IBM Security

Cybersecurity and YOU!!

CYBER RESILIENCE - PREPARE FOR WHEN, NOT IF

James Boyles
Cybersecurity Architect

October 2018

IBM

What is cyber resilience?

Cyber resilience is an organization’s ability to continue delivering the intended outcomes despite adverse cyber incidents.

IBM Cyber Resilience

=

Security + Resiliency + Network solutions

Why is cyber resilience needed?

Cyber attacks are evolving and on the rise.

Top 5 causes of cyber disruptions

61% Phishing and social engineering

45% Malware

37% Spear-phishing attack

24% Denial of service

21% Out-of-date software

Many organizations are unprepared

68% Lack the ability to remain resilient in the wake of a cyber attack

66% Suffer from insufficient planning and preparedness

75% Have ad-hoc, non-existent, or inconsistent cyber security incident response plans

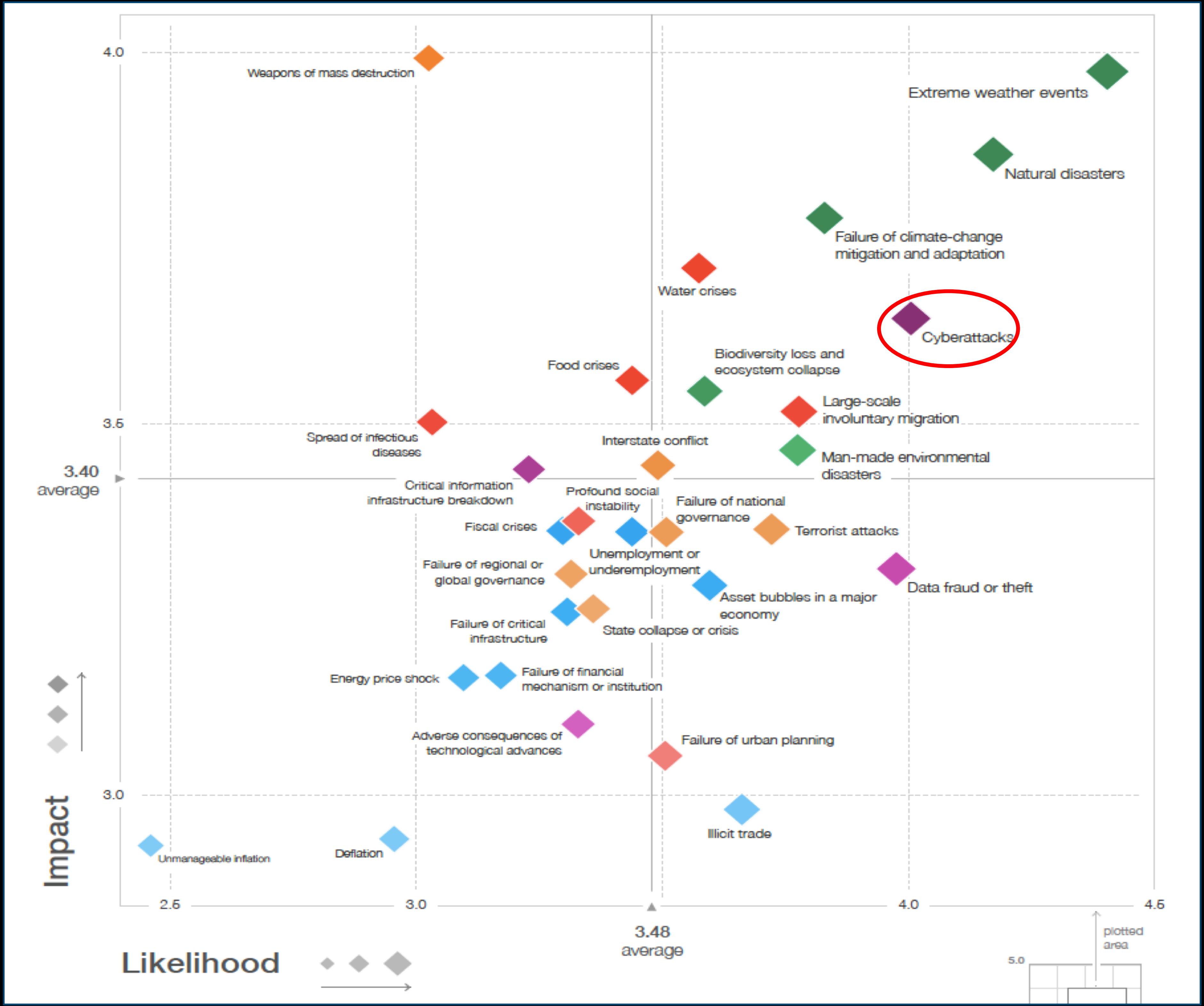
191 days Average amount of time hackers spend inside IT environments before discovery

Sources:
Ponemon Institute 2017 Cost of Data Breach Study: Impact of Business Continuity Management
IBM/Forbes Insights survey of 153 executives at large enterprises worldwide, 2017

World Economic Forum 2018 Global Risks Perception Survey:

Cyberattacks ranked #3

"Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace."



Source: World Economic Forum, 2018

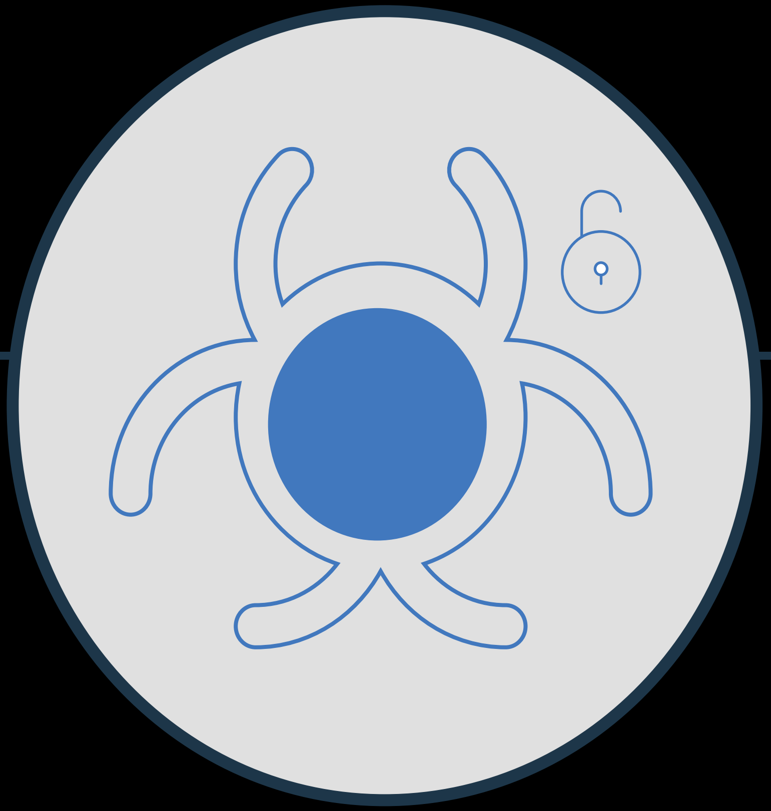
Attacks are becoming more costly and more likely

$3.62 million

Average total cost of
a data breach in 2017

$8 billion

Estimated global cost
of WannaCry attack



$310+ million

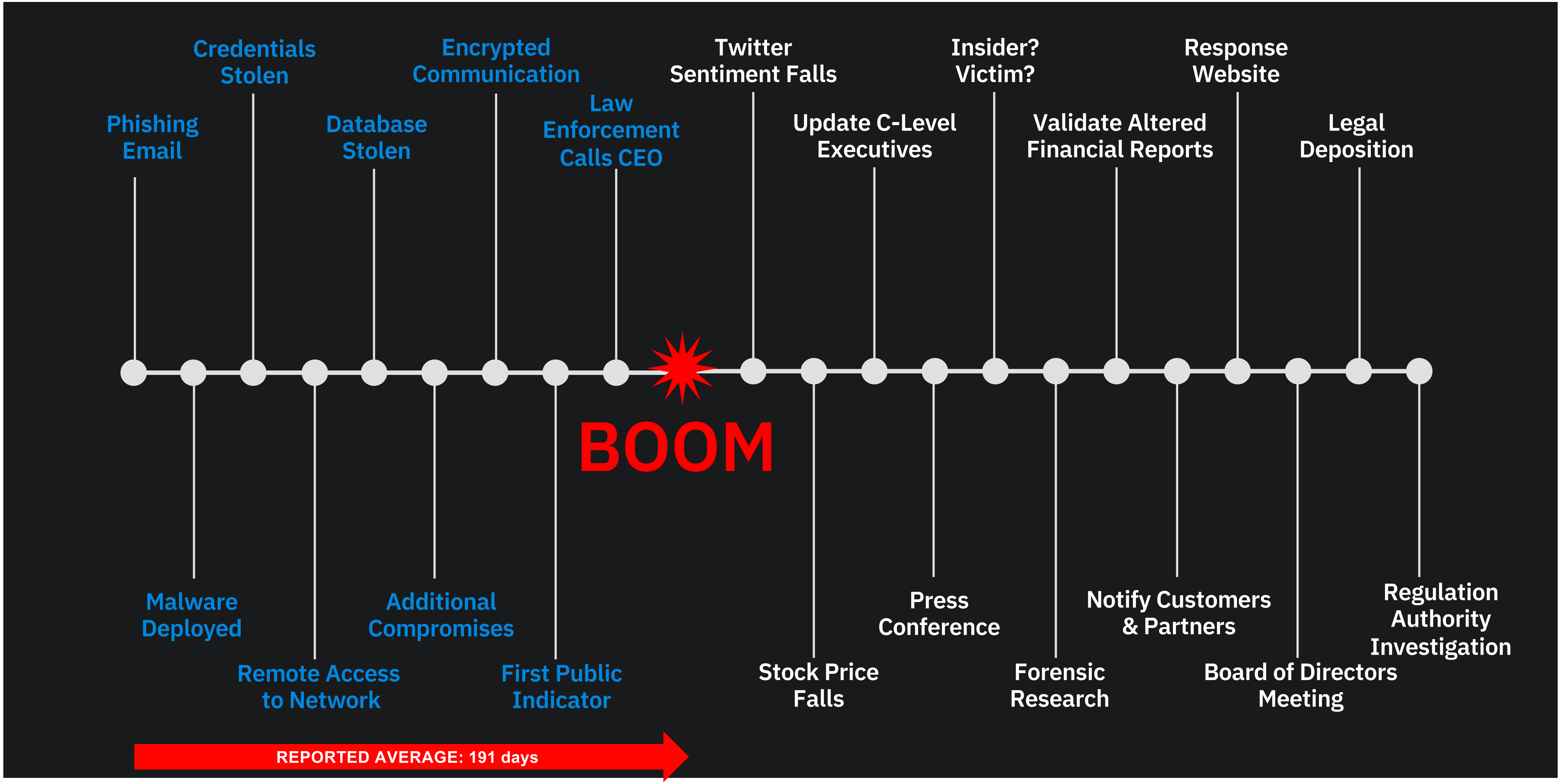
Cost impact for one company
impacted by NotPetya

1 in 4

Odds of experiencing a data breach
over next two years

Source:
Ponemon, 2017 Cost of Data Breach Study - https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&
CBSNews WannaCry ransomware attack losses could reach $4 billion - https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Anatomy of a BOOM event



Phishing Email

Malware Deployed

Credentials Stolen

Remote Access to Network

Database Stolen

Additional Compromises

Encrypted Communication

First Public Indicator

Law Enforcement Calls CEO

BOOM

Twitter Sentiment Falls

Stock Price Falls

Update C-Level Executives

Press Conference

Insider? Victim?

