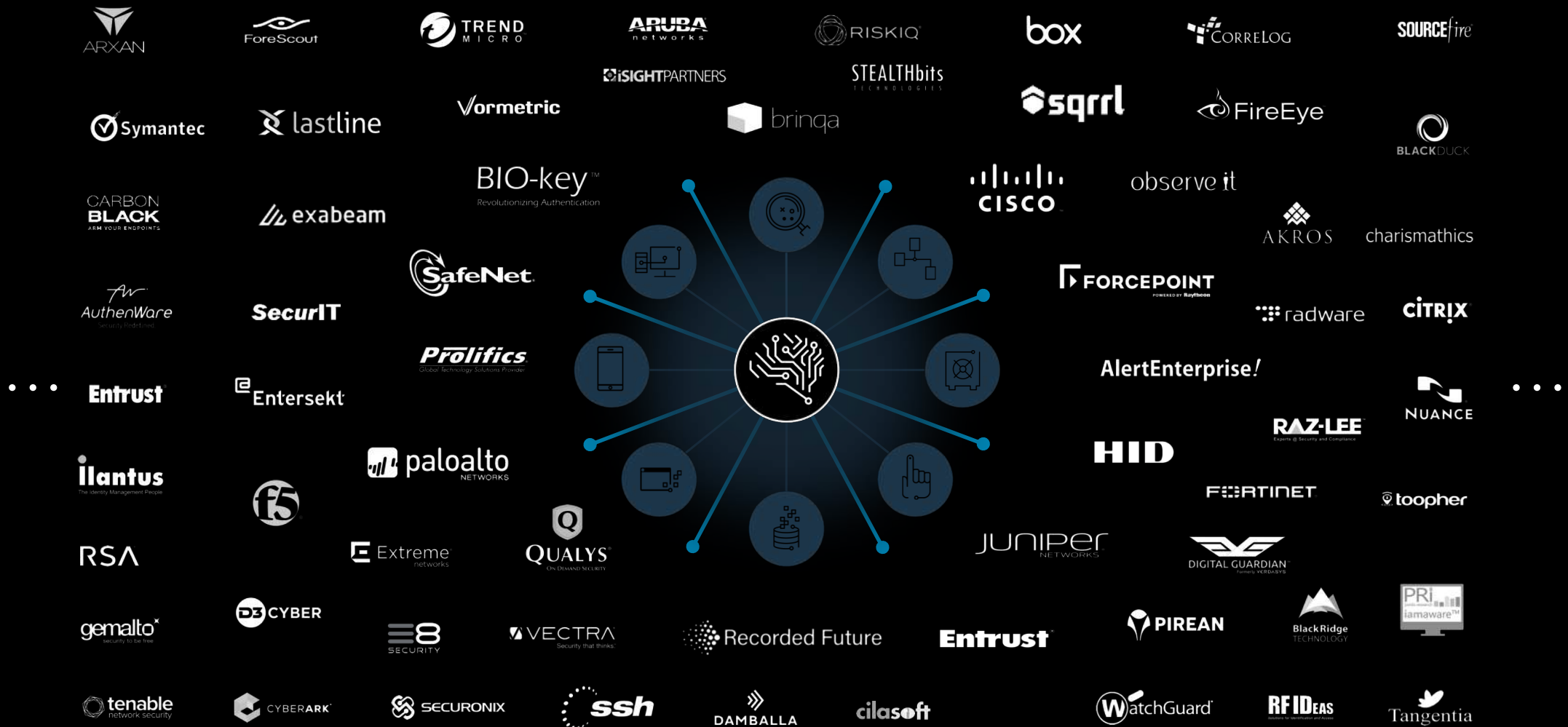


Products  
Services



# Open partner ecosystem

200+ ecosystem partners, 500+ QRadar integrations



# Let's focus on the most critical security use cases

## Outcome-driven security





# PROVE COMPLIANCE

“We need to automate and strengthen our security and endpoint management to better protect Electronic Health Record data and meet HIPAA and federal meaningful use requirements. It’s difficult to meet guidelines using point technologies and manual processes for patching 4,000+ workstations.”



**Get Ahead  
of Compliance**



**Enhance  
Security Hygiene**



**Govern Users  
and Identities**

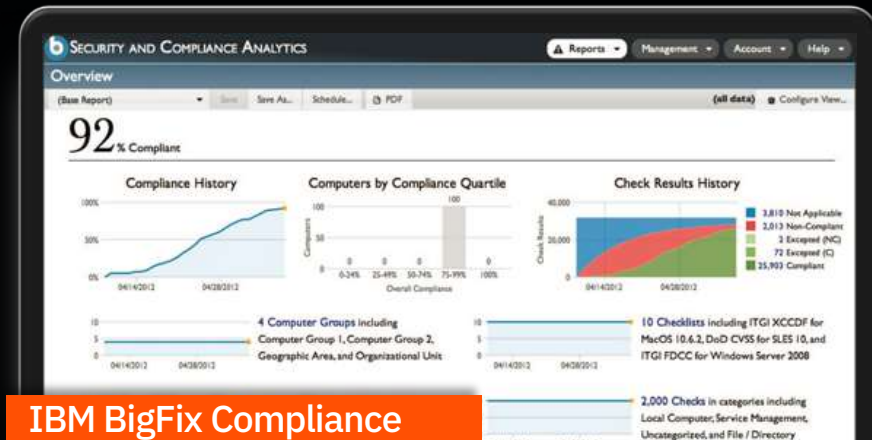


# Get ahead of compliance



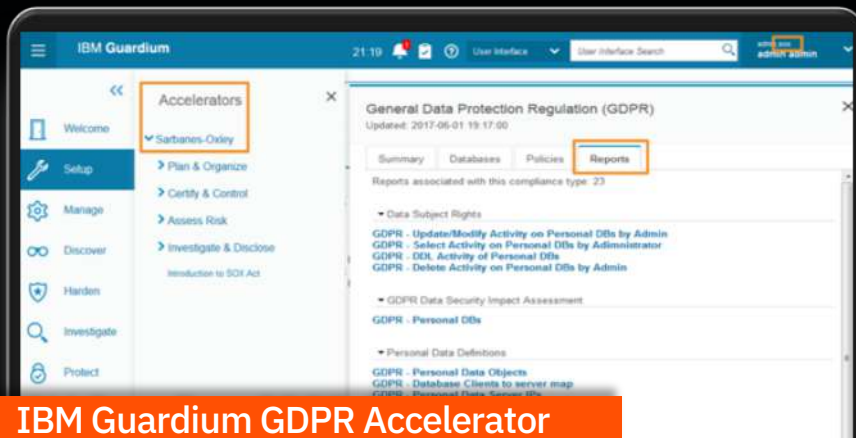
**IBM QRadar**

Monitor and enforce compliance with regulatory, standards and organizational security policies



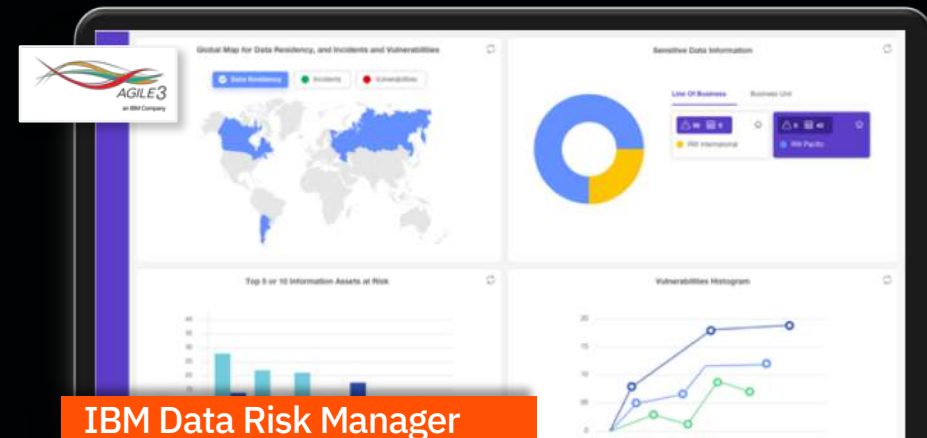
**IBM BigFix Compliance**

Continuous policy enforcement and reporting across endpoints



**IBM Guardium GDPR Accelerator**

Automate continuous control over security privacy and ensure security integrity of your critical data



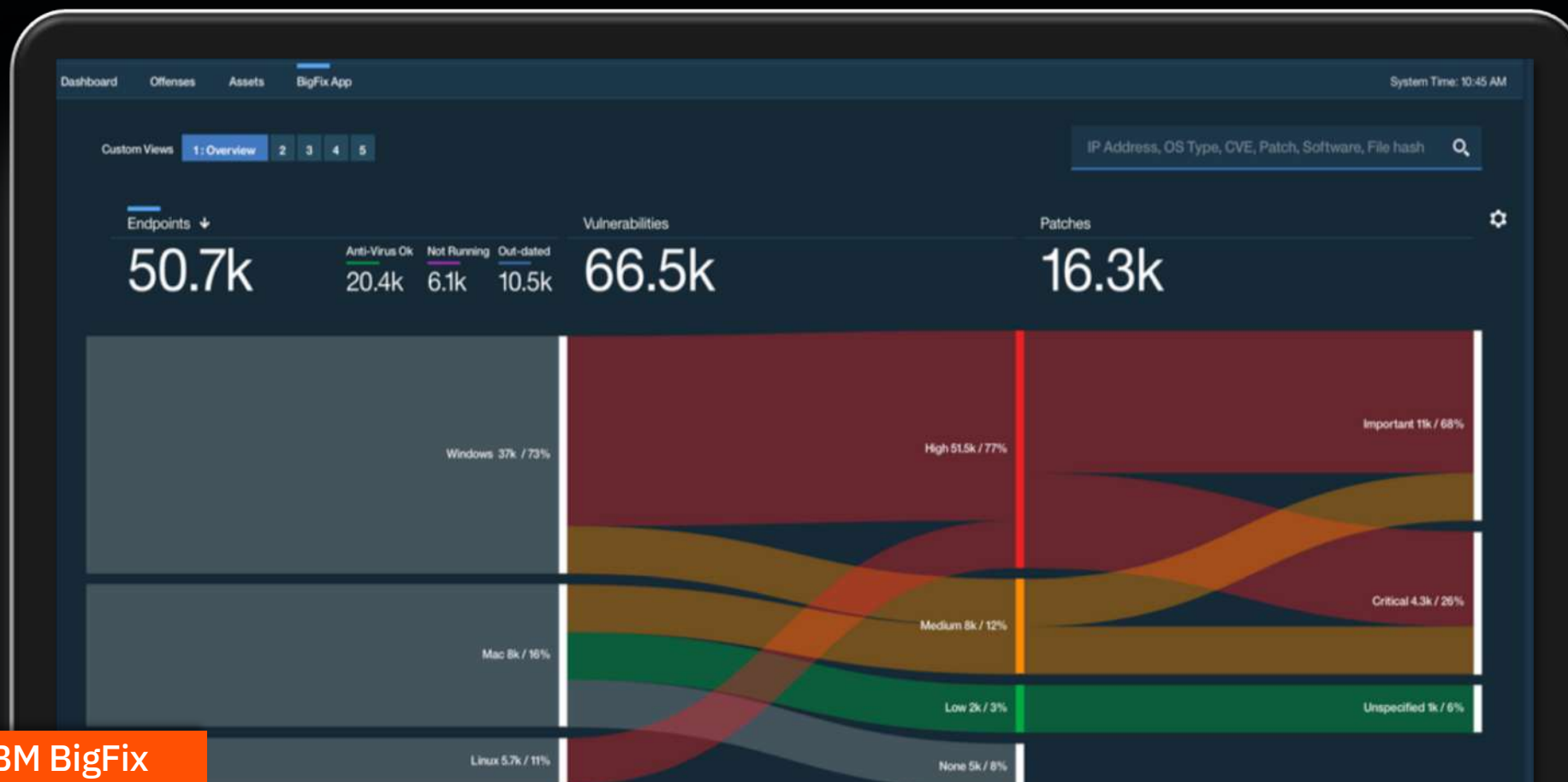
**IBM Data Risk Manager**

End-to-end view of all sensitive information assets, including apps, processes, policies, controls, and more





