

# IBM SECURITY STRATEGY

DRIVING INNOVATION WHILE HELPING TO SECURE 17,500+ CUSTOMERS



**Vu Luu (Luu Danh Anh Vũ)**

Country Manager for Security  
IBM Vietnam

Hanoi, 8 Aug, 2017

# Security drivers are evolving

			
ADVANCED ATTACKS	INSIDERS	NEW INNOVATIONS	COMPLIANCE
<i>From...</i> <ul style="list-style-type: none"><li>• Broad threats</li><li>• Individual hackers</li></ul>	<ul style="list-style-type: none"><li>• Disgruntled employees</li></ul>	<ul style="list-style-type: none"><li>• Technology and linear driven security strategy</li></ul>	<ul style="list-style-type: none"><li>• Checking the box</li><li>• PCI compliance</li></ul>
<i>To...</i> <ul style="list-style-type: none"><li>• Targeted and organized crime (i.e., ransomware)</li></ul>	<ul style="list-style-type: none"><li>• Outsiders and partners becoming insiders</li></ul>	<ul style="list-style-type: none"><li>• Agile security that moves with the business</li></ul>	<ul style="list-style-type: none"><li>• Continuous risk analysis</li><li>• GDPR</li></ul>

Cybercrime will become a  
**\$2.1 trillion**  
problem by 2019

2016 insider attacks were  
**58 percent**  
42% outsider attacks

By 2020, there will be  
**20.8 billion**  
connected “things”

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

# How do I get started when all I see is chaos?

Threat and anomaly detection

Virtual patching

Indicators of compromise

Network visibility and segmentation

Data access control

Cognitive security

Sandboxing

Mainframe security

Incident response

Data monitoring

Access management

Content security

Application security management

IP reputation

Threat sharing

Firewalls

Endpoint patching and management

Criminal detection

Network forensics and threat management

Identity governance and administration

Privileged user management

Malware protection

Fraud protection

Vulnerability management

Workload protection

Threat hunting and investigation

Transaction protection

Endpoint detection and response

IDaaS

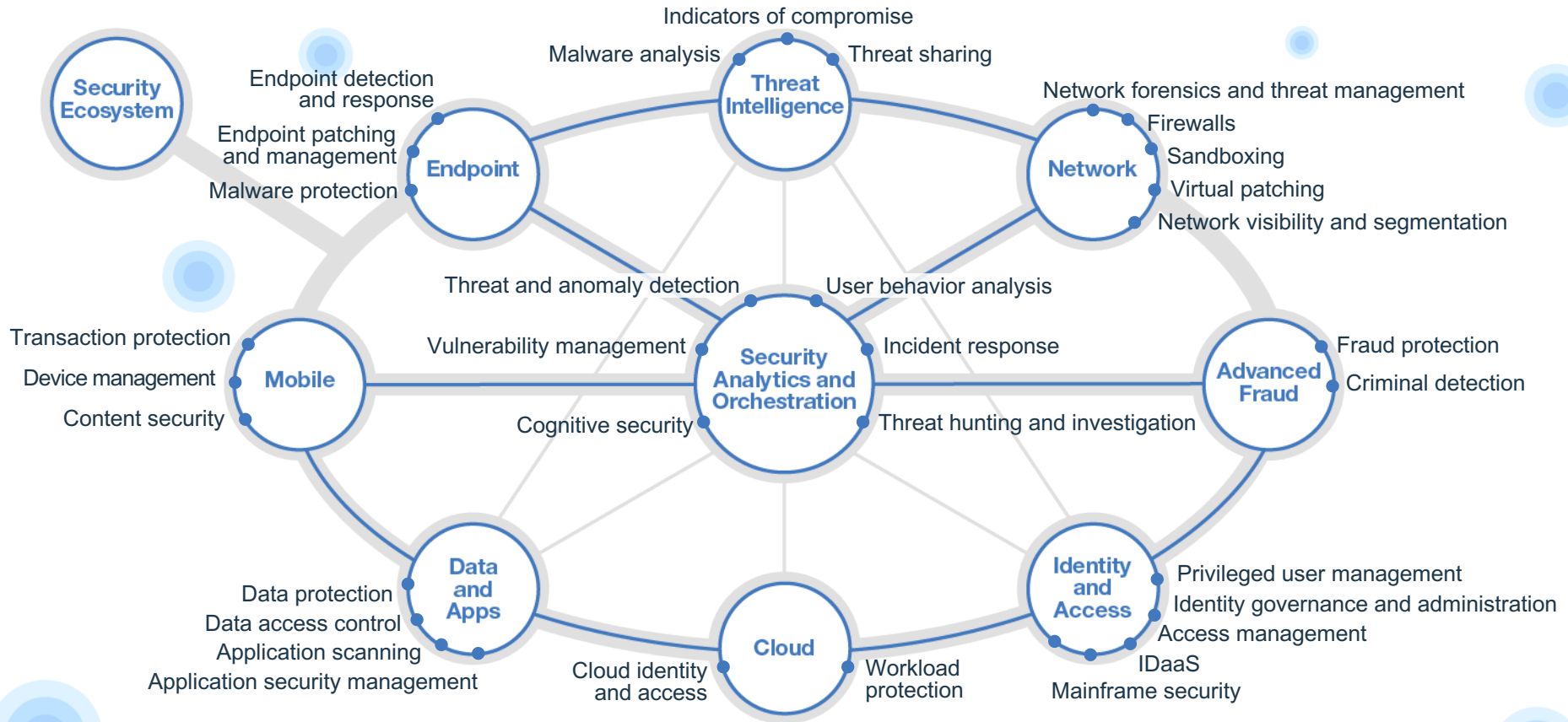
Device management

User behavior analysis

Cloud identity and access

Application scanning

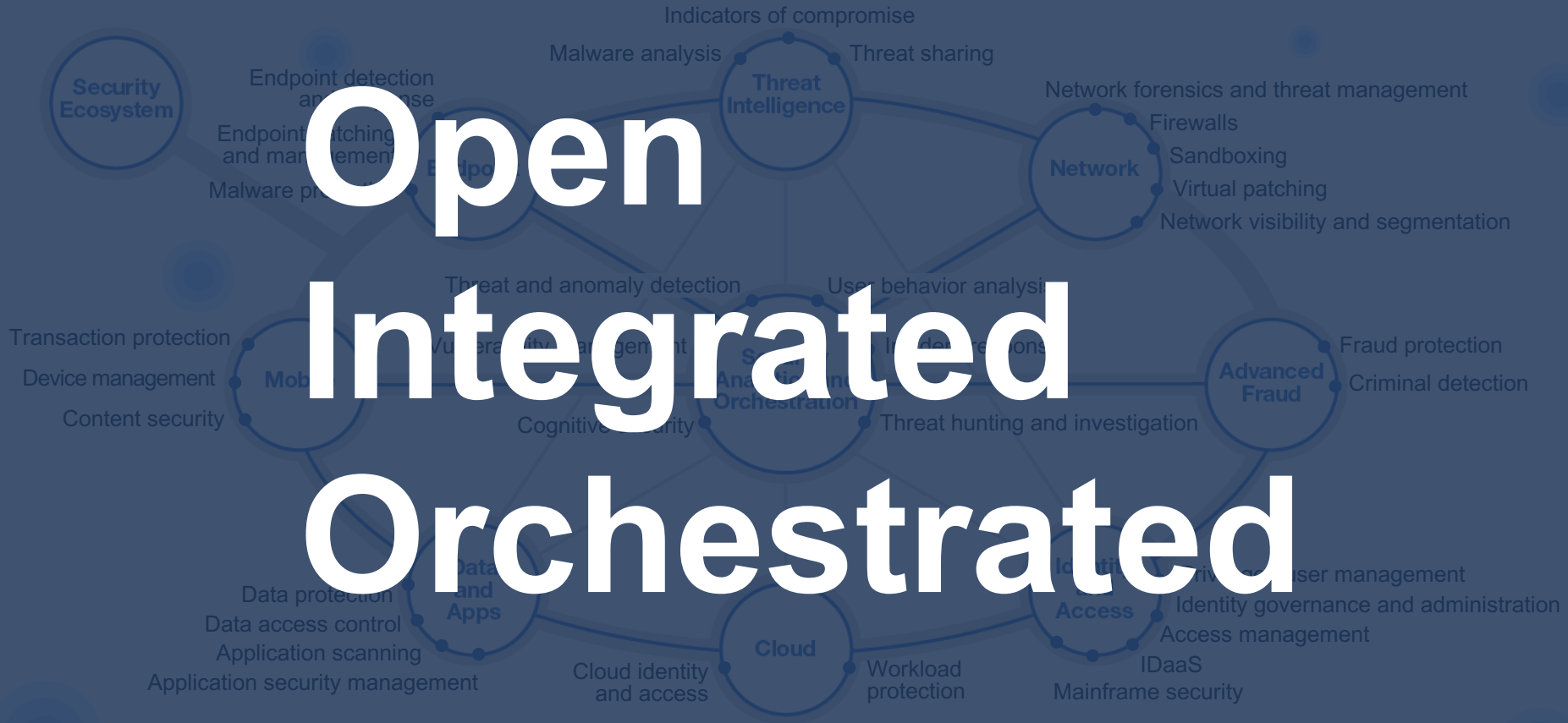
# An integrated and intelligent security immune system