Forensic Research

Validate Altered Financial Reports

Notify Customers & Partners

Response Website

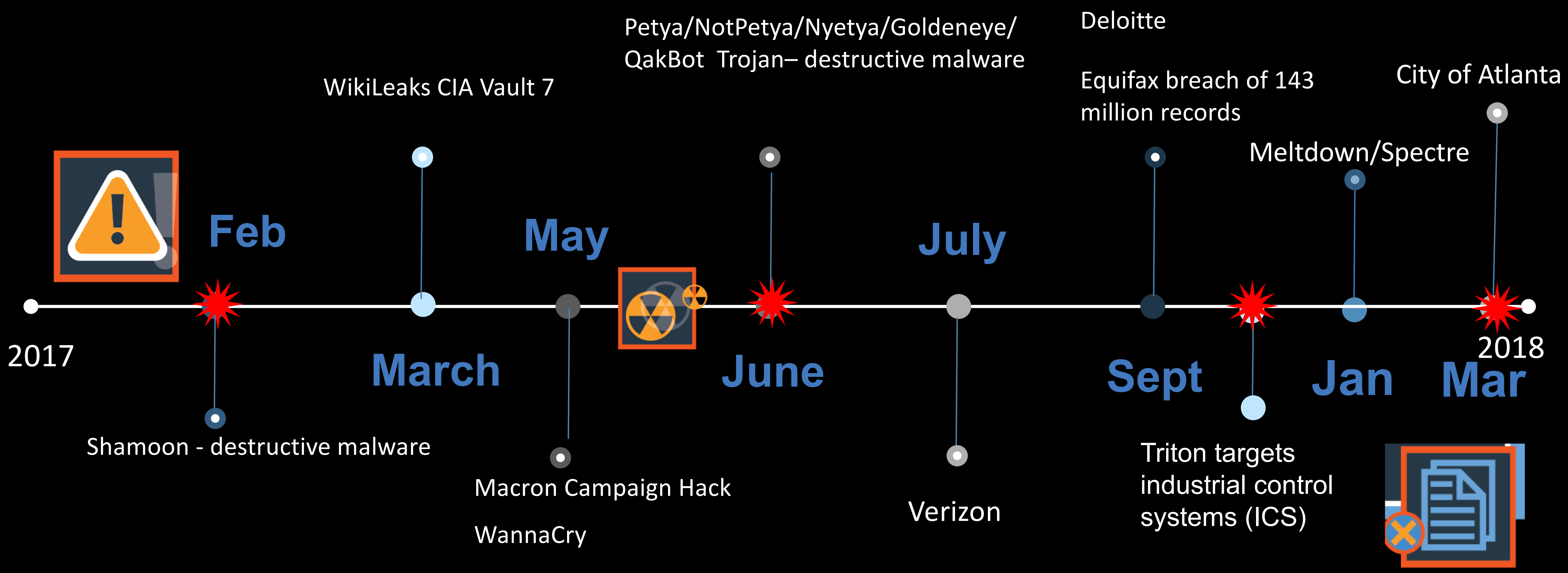
Board of Directors Meeting

Legal Deposition

Regulation Authority Investigation

REPORTED AVERAGE: 191 days

Often these attacks disrupt business operations instead of garnering financial gain



2017

Feb

Shamoon - destructive malware

March

WikiLeaks CIA Vault 7

May

Macron Campaign Hack

WannaCry

June

Petya/NotPetya/Nyetya/Goldeneye/
QakBot Trojan– destructive malware

July

Verizon

Sept

Deloitte

Equifax breach of 143 million records

Triton targets industrial control systems (ICS)

Jan

Meltdown/Spectre

Mar

City of Atlanta

2018

Cyber resilience programs are under pressure

Velocity
DIGITAL TRANSFORMATION

The speed at which organizations evolve must increase

- With the acceleration of cloud SaaS, new asset adoption is rapid
- Business initiatives, such as digital transformation, are moving at an unprecedented pace
- Traditional approaches to threat management can't keep up

Complexity
ADVANCED THREATS

The threat landscape is evolving daily, complexity is on the rise

- The asset landscape is changing rapidly, including Cloud, SaaS, BYOD, and IoT
- Advanced threats leverage new attack vectors, motivations, and stealth
- Traditional threat management struggles to comprehensively address this new level of complexity

Liability
NEW RESPONSIBILITIES

An organization's obligations are in the spotlight

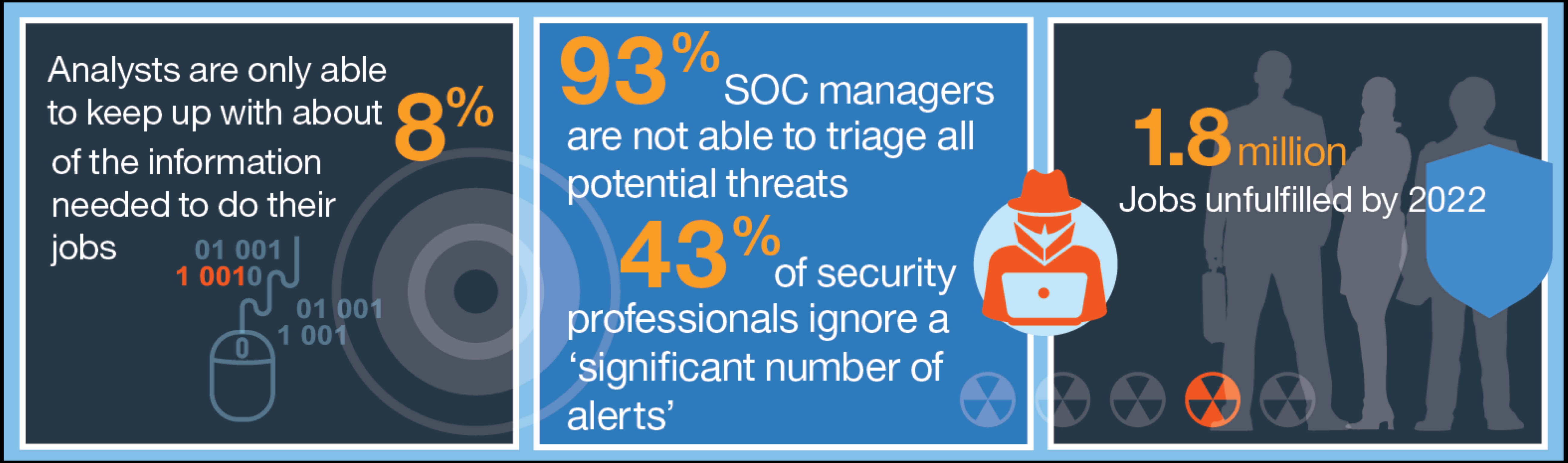
- Businesses are under heavy public scrutiny to protect data
- Growing regulatory emphasis on security and data privacy, combined with fines, and impact to brand reputation have raised the stakes for all organizations
- Traditional threat management lacks the visibility and responsiveness to contain these risks

Organizations are already overwhelmed

Data Overload

Unaddressed Threats

Cyber Skills Shortage



Analysts are only able to keep up with about 8% of the information needed to do their jobs

93% SOC managers are not able to triage all potential threats

43% of security professionals ignore a ‘significant number of alerts’

1.8 million Jobs unfulfilled by 2022

“My workload is overwhelming and repetitive.”

“I don’t know where to focus my time for the quickest response.”

“There is so much information out there, it’s impossible to find what’s useful.”

Challenges we hear from CISOs in Federal Government Agencies

- Lack of sufficient skills and administration
- Meet the demands of digital transformation
- Ensure data privacy and compliance
- Mitigate insider threats
- Improve real-time visibility and continuous monitoring

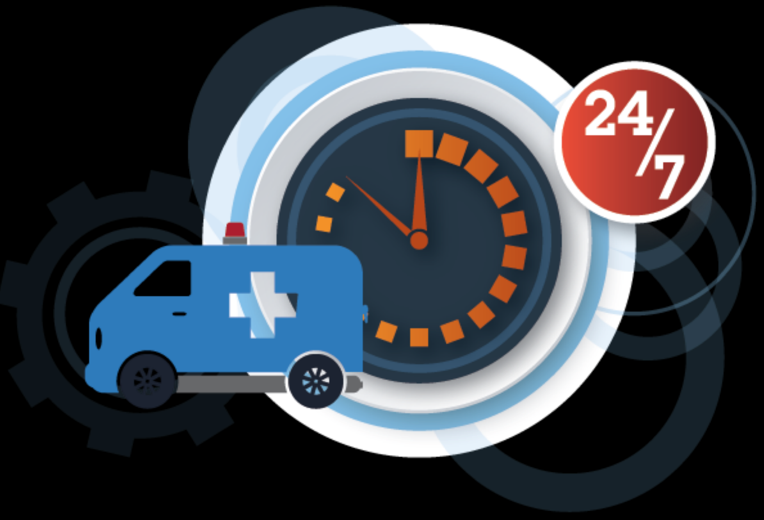
Challenges we hear from CISOs in State and Local Government Agencies

- Deal with aging infrastructures
- Address insufficient IT administration
- Meet the demands of digital transformation
- Ensure data privacy and compliance
- Respond to talent and funding shortage

…and operations teams have a challenging mission

Process intelligence and outthink cyber criminals

Protect critical data, users applications and infrastructure



Respond and recover from incidents quickly

Pain points evolve as cyber attacks increase and change

- Need a more precise, immediate response to a cyber event
- Eliminate extended business interruptions from more frequent attacks
- Retain clean IT and critical business process components to quickly resume company operations
- Demonstrable evidence of capability for audit and compliance

Important questions to build a defense

“Your IT infrastructure or email was wiped out around the world in a matter of hours? ”

Key consideration

Protection against large scale, volume attacks

“Are your networks outdated, reliant on hardware based network appliances with minimal network segmentation? ”

Key consideration

Help maintain business continuity to become cyber resilient

“ How long could you sustain operations if forced to revert to manual operations?”

Key consideration

Know and bolster your security posture

Cyber Resilience

Cyber resilience is the ability of an organization to continue to function with the least amount of disruption in the face of cyberattacks. It is an end to end approach that brings together three critical areas ... information security, business continuity and network resilience of enterprises to ensure organizations continue to function during cyberattacks and cyber outages.

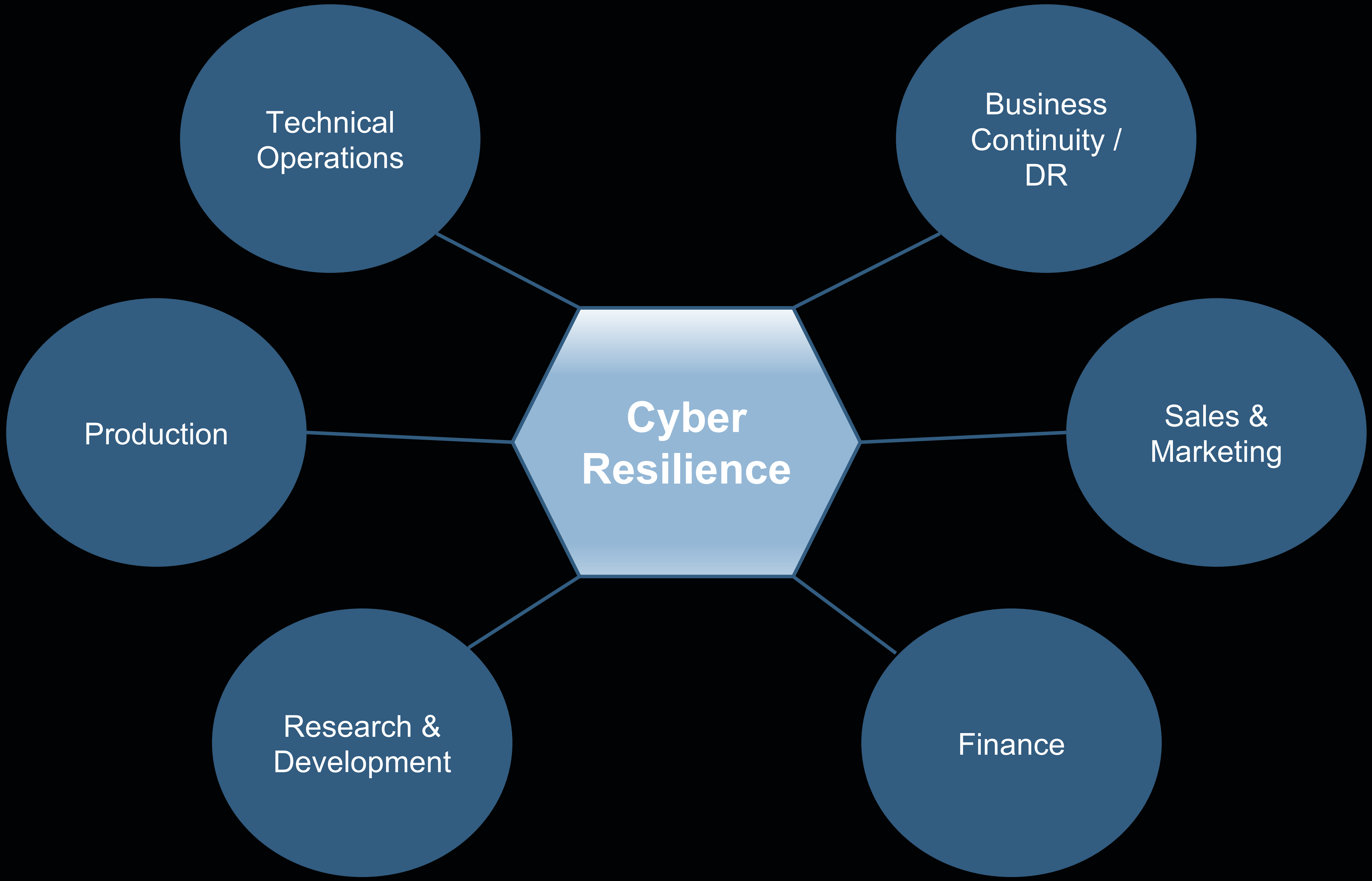
Cyber Security

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyberattack and protects organizations from the deliberate exploitation of its assets.

