Stream Keynote: Security Intelligence

Pulse2013

Optimizing the World's Infrastructure

Security Intelligence Keynote

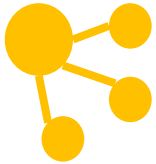
Brendan Hannigan

General Manager, IBM Security Systems Division
IBM Software Group

Innovative technology changes everything

1 trillion connected objects

1 billion mobile workers

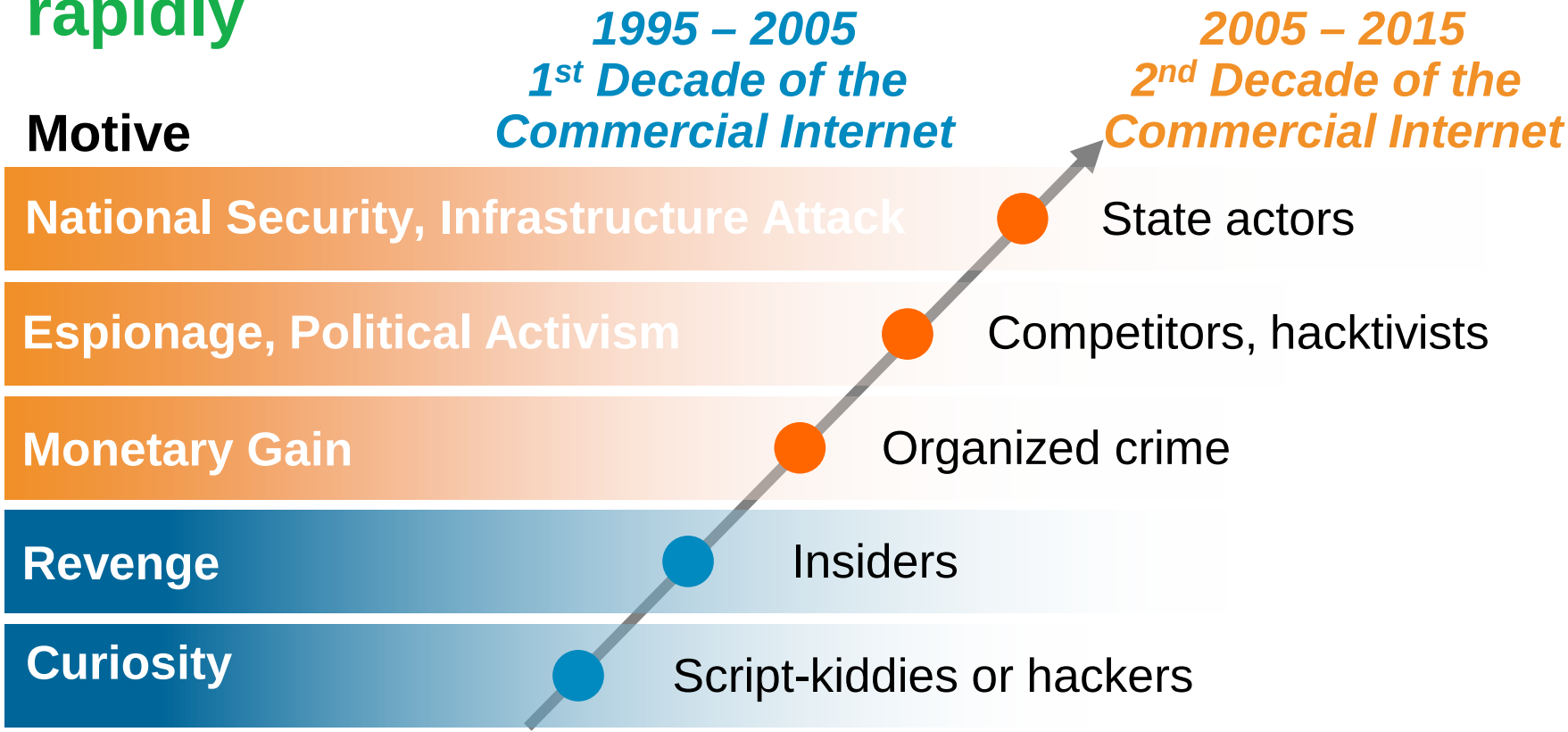


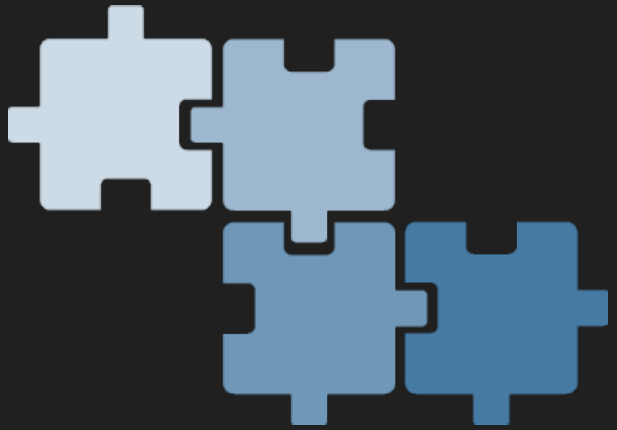
Social business

Cloud and virtualization

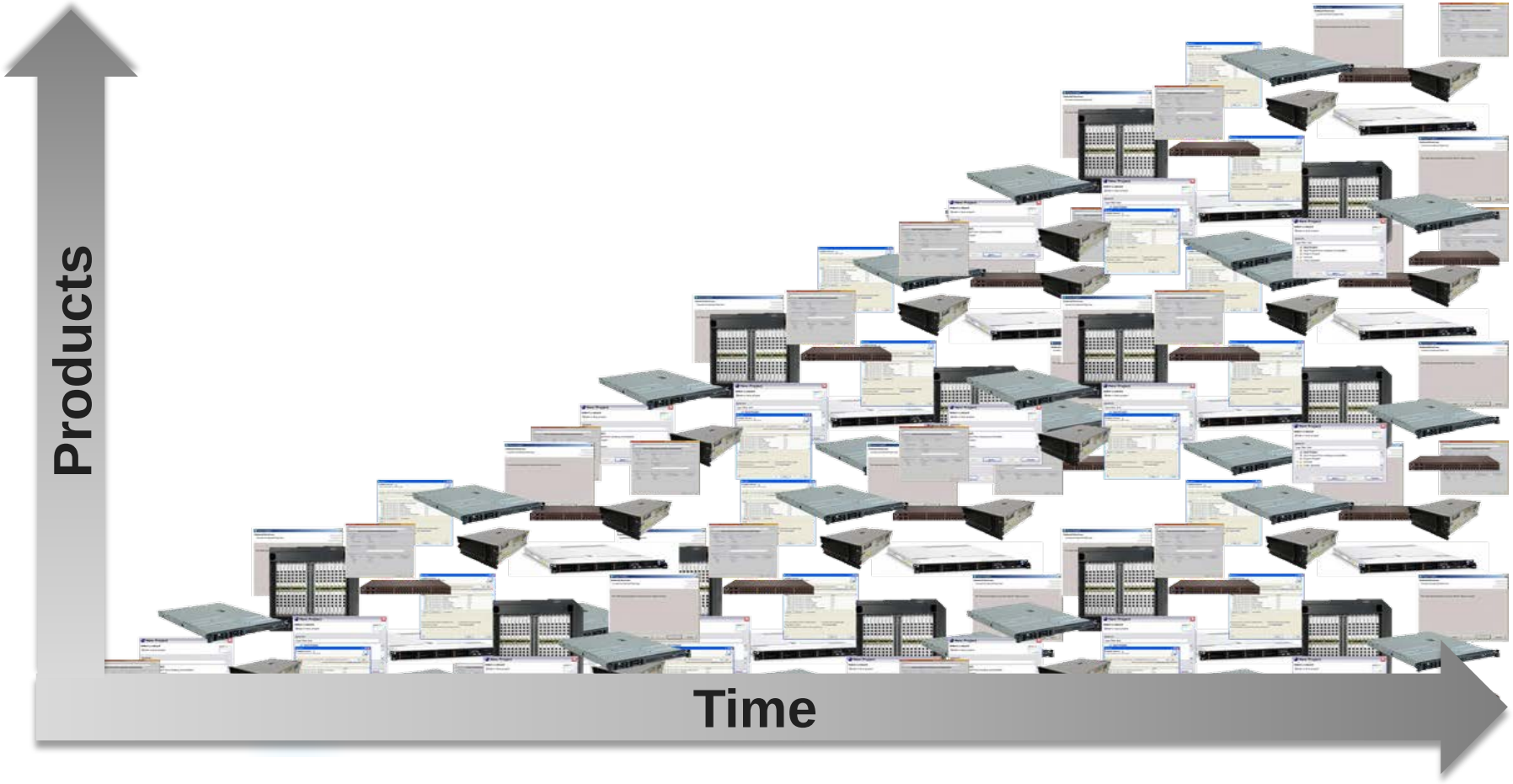
Bring your own IT

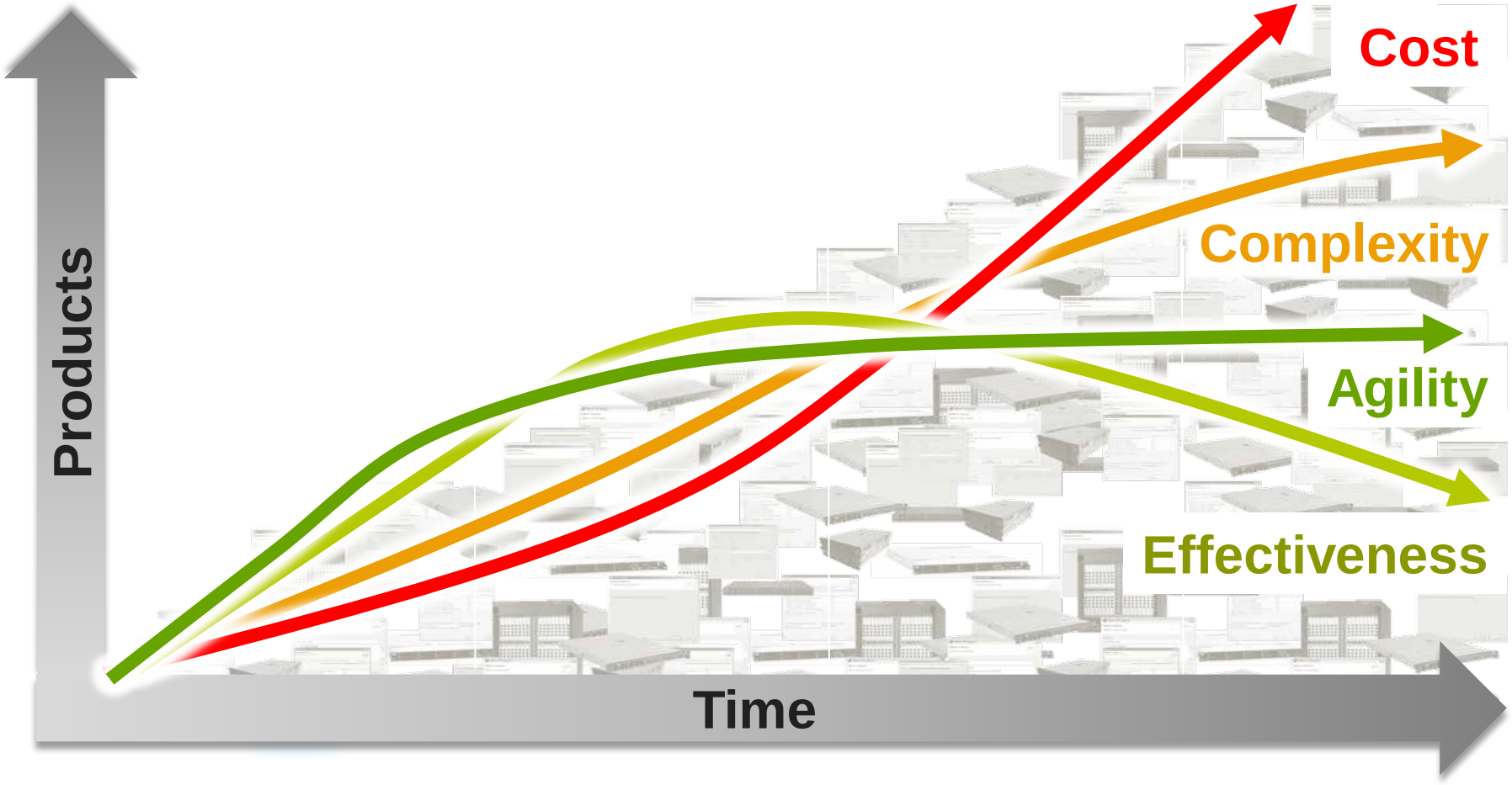
Motivation and sophistication is evolving rapidly