# Enhance security hygiene



IBM BigFix

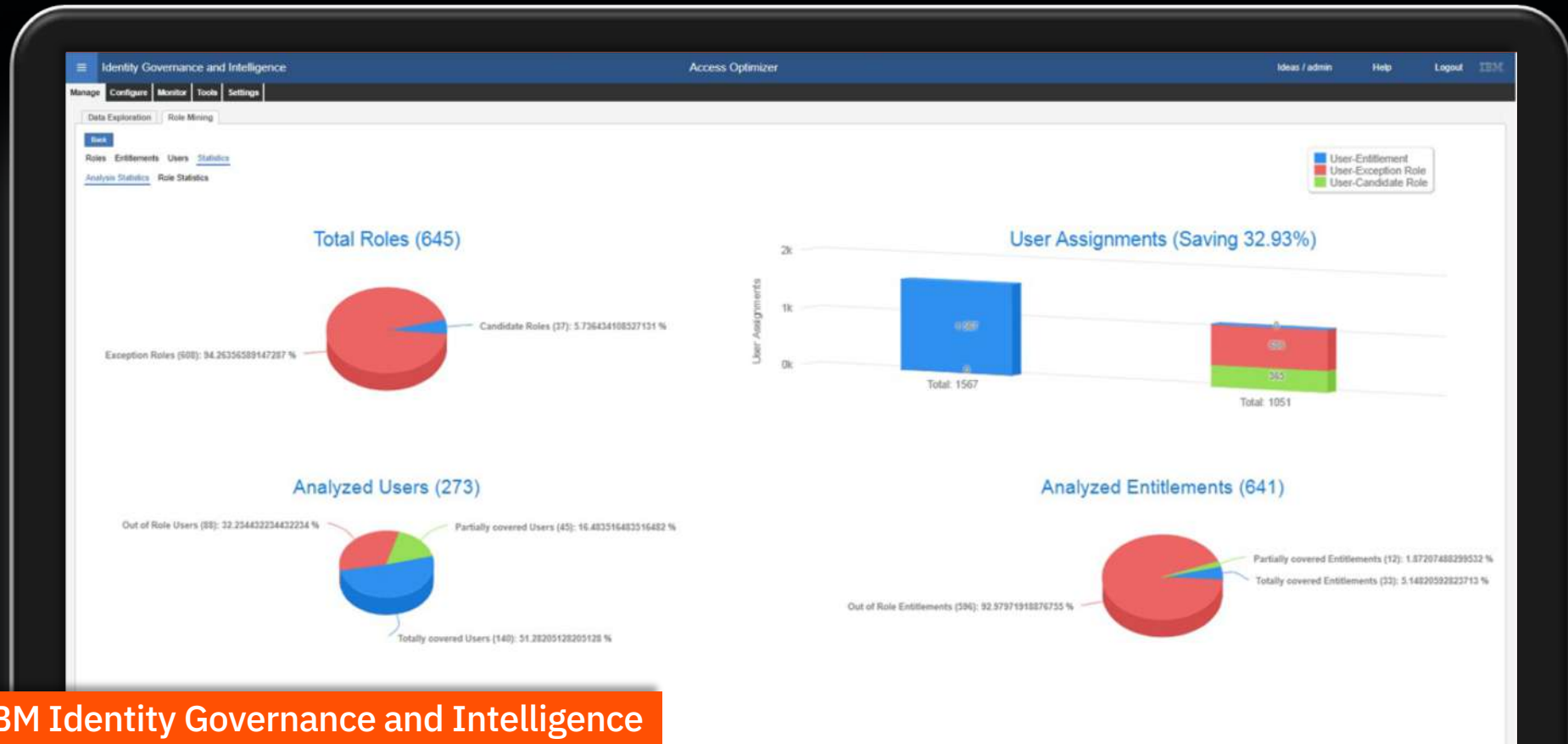
Patching, vulnerability scanning, using endpoint, asset, and user context

- Reduce operational costs
- Compress endpoint management cycles
- Enforce compliance in real-time





# Govern users and identities

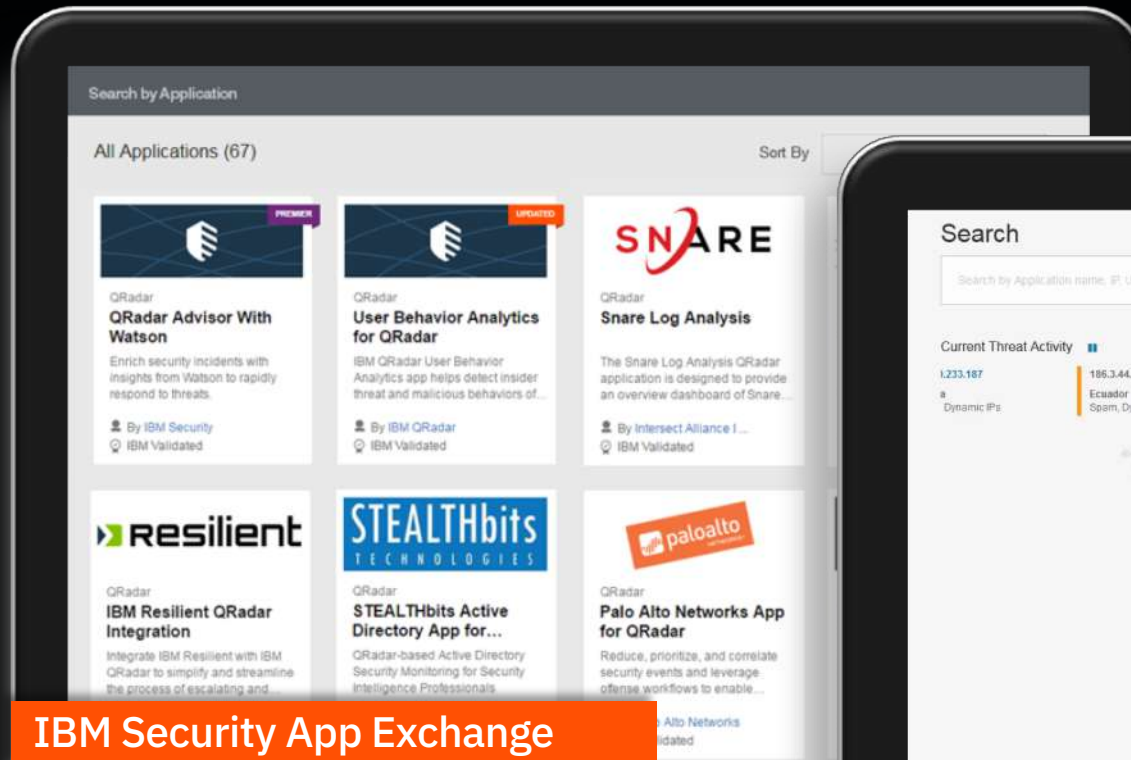


## IBM Identity Governance and Intelligence

Provisioning, governance and monitoring of employees and privileged users

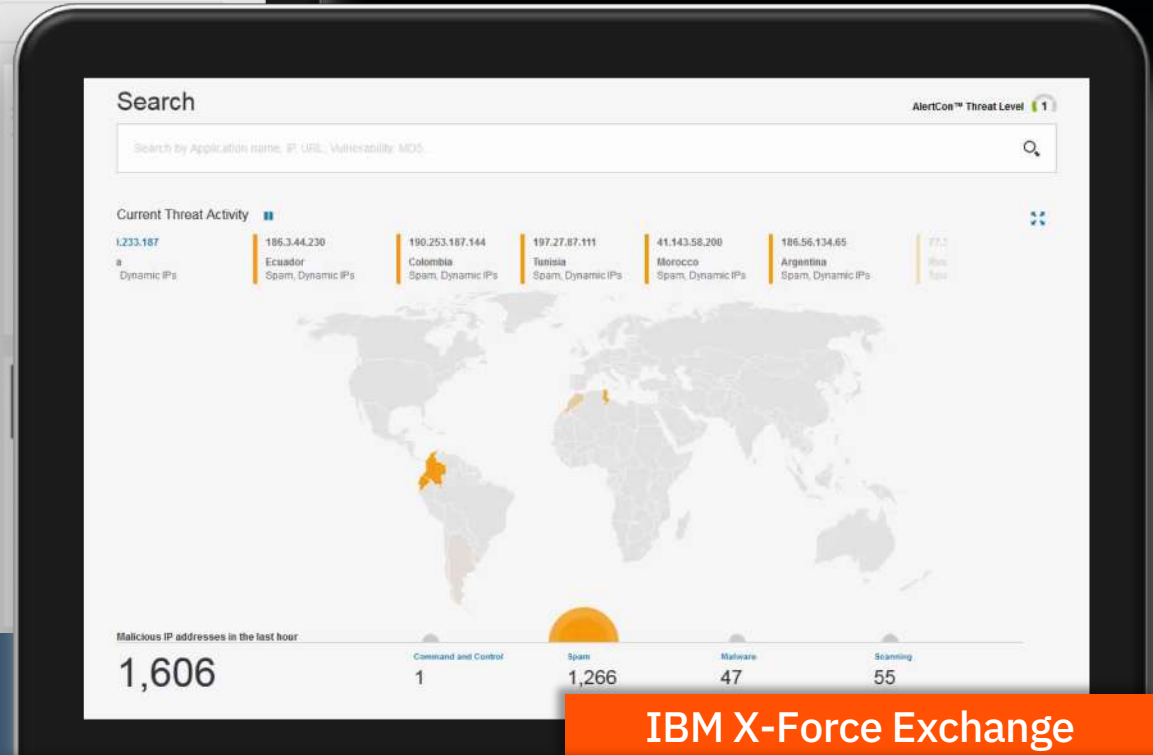
- Identify outliers using visual tools
- Risk-driven access certification with heat maps
- Identify toxic combinations with analytics

# Join an ecosystem of collaborative defenses



## IBM Security App Exchange

Share and download apps based on IBM Security controls  
200+ apps and 145K+ downloads



## IBM X-Force Exchange

Access and share real-time threat intelligence  
Over 35B monitored security events / day

# Prove compliance with help from IBM Security Services



**Help make more informed decisions through security governance and business requirements evaluation.**

- **Security strategy and planning**  
Address regulatory requirements and help protect business from growing threats
- **Ten essential practices assessment**  
Assess security and technical controls to help prepare for and pass security audits
- **Security framework and risk assessment**  
Identify IT security vulnerabilities to help mitigate business risk
- **SAP security and GRC strategy services**  
Protect critical enterprise systems from a data breach
- **Compliance advisory services**  
Enhance security with gap assessments, readiness reviews and remediation reports for compliance
- **Critical infrastructure security**  
Use the new NIST Cybersecurity Framework to better protect critical infrastructure assets

A person is seen from behind, wearing a headset, sitting at a desk in a control room. The room is filled with multiple computer monitors. The central monitor displays a dashboard with a red globe icon, various charts, and data points. Other monitors in the background show a blue shield icon with a white 'X' and a stylized sun logo. The overall scene is dimly lit, emphasizing the digital displays.

# STOP THREATS

“We need help analyzing huge amounts of information in real-time to identify trends and useful information for more actionable insights.”