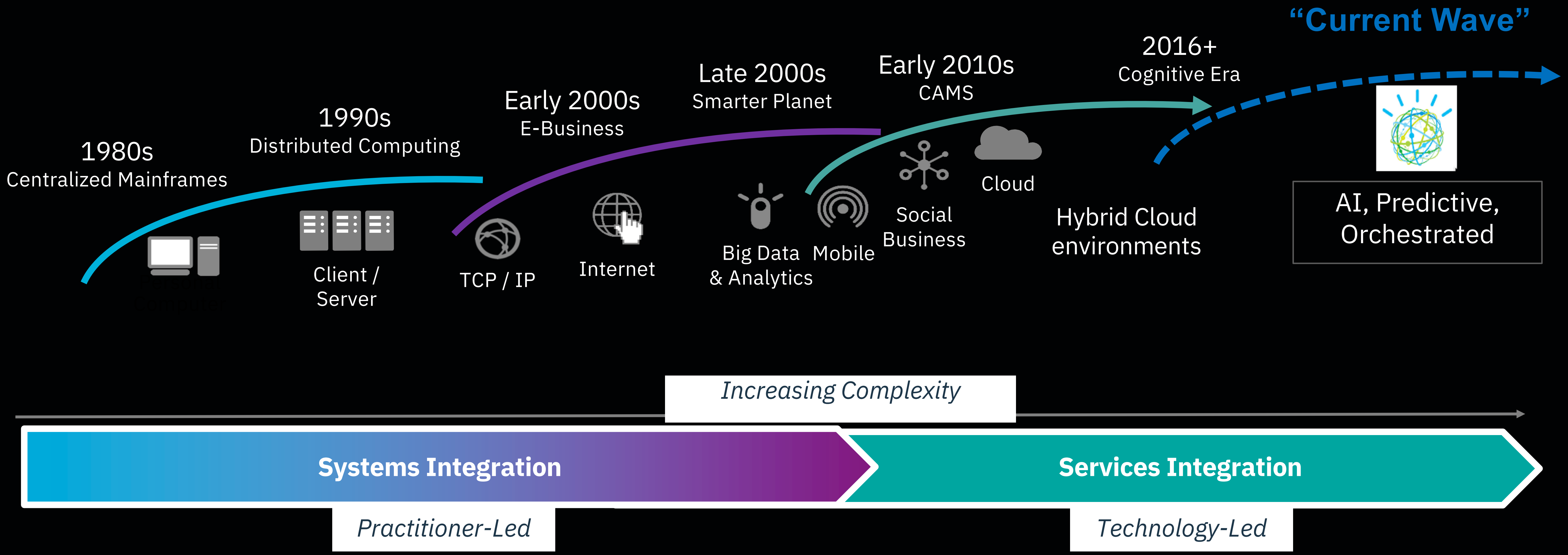
Business Continuity

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for Business continuity address natural catastrophe, accidents and deliberate physical attacks; but now, they must also support resumption of operations following cyberattack disruptions.

Cyber resilience serves a number of IT and risk management disciplines



Cyber Resilience is a business priority that supports "continuous availability" that allows companies to meet their business outcome objectives



1980s
Centralized Mainframes

Personal Computer

1990s
Distributed Computing

Client / Server

Early 2000s
E-Business

TCP / IP

Internet

Late 2000s
Smarter Planet

Big Data & Analytics

Mobile

Early 2010s
CAMS

Social Business

Cloud

2016+
Cognitive Era

Hybrid Cloud environments

“Current Wave”

AI, Predictive, Orchestrated

Increasing Complexity

Systems Integration

Practitioner-Led

Services Integration

Technology-Led

Let’s focus on the most critical security use cases

Outcome-driven security

Prove Compliance

Get Ahead of Compliance

Enhance Security Hygiene

Govern Users and Identities

Stop Threats

Detect & Stop Advanced Threats

Orchestrate Incident Response

Master Threat Hunting

Grow Business

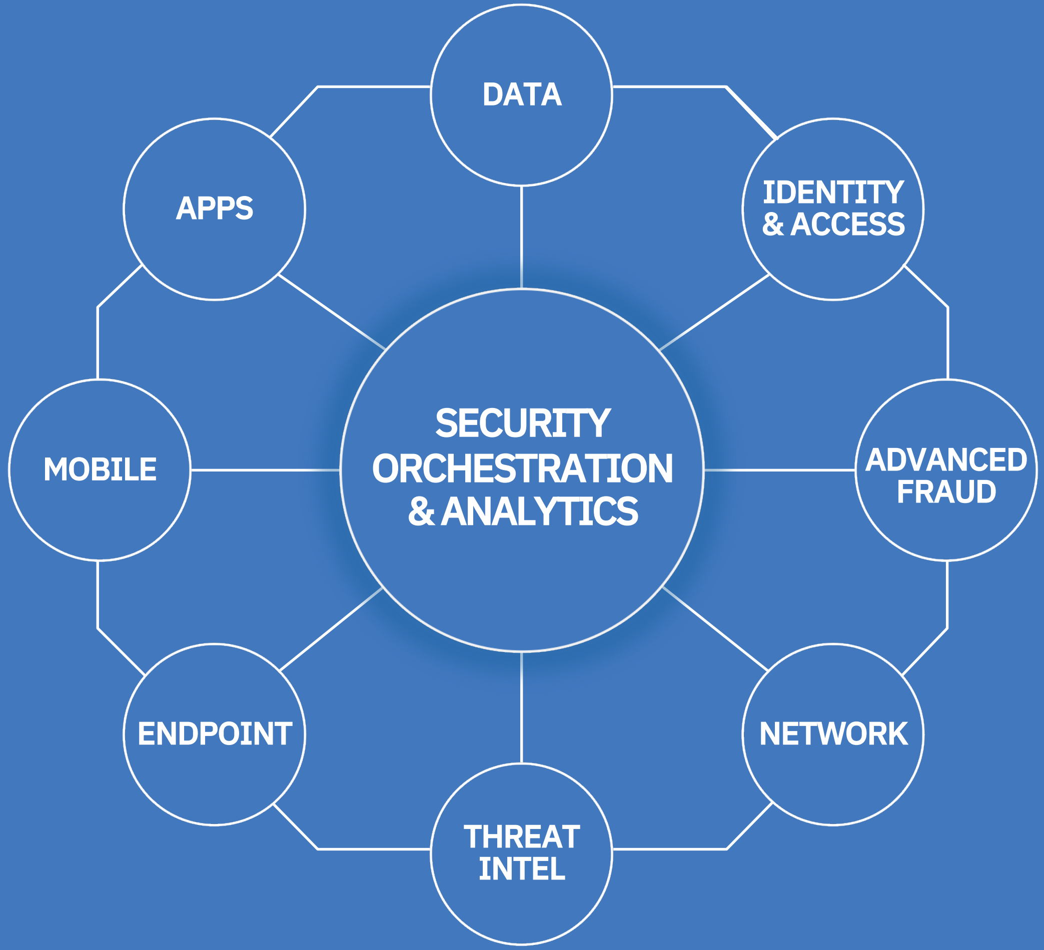
Secure Hybrid Cloud

Protect Critical Assets

Prevent Advanced Fraud

Our unique approach will help transform your security

Build a security immune system



Deploy meaningful innovations

AI and Orchestration

Cloud Security

Collaboration

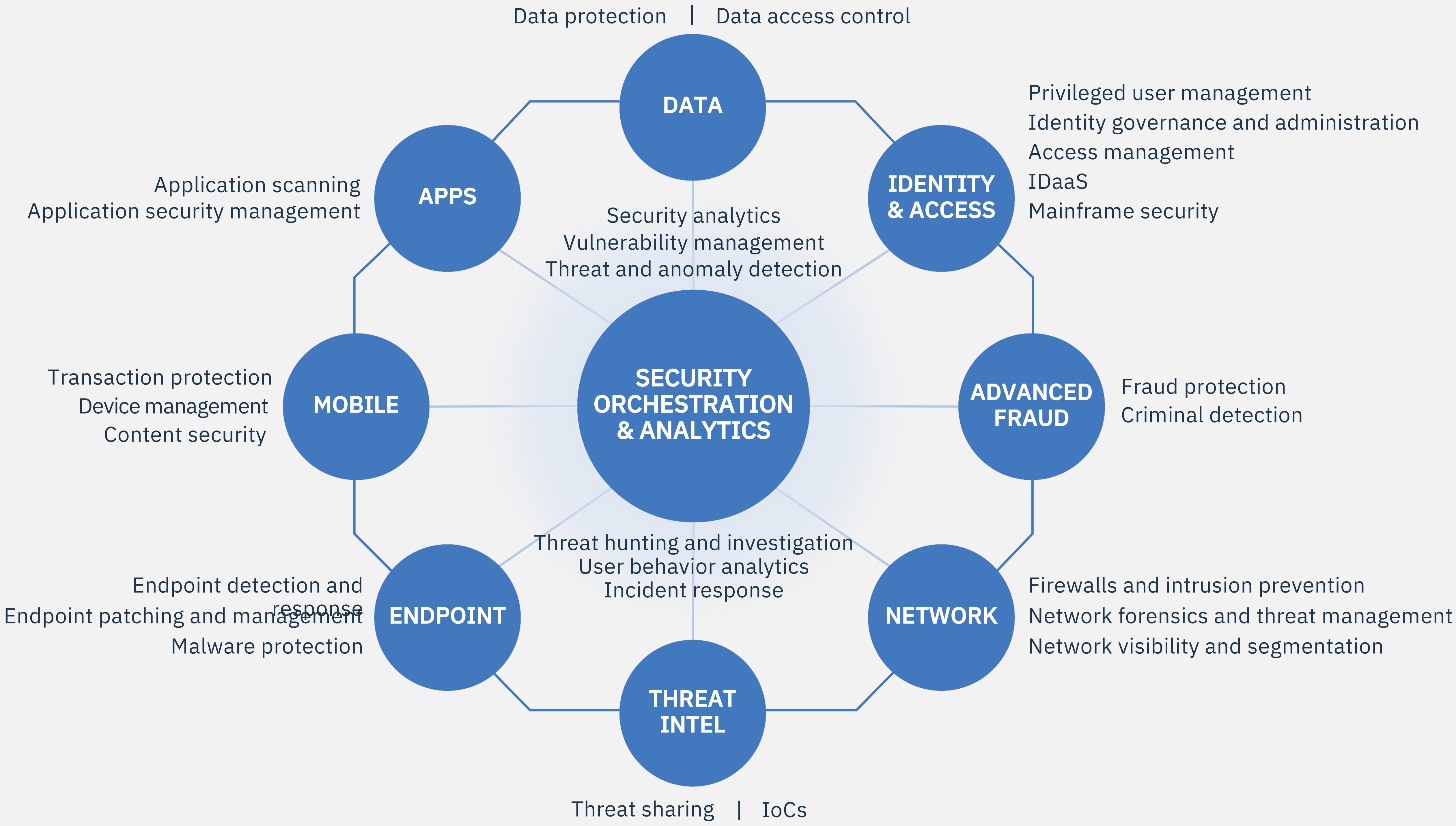
Get help from the experts

Industry Consultants

Research & Development

World Class Designers

Build an integrated security immune system



Data protection | Data access control

DATA

IDENTITY & ACCESS

Privileged user management
Identity governance and administration
Access management
IDaaS
Mainframe security

