



A New Era of Security

Is this familiar?

85



security tools from

45



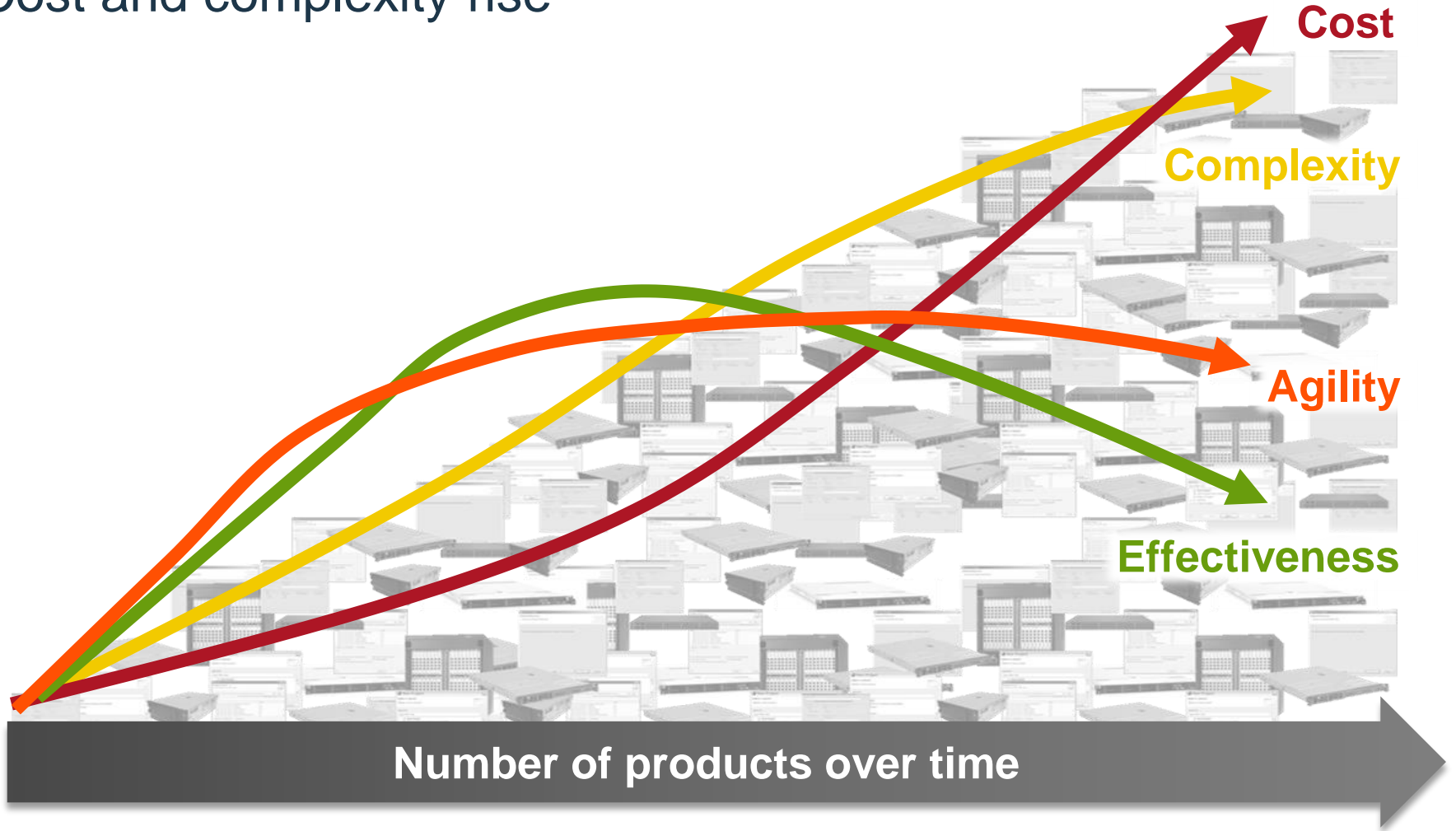
vendors

Source: IBM Client Example



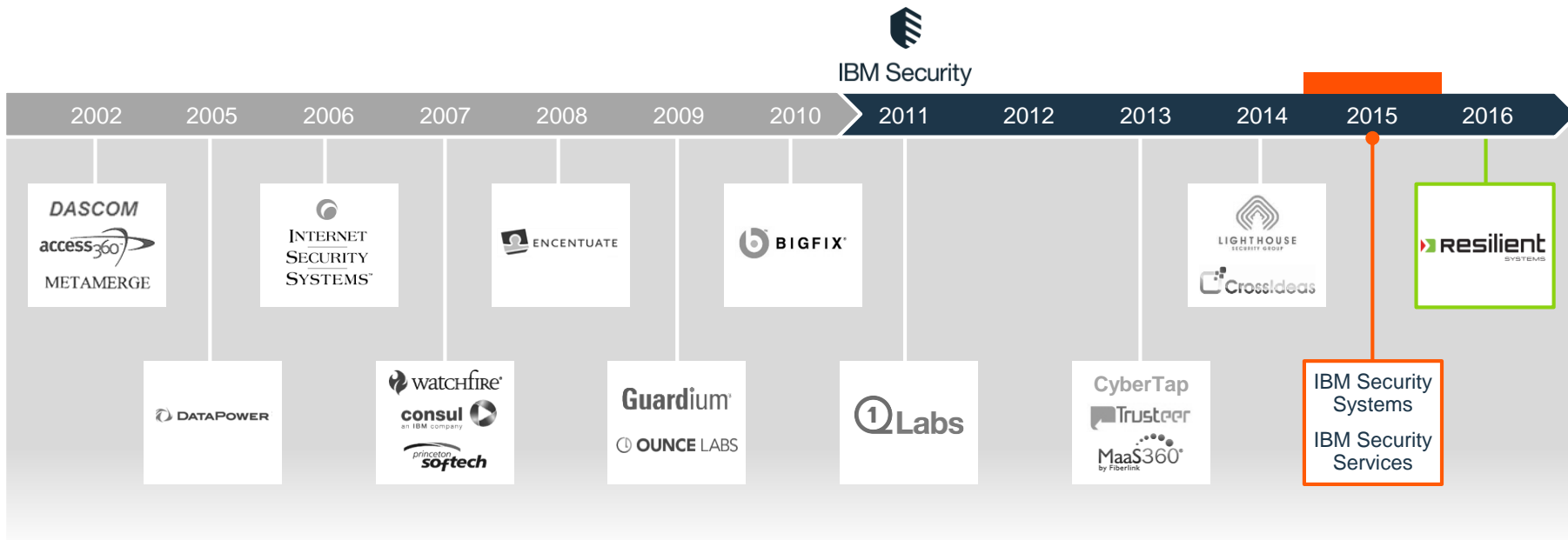
Number of products over time

Cost and complexity rise



The security team sees noise

IBM Security invests in best-of-breed technologies



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

Forbes

Upon close, Resilient Systems will advance the IBM Security strategy to help organizations succeed in an era of escalating cyber attacks



Unites Security Operations and Incident Response

Resilient Systems will extend IBM's offerings to create one of the industry's most complete solutions to prevent, detect, and respond to threats

Delivers a Single Hub for Response Management

Resilient Systems will allow security teams to orchestrate response processes and resolve incidents faster, more effectively, and more intelligently

Integrates Seamlessly with IBM and 3rd Party Solutions

Resilient Systems integrates with QRadar and other IBM and 3rd party solutions so organizations of various sizes can successfully resolve attacks