**Detect & Stop  
Advanced Threats**



**Orchestrate  
Incident Response**

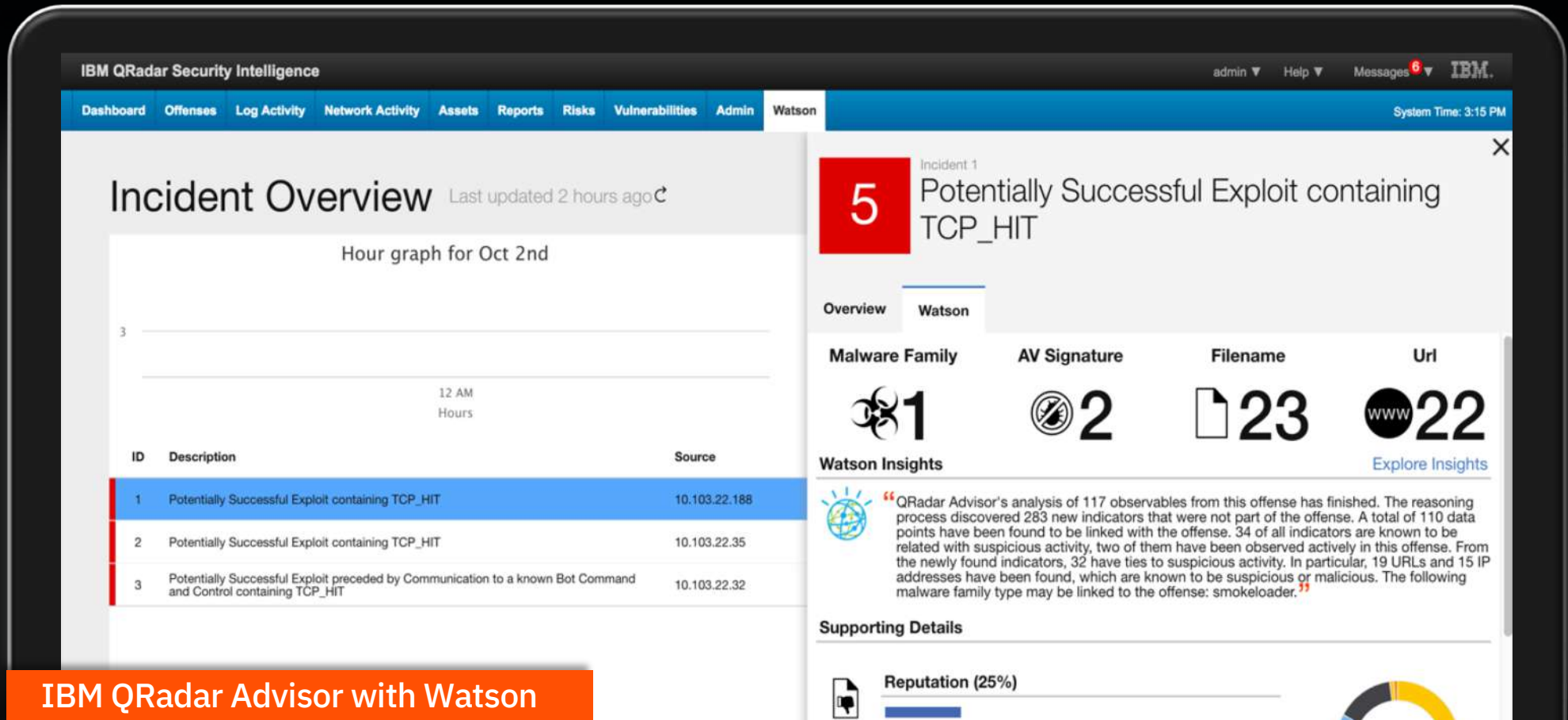


**Master  
Threat Hunting**





# Detect and stop advanced threats



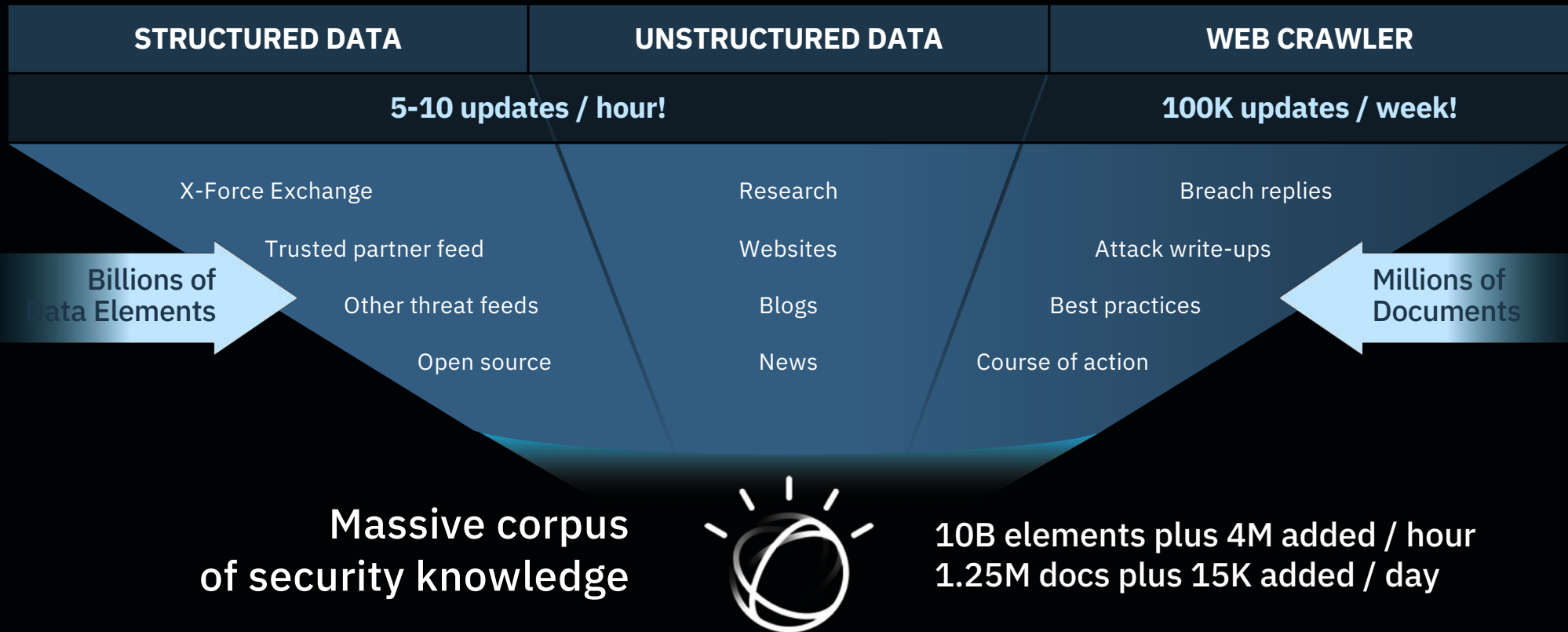
## IBM QRadar Advisor with Watson

Automatically uncover the full scope of a security incident

- **2.3M+** security documents
- **10B+** security data elements
- **80K+** documents read per day
- **250K+** investigations enhanced



# How Watson for Cyber Security works



**50** beta customers  
**140K+** web visits in 5 weeks  
**200+** trial requests

## SEE THE BIG PICTURE

"QRadar Advisor enables us to truly understand our risk and the needed actions to mitigate a threat."



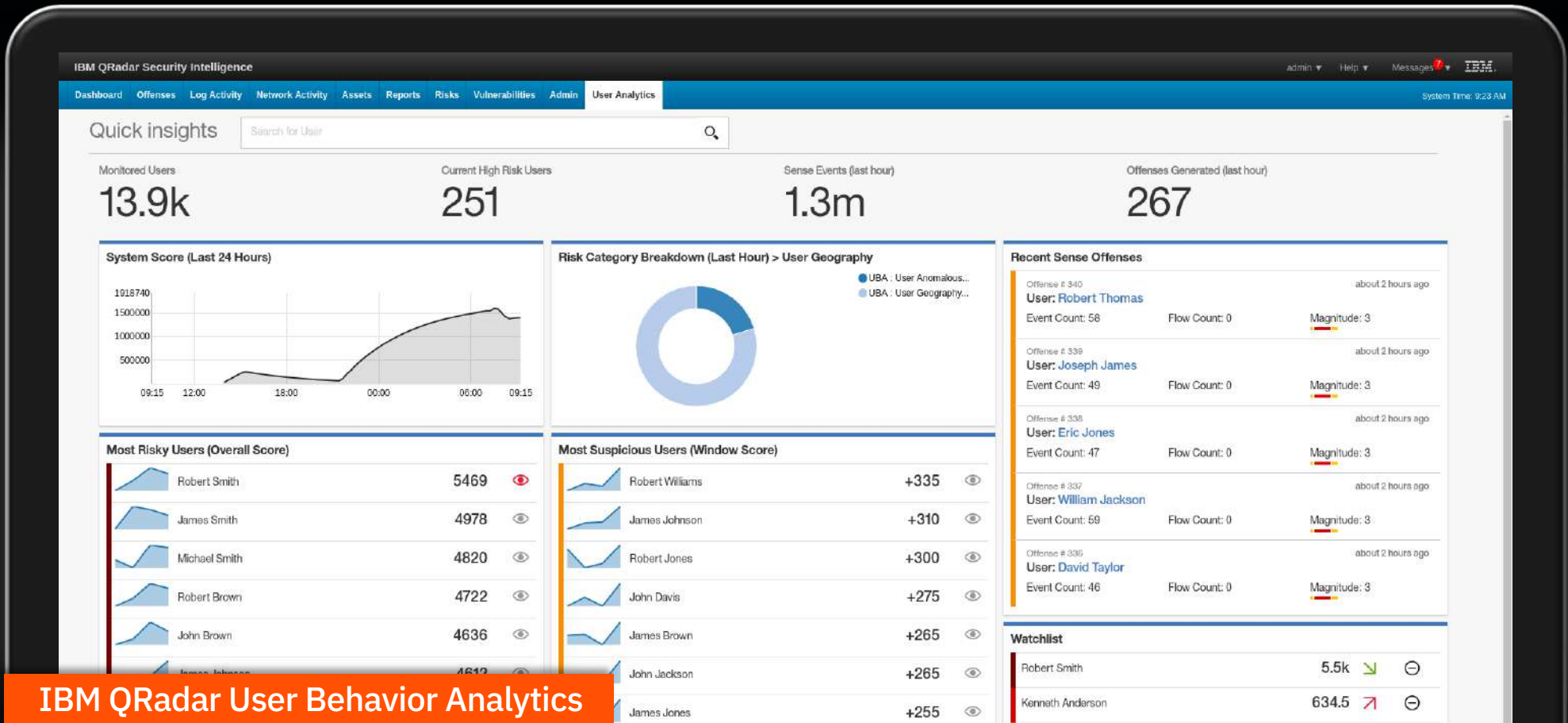
## ACT WITH SPEED & CONFIDENCE

"The QRadar Advisor results in the enhanced context graph is a BIG savings in time versus manual research."





# Detect and stop advanced threats



## IBM QRadar User Behavior Analytics

Advanced analytics for advanced threat detection and response across the enterprise

The User Behavior Analytics dashboard is an integrated part of the QRadar console



# Orchestrate incident response

The screenshot displays the IBM Resilient web interface for incident response. The top navigation bar includes the Resilient logo, a dropdown menu for 'Dashboards', and buttons for 'List Incidents', 'New Incident', 'My Tasks', 'Simulations', and a search bar. The user 'Adam Koblentz' is logged in. The main content area shows details for an incident with a severity of 'High', created on '07/13/2016', and identified as 'Malware'. It lists the destination network, protocol, and QID. Below this, a 'News Feed' tab is selected, showing a timeline of activities: a note by Marc Makowski, a quote from Carlo Alpuerto, a task reassignment by Marc Makowski, and a data table update by Zach Taira. A sidebar on the left lists the incident's creator, owner, and members.

**resilient** Dashboards ▾ List Incidents New Incident My Tasks Simulations Search

Adam Koblentz  
Resilient Systems ▾

Severity: High  
Date Created: 07/13/2016  
Date Occur...: —  
Date Discov...: 07/13/2016  
Data Compr...: Yes  
Incident Type: **Malware**

Destination Network: Net-10-172-192.Net\_192\_168\_0\_0  
Protocol: other(255)  
QID: 28250184

Tasks Details Members Artifacts Notes Attachments **News Feed** Stats Timeline Breach

**People**  
Created By: Tim Armstrong  
Owner: Zach Taira  
Members: Carlo Alpuerto, Jody Cannady, Ethan Goldstein

**Related Incidents**  
#3852 Proofpoint Sample Alert 34342

**News Feed** Show Types All ▾

- an hour ago: Marc Makowski wrote a note on the task [Initial Triage](#)  
“Carlo Alpuerto Can you finish today?”
- an hour ago: Marc Makowski reassigned task [Notify internal management chain \(preliminary\)](#)
- ago: Zach Taira added a row to the Data Table [Task History](#)