How do we solve this?


Products
Time


Products
Time
Cost
Complexity
Agility
Effectiveness

Your security team sees noise

Security challenges are a complex, four-dimensional puzzle …

Security challenges are a complex, four-dimensional puzzle …

Infrastructure

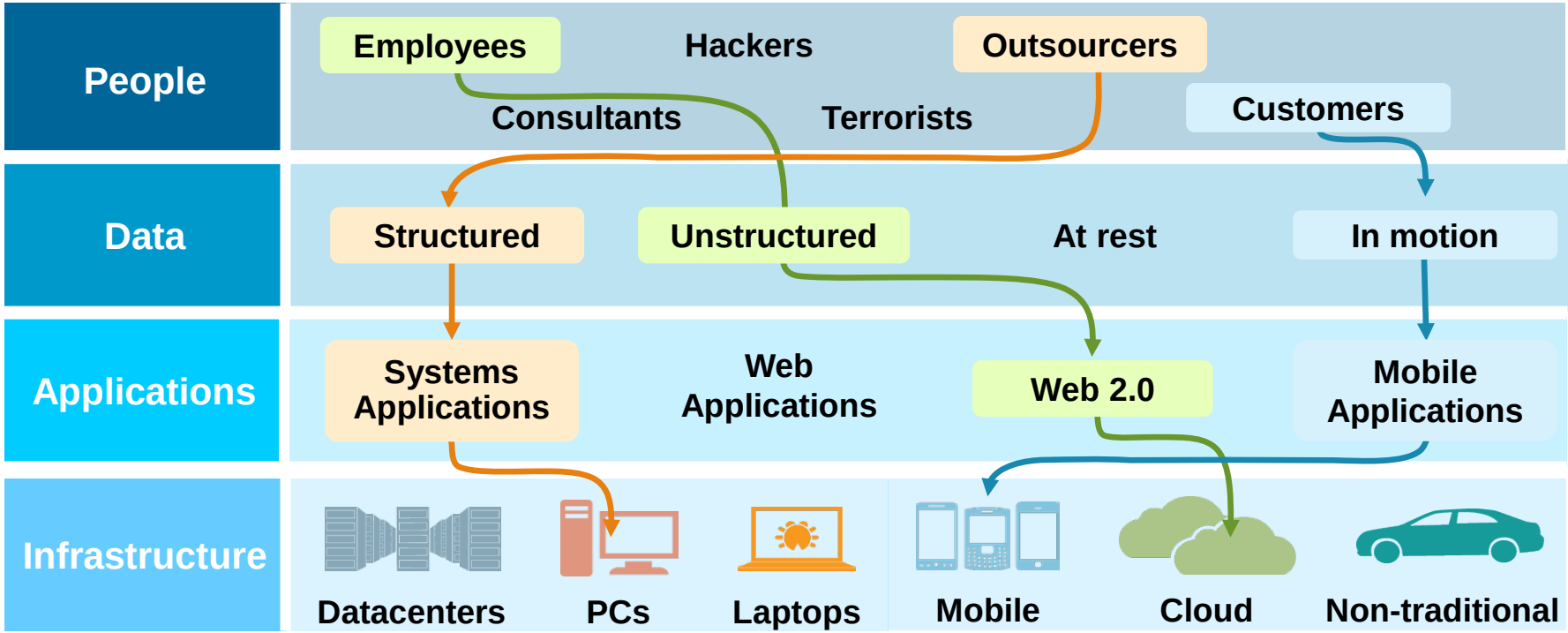
Datacenters

PCs

Laptops

Security challenges are a complex, four-dimensional puzzle …

Security challenges are a complex, four-dimensional puzzle …



… that requires a new approach

Then	Now

… that requires a new approach

	Then	Now
 **People**	Administration	

… that requires a new approach

… that requires a new approach

	Then	Now
People	Administration	Insight
Data		

… that requires a new approach

	Then		Now
People	Administration		Insight
Data	Basic control		Laser-focused

… that requires a new approach

	Then	Now
People	Administration	Insight
Data	Basic control	Laser-focused
Applications	Bolt-on	

… that requires a new approach

	Then		Now
People	Administration		Insight
Data	Basic control		Laser-focused
Applications	Bolt-on		Built-in

… that requires a new approach

	Then		Now
People	Administration		Insight
Data	Basic control		Laser-focused
Applications	Bolt-on		Built-in
Infrastructure	Thicker walls		