IBM Security Strategy

SUPPORT the CISO agenda



CISO, CIO, and Line-of-Business

- Strategy and leadership
- Rapid transformation
- Integrated solutions

INNOVATE around key trends



Advanced Threats



Compliance Mandates



Cloud



Skills Shortage



Mobile and Internet of Things

LEAD in selected segments

IBM Security Capability Framework

Strategy, Risk and Compliance

Cybersecurity Assessment and Response

Security Operations and **Incident Response Platform** *(upon close)*

Advanced Fraud
Protection

Identity and Access
Management

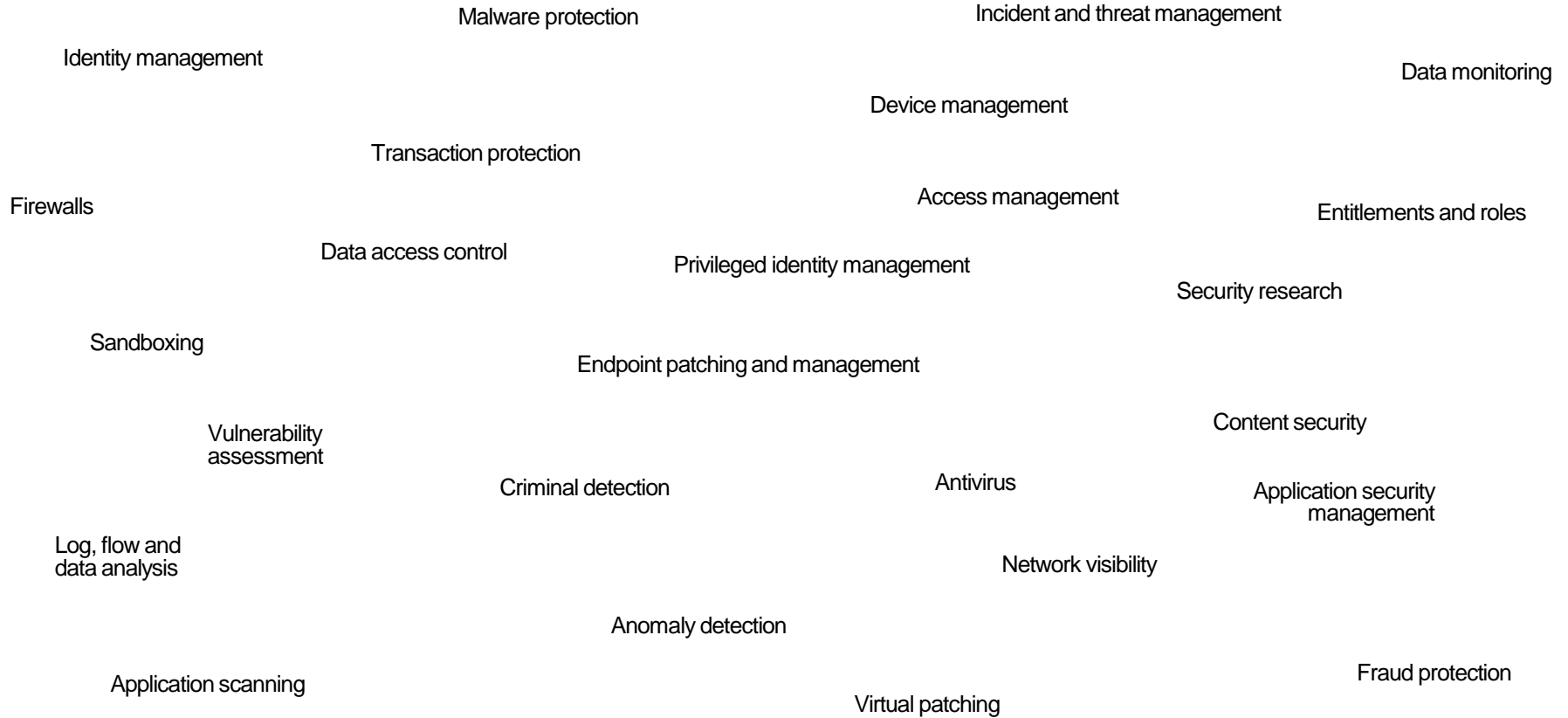
Data
Security

Application
Security

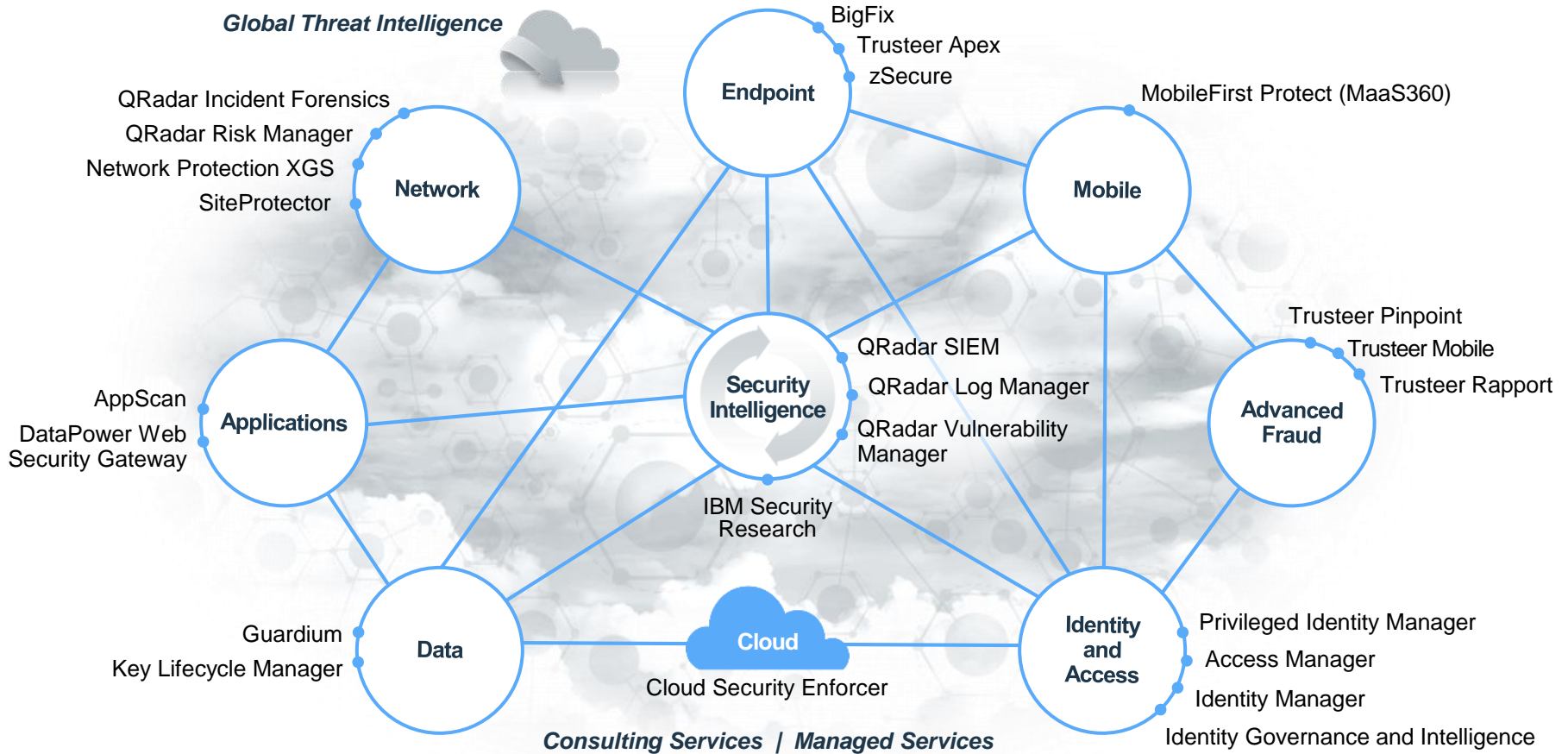
Network, Mobile and
Endpoint Protection

Advanced Threat and Security Research

Establish security as an immune system