APPS

Application scanning
Application security management

Security analytics
Vulnerability management
Threat and anomaly detection

MOBILE

Transaction protection
Device management
Content security

SECURITY ORCHESTRATION & ANALYTICS

ADVANCED FRAUD

Fraud protection
Criminal detection

Threat hunting and investigation
User behavior analytics
Incident response

ENDPOINT

Endpoint detection and response
Endpoint patching and management
Malware protection

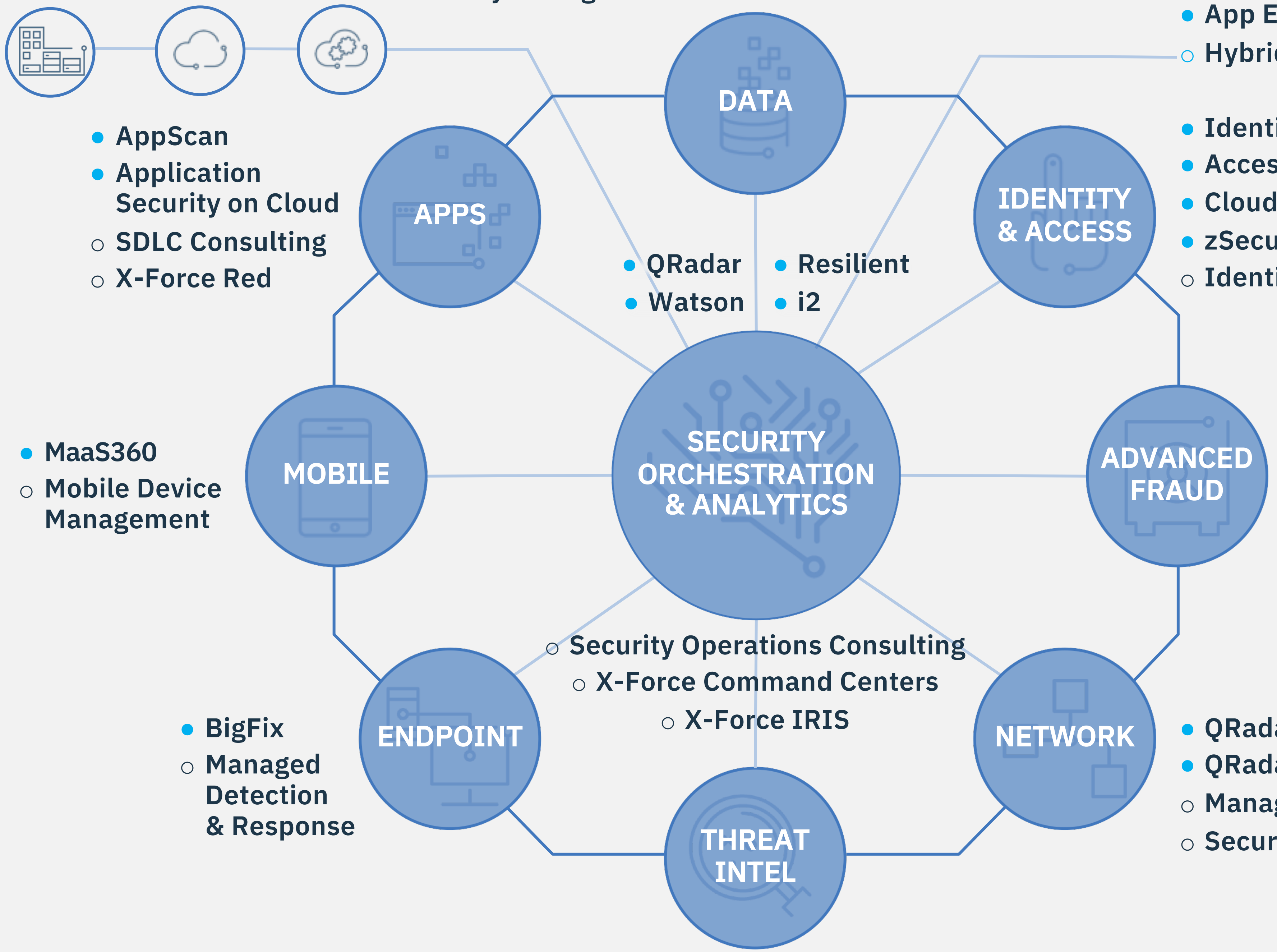
NETWORK

Firewalls and intrusion prevention
Network forensics and threat management
Network visibility and segmentation

THREAT INTEL

Threat sharing | IoCs

IBM Security Immune System



DATA

● Guardium ● Multi-cloud Encryption
● Key Manager ○ Critical Data Protection Services

SECURITY ECOSYSTEM

● App Exchange
○ Hybrid Cloud Security Services

APPS

● AppScan
● Application Security on Cloud
○ SDLC Consulting
○ X-Force Red

IDENTITY & ACCESS

● Identity Governance
● Access Manager
● Cloud Identity
● zSecure
○ Identity Management Services

SECURITY ORCHESTRATION & ANALYTICS

● QRadar ● Resilient
● Watson ● i2

○ Security Operations Consulting
○ X-Force Command Centers
○ X-Force IRIS

MOBILE

● MaaS360
○ Mobile Device Management

ADVANCED FRAUD

● Trusteer
○ Financial Malware Research

ENDPOINT

● BigFix
○ Managed Detection & Response

NETWORK

● QRadar Incident Forensics
● QRadar Network Insights
○ Managed Network Security
○ Secure SD-WAN

THREAT INTEL

● X-Force Exchange ○ X-Force IRIS

● Products
○ Services

Deploy meaningful innovations

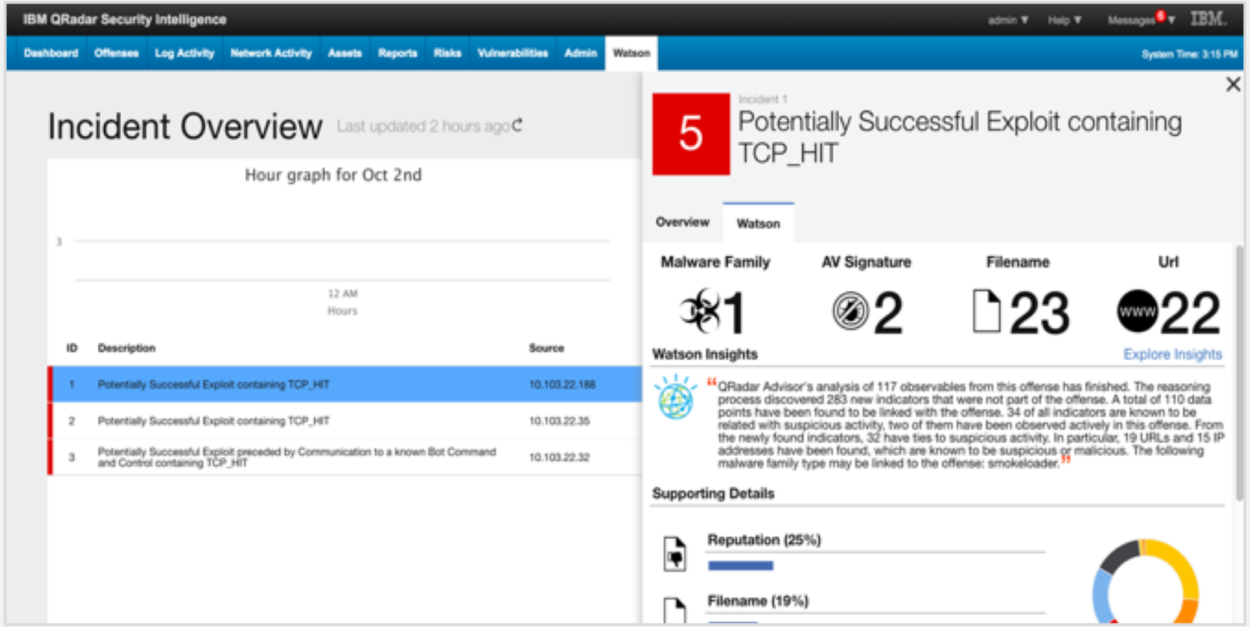
AI and Orchestration

Cloud Security

Collaboration

The future of security is AI and Orchestration

What if you could augment your teams' intelligence and response?



Incident Overview Last updated 2 hours ago

ID	Description	Source
1	Potentially Successful Exploit containing TCP_HIT	10.103.22.188
2	Potentially Successful Exploit containing TCP_HIT	10.103.22.35
3	Potentially Successful Exploit preceded by Communication to a known Bot Command and Control containing TCP_HIT	10.103.22.32

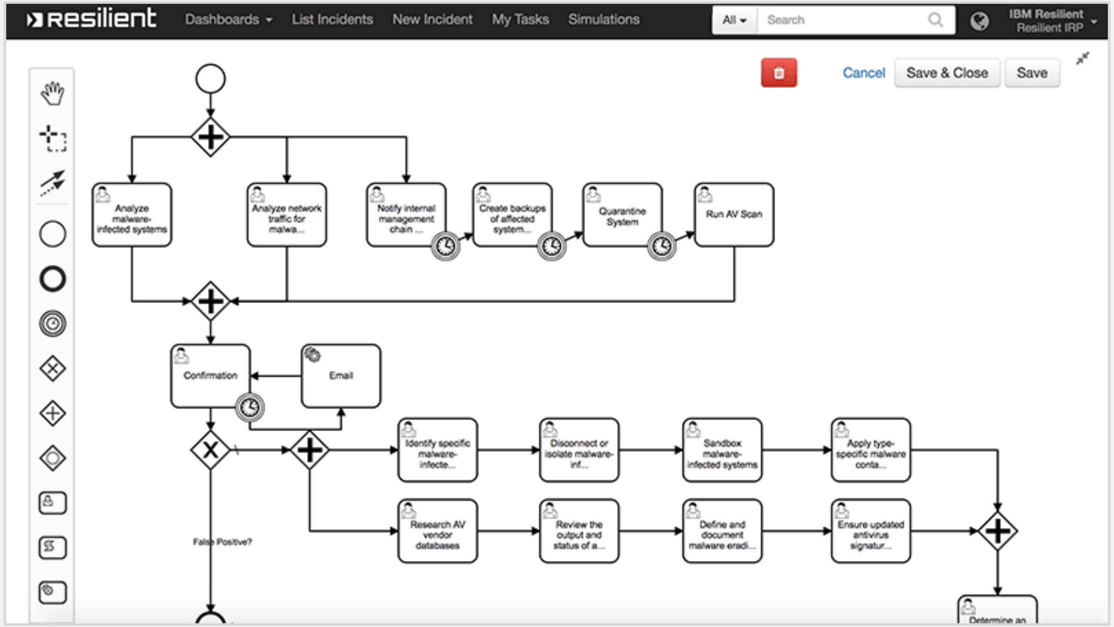
Incident 1

5 Potentially Successful Exploit containing TCP_HIT

Watson Insights

"QRadar Advisor's analysis of 117 observables from this offense has finished. The reasoning process discovered 283 new indicators that were not part of the offense. A total of 110 data points have been found to be linked with the offense. 34 of all indicators are known to be related with suspicious activity, two of them have been observed actively in this offense. From the newly found indicators, 32 have ties to suspicious activity. In particular, 19 URLs and 15 IP addresses have been found, which are known to be suspicious or malicious. The following malware family type may be linked to the offense: smokeloader."

Supporting Details


Resilient
Dashboards
List Incidents
New Incident
My Tasks
Simulations
All
Search
IBM Resilient
Resilient IRP
Cancel
Save & Close
Save
Analyze malware-infected systems
Analyze network traffic for malwa...
Notify internal management chain ...
Create backups of affected system...
Quarantine System
Run AV Scan
Confirmation
Email
Identify specific malware-infecte...
Disconnect or isolate malware-inf...
Sandbox malware-infected systems
Apply type-specific malware conta...
Research AV vendor databases
Review the output and status of a...
Define and document malware eradi...
Ensure updated antivirus signatur...
False Positive?
Determine an

Use AI to gain a head start

Automatically investigate incidents and anomalies to identify the most likely threats

- Quickly gather insights from millions of external sources
- Apply cognitive reasoning to build relationships

IBM QRadar Advisor with Watson

Respond quickly with confidence

Orchestrate a complete and dynamic response, enabling faster, more intelligent remediation

- Create dynamic playbooks built on NIST / CERT / SANS
- Deploy response procedures and expertise

IBM Resilient

The future of security is Cloud

Can you confidently say yes to digital transformation?

box · CONCUR · Google Apps · Office 365 · salesforce · workday.