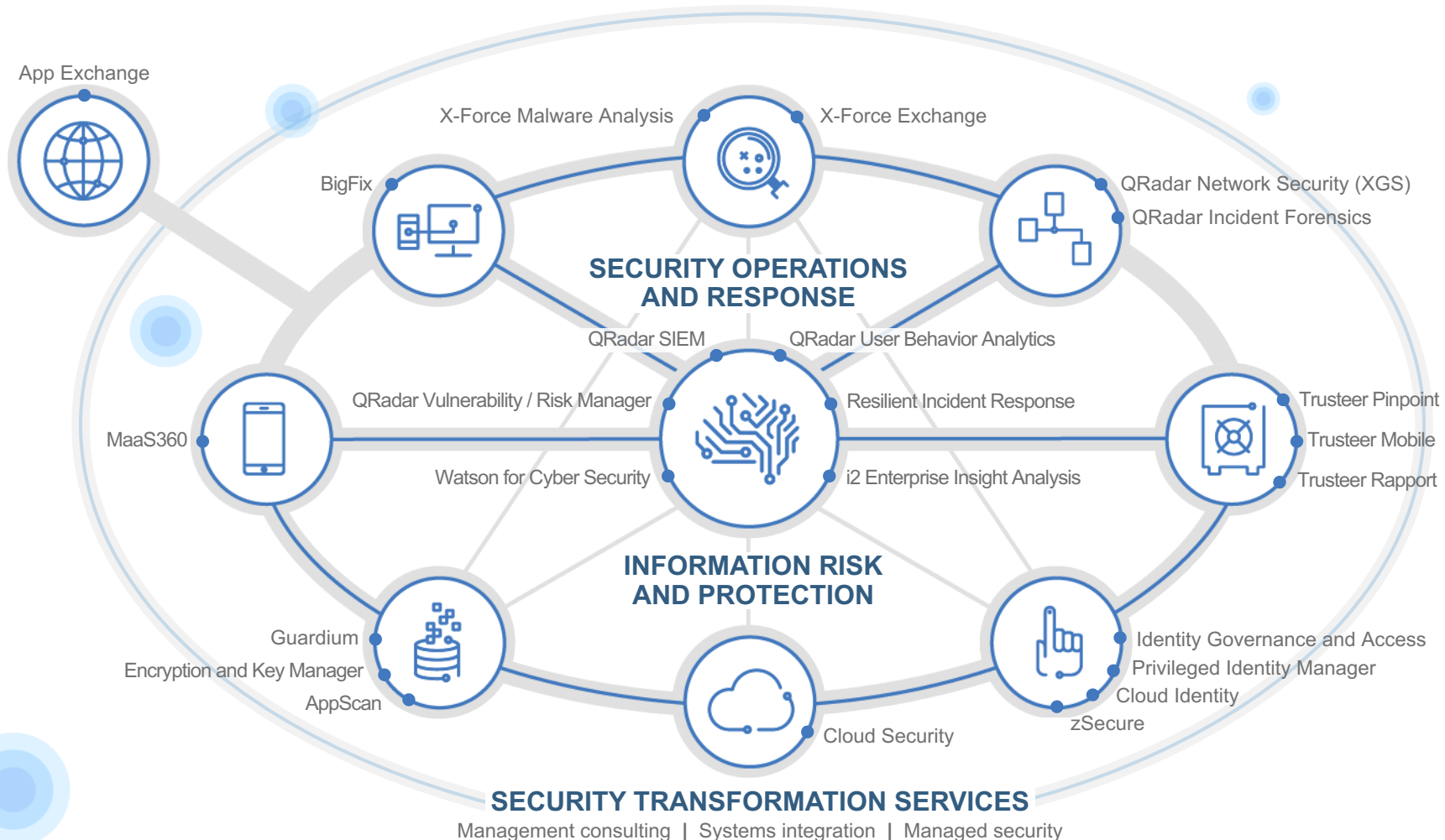


An integrated and intelligent security immune system

# Open Integrated Orchestrated



# IBM has the world's broadest and deepest security portfolio



# Open partner ecosystem



# The next era of security



**PERIMETER  
CONTROLS**



**INTELLIGENCE, INTEGRATION,  
and ORCHESTRATION**



**COGNITIVE, CLOUD,  
and COLLABORATION**

Security Operations and Response (SOAR)



# Build a Cognitive SOC

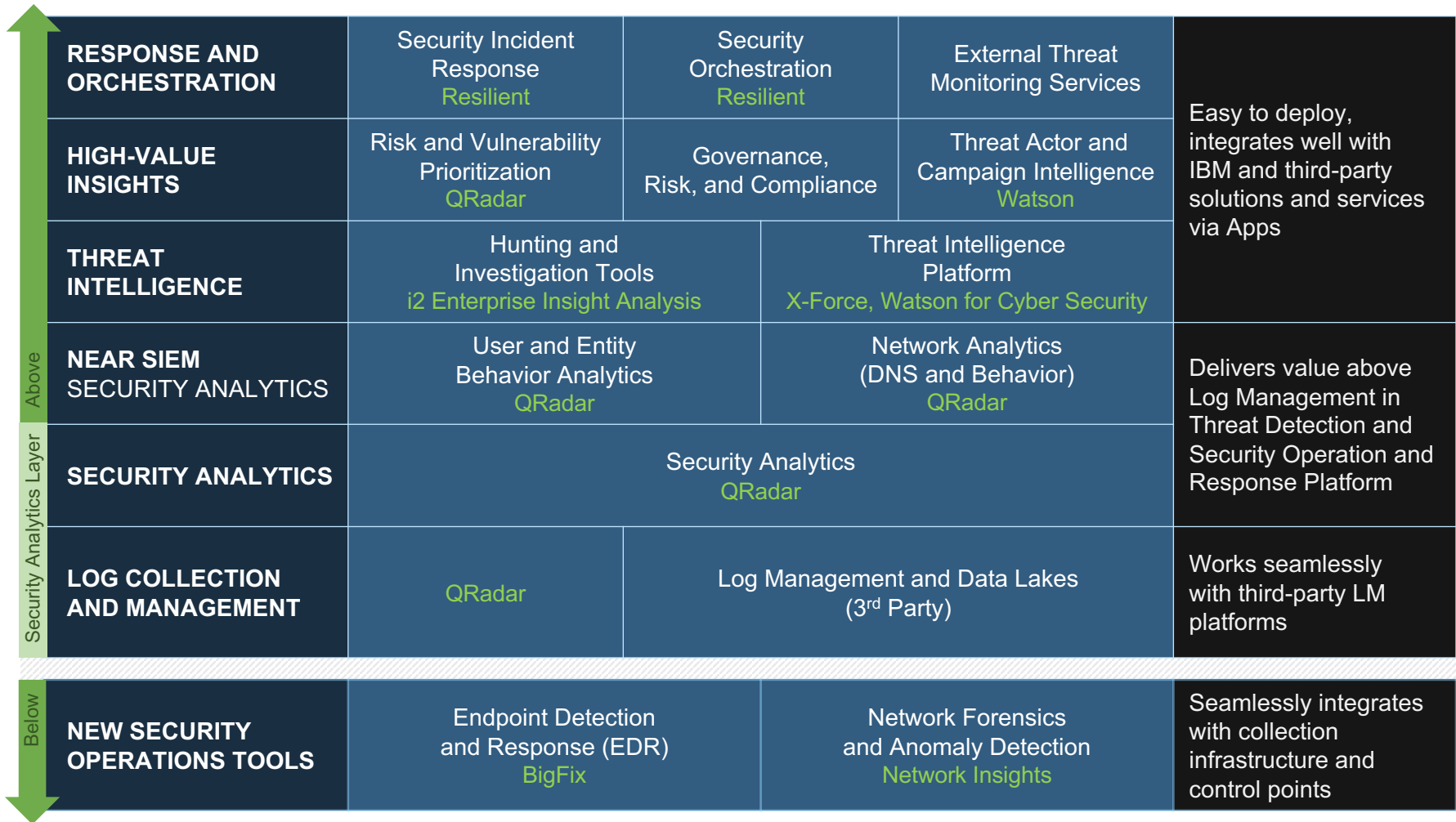
Uncover  
new insights

Hunt  
for threats

Orchestrate  
your response

Share threat  
intelligence

# Security Operations and Response: Build a Cognitive SOC



# Unlock the power of cognitive security

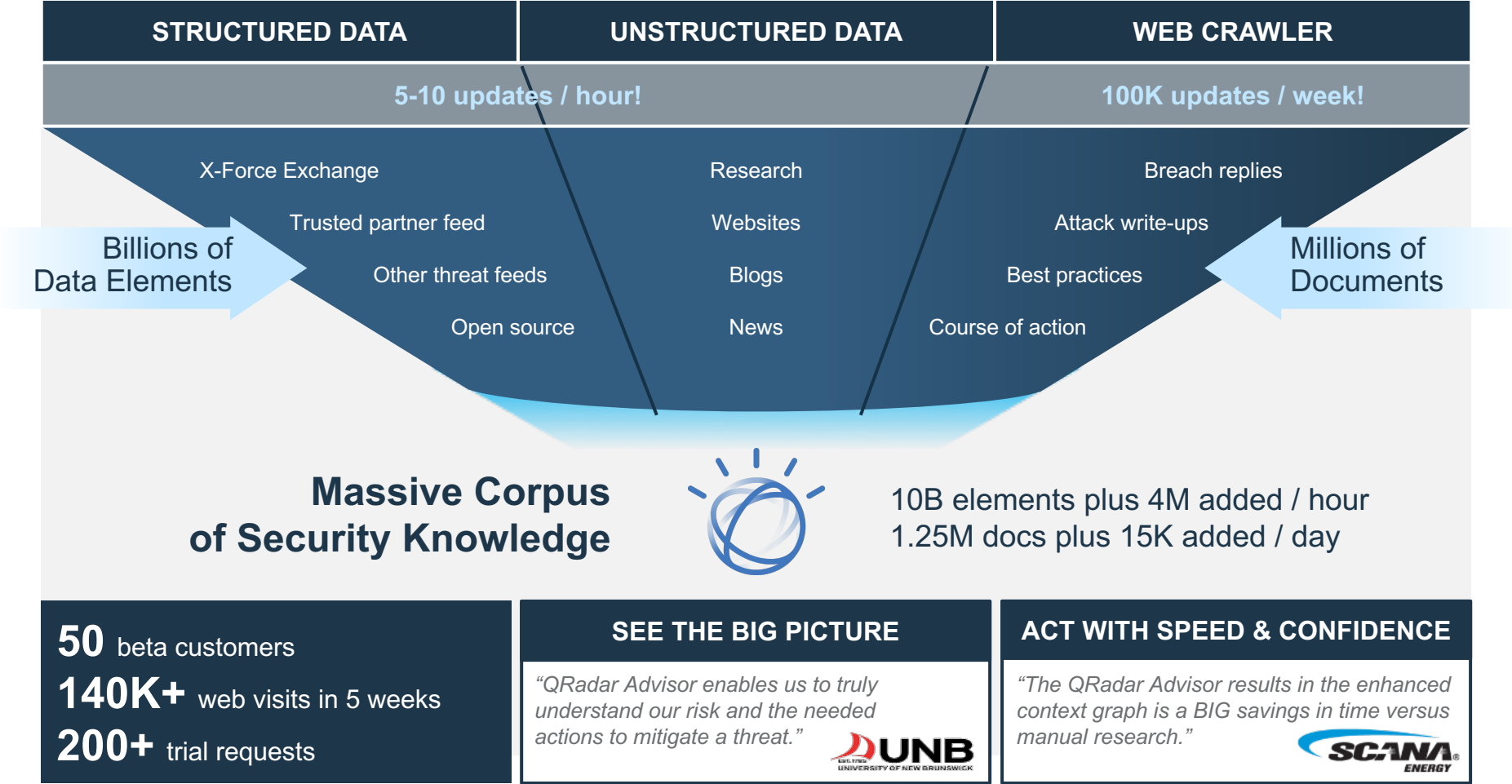
Watson for Cyber Security helps security professionals work smarter