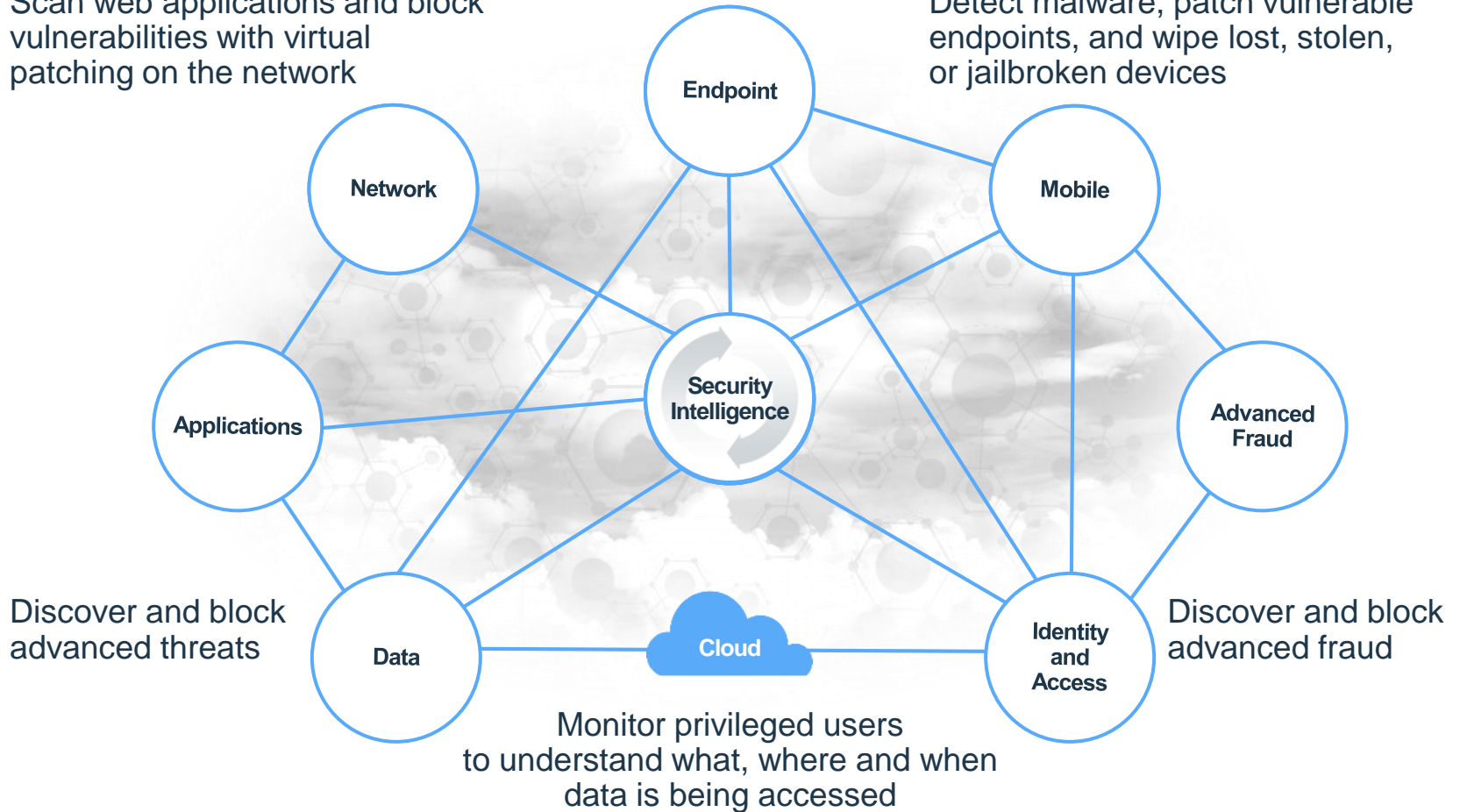
IBM has the world's broadest and deepest security portfolio



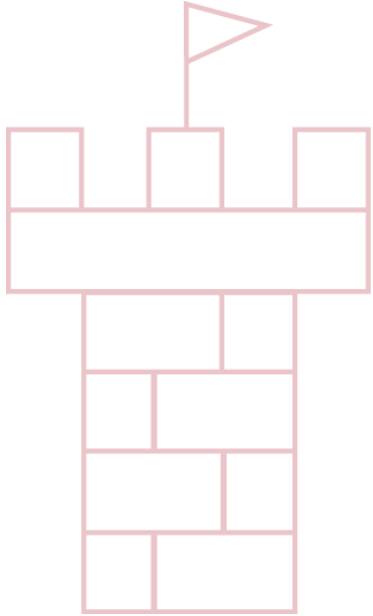
Integrated protection to optimize security posture

Scan web applications and block vulnerabilities with virtual patching on the network

Detect malware, patch vulnerable endpoints, and wipe lost, stolen, or jailbroken devices