… that requires a new approach

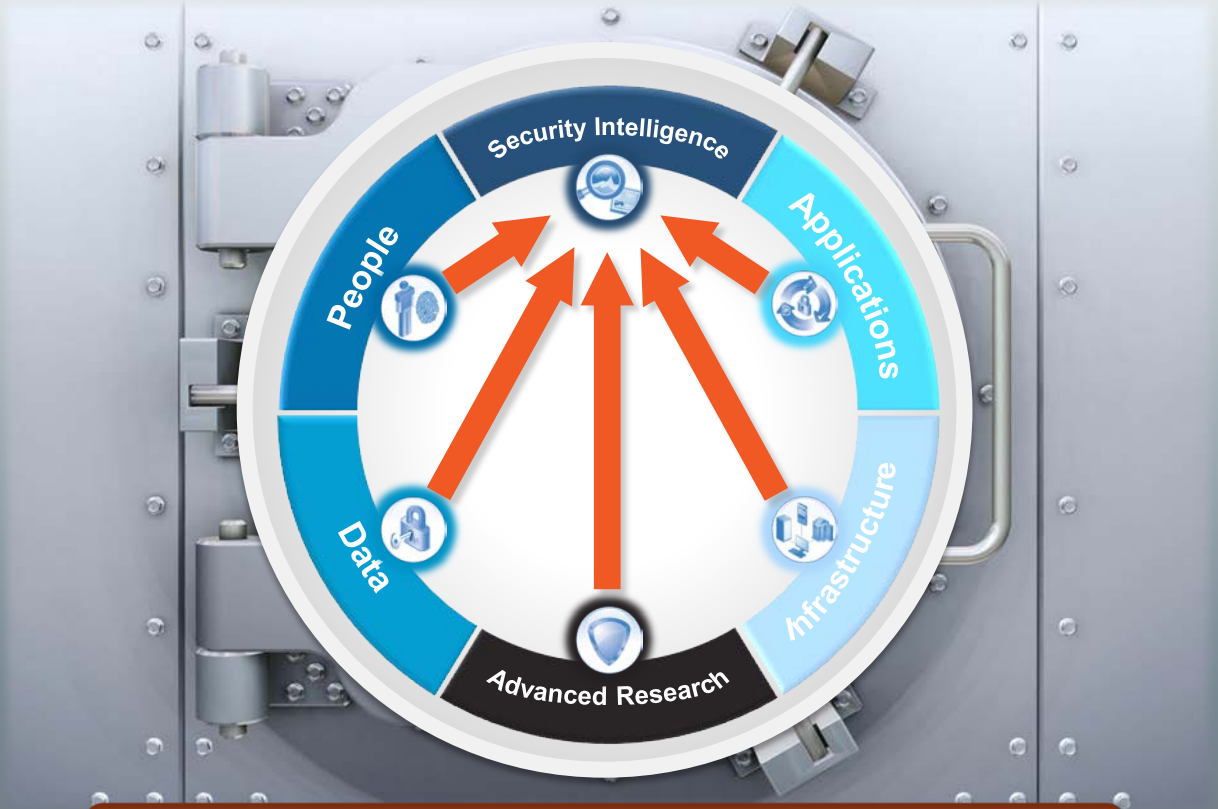
	Then	Now
People	Administration	Insight
Data	Basic control	Laser-focused
Applications	Bolt-on	Built-in
Infrastructure	Thicker walls	Smarter defenses




… that requires a new approach

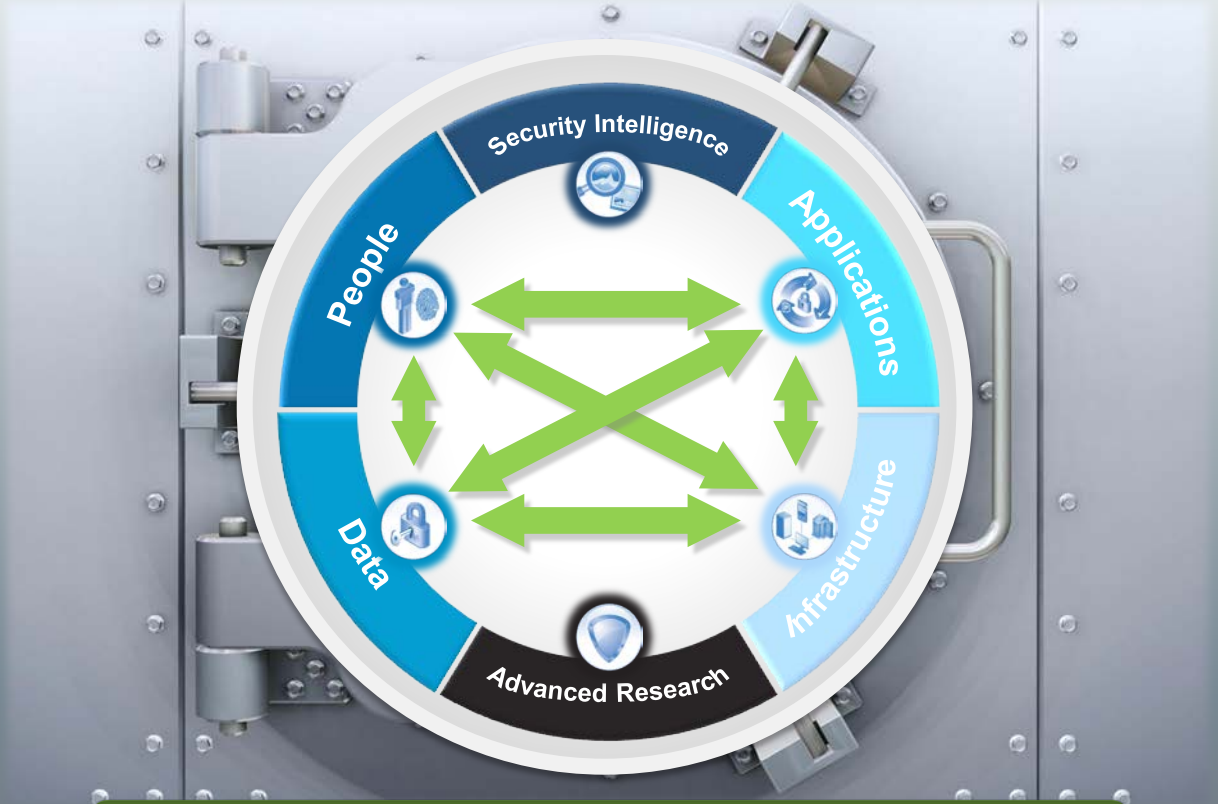
	Then		Now
People	Administration		Insight
Data	Basic control		Laser-focused
Applications	Bolt-on		Built-in
Infrastructure	Thicker walls		Smarter defenses