- **Augment security expertise** with cognitive systems that use natural language processing to ingest, understand, and uncover insights from structured and unstructured data
- **Combat emerging threats** with cognitive analysis such as machine learning, clustering, graph mining, and entity relationship modeling
- **Strengthen application security** with cognitive systems that understand semantic context of analytics while quickly identifying problem source code
- **Improve enterprise risk** through fast and accurate risk profiling from cognitive systems that analyze corpuses of in-context interactions

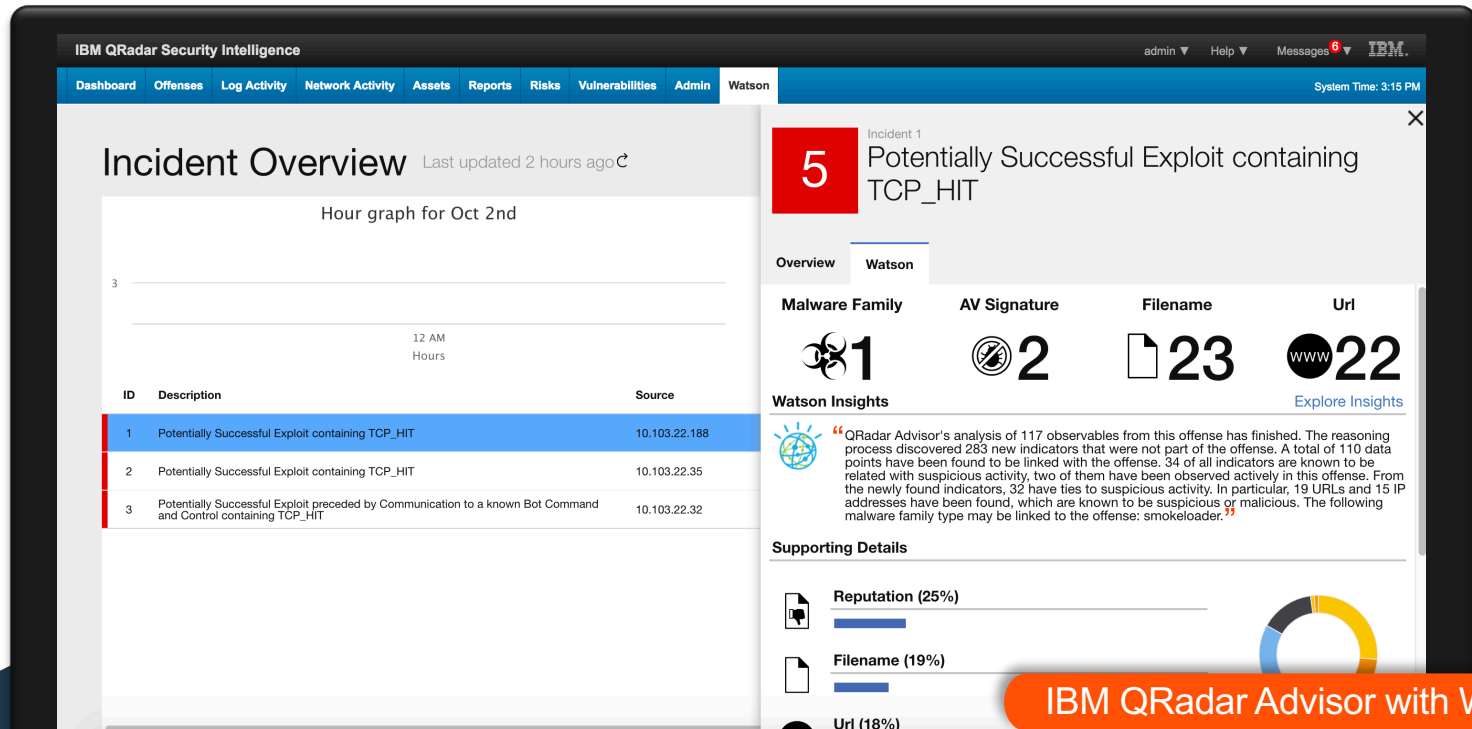




# How Watson for Cyber Security works



# Revolutionize how security analysts work



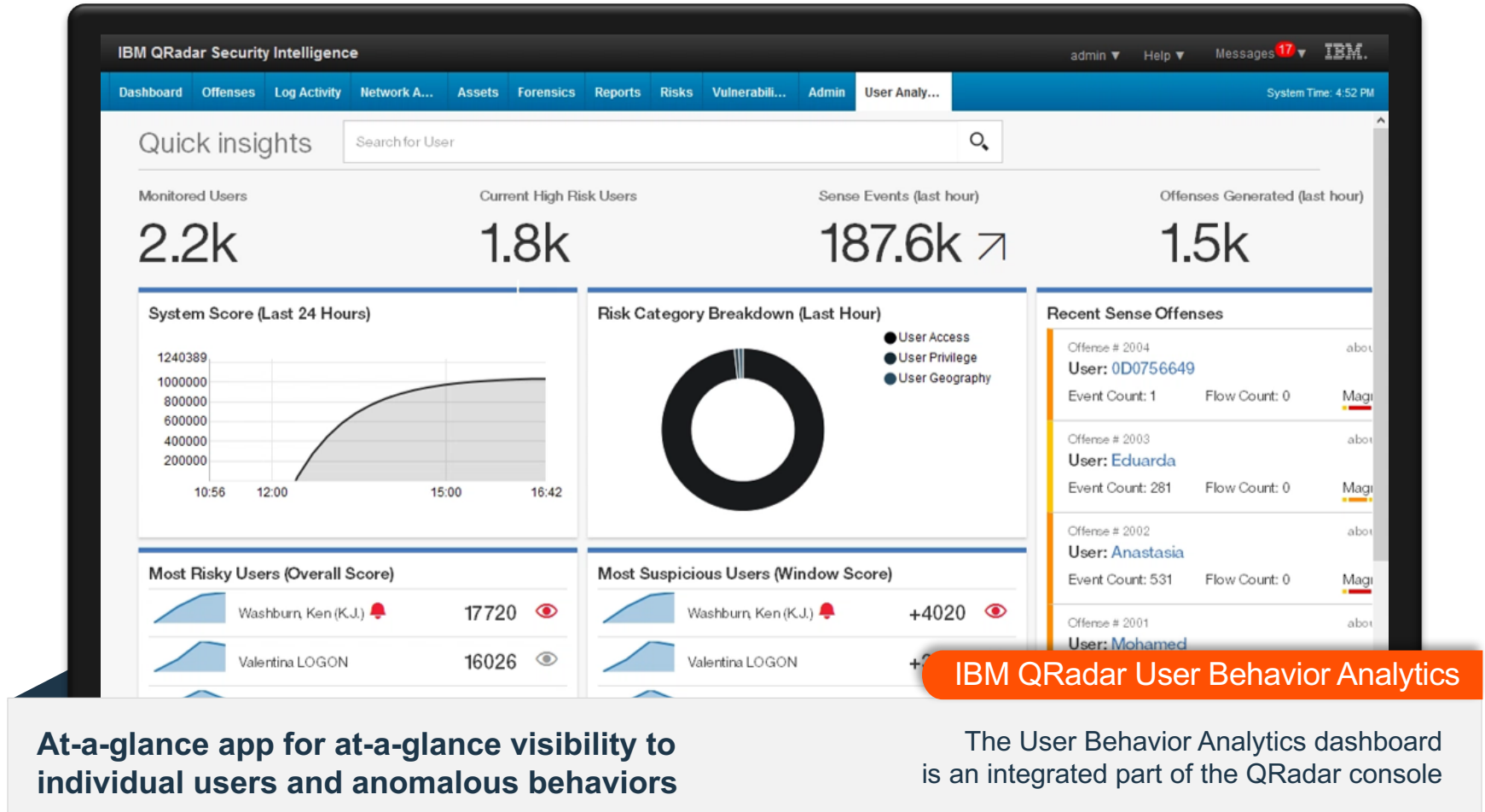
IBM QRadar Advisor with Watson

**Automatically uncover new security context and full scope of an incident**

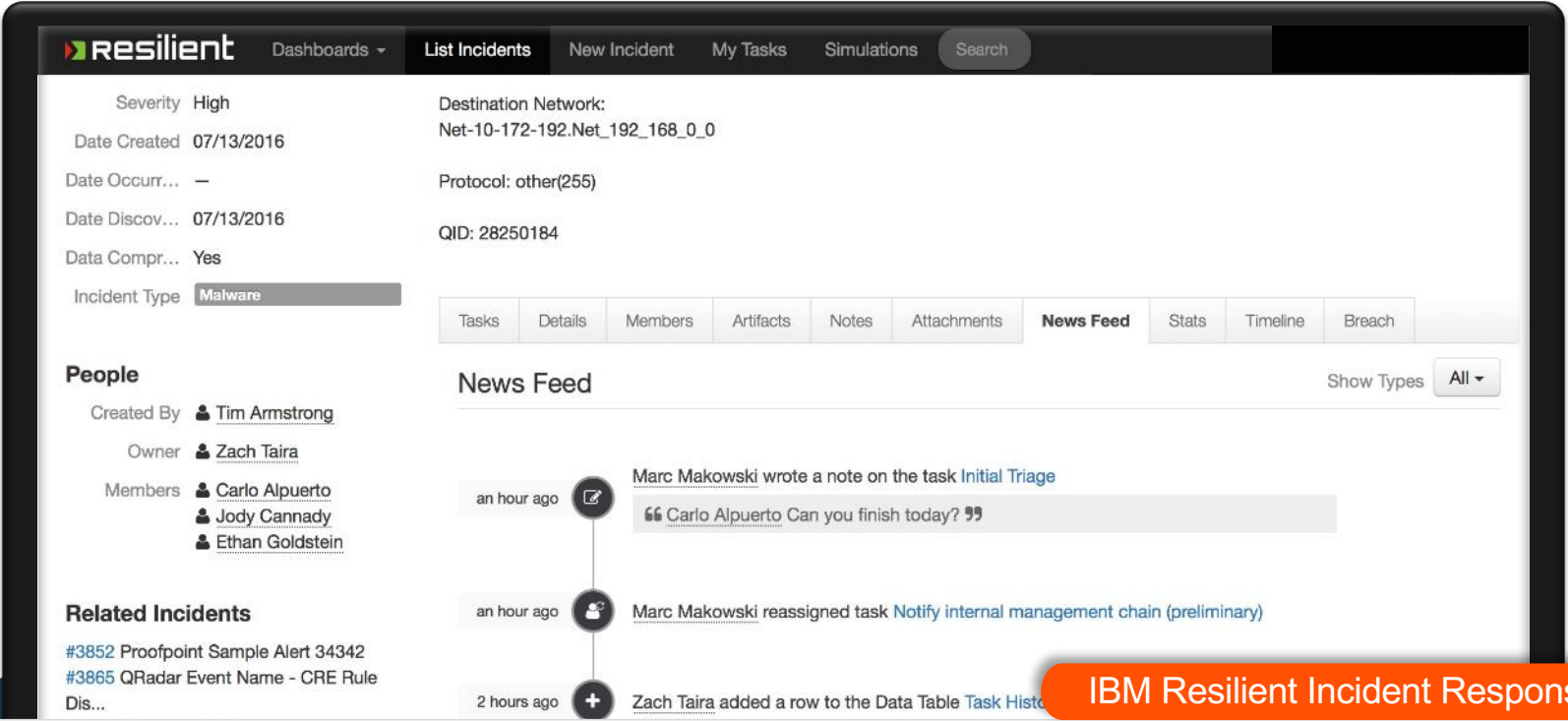
- **2.3M+** security documents
- **10B+** security data elements
- **80K+** documents read per day
- **250K+** investigations enhanced in just six months

# QRADAR ADVISOR with WATSON VIDEO

# Detect abnormal behavior in one click



# Collaboratively respond in minutes

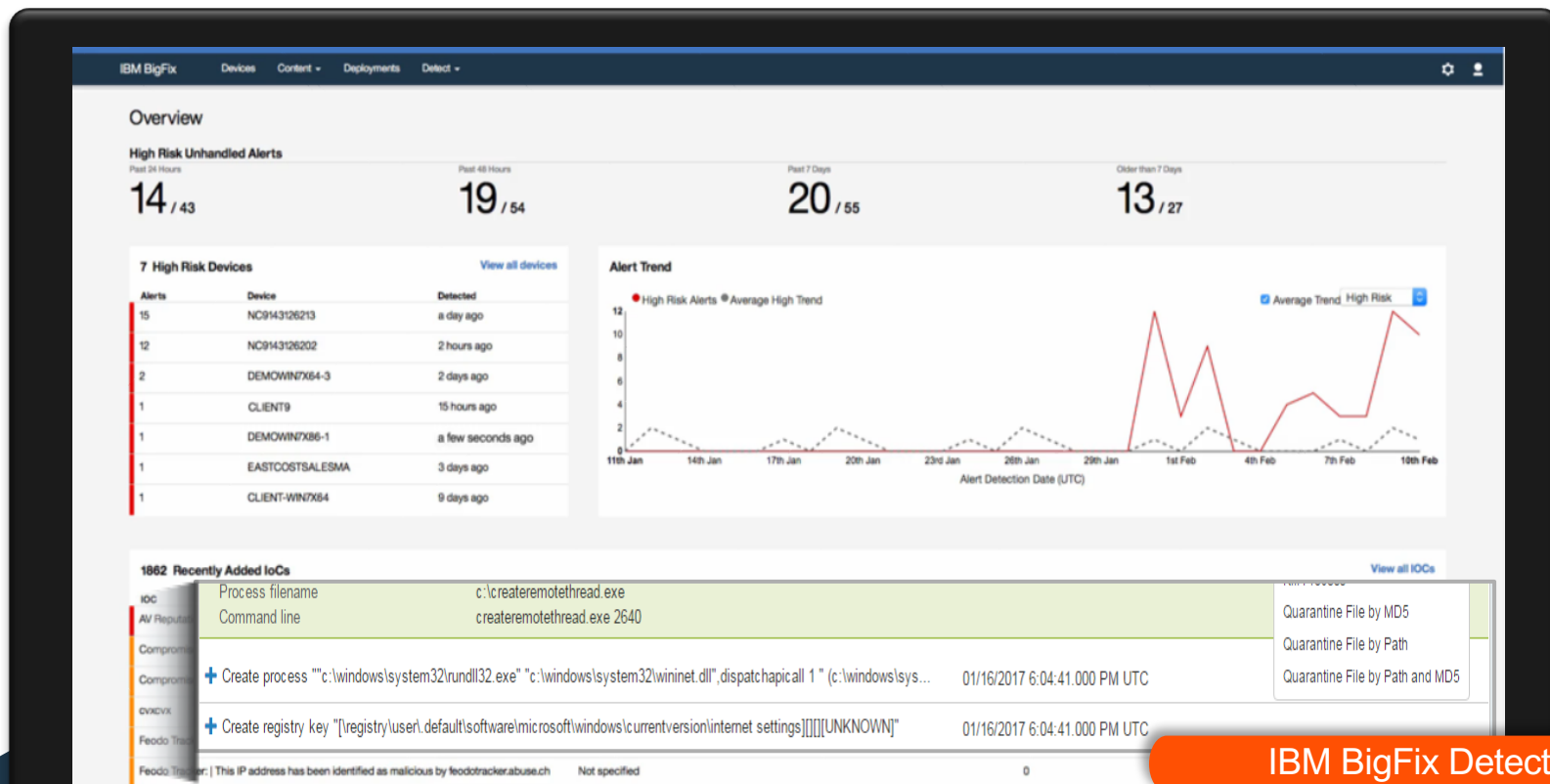