IBM Cloud · amazon web services™ · Microsoft Azure · vmware®

Protect Data

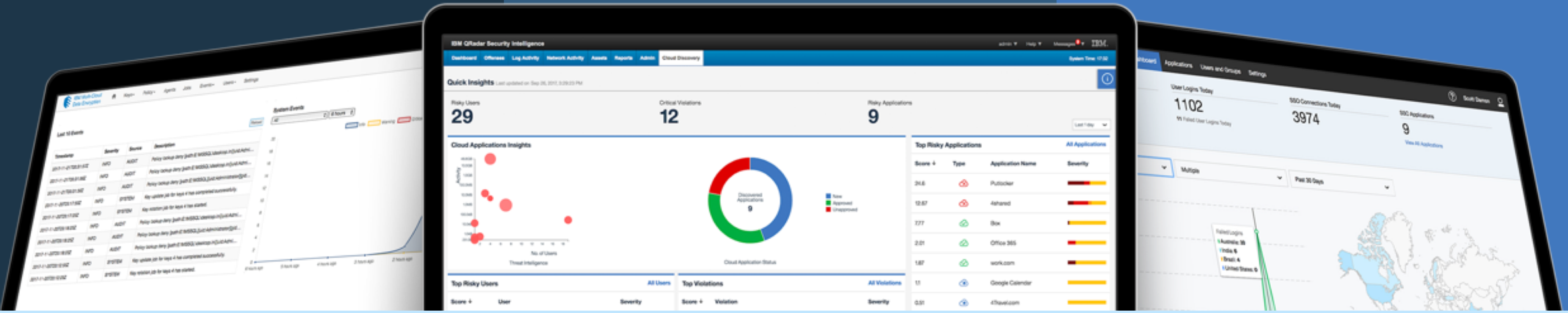
IBM Multi-Cloud Data Encryption

Gain Visibility

IBM QRadar Cloud Security Analytics

Manage Access

IBM Cloud Identity Connect



IBM QRadar Security Intelligence

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin | Cloud Discovery

Quick Insights

Risky Users 29 | Critical Violations 12 | Risky Applications 9

Cloud Applications Insights

Top Risky Applications

Score	Type	Application Name	Severity
24.6		Putlocker	
12.67		4shared	
7.77		Box	
2.01		Office 365	
1.87		work.com	
1.1		Google Calendar	
0.51		47travel.com	

Top Risky Users

Top Violations

User Logins Today 1102

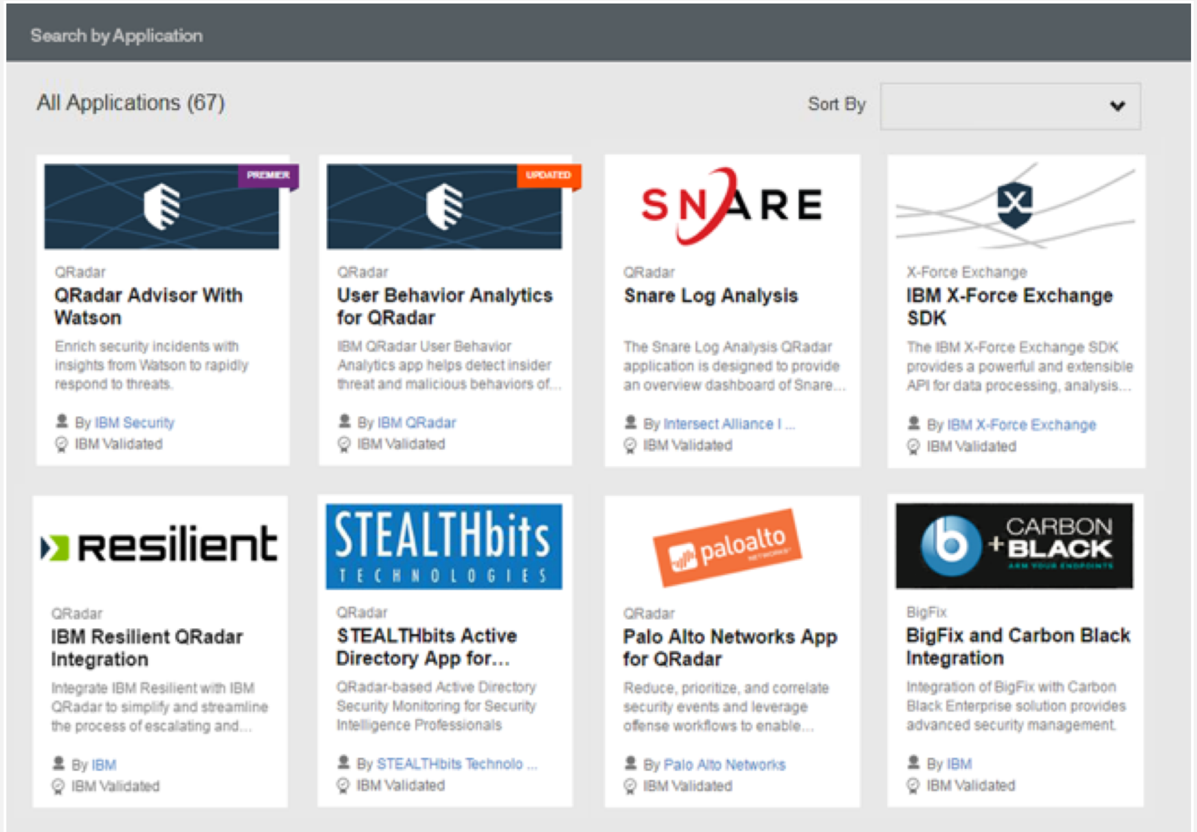
SSO Connections Today 3974

SSO Applications 9

Get Help from Experts | IBM X-Force Cloud Security Service

The future of security is Collaboration

Are you part of the bigger picture?



Search by Application

All Applications (67)

Sort By

PREMIER

QRadar
QRadar Advisor With Watson
Enrich security incidents with insights from Watson to rapidly respond to threats.
By IBM Security
IBM Validated

UPDATED

QRadar
User Behavior Analytics for QRadar
IBM QRadar User Behavior Analytics app helps detect insider threat and malicious behaviors of...
By IBM QRadar
IBM Validated

QRadar
Snare Log Analysis
The Snare Log Analysis QRadar application is designed to provide an overview dashboard of Snare...
By Intersect Alliance I ...
IBM Validated

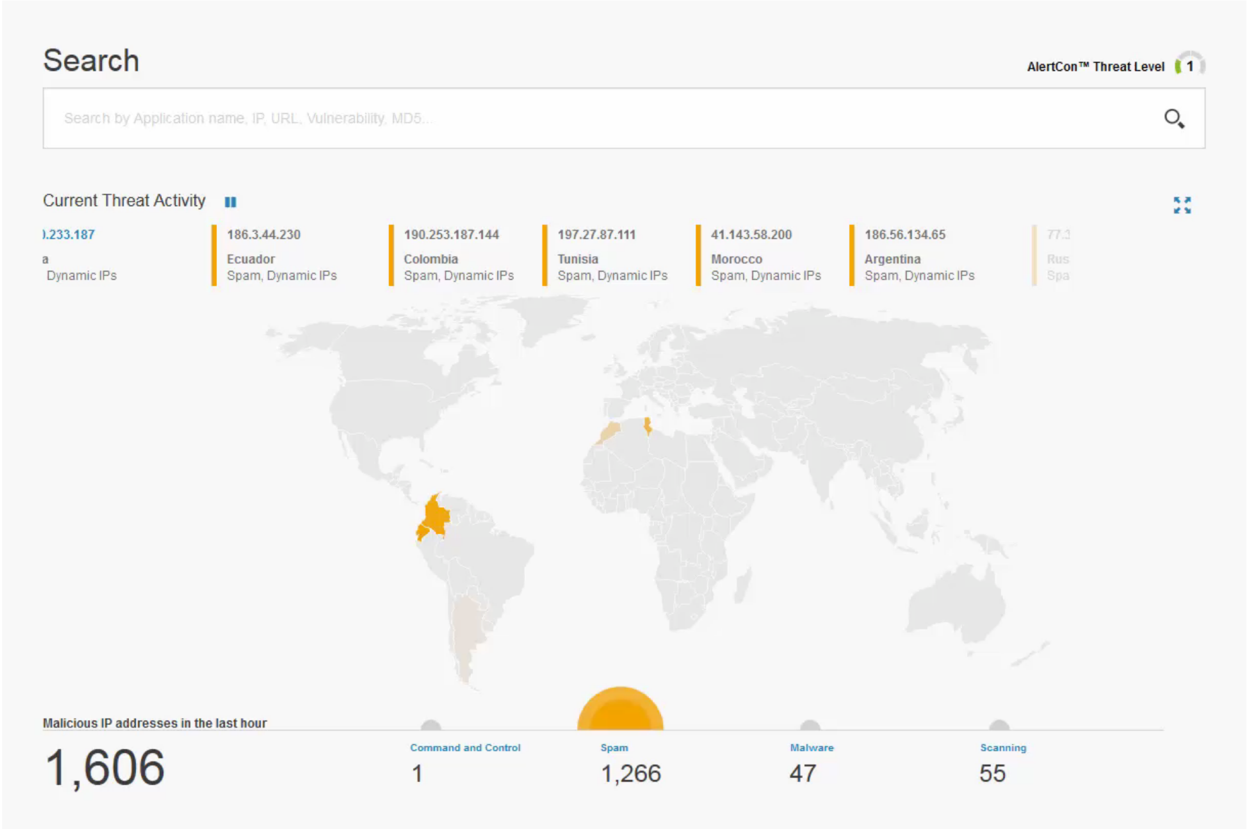
X-Force Exchange
IBM X-Force Exchange SDK
The IBM X-Force Exchange SDK provides a powerful and extensible API for data processing, analysis...
By IBM X-Force Exchange
IBM Validated

QRadar
IBM Resilient QRadar Integration
Integrate IBM Resilient with IBM QRadar to simplify and streamline the process of escalating and...
By IBM
IBM Validated

QRadar
STEALTHbits Active Directory App for...
QRadar-based Active Directory Security Monitoring for Security Intelligence Professionals
By STEALTHbits Technolo ...
IBM Validated

QRadar
Palo Alto Networks App for QRadar
Reduce, prioritize, and correlate security events and leverage offense workflows to enable...
By Palo Alto Networks
IBM Validated

BigFix
BigFix and Carbon Black Integration
Integration of BigFix with Carbon Black Enterprise solution provides advanced security management.
By IBM
IBM Validated



Search

AlertCon™ Threat Level 1

Search by Application name, IP, URL, Vulnerability, MD5...

Current Threat Activity

).233.187
a
Dynamic IPs

186.3.44.230
Ecuador
Spam, Dynamic IPs

190.253.187.144
Colombia
Spam, Dynamic IPs

197.27.87.111
Tunisia
Spam, Dynamic IPs

41.143.58.200
Morocco
Spam, Dynamic IPs

186.56.134.65
Argentina
Spam, Dynamic IPs

77.:
Rus
Spa

Malicious IP addresses in the last hour
1,606

Command and Control	Spam	Malware	Scanning
1	1,266	47	55

Join an ecosystem of defenses

Customize your security with 140+ apps on the IBM Security App Exchange

Share real-time threat intelligence

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

Supported by hundreds of open integrations

CISCO · vmware · Check Point SOFTWARE TECHNOLOGIES LTD. · McAfee · splunk> · amazon web services · Carbon Black. · CROWDSTRIKE · Recorded Future

servicenow · Gigamon · tripwire · bioconnect. · wandera · Lookout · digitalPersona.

Symantec · RISKIQ · TREND MICRO · observe it · FireEye · IWS · everbridge

lastline · ForeScout · cybereason · STEALTHbits TECHNOLOGIES · BLACKDUCK · BLUVECTOR.

. . .

. . .