Collect and Analyze Everything



Monitor Everything

Consume Threat Intelligence



Integrate Across Domains

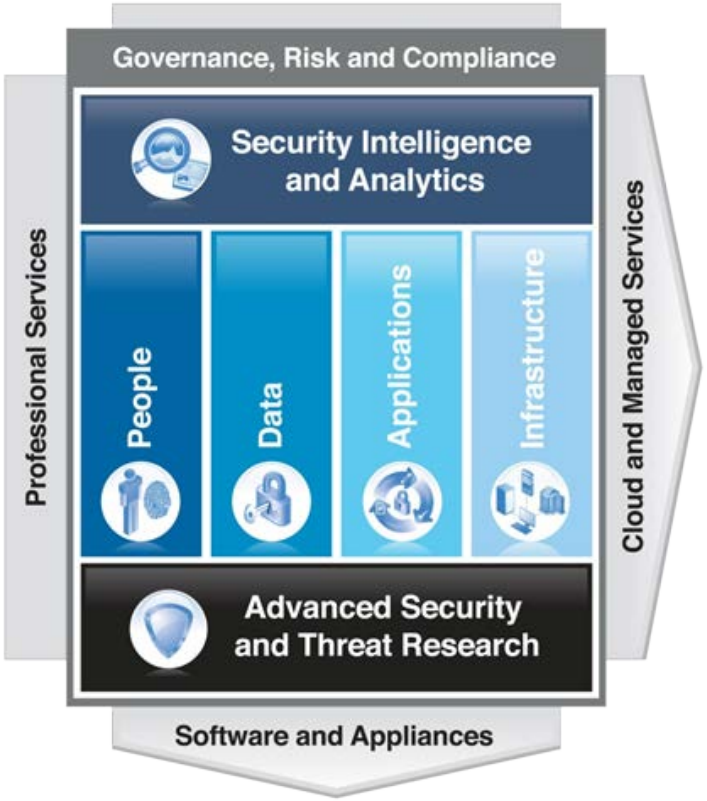
Applying these principles

IBM delivers security solutions across a comprehensive framework

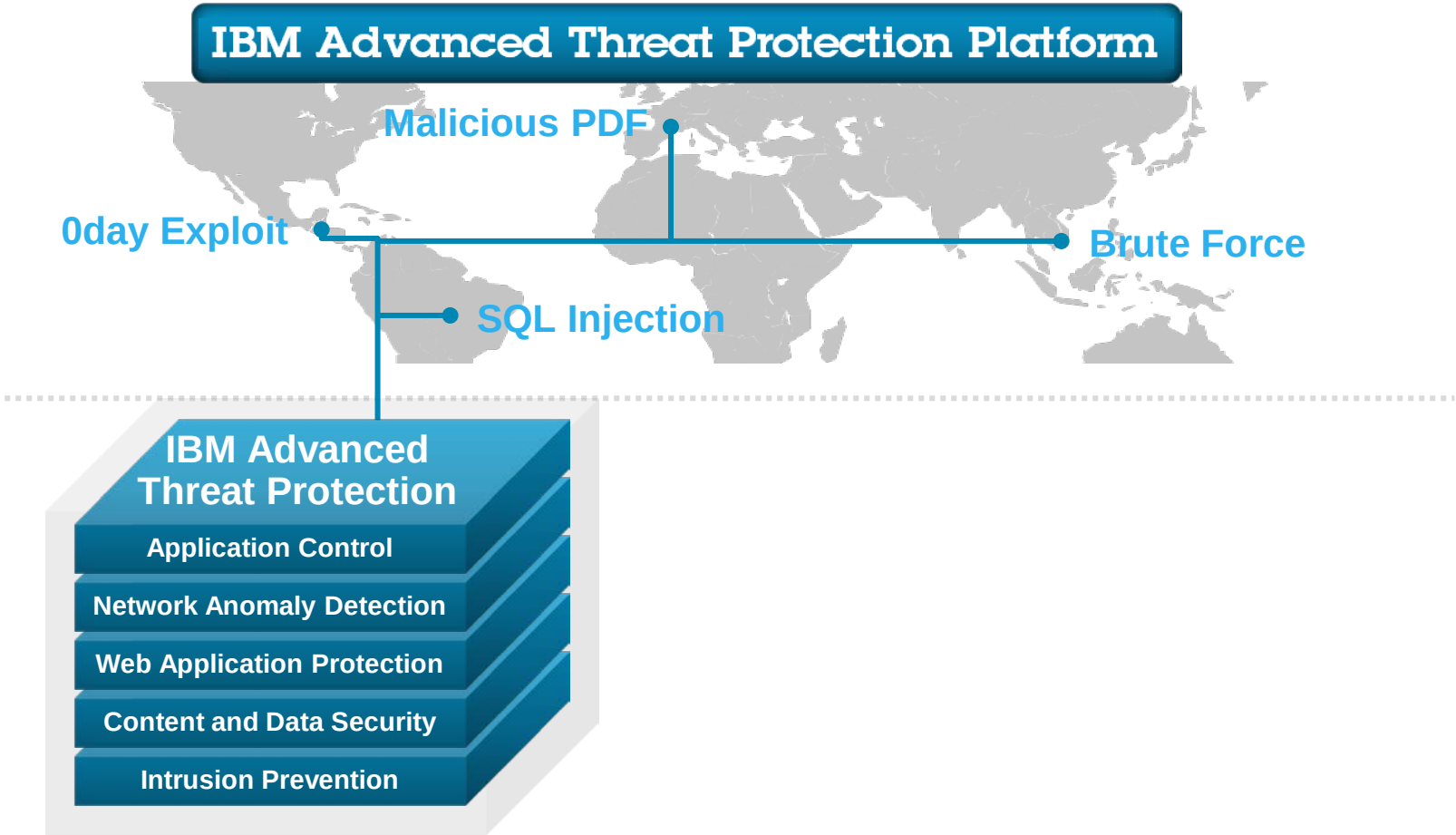
Intelligence

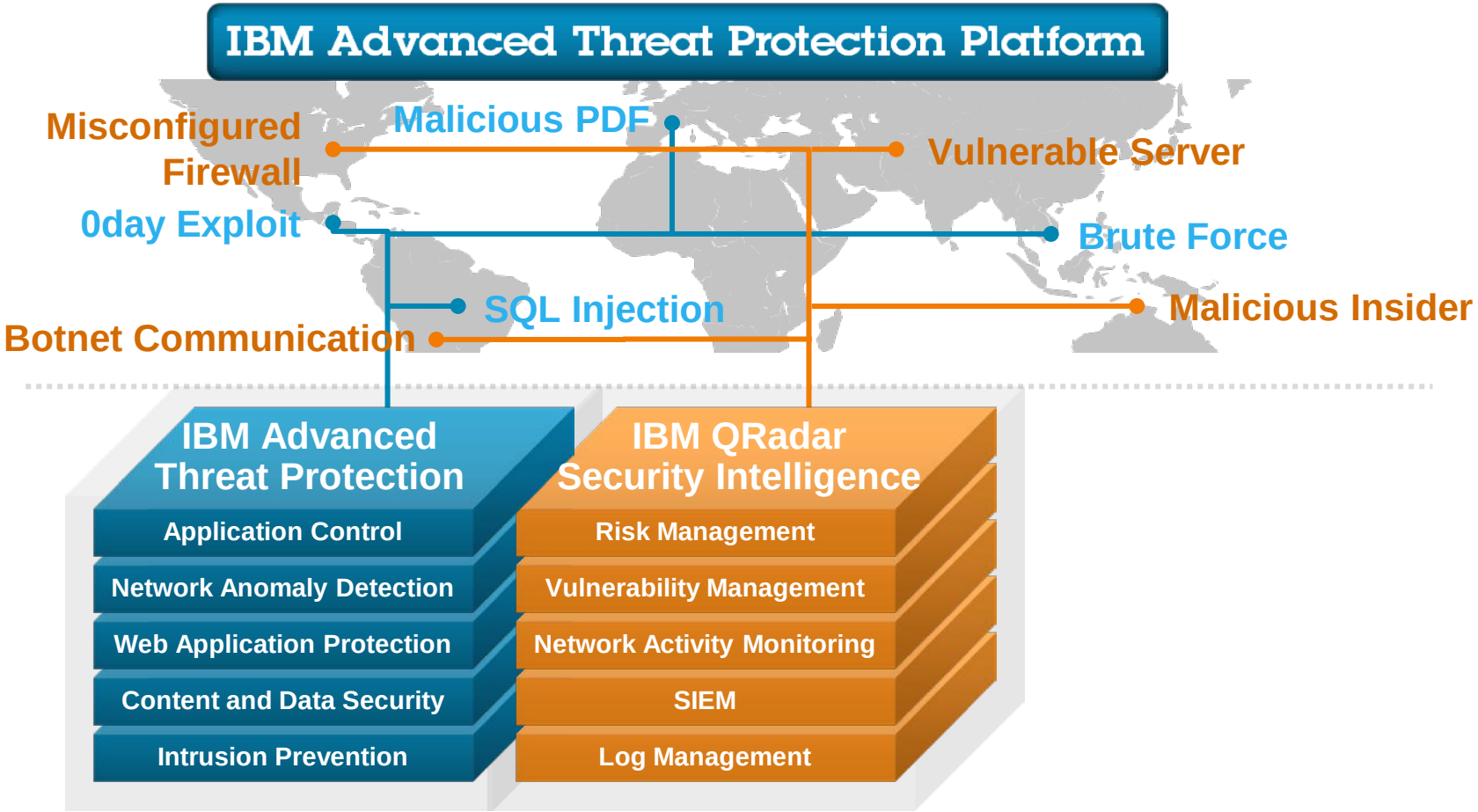
Integration

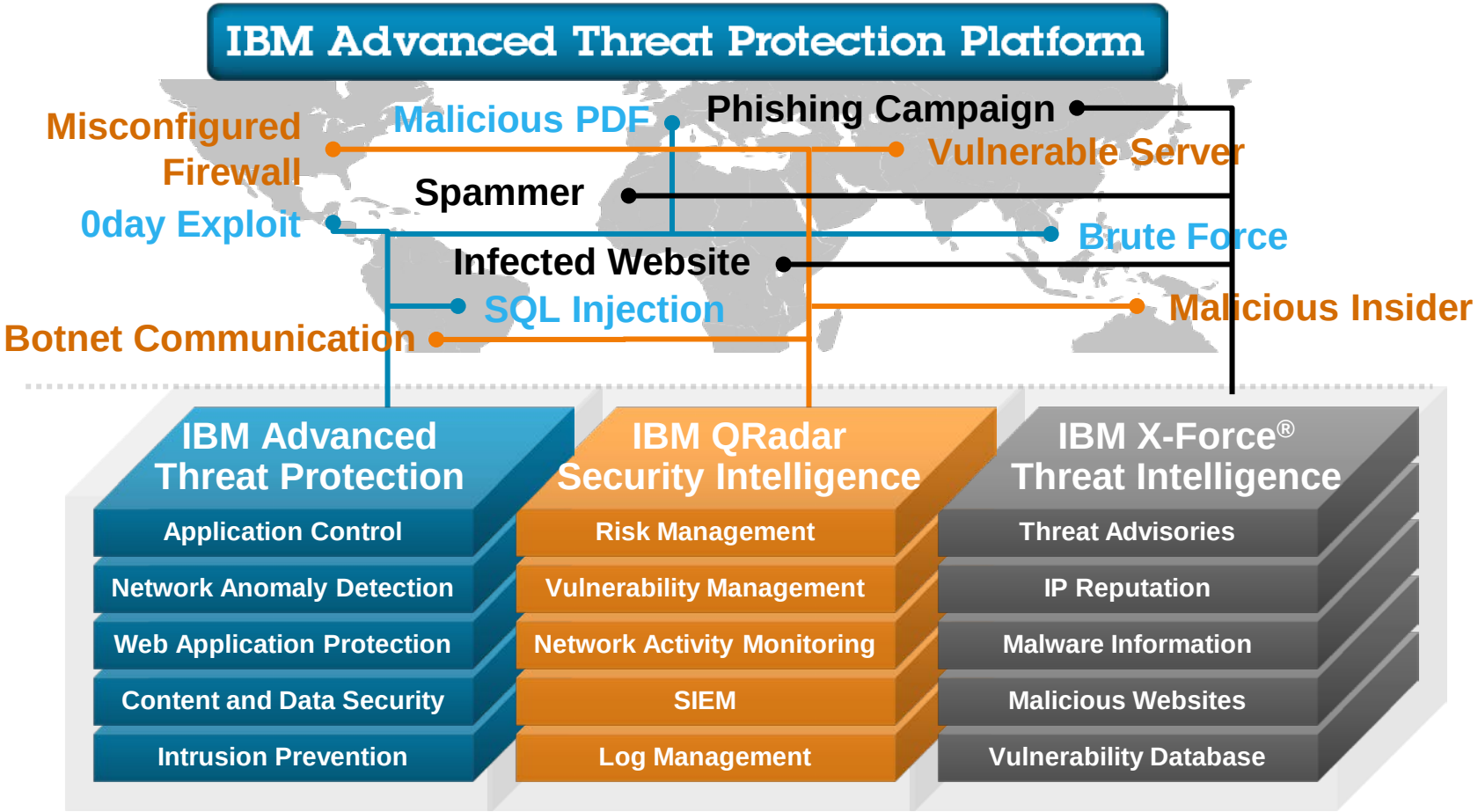