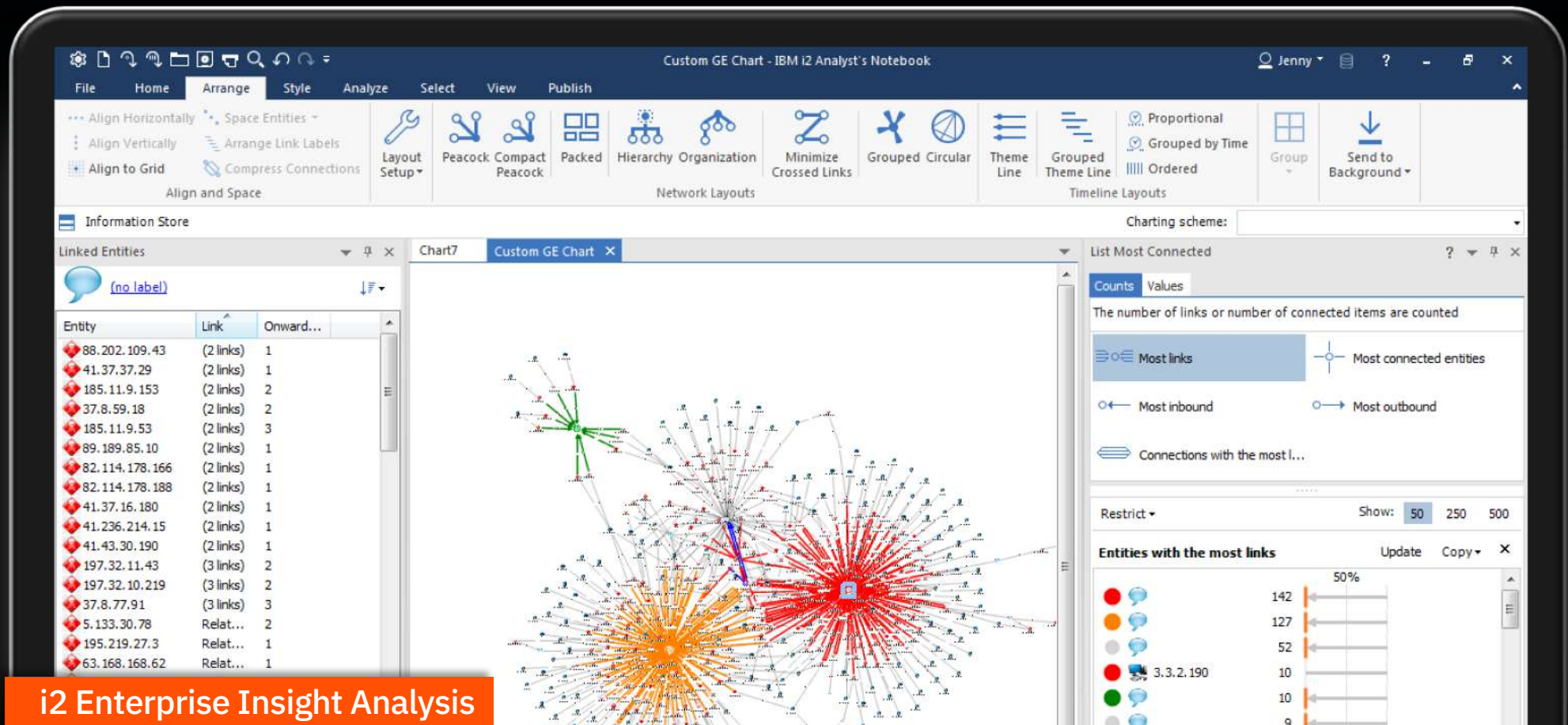
## IBM Resilient Incident Response

End-to-end workflow, collaboration, actions and expertise to respond with confidence

- Hunt for indicators using deep forensics
- Deploy response procedures and expertise



# Master threat hunting



## i2 Enterprise Insight Analysis

Analyst-driven investigations using big data and threat intelligence to get ahead of the threats

- Visually investigate with built-in analytics to uncover hidden threats faster
- Easily combine both structured and unstructured data to support investigative analysis





# GROW BUSINESS

“We need to secure the records of 475,000+ members while managing critical database access across our hybrid environment... we need help.”



Secure  
Hybrid Cloud



Protect  
Critical Assets



Deliver  
Digital Trust



# Secure hybrid cloud



## Protect data

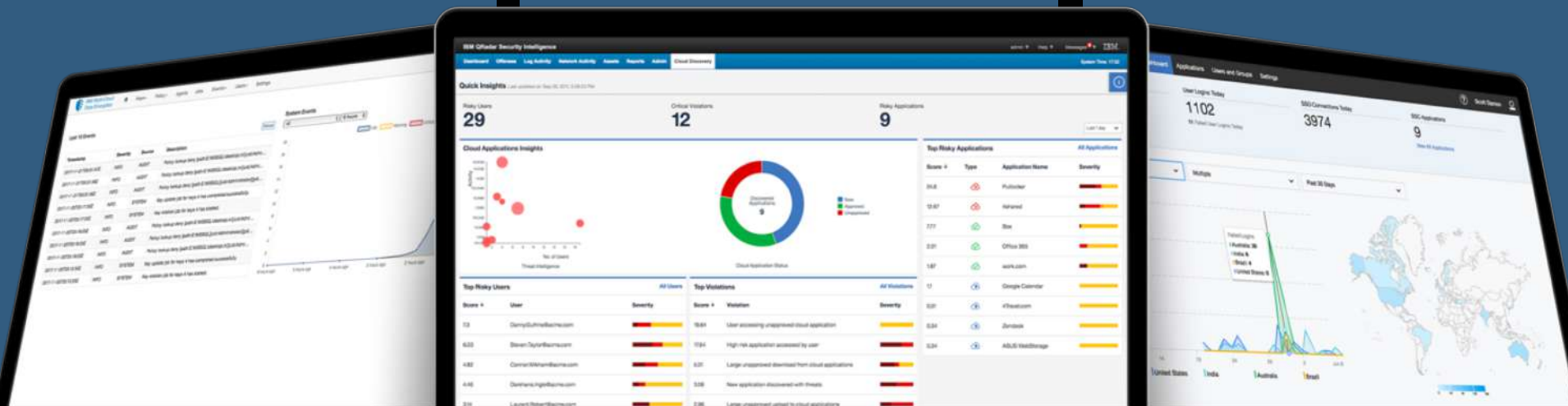
IBM Multi-Cloud Data Encryption

## Gain visibility

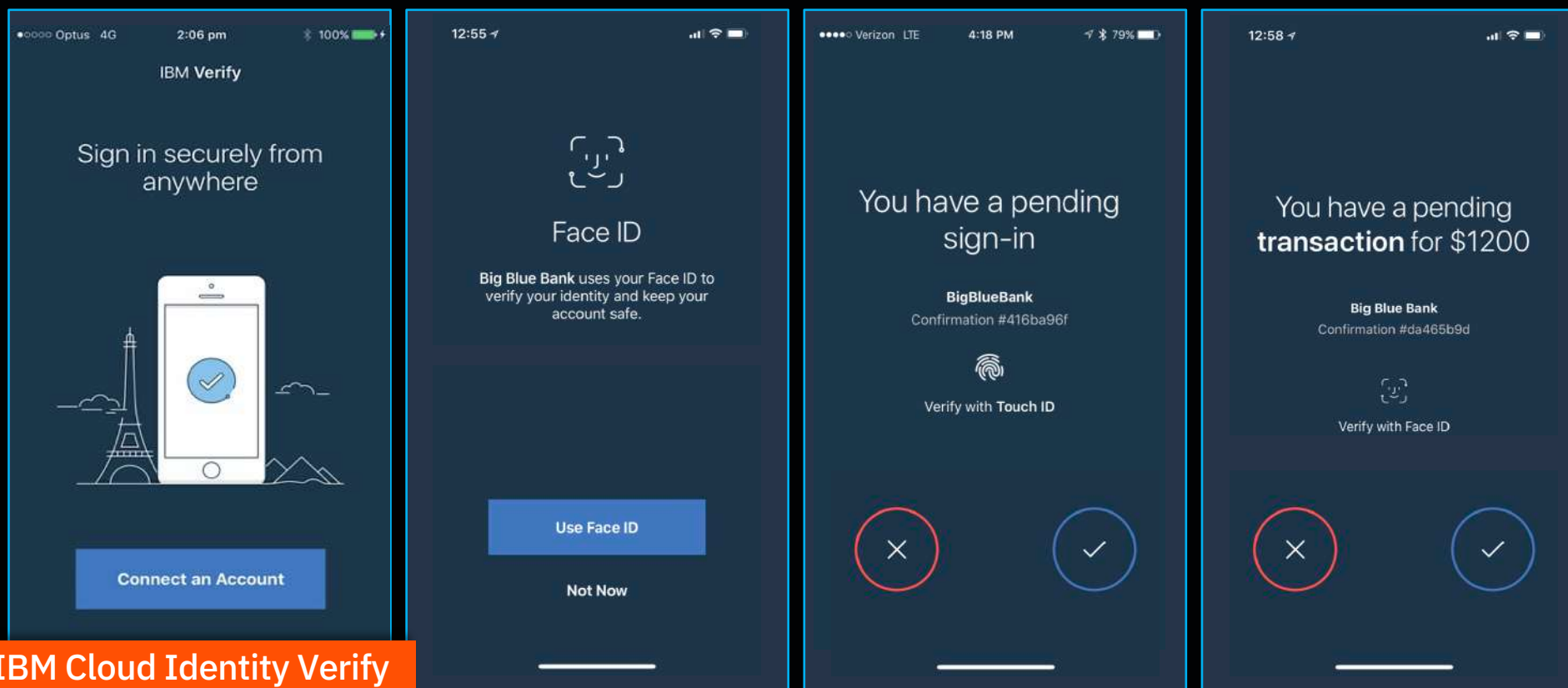
IBM QRadar Cloud Discovery App

## Manage access

IBM Cloud Identity Connect



# Secure hybrid cloud



## IBM Cloud Identity Verify

Bring simple and strong multi-factor authentication to online services



- Simple strong authentication from the cloud
- Check-box risk assessment and user authentication policies
- IBM Verify App with push driven TouchID and FaceID authentication

# Secure hybrid cloud



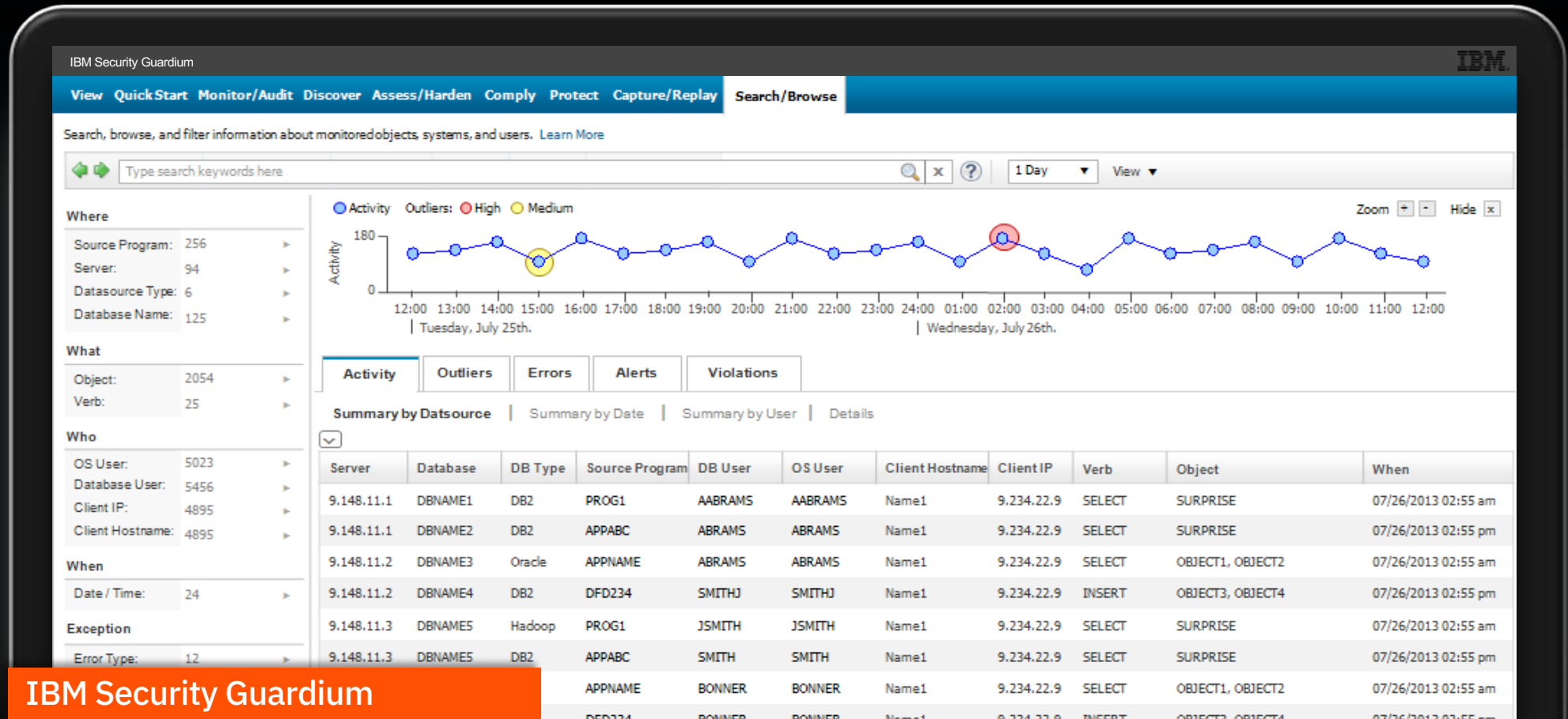
IBM Security Guardium

Secure applications built  
in a multi-cloud environment

- Automatically discover and classify sensitive data
- Understand data access, spot anomalies, stop data loss