Entersekt · CounterTack · QUALYS ON DEMAND SECURITY · onapsis · f5 · FORTINET

whispir. · gemalto security to be free · paloalto NETWORKS · CyberX Trusted. Industrial. Cybersecurity. · DIGITAL GUARDIAN Formerly VERDASYS · REDSEAL

RSA · REVERSING LABS · SECURONIX · algosec · JUNIPER NETWORKS · CYBERARK · ANOMALI

tenable network security · digital shadows_ · Entrust · DOMAINTOOLS · ziften · THREAT CONNECT · ARXAN

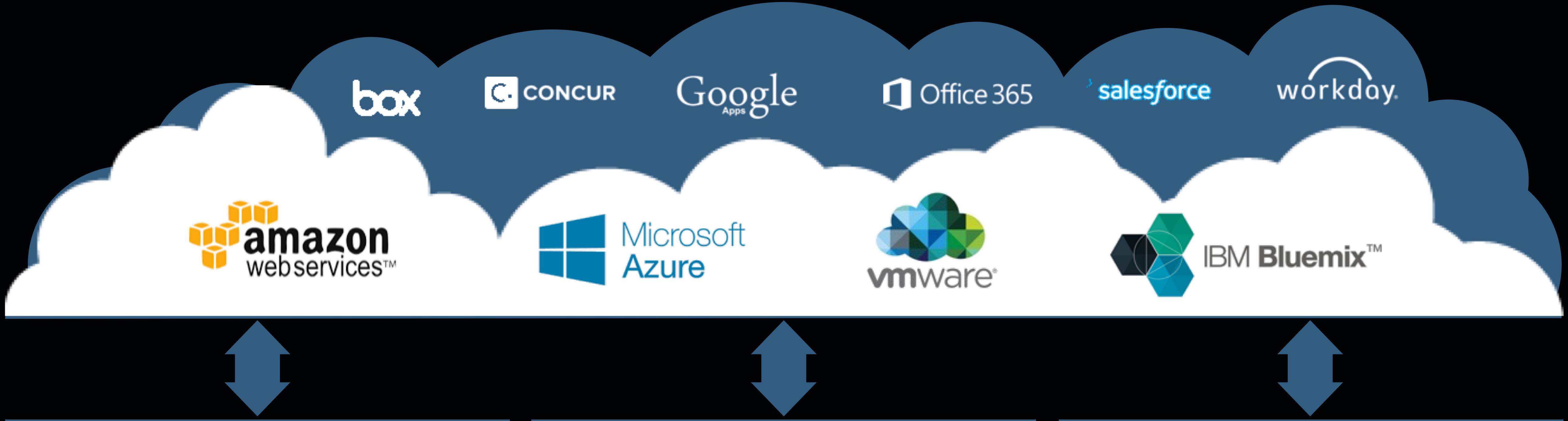
> “We need to secure the records of 475,000+ members while managing critical database access across our hybrid environment… we need help.”

Secure Hybrid Cloud

Protect Critical Assets

Prevent Advanced Fraud

Secure hybrid cloud



Protect data

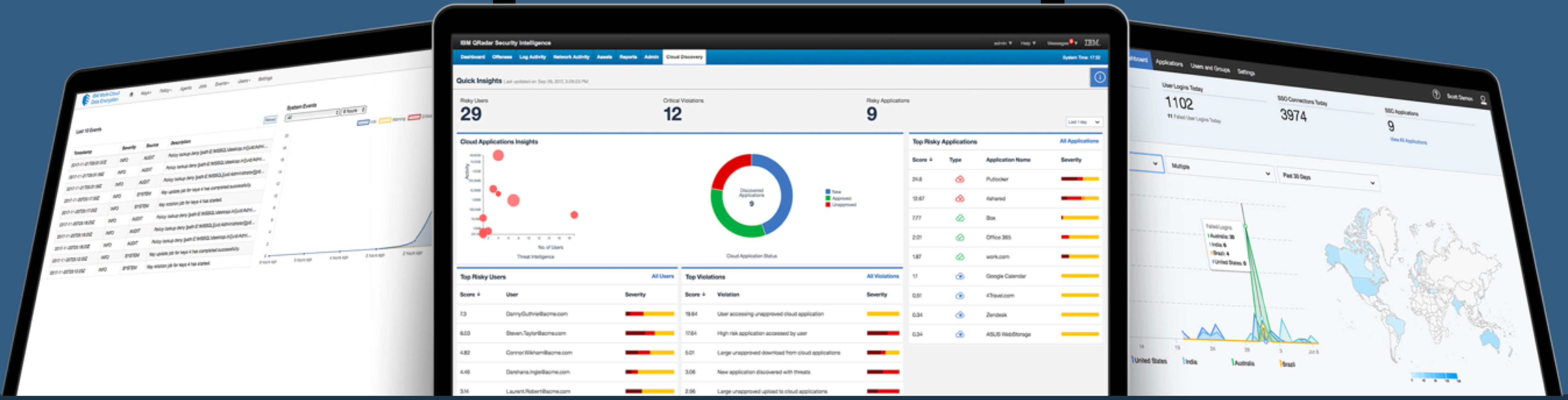
IBM Multi-Cloud Data Encryption

Gain visibility

IBM QRadar Cloud Discovery App

Manage access

IBM Cloud Identity Connect



IBM QRadar Security Intelligence

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Admin | Cloud Discovery

Quick Insights Last updated on Sep 26, 2017, 3:29:23 PM

Risky Users 29 | Critical Violations 12 | Risky Applications 9

Cloud Applications Insights

Discovered Applications 9 — New, Approved, Unapproved

Cloud Application Status

Top Risky Applications

Score	Application Name
24.6	Putlocker
12.67	4shared
7.77	Box
2.01	Office 365
1.87	work.com
1.1	Google Calendar
0.51	4Travel.com
0.34	Zendesk
0.34	ASUS WebStorage

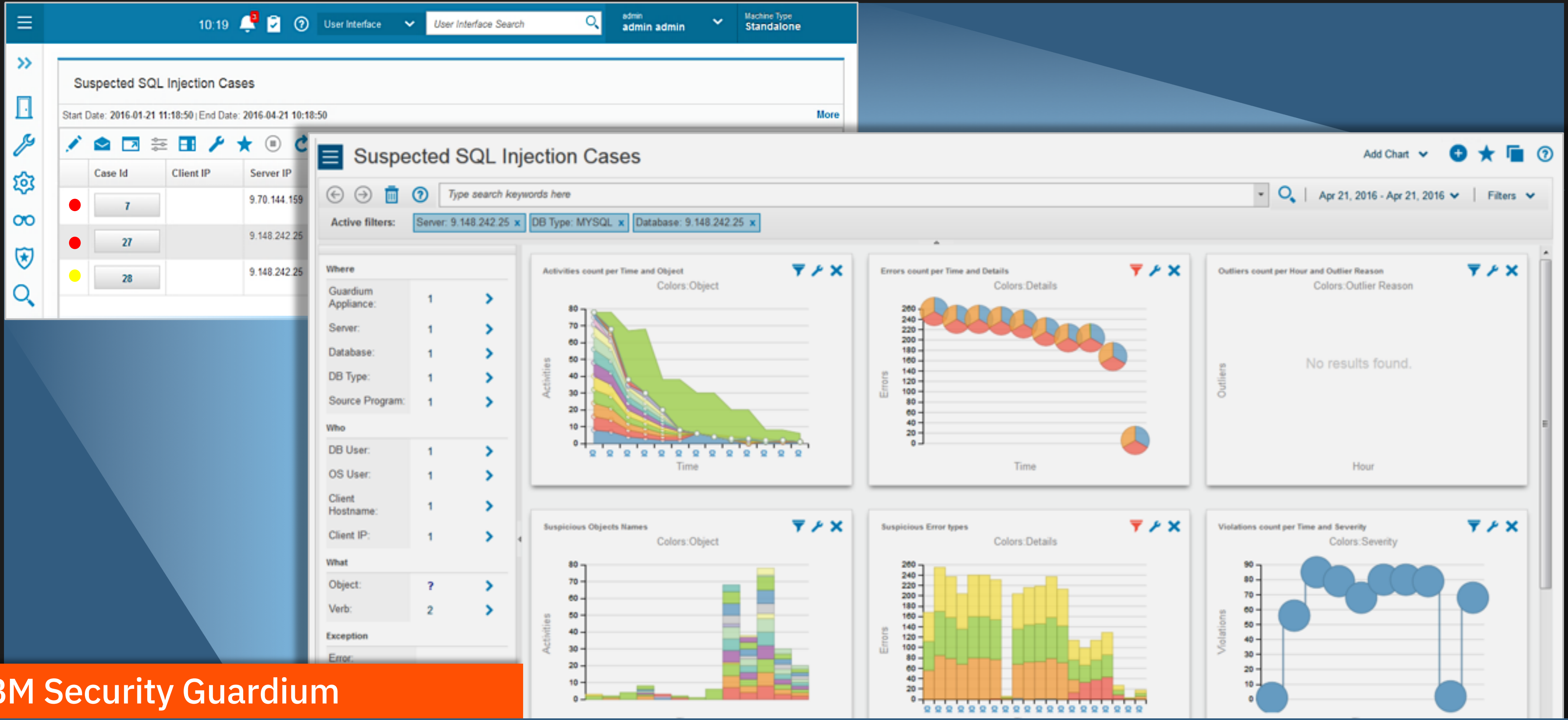
Top Risky Users

Score	User
7.3	DannyGuthrie@acme.com
6.03	Steven.Taylor@acme.com
4.82	ConnorWikham@acme.com
4.46	Darshana.Ingle@acme.com
3.14	Laurent.Robert@acme.com

Top Violations

Score	Violation
19.64	User accessing unapproved cloud application
17.64	High risk application accessed by user
5.01	Large unapproved download from cloud applications
3.06	New application discovered with threats
2.96	Large unapproved upload to cloud applications

Secure hybrid cloud



Suspected SQL Injection Cases

Start Date: 2016-01-21 11:18:50 | End Date: 2016-04-21 10:18:50

Case Id	Client IP	Server IP
7		9.70.144.159
27		9.148.242.25
28		9.148.242.25

Suspected SQL Injection Cases

Apr 21, 2016 - Apr 21, 2016

Active filters: Server: 9.148.242.25 | DB Type: MYSQL | Database: 9.148.242.25

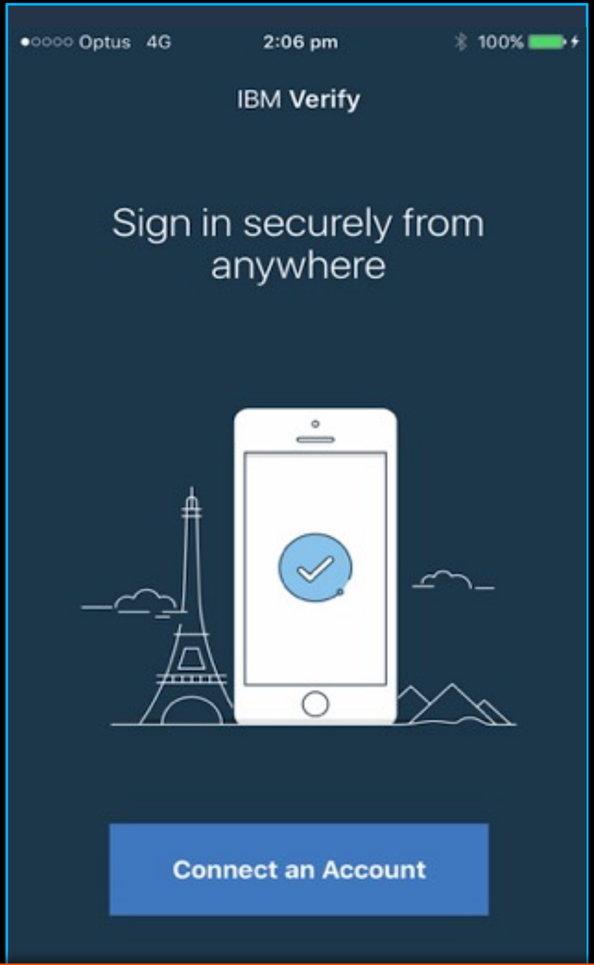
Where	
Guardium Appliance:	1
Server:	1
Database:	1
DB Type:	1
Source Program:	1
Who	
DB User:	1
OS User:	1
Client Hostname:	1
Client IP:	1
What	
Object:	?
Verb:	2
Exception	
Error:	