Expertise



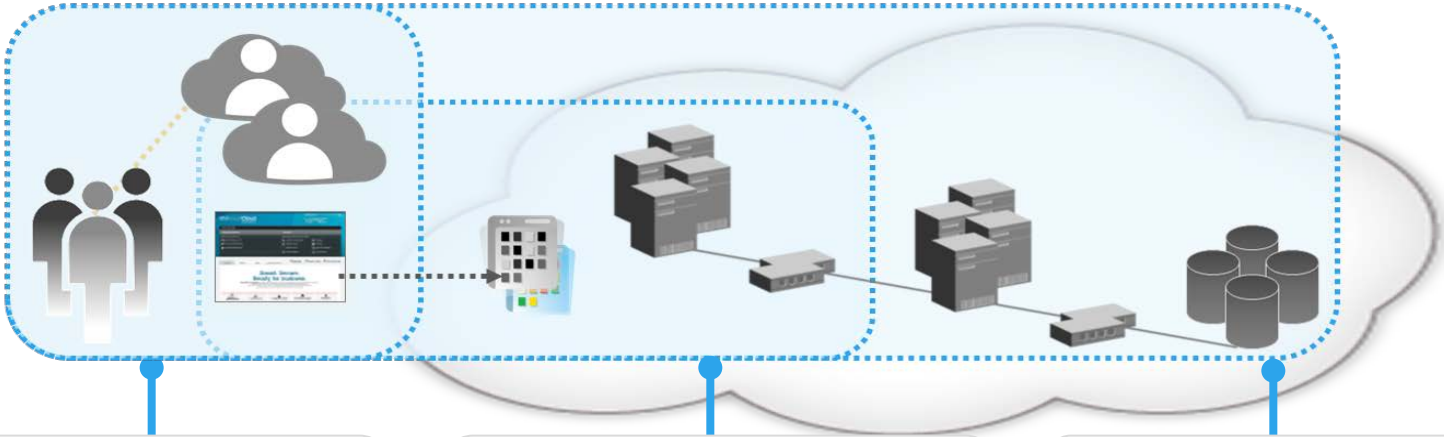
IBM Advanced Threat Protection Platform


IBM Advanced Threat Protection Platform
Malicious PDF
0day Exploit
Brute Force
SQL Injection
IBM Advanced Threat Protection
Application Control
Network Anomaly Detection
Web Application Protection
Content and Data Security
Intrusion Prevention


IBM Advanced Threat Protection Platform
Misconfigured Firewall
Malicious PDF
Vulnerable Server
0day Exploit
Brute Force
SQL Injection
Malicious Insider
Botnet Communication
IBM Advanced Threat Protection
Application Control
Network Anomaly Detection
Web Application Protection
Content and Data Security
Intrusion Prevention
IBM QRadar Security Intelligence
Risk Management
Vulnerability Management
Network Activity Monitoring
SIEM
Log Management