The screenshot displays the IBM Resilient web interface for incident response. The top navigation bar includes 'resilient', 'Dashboards', 'List Incidents' (selected), 'New Incident', 'My Tasks', 'Simulations', and a 'Search' button. The incident details on the left show: Severity: High, Date Created: 07/13/2016, Date Occurred: —, Date Discovered: 07/13/2016, Data Compromised: Yes, Incident Type: Malware. The right side shows Destination Network: Net-10-172-192.Net\_192\_168\_0\_0, Protocol: other(255), and QID: 28250184. Below these are tabs for Tasks, Details, Members, Artifacts, Notes, Attachments, News Feed (selected), Stats, Timeline, and Breach. The 'People' section lists: Created By: Tim Armstrong, Owner: Zach Taira, and Members: Carlo Alpuerto, Jody Cannady, and Ethan Goldstein. The 'Related Incidents' section lists: #3852 Proofpoint Sample Alert 34342 and #3865 QRadar Event Name - CRE Rule Dis... The 'News Feed' section shows a timeline of collaborative actions: 'an hour ago' - Marc Makowski wrote a note on the task Initial Triage (quote: 'Carlo Alpuerto Can you finish today?'); 'an hour ago' - Marc Makowski reassigned task Notify internal management chain (preliminary); '2 hours ago' - Zach Taira added a row to the Data Table Task History. An orange banner at the bottom right of the screenshot reads 'IBM Resilient Incident Response'.