# Protect critical assets



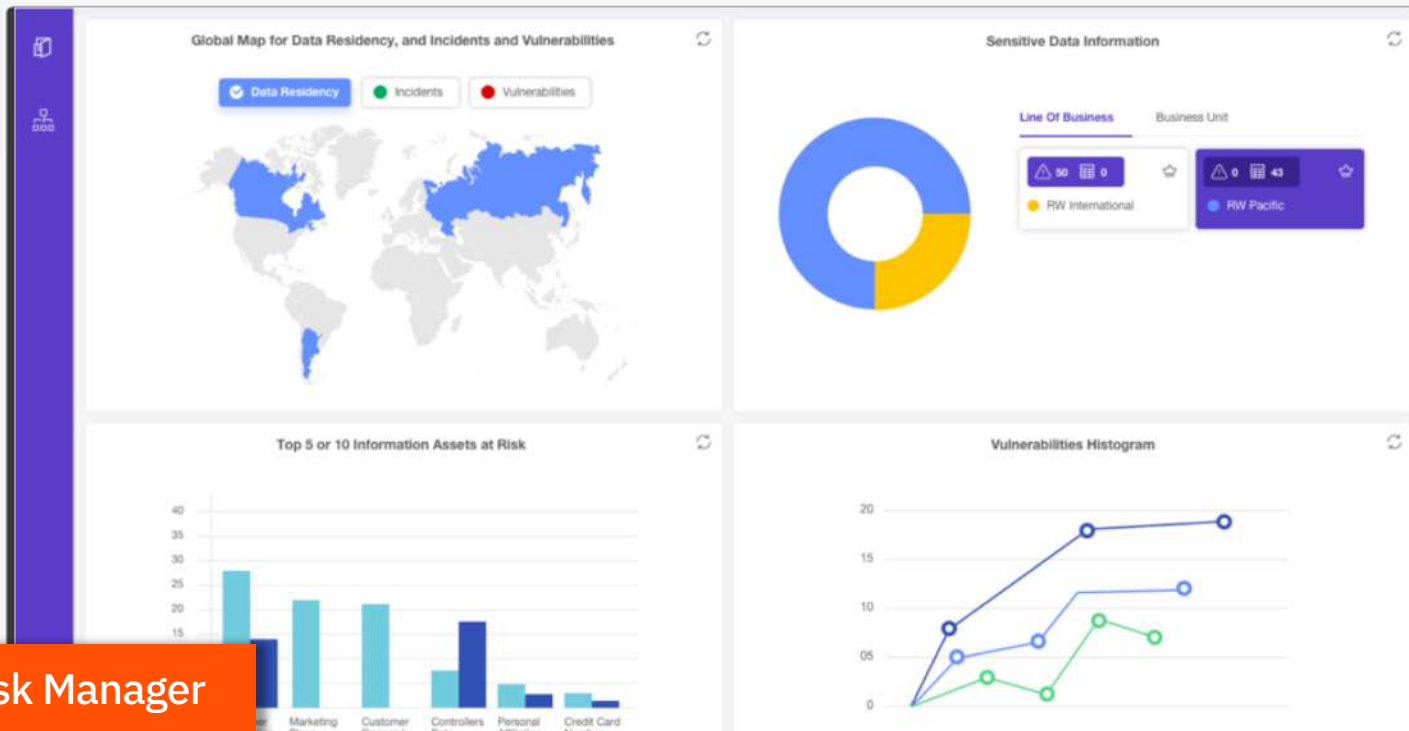
## IBM Security Guardium

Shield the business from data risk with automated compliance and audit capabilities

- Automatically discover and classify sensitive data
- Understand data access, spot anomalies, stop data loss



# Protect critical assets



## IBM Data Risk Manager

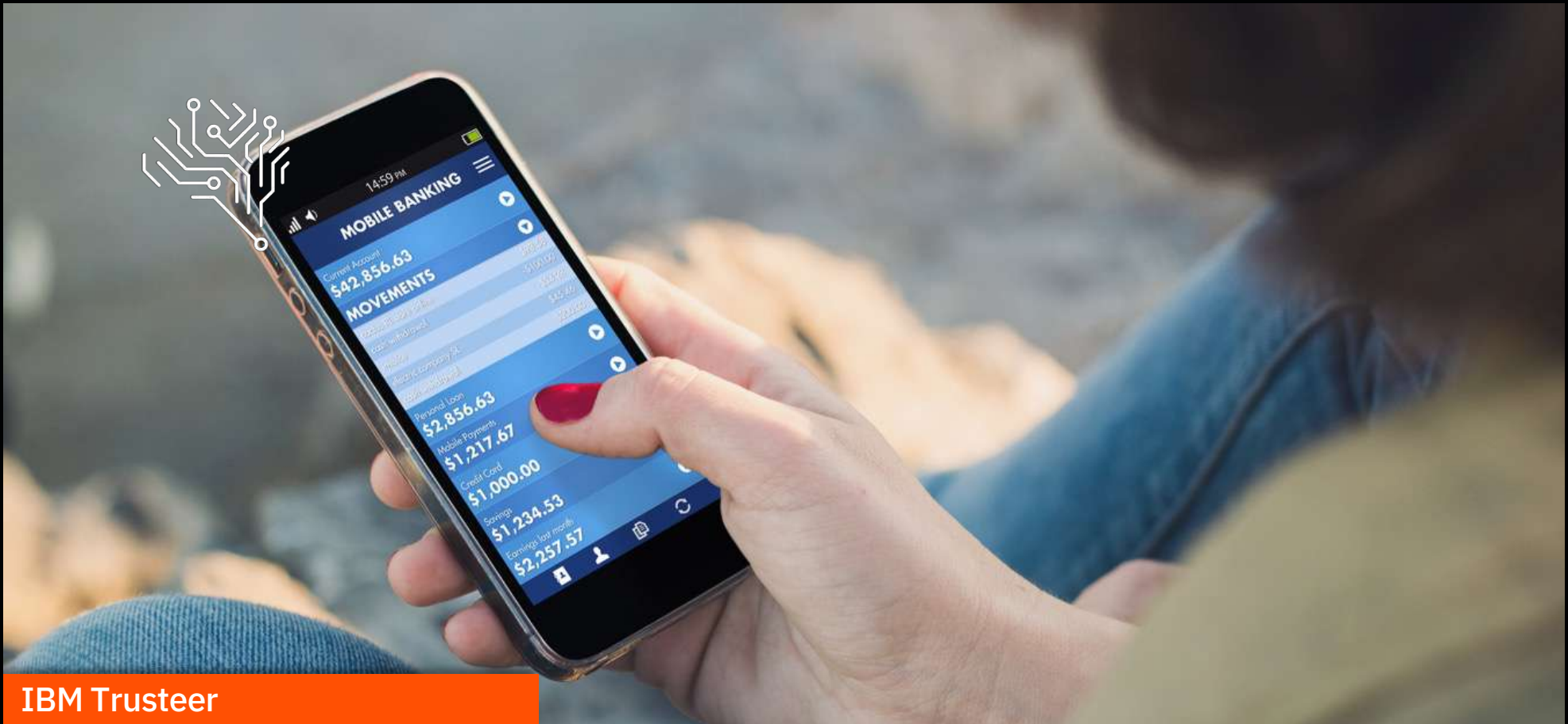
Uncover, analyze and visualize data-related business risks

- Identify specific, high-value, business-sensitive information assets
- Gain early visibility into potential risks to data and processes
- Inform executives with a business-consumable data risk control center





# Deliver Digital Trust



## IBM Trusteer

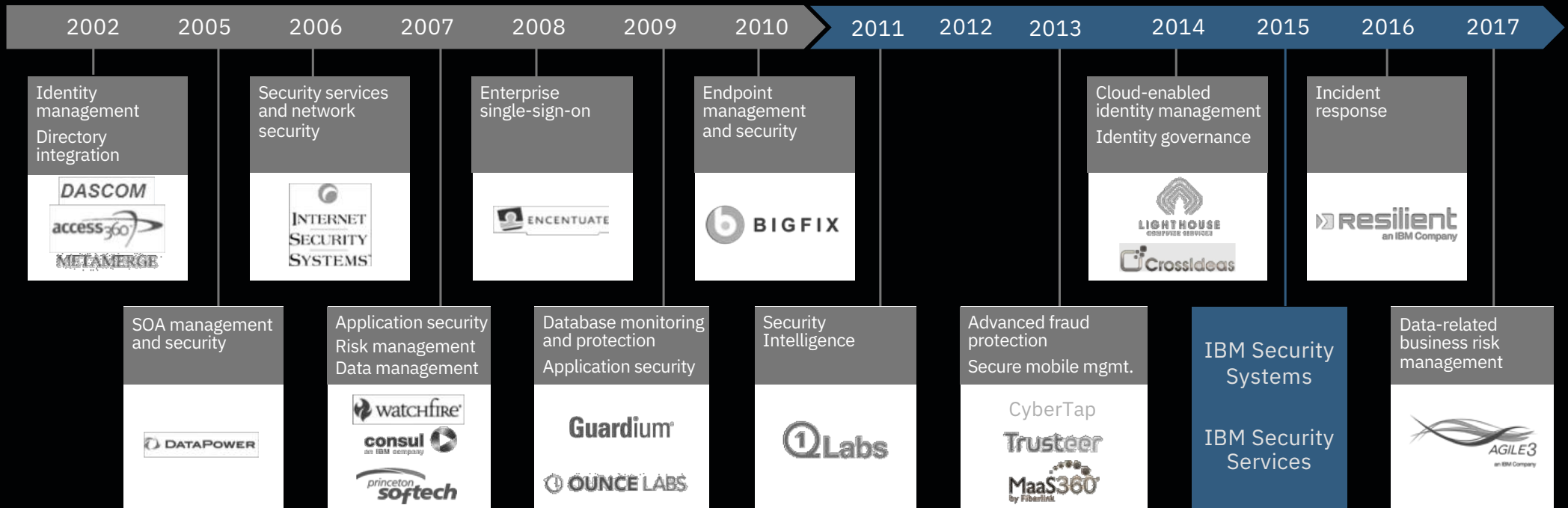
**Helps organizations seamlessly establish identity trust across the omnichannel customer journey**

- Intelligence service layered with advanced AI and machine learning capabilities
- Scalable and agile cloud platform providing real-time assessments
- Continuous digital identity assurance

# We've built the largest security start-up in the world



IBM Security



“...IBM Security is making all the right moves...”