The next era of security



Moats,
Castles



Intelligence,
Integration



Cloud, Collaboration,
Cognitive

Cloud

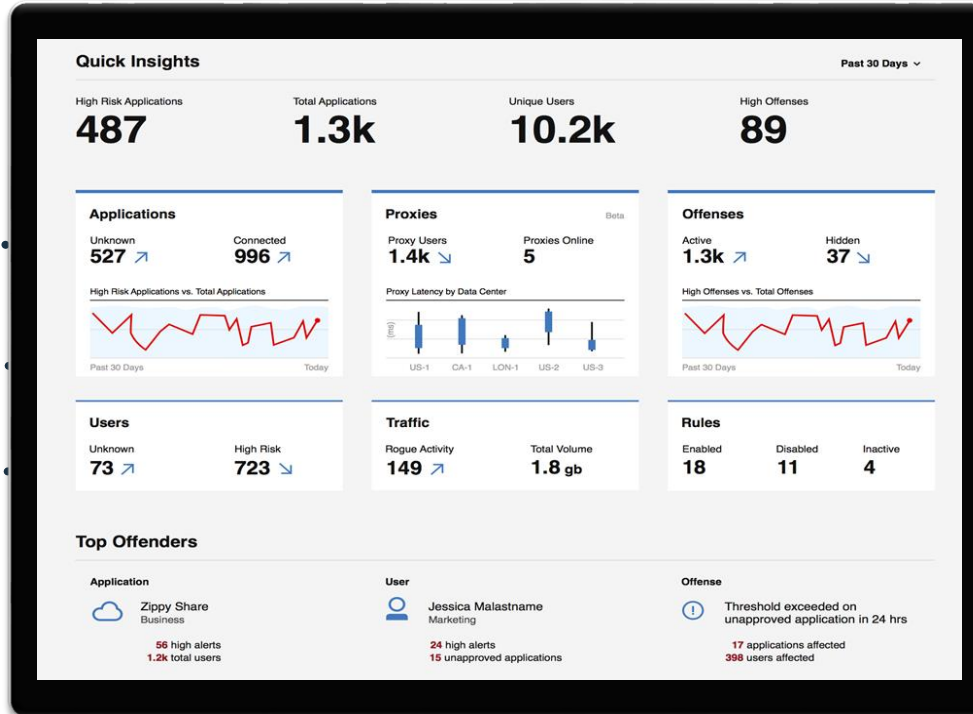
IBM Cloud Security Enforcer

EMPLOYEES

 **BYOD**

 **ON PREM**

 **MOBILE**



RISKY APPS

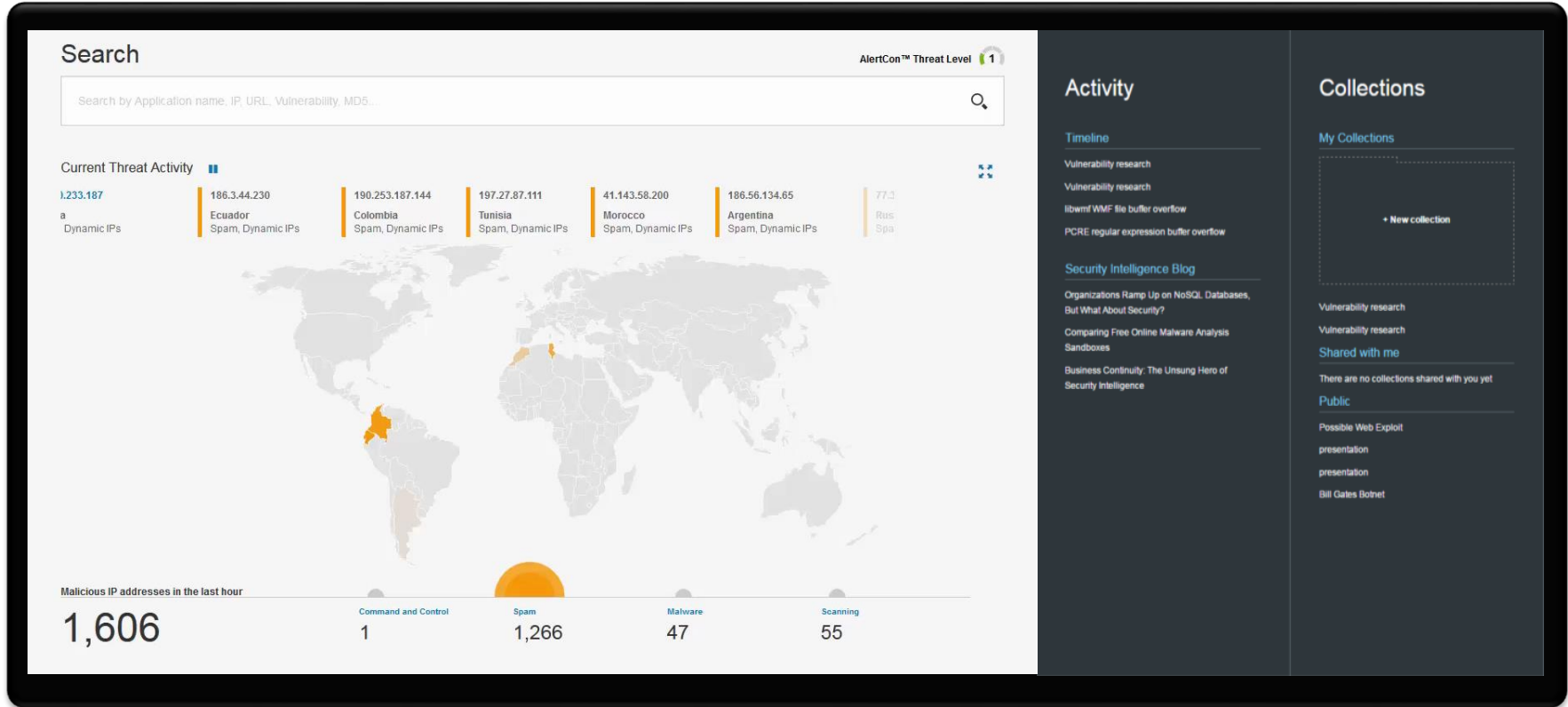


APPROVED APPS



Collaboration

IBM X-Force Exchange



<https://exchange.xforce.ibmcloud.com>

Collaboration

IBM App Exchange

The screenshot displays the IBM X-Force Exchange App Exchange interface. The header includes the IBM X-Force Exchange logo and a search bar. A left sidebar allows for refining results by industry (currently set to 'All Industries') and type (Application, Custom Properties, Custom Qid Map Entries, Custom Rule). The main content area is titled 'App Exchange' and features a 'Featured' section with four application cards: BrightPoint Security Sentinel, Carbon Black App for IBM QRadar, Exabeam User Behavior Analytics, and Resilient Systems Integration for QRadar. Below this is an 'All Applications (27)' section with a 'Sort By' dropdown set to 'A-Z', displaying four more application cards: Bit9 Parity Custom Properties, Blue Coat Custom Properties, BrightPoint Security Sentinel, and Carbon Black App for IBM QRadar. Each card includes the provider's logo, the application name, a brief description, and a star rating.

<https://exchange.xforce.ibmcloud.com>

Evolving to Cognitive *Watson Security Advisor*



Security that...

Understands

Reasons

Learns

Check your corpus that is deployed to test by asking questions.