**Orchestrate incident response with a single hub to align people, process, and technology**

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

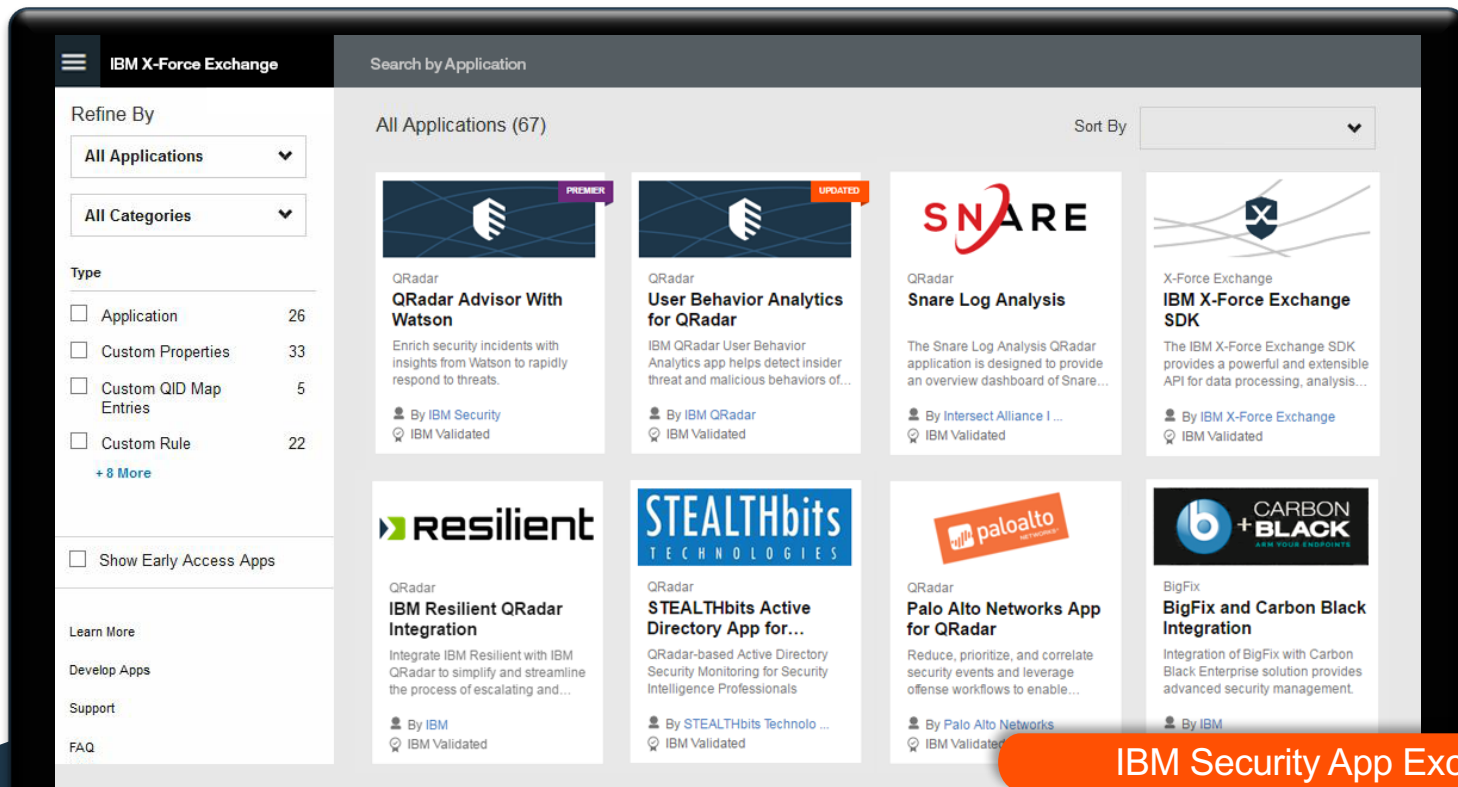
# Endpoint detection, response, and remediation in ONE solution



**Bridging the gap between attack detection and remediation**

- Detect evasive attacks
- Enterprise-wide remediation
- Guided incident investigation

# Leverage an ecosystem of collaborative defenses



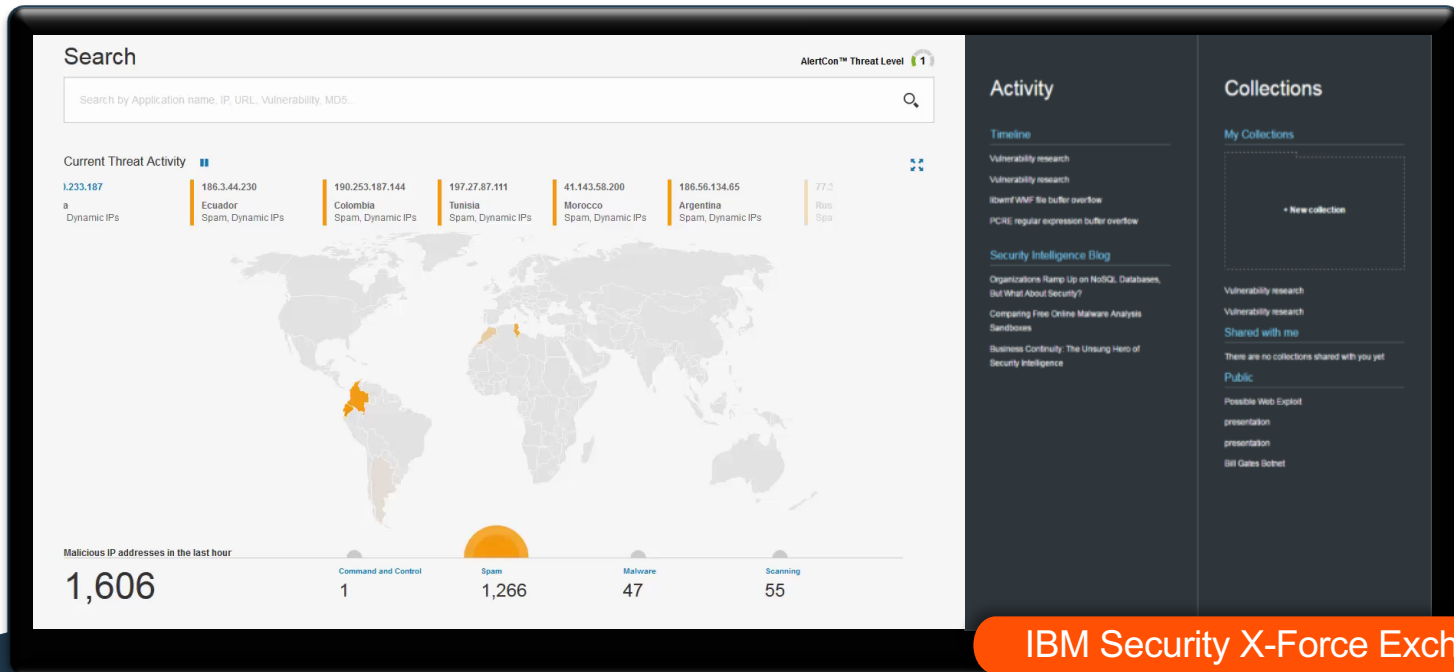
**Share and download apps  
based on IBM security technologies**

- **90+** IBM and partner generated apps

- **49K+** visits and **28K+** app downloads  
Since introduced in December of 2015



# Crowd-sourced sharing based on 800TB+ of threat intelligence



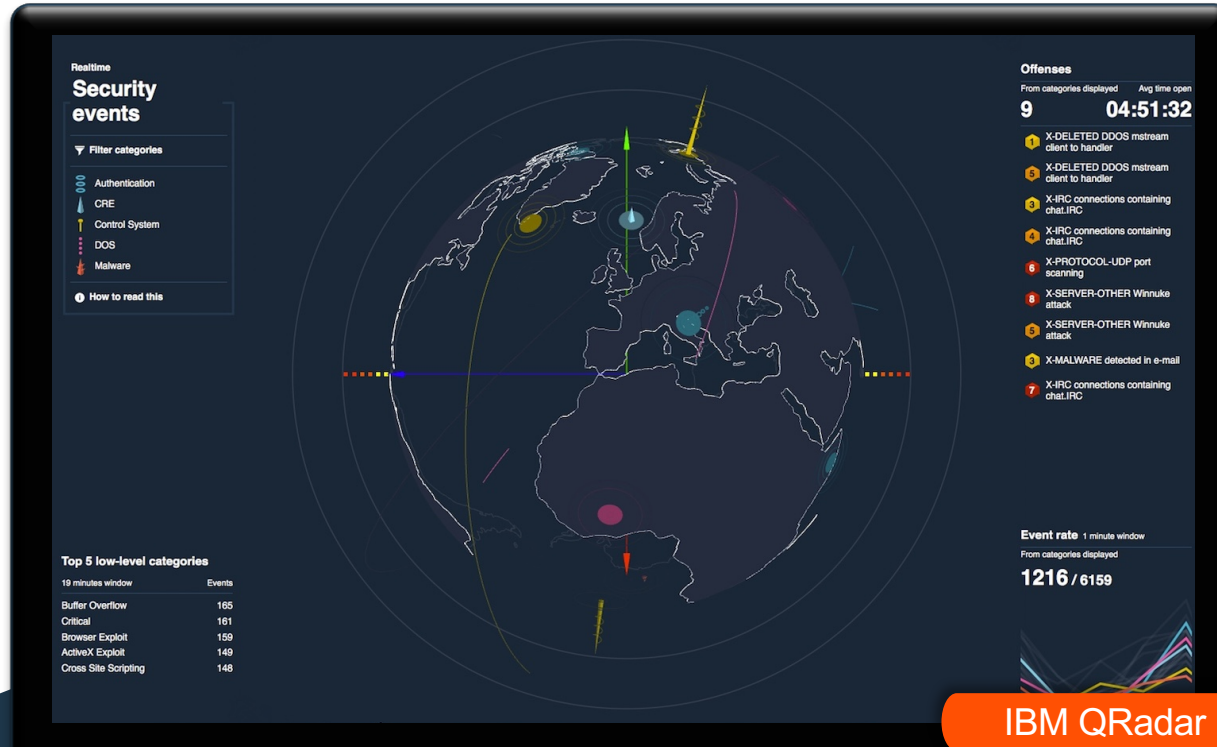
IBM Security X-Force Exchange

## Gain integrated, real-time threat intelligence

- **15B+** monitored security events / day
- **1M+** malicious IP addresses
- Malware threat intelligence from **270M+** endpoints
- **1,000+** financial malware sampled daily