Forbes

# IBM Security: Leader across 12 security market segments

DOMAIN	SEGMENT	MARKET SEGMENT / REPORT	ANALYST RANKINGS
Security Operations and Response	Security Intelligence	Security Information and Event Management (SIEM)	LEADER
		Security Analytics	LEADER
	Network & Endpoint Protection	Endpoint: Client Management Tools	LEADER
Information Risk and Protection	Identity Governance & Access Management	Identity and Access Governance	LEADER
		Access Management (worldwide)	LEADER
		Identity and Access Management as a Service (IDaaS)	LEADER
		Identity Provisioning Management	LEADER
	Data Security	Database Security	LEADER
	Application Security	Application Security Testing (dynamic and static)	LEADER
	Mobile Protection	Enterprise Mobility Management (MaaS360)	LEADER
	Fraud Protection	Web Fraud Detection (Trusteer)	LEADER
Security Transformation Services	Consulting and Managed Services	Managed Security Services (MSS)	LEADER

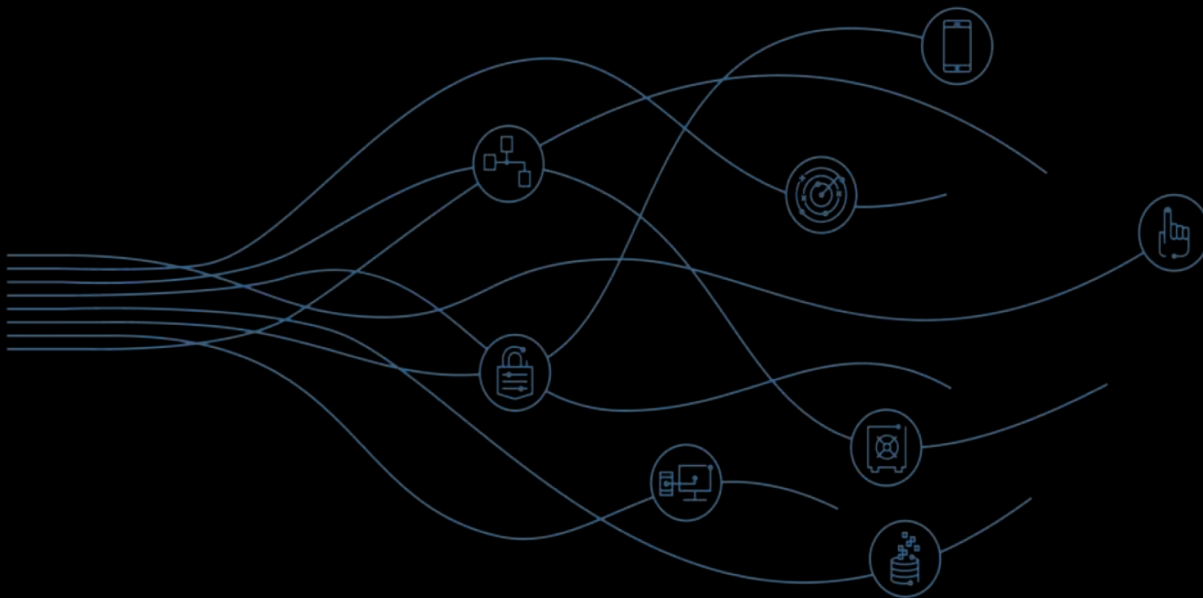
Note: This is a collective view of top analyst rankings, compiled as of April, 2018

# A global leader in enterprise security



IBM Security


- **LEADER** in 12 out of 12 security market segments
- **8,000+** employees
- **17,500+** customers
- **133** countries
- **3,500+** security patents
- **20** acquisitions since 2002





# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [ibm.com/security/community](https://ibm.com/security/community)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2018. 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.







Help clients stop threats

**60x faster**

security threat investigations with Watson  
compared to manual analysis

**5x increase**

in volume of security incidents analyzed  
over the course of the tournament

**Zero**

breaches impacted the 2017 Wimbledon  
website and brand

IBM Security helps  
protect the oldest  
brand in tennis  
with the latest in  
cognitive security.



## Help clients prove compliance

**95%** **lower time and cost**

Reduced endpoint licensing costs and reduced time to deploy software by 95%

**90%** **patch compliance**

Went from an average of 40% patch compliance to 90%

Infirmity Health System helps secure endpoints and better detect and respond to threats across the organization while meeting all data security requirements and easily demonstrate compliance for federal incentives.

“We can now quickly, easily and accurately produce audit reports for HIPAA and meaningful use compliance.”

Chief Information Officer  
Infirmity Health System



# Cybersecurity is a universal challenge

By 2020, there will be...

**20.8 billion**

“things” to secure

**5 billion**

personal data records stolen

**\$8 trillion**

lost to cybercrime

...while security pressures continue to grow



**COMPLIANCE  
MANDATES**

GDPR fines can cost

**billions**

for large global companies



**SKILLS  
SHORTAGE**

By 2022, there will be

**1.8 million**

unfulfilled cybersecurity jobs



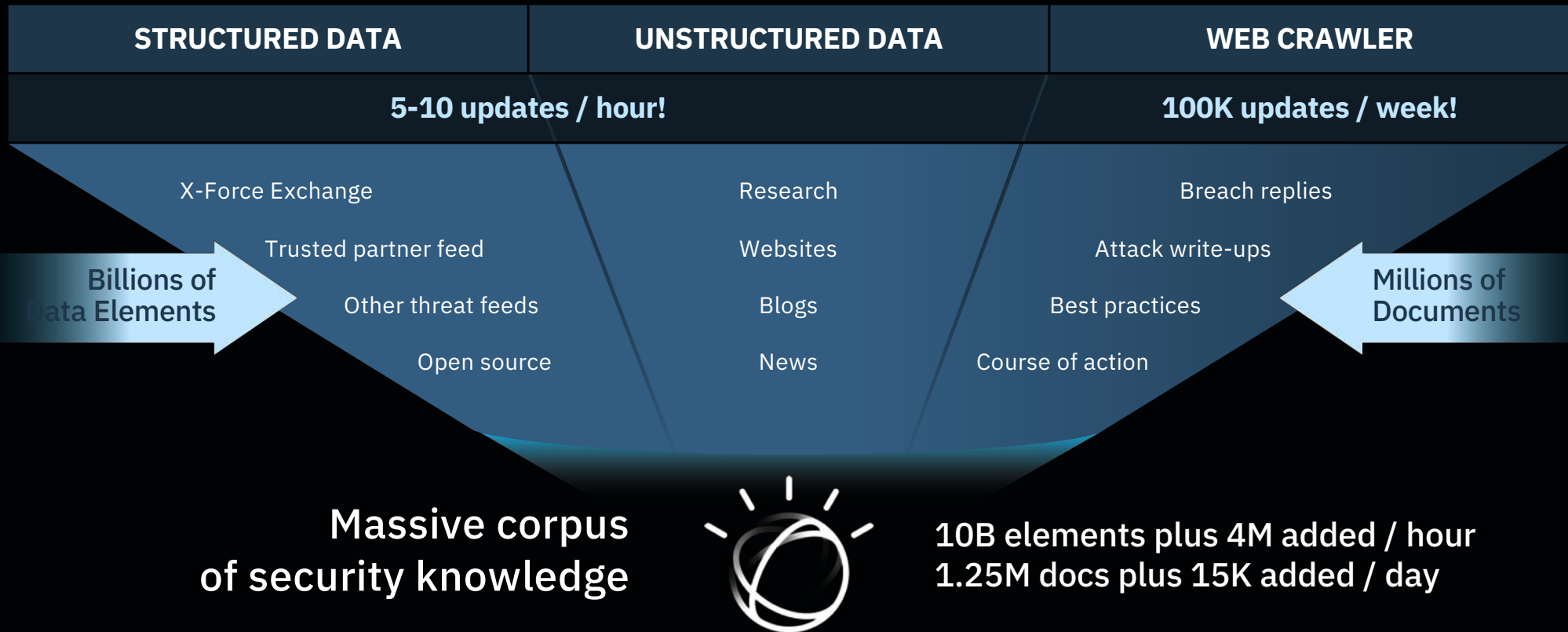
**TOO MANY  
TOOLS**

Organizations are using

**too many**

tools from too many vendors

# How Watson for Cyber Security works



**50** beta customers  
**140K+** web visits in 5 weeks  
**200+** trial requests

## SEE THE BIG PICTURE

"QRadar Advisor enables us to truly understand our risk and the needed actions to mitigate a threat."

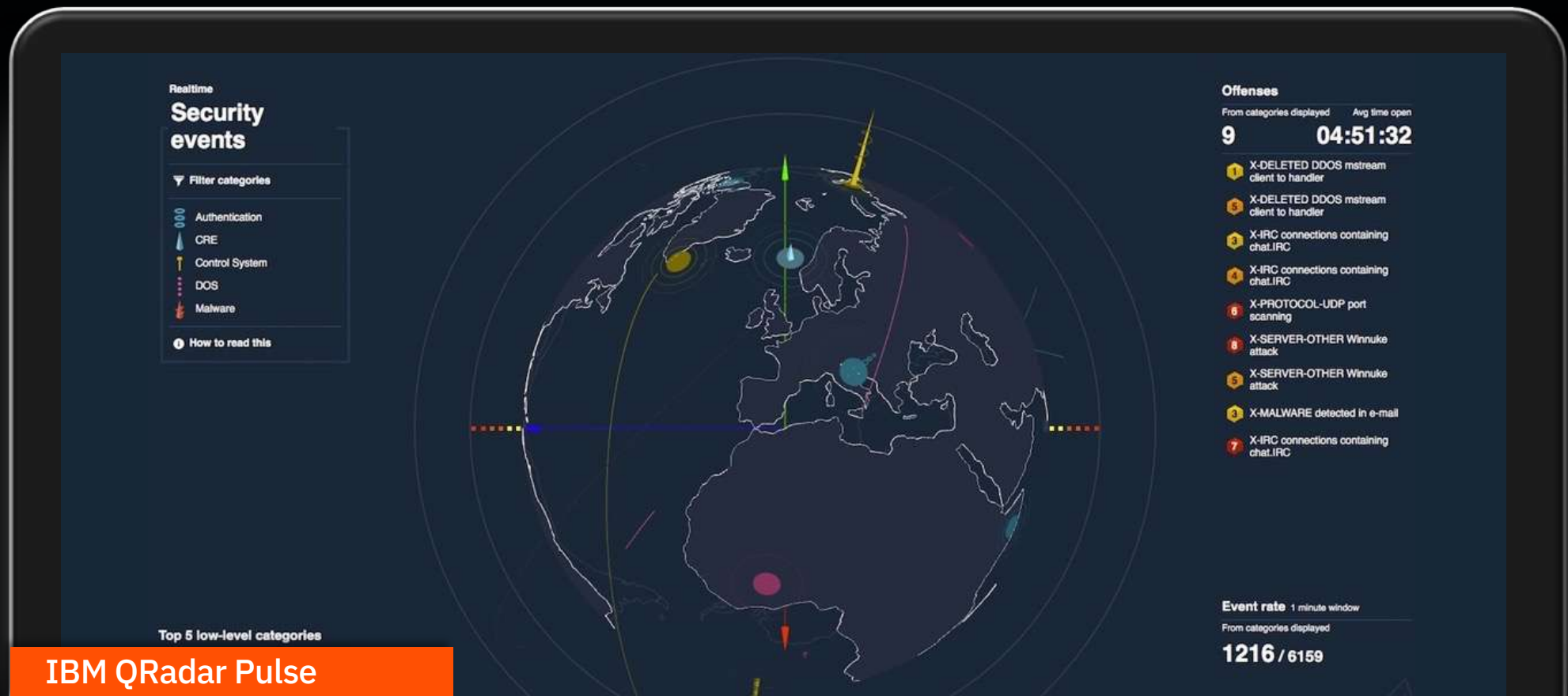


## ACT WITH SPEED & CONFIDENCE

"The QRadar Advisor results in the enhanced context graph is a BIG savings in time versus manual research."