Watson
Watson Security Advisor

Security Analyst: What are common types of malware?

Watson Security Advisor: Malware, or malicious code/software, represents one of the best-known types of threats to information systems. There are numerous types of malware, some detailed in Table 7.2, that have evolved over the years to continually cause stress to operations.
Table 7.2.

Types of Malware.	
Malicious Code	Description
Virus	A virus is malware that does not self propagate: it requires a carrier, such as a human manually moving an infected USB device from one system to another
Macro virus	A macro virus is malware that infects Microsoft Office documents by means of embedding malicious macros within them

IBM WATSON. Send

Responses that you see here come from searches of the corpus documents. The responses do not include answers that are identified in the Expert Training tool.
Define the appearance and behavior of this window in the Configuration tool.

Learn more about IBM Security

No. 1 fastest growing worldwide security software vendor

24 industry analyst reports rank IBM Security as a **LEADER**

130+ countries where IBM delivers managed security services

14K+ clients protected *including...*

90% of the Fortune 100 companies



Visit our website
ibm.com/security



Watch our videos on YouTube
[IBM Security Channel](#)



Read new blog posts
SecurityIntelligence.com



Join IBM X-Force Exchange
xforce.ibmcloud.com



Follow us on Twitter
[@ibmsecurity](#)

outthink threats



IBM Security