Data sourced from  
2,000 organizations  
across 16 industries

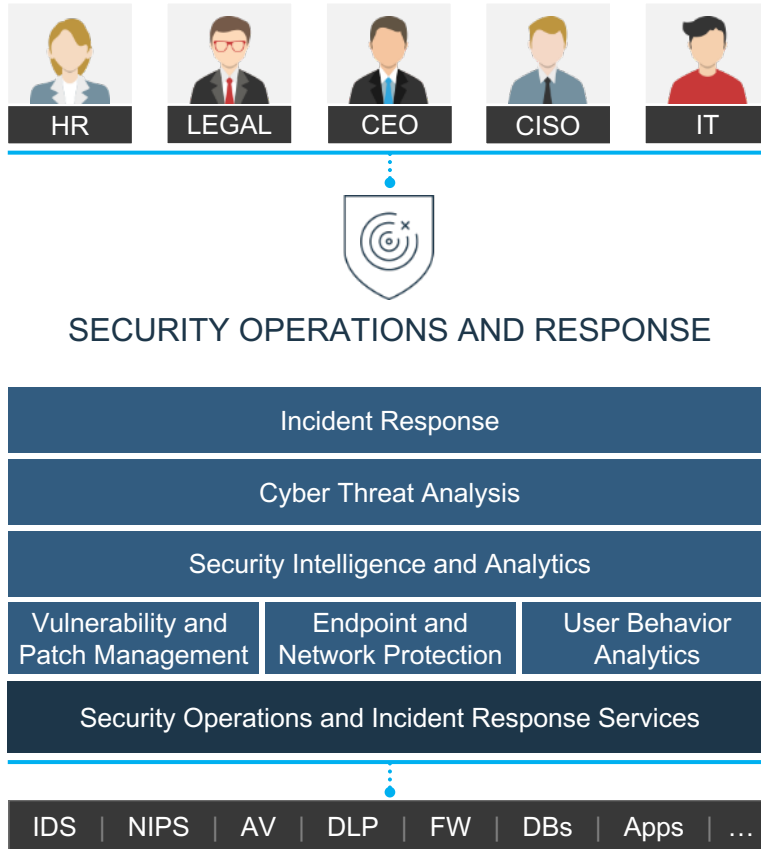
# Visualize critical threats



**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

# Stop threats with an intelligent, orchestrated, automated platform



## Security Operations and Response Platform

- See, understand, and act on all endpoint threats  
IBM BigFix
- Prevent network exploits and limit malware  
IBM QRadar Network Security (XGS)
- Use advanced analytics to eliminate threats  
IBM QRadar Security Intelligence
- Reduce threat research and response time  
IBM QRadar Advisor with Watson
- Hunt for attackers and predict threats  
IBM i2 Enterprise Insight Analysis
- Orchestrate and automate incident response  
IBM Resilient Incident Response Platform
- Investigate and detect attacks with threat intelligence  
IBM X-Force Exchange
- Defend your organization with apps and add-ons  
IBM App Exchange
- Implement best practices and access experts  
IBM Security Transformation Services



## Take control of digital risk

Move to  
the cloud

Eliminate  
passwords

Build secure  
applications

Protect  
your data

# Information Risk and Protection: Take control of digital risks

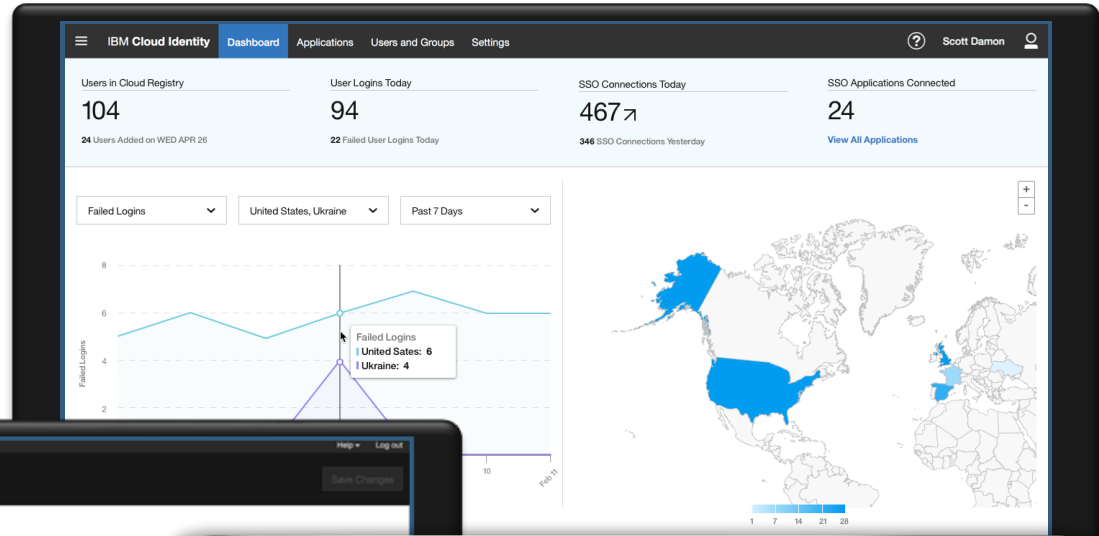
BUSINESS RISK	SECURITY GRC AND ORCHESTRATION	Information Security Risk Management CISO Risk Dashboard with Watson			
	INFORMATION RISK ANALYTICS	Information Risk Assessment and Insights IRP Data Lake on IBM Cloud			
COMPLIANCE	CLOUD SECURITY CONTROLS	Identity as a Service Cloud Identity		AppSec on Cloud ASoC	Multi-Cloud Data Protection Guardium
	LOB-DRIVEN SECURITY CONTROLS	Multi-Factor Authentication Verify	Advanced Fraud Prevention Trusteer	Mobile & IoT Management MaaS360	Data Encryption MDE
	ENTERPRISE-DRIVEN SECURITY CONTROLS	Access Management ISAM	Identity Governance IGI	Application Scanning AppScan	Data Protection Guardium
		IDENTITY & FRAUD		APP & MOBILE	DATA

# Seamless access across hybrid cloud environments

## Born-in-the-cloud, non-disruptive solutions



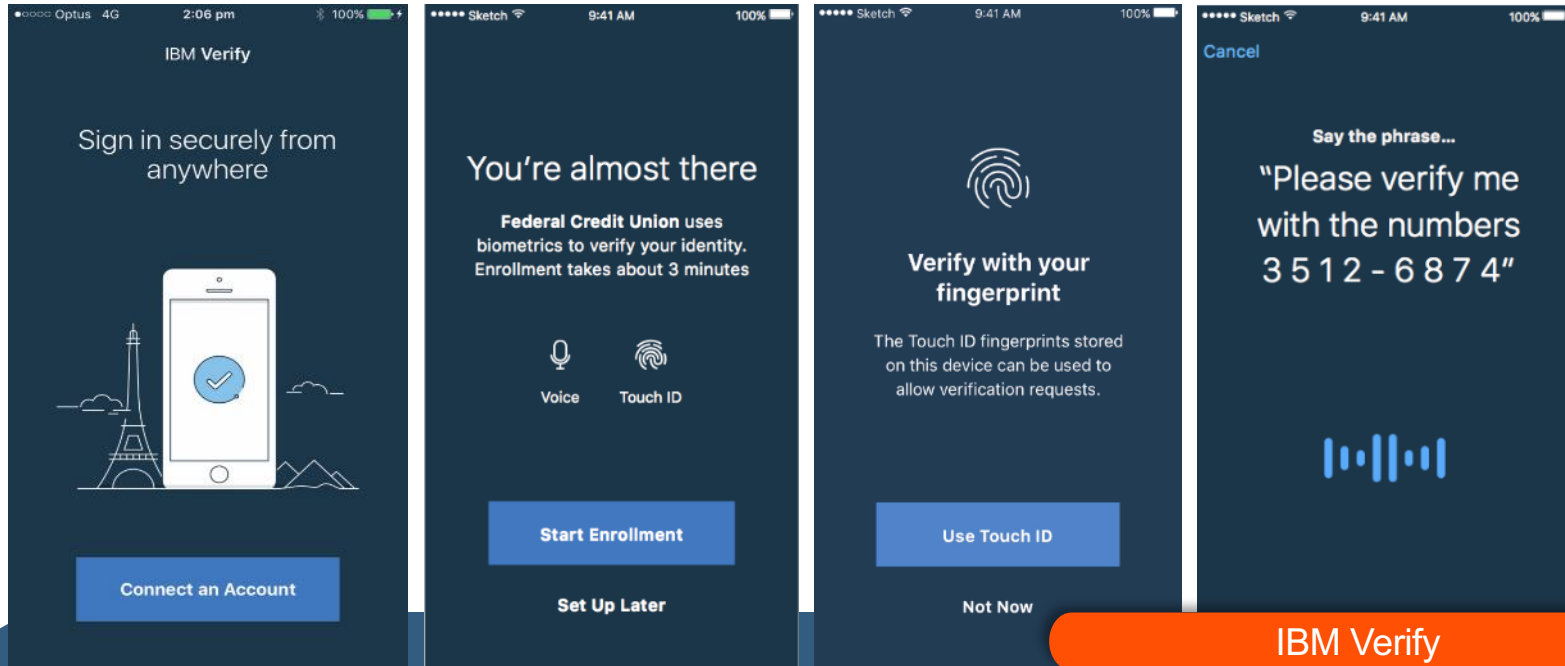
- Speed business agility to adopt cloud apps
- Secure user productivity with SSO from any device
- Enable greater IT efficiency extending existing infrastructure



The image displays three overlapping screenshots of IBM security and identity management tools. The top screenshot shows the IBM Cloud Identity Dashboard. The middle screenshot shows the IBM Cloud Identity Connect interface, which lists various service providers like 'Generic SAML2.0 Service Provider' and 'Office 365 as SAML2.0 Service Provider'. The bottom screenshot shows the IBM MaaS360 Insights dashboard, which provides security insights and risk exposure for various devices and applications.