# Visualize critical threats



## IBM QRadar Pulse

Experience the 'Pulse' of your security environment in beautiful 3D

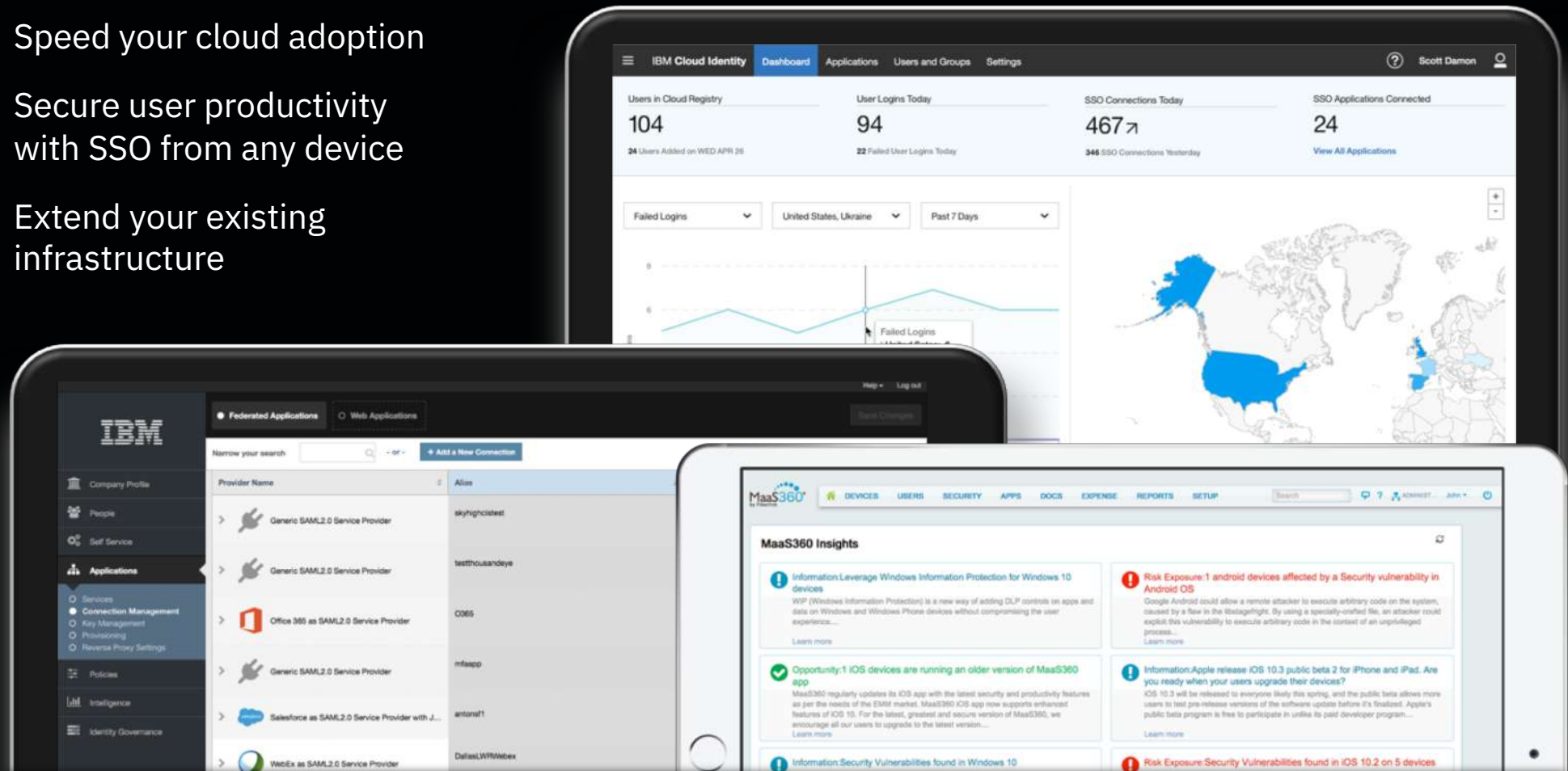
- Provides a quick overview of near real-time offenses – perfect for large viewing in a SOC
- Tracks security threats from around the globe



# Give users and employees quick access to the cloud

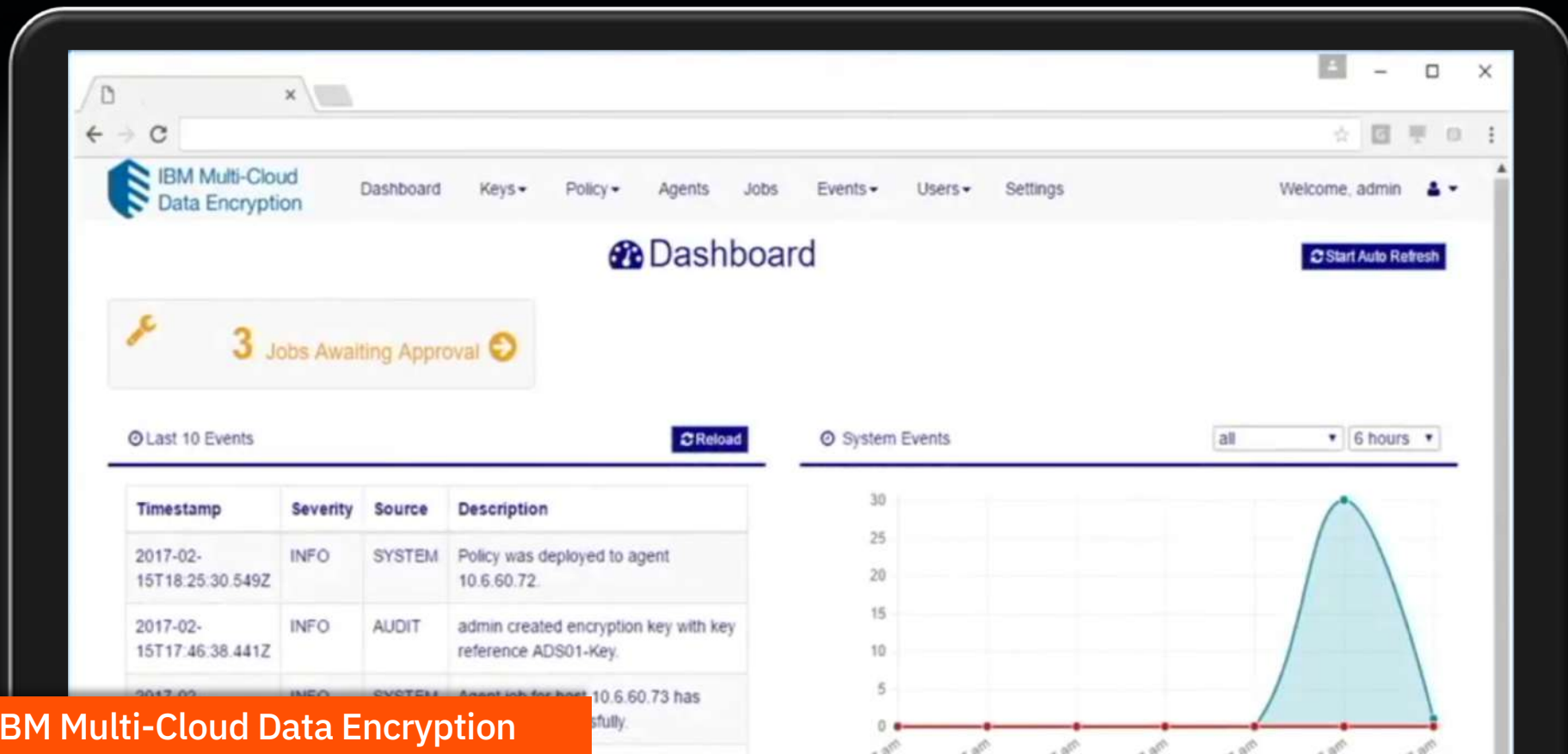
## New born-in-the-cloud solutions to...

- Speed your cloud adoption
- Secure user productivity with SSO from any device
- Extend your existing infrastructure



IBM Cloud Identity Service | IBM Cloud Identity Connect | IBM MaaS360 with Watson

# Protect data in single, multiple, or hybrid cloud environments

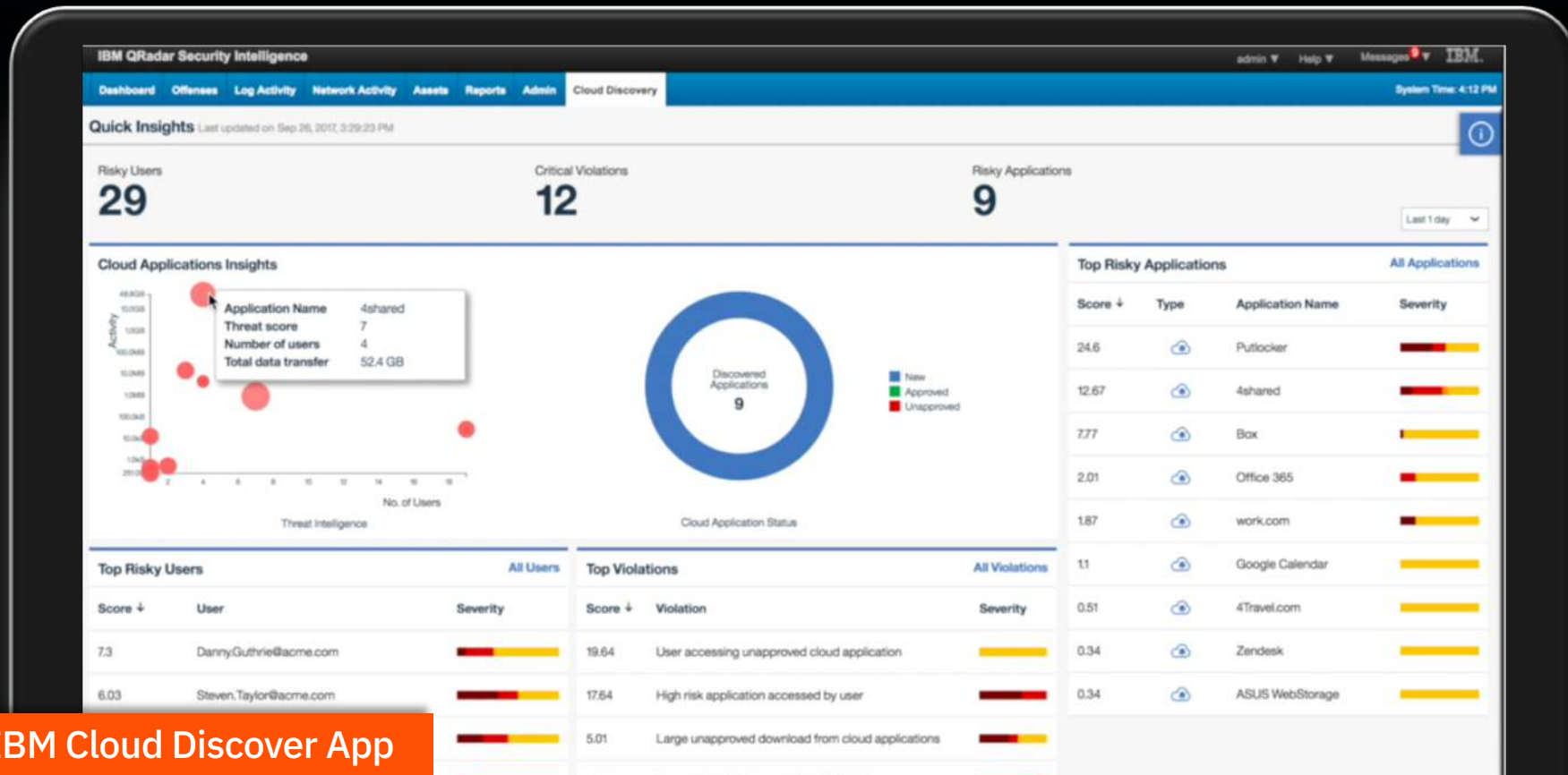


## IBM Multi-Cloud Data Encryption

Encrypt files and volume data while maintaining access control and compliance mandates

- Protects data from misuse
- Supports compliance requirements
- Encrypts data and provides access control

# Connect users to Cloud apps in seconds



## IBM Cloud Discover App

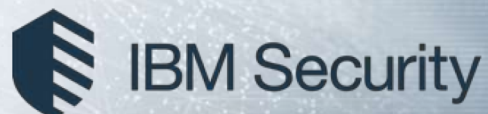
CASB solution with integrated access control, visibility, and threat protection

- Detect app usage and user activity
- Connect users to approved cloud apps
- Protect against cloud-related threats

# Cisco and IBM Security join forces to tackle cybercrime

Offering integrated technologies, services, and threat intelligence collaboration

IBM Security Analytics and Cisco Infrastructure		Insider Threat Containment	Incident Response Enrichment	Threat Intelligence Collaboration
Cisco FirePower: NGFW, IPS, AMP		Cisco Identity Services Engine	Cisco AMP ThreatGrid	Cisco Talos
IBM Security Analytics and Orchestration				IBM X-Force
IBM QRadar SIEM	IBM QRadar with Watson	IBM QRadar User Behavior Analytics	IBM Resilient Incident Response Platform	
IBM and Cisco Security Services				



# Modernize your identity and access management program

## Identity Management

- Identity governance and intelligence
- User lifecycle management
- Privileged identity control



## Access Management

- Adaptive access control and federation
- Application content protection
- Authentication and single-sign-on
- Access administration and auditing

## IAM strategic imperatives

- Help prevent insider threat and reduce identity fraud
- Support productivity and innovation for your business
- Achieve and maintain better regulatory compliance management
- Manage your identity in the cloud to monitor who has access to sensitive resources



# Gain security maturity through around-the-clock expertise



## Operational Expertise Blueprint

1. Assess your SOC maturity
2. Plan your SOC strategy
3. Design and build a SOC
4. Implement and optimize your security technologies
5. Transition to your newly transformed steady state

# Transform your security program

## ACCESS EXPERIENCE

Global security experts to help organizations identify threats before they become mainstream