IBM Security Guardium

Secure applications built in a multi-cloud environment

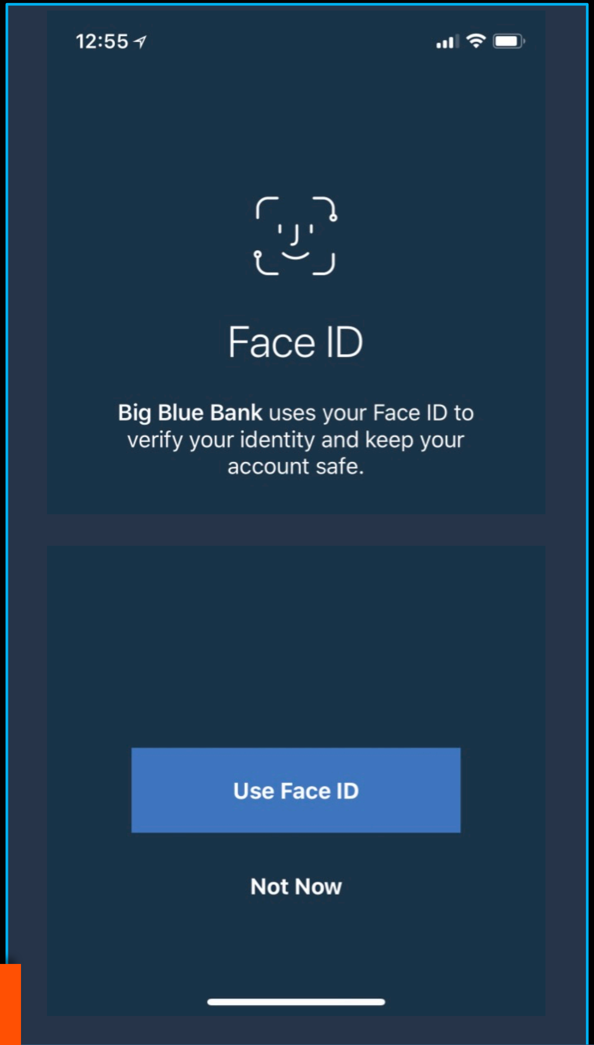
- Automatically discover and classify sensitive data
- Understand data access, spot anomalies,

Secure hybrid cloud



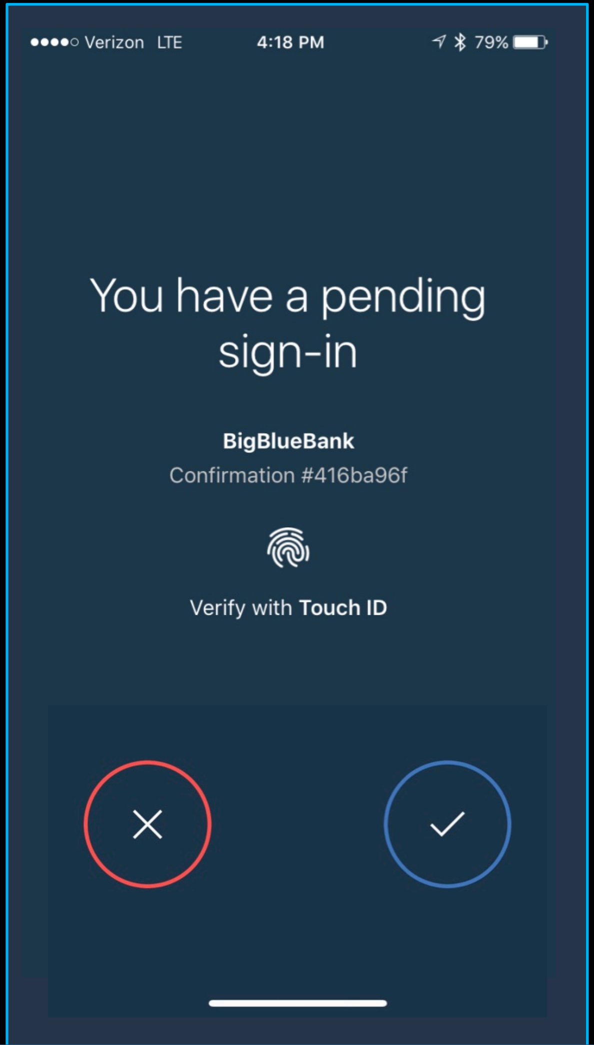
IBM Verify

Sign in securely from anywhere



Face ID

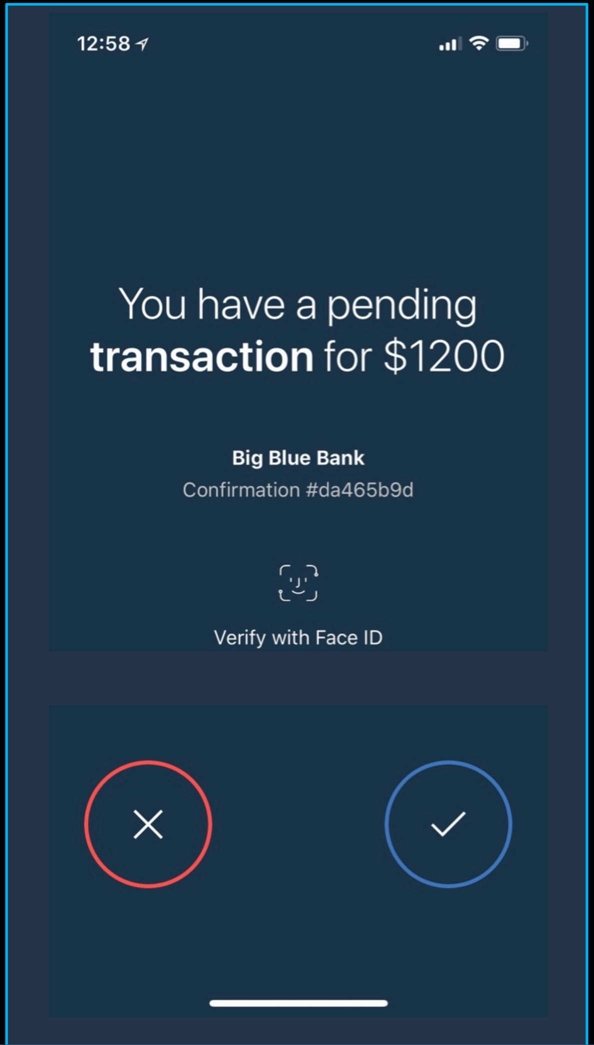
Big Blue Bank uses your Face ID to verify your identity and keep your account safe.



You have a pending sign-in

BigBlueBank
Confirmation #416ba96f

Verify with **Touch ID**



You have a pending **transaction** for $1200

Big Blue Bank
Confirmation #da465b9d

Verify with Face ID

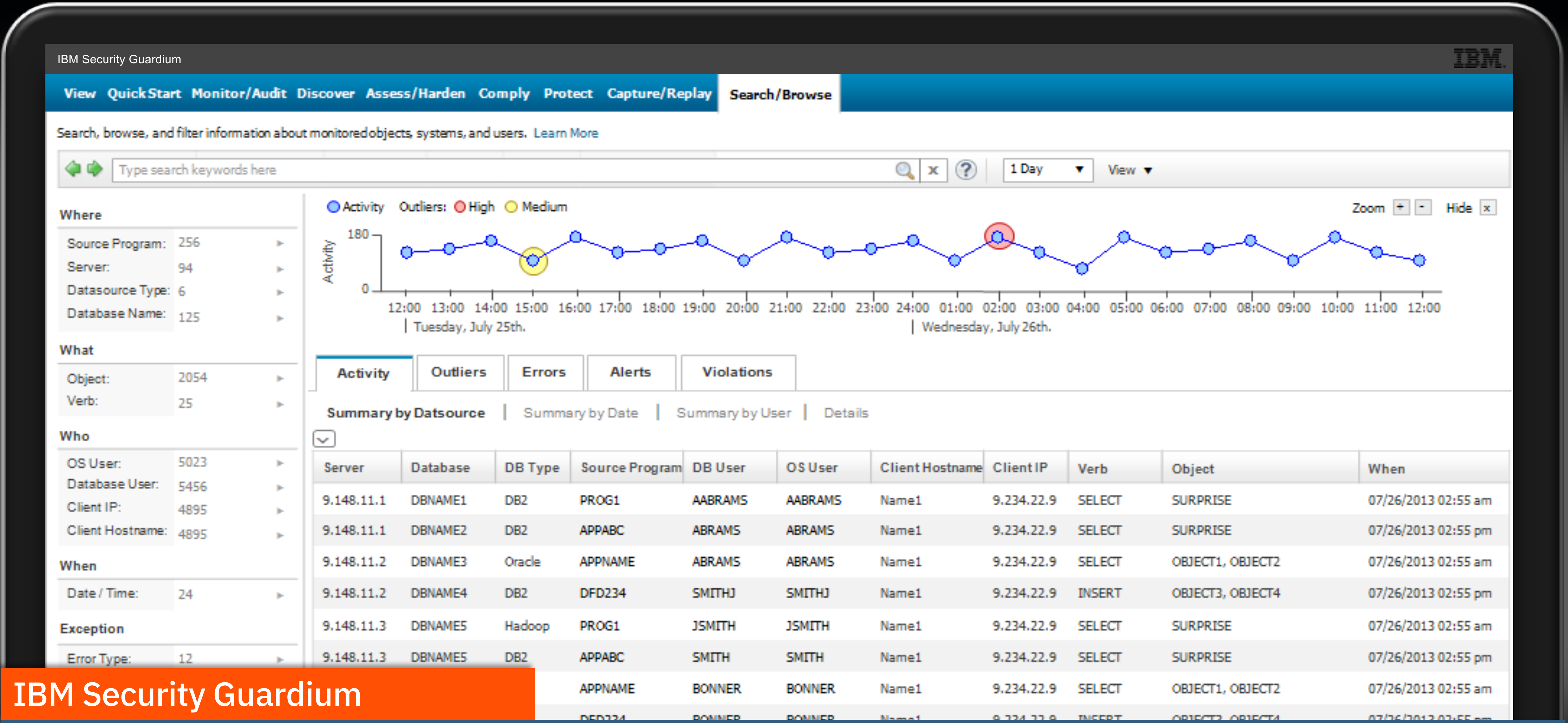
IBM Cloud Identity Verify

Bring simple and strong multi-factor authentication to online services

iOS android

- Simple strong authentication from the cloud
- Check-box risk assessment and user authentication policies

Protect critical assets


IBM Security Guardium

Search, browse, and filter information about monitored objects, systems, and users. Learn More

Where

Source Program:	256
Server:	94
Datasource Type:	6
Database Name:	125

What

Object:	2054
Verb:	25

Who

OS User:	5023
Database User:	5456
Client IP:	4895
Client Hostname:	4895

When

Date / Time:	24

Exception

Error Type:	12

Server	Database	DB Type	Source Program	DB User	OS User	Client Hostname	Client IP	Verb	Object	When
9.148.11.1	DBNAME1	DB2	PROG1	AABRAMS	AABRAMS	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.11.1	DBNAME2	DB2	APPABC	ABRAMS	ABRAMS	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm
9.148.11.2	DBNAME3	Oracle	APPNAME	ABRAMS	ABRAMS	Name1	9.234.22.9	SELECT	OBJECT1, OBJECT2	07/26/2013 02:55 am
9.148.11.2	DBNAME4	DB2	DFD234	SMITHJ	SMITHJ	Name1	9.234.22.9	INSERT	OBJECT3, OBJECT4	07/26/2013 02:55 pm
9.148.11.3	DBNAME5	Hadoop	PROG1	JSMITH	JSMITH	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 am
9.148.11.3	DBNAME5	DB2	APPABC	SMITH	SMITH	Name1	9.234.22.9	SELECT	SURPRISE	07/26/2013 02:55 pm
			APPNAME	BONNER	BONNER	Name1	9.234.22.9	SELECT	OBJECT1, OBJECT2	07/26/2013 02:55 am
			DFD234	BONNER	BONNER	Name1	9.234.22.9	INSERT	OBJECT3, OBJECT4	07/26/2013 02:55 pm