IBM Cloud Identity Service, IBM Cloud Identity Connect, and IBM MaaS360 with Watson

# Simple and strong authentication for web and mobile experiences



**Strike a balance between usability and security  
with multi-factor authentication**





# Improve mobile productivity and protection with cognitive insights

**MaaS360 Insights**

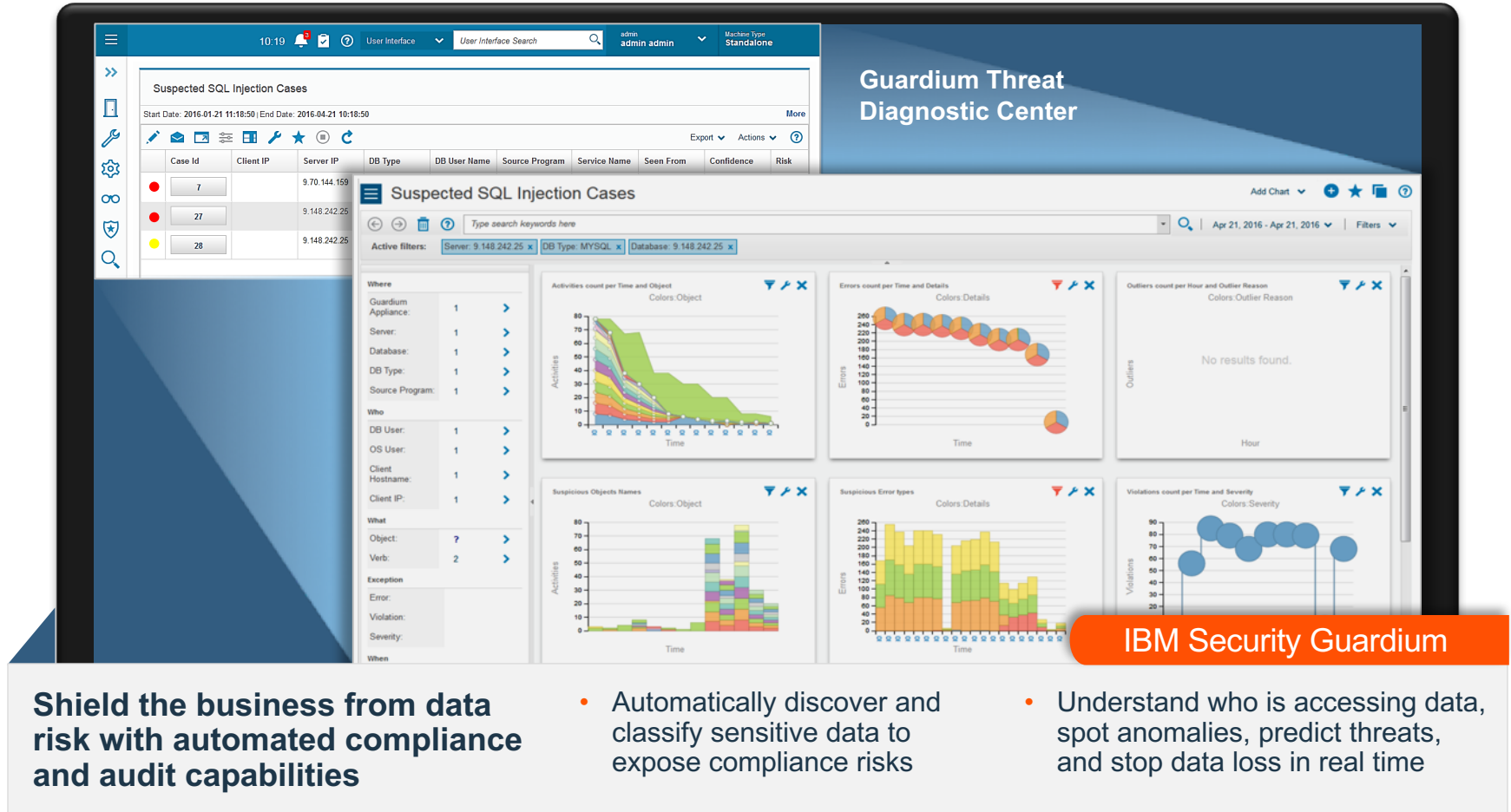
- Information: Security Vulnerabilities found in Windows 10**  
Devices with Windows 10 could allow an attacker to compromise current user context and run arbitrary code via compromised websites or websites that host user-provided content and advertisements...  
[Learn more](#)
- Risk Exposure: Security 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](#) [What do I do?](#)
- Information: MaaS360 announces new features in 10.59 release on Feb 3, 2017**  
As a part of the recent cloud release, MaaS360 announces new features like Windows 10 MDM enhancements, bulk enrollments by admins on behalf of users, enhanced app config community integration, VPP workflow optimization and new macOS policies. Click the link for more details....  
[Learn more](#)
- Information: MaaS360 Insights Advisor and Mobile Metrics is now available and enabled for your account**  
MaaS360 Insights Advisor is a cognitive engine to advise administrators on contextual best practices and emerging threats. Mobile Metrics is the industry's first mobile benchmarking tool that allows you to compare your EMM deployment against industry vertical and the MaaS360 community....  
[Learn more](#)
- Risk Exposure: 4 of your devices have iOS 9.3.4 or lower making them vulnerable to the Trident Exploit (CVE-2016-4656) for jailbreak**  
Users can install unmanaged apps or visit a malicious website that can corrupt the device and intercept communications including email...  
[Learn more](#) [What do I do?](#)
- Opportunity: Manage your corporate owned iOS devices through DEP**  
Manage your Corporate Owned iOS devices with greater control and tighter security through Apple's Device Enrollment Program. DEP allows for Supervised app compliance, which allows admins to actually hide apps on the devices, displaying only approved or managed applications....  
[Learn more](#)

**IBM MaaS360 with Watson**

- Identify policy and app deployment improvements
- Proactively address vulnerabilities in real time
- Utilize peer benchmarks and tailored recommendations

iOS Windows 10

# Protect critical data and reduce compliance costs



# Security Transformation Services (STS)



IBM X-Force Command Center  
ATLANTA



## Transform your security program

Build a security  
program strategy

Access  
the right skills

Reduce complexity  
and increase  
productivity

Apply real-time  
threat intelligence

# Security Transformation Services: Transform your security program



# Safeguard your hybrid cloud environments



## IBM Security Cloud Services

### An automated and agile approach to cloud security

- Scalable cloud computing strategy using best practice skills and expertise
- Visibility across multiple hybrid cloud platforms
- Faster time-to-value with online risk assessments
- Asset and server outage protection
- Cloud identity and access management
- Best practice skills and expertise

# A Global Leader in Enterprise Security



## IBM Security

- **#1** fastest growing of the Top 5 security vendors\*
- **8,000+** employees
- **17,500+** customers
- **133** countries
- **3,500+** security patents
- **20** acquisitions since 2002

\* According to 2015 Gartner Market Share



# IBM LinuxONE – Linux on Mainframe

Copyright Steven Ginn  
Used with permission





# IBM LinuxONE



**A single platform  
for all business workloads**

- Exceptional service delivery
  - Multi-dimensional growth
  - Non-disruptive scalability
- Leadership performance
- Unparalleled qualities of service
  - Highest availability
  - Absolute security
- Economic advantage

# Two systems to choose from depending on business needs



## Emperor

With a huge capacity range, grow with virtually limitless scale to handle the most demanding workloads



## Rockhopper

An entry point model offering with similar value but in a flexible smaller package

LinuxONE tests and data in this document pertain to Emperor model.

# LinuxOne Rockhopper is perfect mid-range option

- Up to 20 cores total
  - 4.3 GHz clock speed
  - 2 threads per core (SMT)
  - Single instruction, multiple data (SIMD)
  - 100% Linux
- 3 levels of on-chip cache, plus L4 cache on separate chip
- 3 separate cores dedicated to handling I/O exclusively
- Up to 4TB memory
- Up to 96 PCIe slots for I/O



# LinuxOne Emperor packs a data center's worth of resources into on box

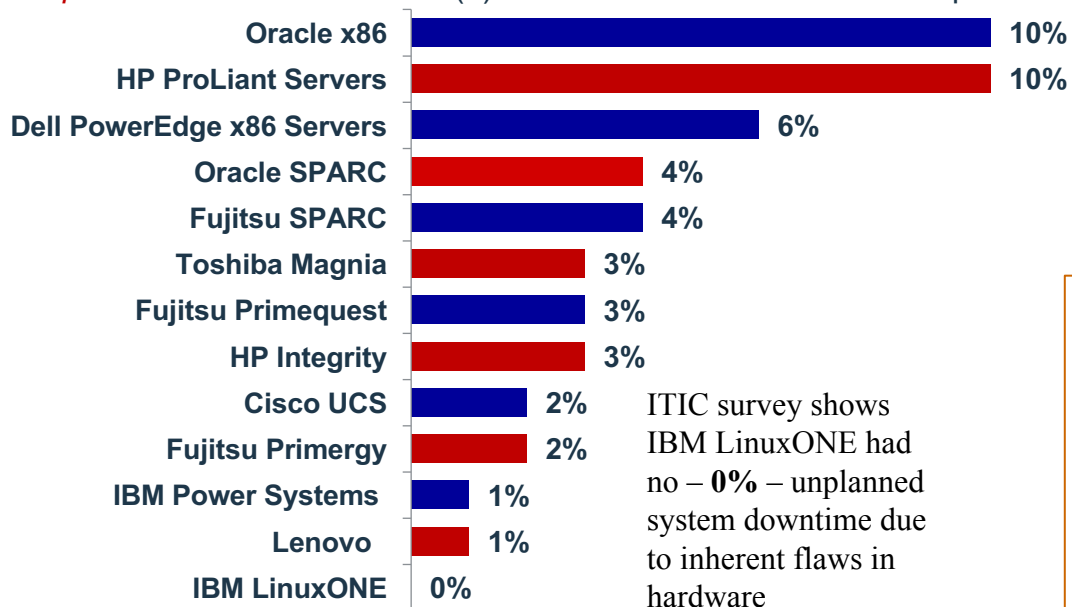
- Up to 141 cores total
  - 5.0 GHz fastest commercially available
  - 2 threads per core (SMT)
  - Single instruction, multiple data (SIMD)
  - 100% Linux
- 3 levels of on-chip cache, plus L4 cache on separate chip
- 24 separate cores dedicated to handling I/O exclusively
- Up to 10TB memory
- Up to 160 PCIe slots for I/O