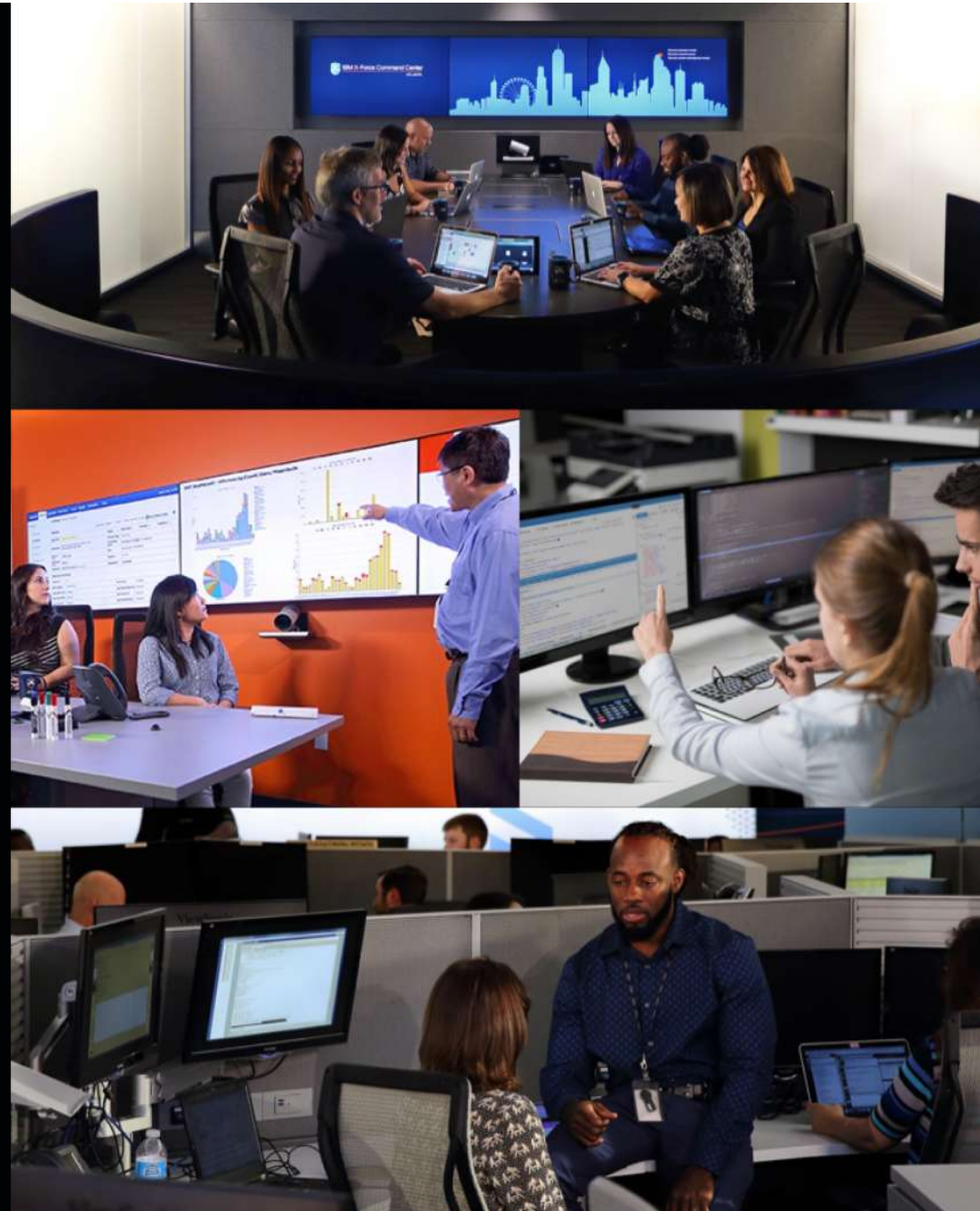
## REDUCE COMPLEXITY

From standalone solutions to centrally managed and outsourced security management, we transform security programs to reduce complexity and improve productivity


## LEVERAGE OUR BREADTH

Integrated portfolio of security services including:

- 100+ technology partners
- 150+ professional security certifications







## Security culture: Training tomorrow's cyber leaders today

# 1,450+










Executives trained in security best practices using our immersive state-of-the-art Cyber Range

“The cyber range training exceeded my expectations. We now are aware of the need to be prepared, regardless of what is documented in our procedures, good execution is vital.”

General Council  
Large International Bank

IBM Cyber Range customers are proud to share their detailed highly-ranked runbooks with us. But when put to the test in a live attack simulation, their actual lack of preparedness is startling.

# IBM Security key offering solutions aligned to client imperatives

PROVE COMPLIANCE			STOP THREATS			GROW BUSINESS		
 <b>Get Ahead of Compliance</b> Monitor and enforce compliance with regulatory, standards and organizational security policies	 <b>Enhance Security Hygiene</b> Patching, vulnerability scanning, using endpoint, asset, and user context	 <b>Govern Users and Identities</b> Provisioning, governance and monitoring of employees and privileged users	 <b>Detect and Stop Advanced Threats</b> Advanced analytics for internal threat detection and response across the enterprise	 <b>Orchestrate Incident Response</b> End-to-end workflow, collaboration, actions and expertise to respond with confidence	 <b>Master Threat Hunting</b> Analyst-driven investigations using big data and threat intelligence to get ahead of the threats	 <b>Secure Hybrid Cloud</b> Secure applications built in a multi-cloud environment	 <b>Protect Critical Assets</b> Stop breaches with code scanning, sensitive data monitoring, device security and encryption	 <b>Prevent Advanced Fraud</b> Malware prevention, phishing detection and strong authentication to stop cybercrime and establish digital trust
KEY PRODUCTS								
<ul style="list-style-type: none"> <li>• QRadar</li> <li>• Guardium</li> <li>• BigFix</li> <li>• Identity Governance</li> </ul>	<ul style="list-style-type: none"> <li>• BigFix</li> <li>• QRadar</li> <li>• ISAM / Cloud Identity</li> <li>• AppScan / App Sec On Cloud</li> </ul>	<ul style="list-style-type: none"> <li>• Identity Governance</li> <li>• ISAM / Cloud Identity</li> <li>• Guardium</li> <li>• QRadar User Behavior Analytics</li> </ul>	<ul style="list-style-type: none"> <li>• QRadar + Advisor with Watson</li> <li>• QRadar User Behavior Analytics</li> <li>• ISAM</li> <li>• Identity Governance</li> </ul>	<ul style="list-style-type: none"> <li>• Resilient</li> <li>• QRadar + Advisor with Watson</li> </ul>	<ul style="list-style-type: none"> <li>• i2</li> <li>• QRadar + Advisor with Watson</li> <li>• QRadar User Behavior Analytics</li> </ul>	<ul style="list-style-type: none"> <li>• Guardium</li> <li>• AppScan / App Sec On Cloud</li> <li>• Cloud Identity</li> <li>• QRadar</li> </ul>	<ul style="list-style-type: none"> <li>• Guardium</li> <li>• AppScan / App Sec On Cloud</li> <li>• MaaS360</li> <li>• BigFix</li> </ul>	<ul style="list-style-type: none"> <li>• Trusteer</li> <li>• i2</li> <li>• ISAM / Cloud Identity</li> <li>• MaaS360</li> </ul>
KEY CONSULTING SERVICES								
<ul style="list-style-type: none"> <li>◦ Security Strategy, Risk &amp; Compliance</li> <li>◦ Data Security</li> <li>◦ Identity &amp; Access Management</li> </ul>	<ul style="list-style-type: none"> <li>◦ X-Force Red</li> <li>◦ Application Security Services</li> <li>◦ Identity &amp; Access Management</li> </ul>	<ul style="list-style-type: none"> <li>◦ Identity &amp; Access Management</li> </ul>	<ul style="list-style-type: none"> <li>◦ SOC Consulting</li> <li>◦ Identity &amp; Access Management</li> <li>◦ X-Force IRIS</li> <li>◦ X-Force Red</li> </ul>	<ul style="list-style-type: none"> <li>◦ X-Force IRIS</li> </ul>	<ul style="list-style-type: none"> <li>◦ X-Force IRIS</li> </ul>	<ul style="list-style-type: none"> <li>◦ Cloud Security Services</li> <li>◦ X-Force IRIS</li> </ul>	<ul style="list-style-type: none"> <li>◦ X-Force Red</li> <li>◦ Application Security Services</li> <li>◦ Data Security Services</li> </ul>	<ul style="list-style-type: none"> <li>◦ Identity &amp; Access Management</li> </ul>
KEY MANAGED SECURITY SERVICES								
<ul style="list-style-type: none"> <li>◦ Managed Guardium</li> </ul>	<ul style="list-style-type: none"> <li>◦ Managed SIEM</li> </ul>	<ul style="list-style-type: none"> <li>◦ Managed Identity</li> <li>◦ Managed Guardium</li> </ul>	<ul style="list-style-type: none"> <li>◦ Managed SIEM</li> <li>◦ Managed Detection &amp; Response</li> </ul>	<ul style="list-style-type: none"> <li>◦ Endpoint Management Services</li> </ul>	<ul style="list-style-type: none"> <li>◦ Managed SIEM</li> <li>◦ Managed Detection &amp; Response</li> </ul>	<ul style="list-style-type: none"> <li>◦ Hybrid Cloud Security Services</li> <li>◦ Managed SIEM</li> <li>◦ Managed Guardium</li> </ul>	<ul style="list-style-type: none"> <li>◦ Managed Guardium</li> </ul>	<ul style="list-style-type: none"> <li>◦ Endpoint Management Services</li> </ul>
BUSINESS PARTNER SERVICES								

# IBM Security Strategy

## SUPPORT the CISO agenda



Advanced  
Threats



Cloud



Mobile and  
Internet of Things



Compliance  
Mandates



Skills  
Shortage

## ACCELERATE with key innovations

AI and  
Orchestration



Cloud  
Security



Collaboration



## LEAD in strategic domains



SECURITY MATURITY MODEL	BASIC		PROFICIENT		OPTIMIZED	
	Capability	IBM Security Solution	Capability	IBM Security Solution	Capability	IBM Security Solution
Security Orchestration & Analytics	Log management Vulnerability management	QRadar Log Manager QRadar Vulnerability Manager	SIEM  Threat & anomaly detection GRC	QRadar SIEM, QRadar on Cloud, SOC Consulting, Managed SIEM QFLOW / VFLOW GRC Consulting, OpenPages	Forensics  Predictive analytics  User behavior analytics Incident response Threat hunting & investigation	QRadar Incident Forensics, Identity Insight QRadar Advisor with Watson QRadar UBA Resilient i2 Enterprise Insight Analysis
Fraud Protection	Online fraud detection	Trusteer Rapport, Trusteer Pinpoint	Digital (online and mobile) fraud protection	Trusteer Rapport, Trusteer Pinpoint	Omnichannel fraud protection	Trusteer Mobile
Identity & Access Management	Web access management Directory management Mainframe security	Access Manager Directory Suite zSecure	Advanced access management IDaaS Identity governance & administration	Access Manager  Cloud Identity Service Identity Governance & Intelligence	Privileged user management	Privileged Identity Manager
Data Protection	Encryption	Guardium Data Encryption	Data / file activity monitoring Test data masking Data loss prevention	Guardium  MaaS360, Guardium, Optim Data Privacy BigFix Protection, GTS partners	Data discovery & classification Encryption key management	Critical Data Protection Services, eDiscovery, StoredIQ Key Lifecycle Manager
Application Security	Dynamic vulnerability analysis	AppScan Standard	Static source code scanning Web application protection	AppScan Source  DataPower	Hybrid scanning & correlation	AppScan Enterprise, Application Security on Cloud, X-Force Red Offensive Security & Vulnerability Management
Endpoint Protection	Antivirus Endpoint patch management	Endpoint Managed Security on Cloud	Compliance and malware protection, endpoint detection & response, software asset management	BigFix	Patch management, UEM Professional assessment & remediation Managed services	BIgFix X-Force IRIS Managed Detection and Response Services
Network Protection	Firewalls Sandboxing	Security & Network Services QRadar	NGNFW / IPS Network forensics & threat management Virtual patching Network visibility & segmentation	Cisco Partnership QRadar Incident Forensics  Endpoint Manager QRadar Network Insights	Professional assessment & remediation Managed services	X-Force IRIS  Managed Network Security Services
Mobile Security	Mobile Device Management	MaaS360	EMM (MDM plus content and application management)	MaaS360	UEM with contextual analytics extending to IoT	X-Force IRIS Mobile Device Management Services