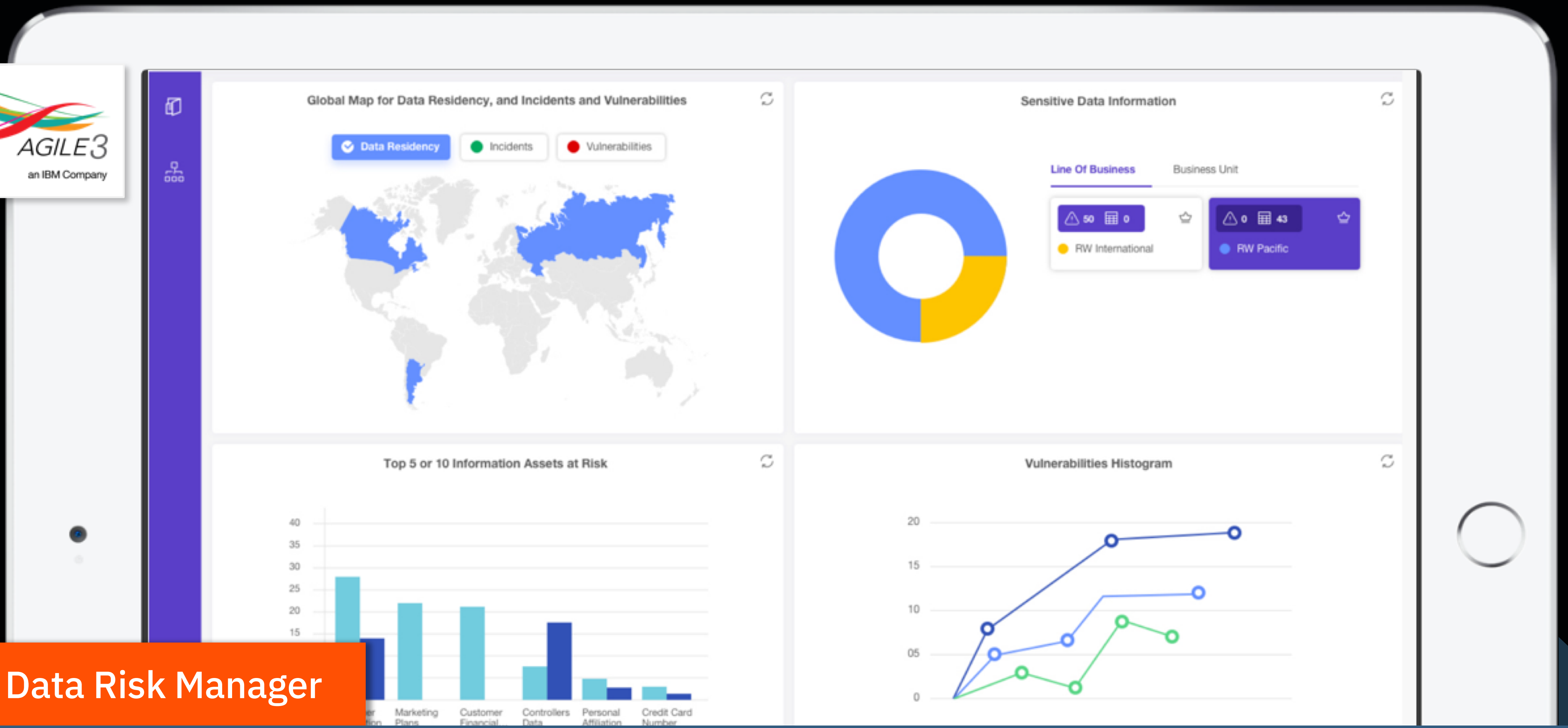
IBM Security Guardium

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

AGILE3
an IBM Company

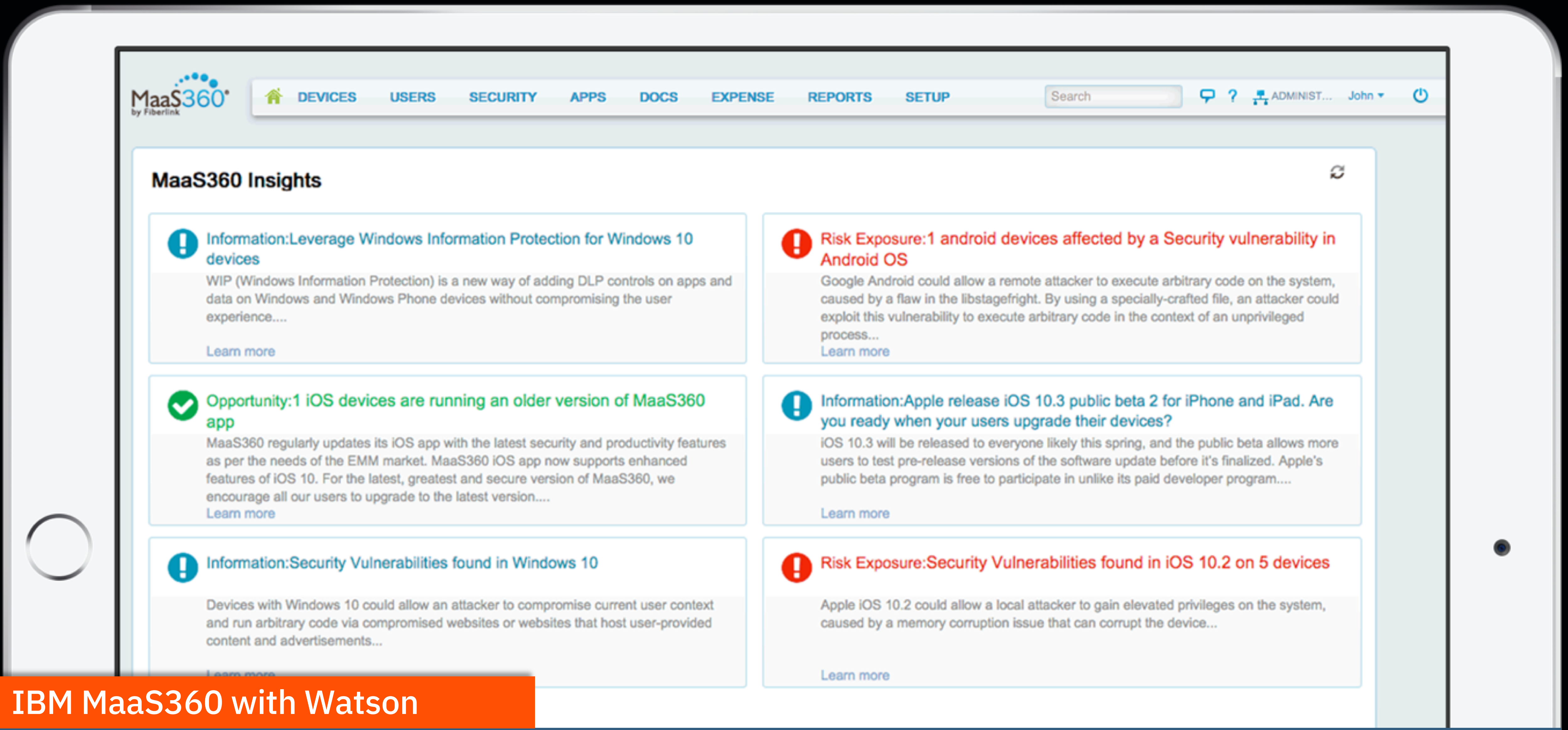


IBM Data Risk Manager

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

Protect critical assets



MaaS360 Insights

Information:Leverage Windows Information Protection for Windows 10 devices

WIP (Windows Information Protection) is a new way of adding DLP controls on apps and data on Windows and Windows Phone devices without compromising the user experience....

Learn more

Risk Exposure:1 android devices affected by a Security vulnerability in Android OS

Google Android could allow a remote attacker to execute arbitrary code on the system, caused by a flaw in the libstagefright. By using a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code in the context of an unprivileged process...

Learn more

Opportunity:1 iOS devices are running an older version of MaaS360 app

MaaS360 regularly updates its iOS app with the latest security and productivity features as per the needs of the EMM market. MaaS360 iOS app now supports enhanced features of iOS 10. For the latest, greatest and secure version of MaaS360, we encourage all our users to upgrade to the latest version....

Learn more

Information:Apple release iOS 10.3 public beta 2 for iPhone and iPad. Are you ready when your users upgrade their devices?

iOS 10.3 will be released to everyone likely this spring, and the public beta allows more users to test pre-release versions of the software update before it's finalized. Apple's public beta program is free to participate in unlike its paid developer program....

Learn more

Information:Security Vulnerabilities found in Windows 10

Devices with Windows 10 could allow an attacker to compromise current user context and run arbitrary code via compromised websites or websites that host user-provided content and advertisements...

Learn more

Risk Exposure:Security Vulnerabilities found in iOS 10.2 on 5 devices

Apple iOS 10.2 could allow a local attacker to gain elevated privileges on the system, caused by a memory corruption issue that can corrupt the device...

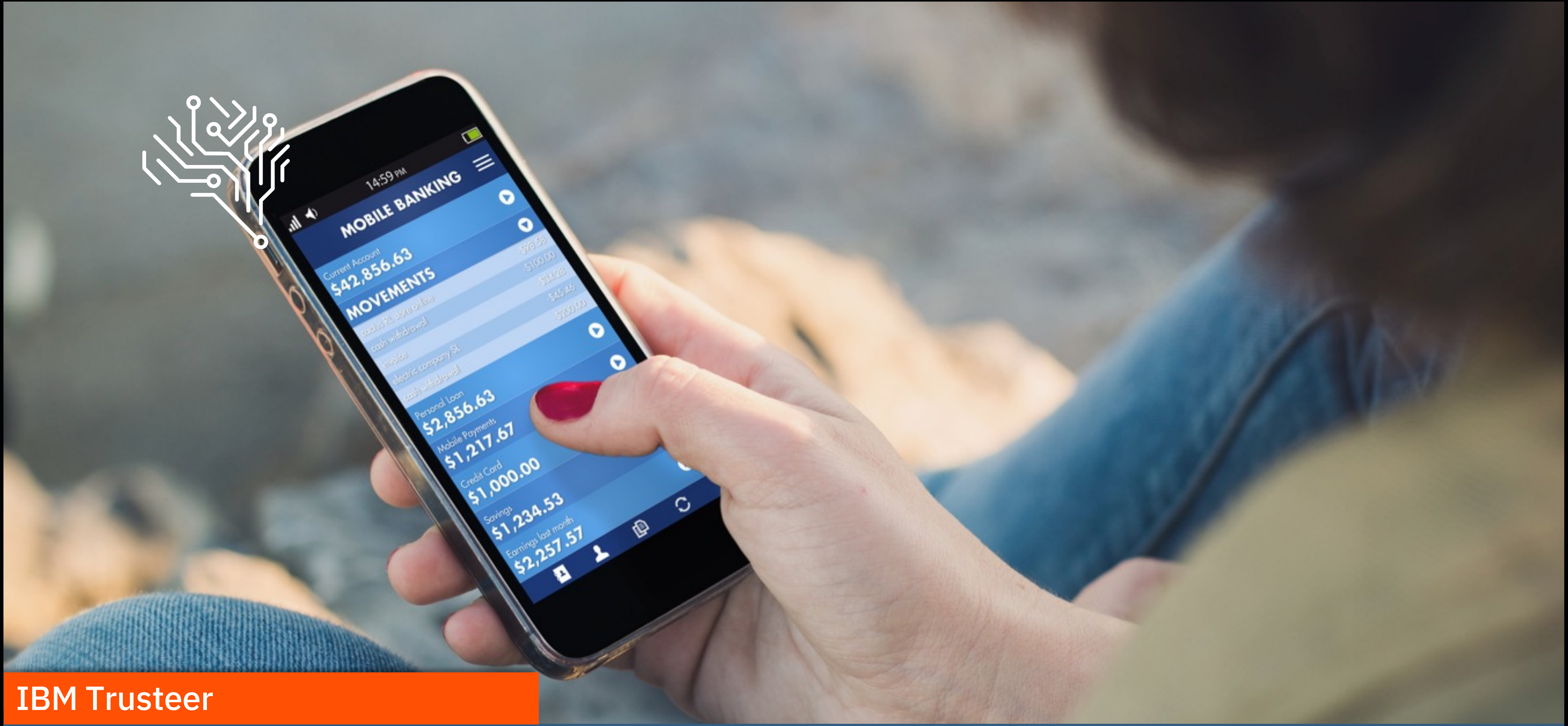
Learn more

IBM MaaS360 with Watson

Simplify the management and security of smartphones, tablets, laptops, wearables and IoT

- Cognitive insights to identify policy and app improvements
- Proactively address new vulnerabilities

Discover identity, build 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

Grow business with IBM Security Services

IBM Hybrid Cloud Security Services

- **Real-time visibility across multi-cloud environments**, enforcing security policy across shadow and IT-sanctioned workloads
- **One centralized and simplified view** to manage and monitor security operations
- **Prioritizes roadmap actions** needed to protect workloads
- **Implements an integrated threat management program** to detect, prevent and respond to malicious activity

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- 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.

IBM®