*Up to 85 logical partitions  
Capable of support over 7,000 VMS*

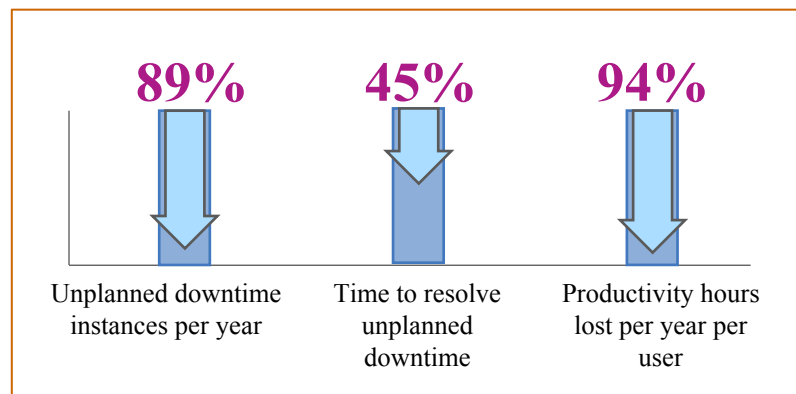
# LinuxONE is designed for minimal unplanned downtime

*Unplanned Downtime* of >four (4) hours on each server hardware platform (2015)

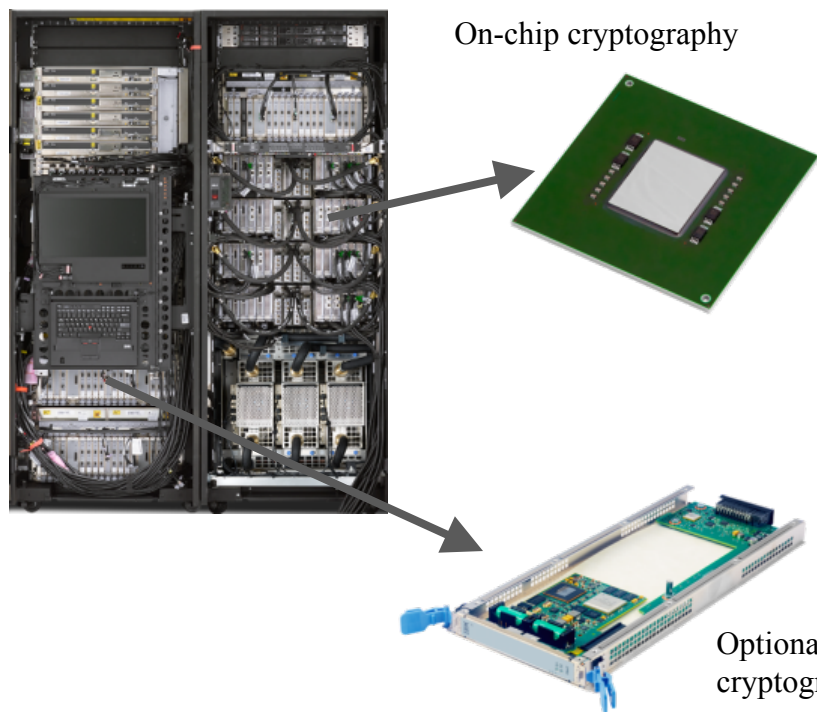


ITIC survey shows IBM LinuxONE had no – **0%** – unplanned system downtime due to inherent flaws in hardware

Recent IDC study concludes clients who leverage LinuxONE can virtually eliminate lost productivity caused by downtime

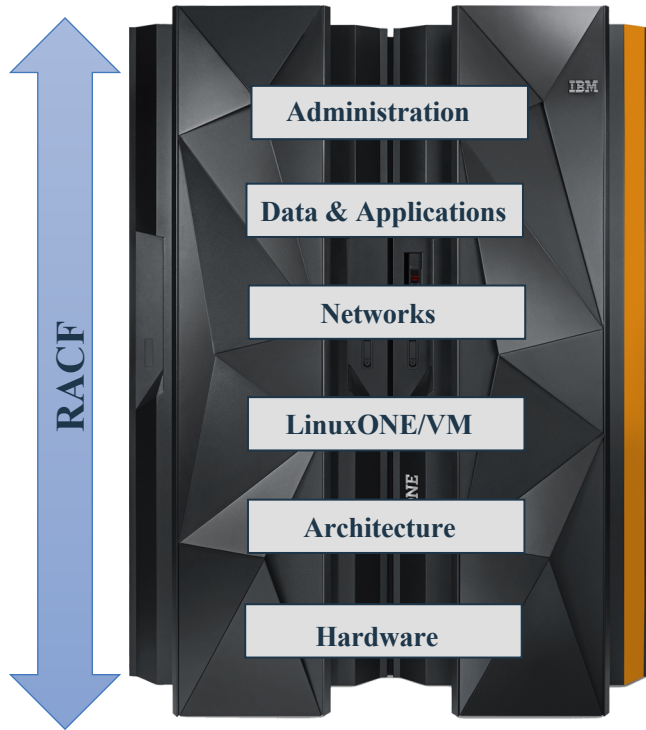


# Advanced cryptography is handled at multiple levels depending on business requirements



- Each core has its own cryptographic co-processor
  - Optimized for encryption functions
- Crypto Express5S PCIe card (optional) adds additional crypto capability
  - Elliptic Curve, SHA3, Visa FPE, etc.
- Meets FIPS, ANSI, PKI, and DK standards

# Top to bottom security is built in, not bolted on



Resource Access Control Facility (RACF) is the backbone of LinuxONE security

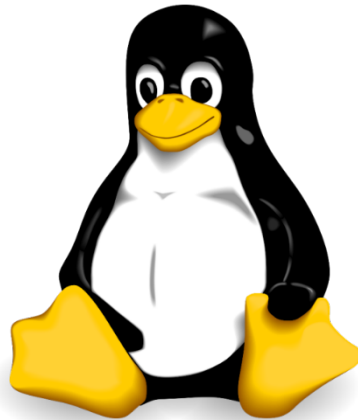
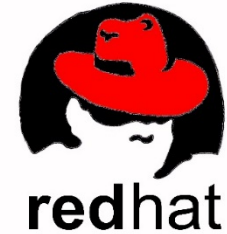
- Access control to all classes of resources
- Integrated into LinuxONE/VM
- Supports cryptographic services
- Supports digital certificates

**Enables application and database security without modifying applications**

**Reduces security complexity and expense:**

- Central security process that is easy to apply to new workloads or as user base increases
- Tracks activity to address audit and compliance requirements

# LinuxONE supports a choice of standard distributions, and thousands of applications



Over 3,000 Linux applications available...





# A wide array of Open Source software runs on LinuxONE



Languages and Dev Environment	Database & Messaging	Cloud infrastructure	App development & DevOps	Configuration, monitoring management and tools
Node.js Ruby Rails Python LLVM OpenJDK, GCCGO oCaml Erlang Apache HTTP Web Server PHP	MySQL PostgreSQL MariaDB MongoDB Cassandra Redis CouchDB Gemfire RabbitMQ	Docker Chef Puppet	Xerces-c XMLSec protobuf Doxygen ANTLR Maven	Fluentd
			<b>Web Application Development</b>	<b>eCommerce &amp; Application server</b>
			jMeter Wordpress Ceilometer	jBoss

Others in process or in plan

include:

R (language)  
OpenStack  
CloudFoundry  
Node.js  
Apache Spark  
Apache Tomcat  
Apache Hadoop  
...and many more



See updates at  
<https://www.ibm.com/developerworks/community/forums/html/topic?id=5dee144a-7c64-4bfe-884f-751d6308dbdf>

# IBM LinuxONE is a better choice if...



IBM **LinuxONE**™

...You're running very large I/O- or cache-intensive workloads like database applications or transaction processing

...You're looking to consolidate large numbers of servers

...Your software license costs are unsustainable

...Even the smallest system failure is unacceptable

...A security breach would be catastrophic to your business

...You're looking to reduce overall operational expenses




IBM **LinuxONE™**





# THANK YOU

## FOLLOW US ON:

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

© Copyright IBM Corporation 2017. 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.

# IBM Security product portfolio

## Security Operations and Response

### Incident Response

Resilient Incident Response Platform

### Cyber Threat Analysis

i2 Enterprise Insight Analysis

### Security Intelligence and Analytics

QRadar SIEM | QRadar on Cloud | QRadar Incident Forensics

QRadar Advisor with Watson

### Vulnerability and Patch Management

QRadar Vulnerability Manager

BigFix

### Endpoint and Network Protection

BigFix

Carbon Black Protection / Response

QRadar Network Security (XGS)

### User Behavior Analytics

QRadar User Behavior Analytics

## Information Risk and Protection

### Mobile Security

MaaS360

### Identity Governance and Access Management

Identity Governance and Intelligence | Cloud Identity

Access Manager | Privileged Identity Manager

Directory Suite | zSecure suite

### Advanced Fraud Prevention

Trusteer Rapport | Trusteer Fraud Protection

Trusteer Pinpoint Malware Detection | Trusteer Mobile

### Data Protection

Guardium

Key Lifecycle Manager

Multi-Cloud Data Encryption

### Application Security

AppScan

Application Security on Cloud

Arxan App Protection

## Security Research and Threat Intelligence

X-Force | X-Force Exchange | App Exchange