IBM Advanced Threat Protection Platform
Misconfigured Firewall
Malicious PDF
Phishing Campaign
Vulnerable Server
Spammer
0day Exploit
Brute Force
Infected Website
SQL Injection
Malicious Insider
Botnet Communication
IBM Advanced Threat Protection
Application Control
Network Anomaly Detection
Web Application Protection
Content and Data Security
Intrusion Prevention
IBM QRadar Security Intelligence
Risk Management
Vulnerability Management
Network Activity Monitoring
SIEM
Log Management
IBM X-Force® Threat Intelligence
Threat Advisories
IP Reputation
Malware Information
Malicious Websites
Vulnerability Database

IBM SmartCloud Security



Identity Protection

- Administer, extend and help secure identity and access to / from the cloud

Data and Application Protection

- Help secure enterprise databases
- Build, test and maintain cloud applications

Threat Protection

- Help prevent advanced threats with layered protection and analytics

IBM Mobile Security

Device Management

Security for endpoint device and data

Network, Data, and Access Security

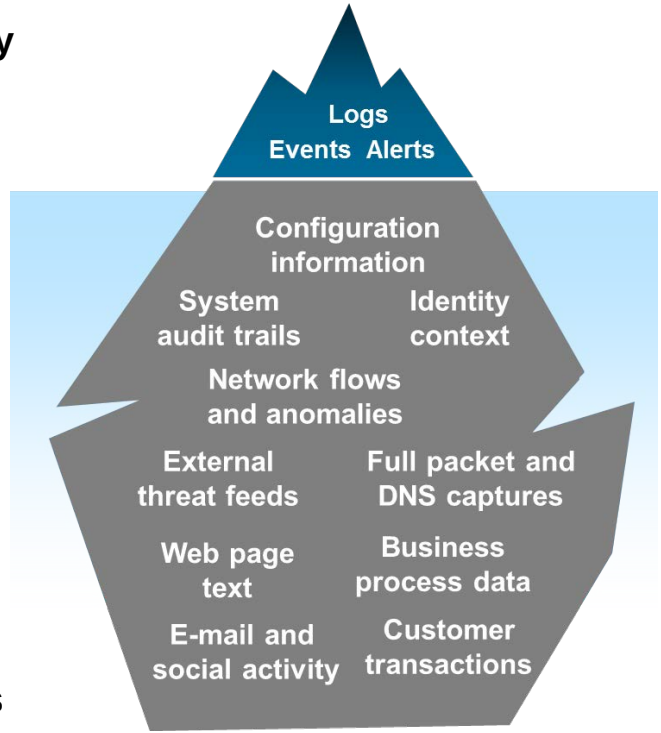
Achieve visibility and adaptive security policies

Application Layer Security

Develop and test applications

Variety and *volume* of data is driving new Big Data use cases

Traditional Security Operations and Technology



Big Data Analytics

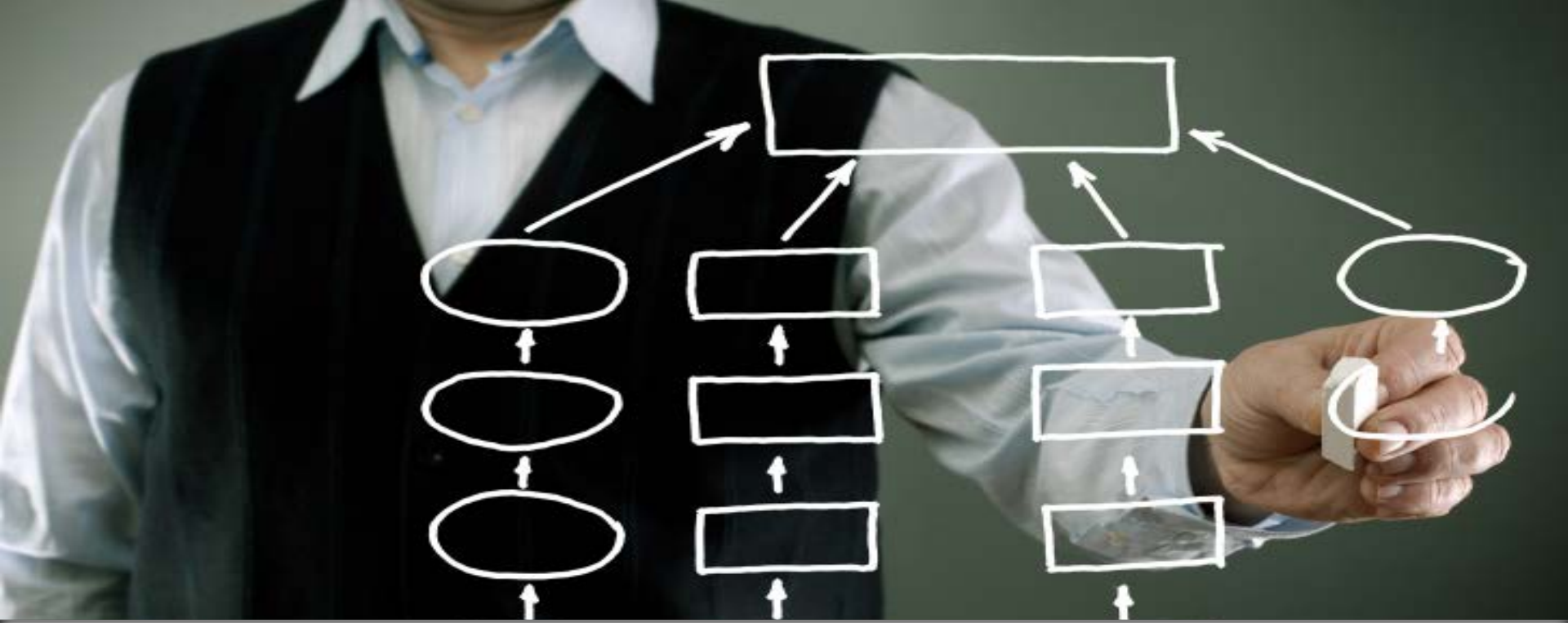
Large FSS Customer

- **250,000** managed firewalls
- **30,000** network devices
- **500,000** open port combinations
- **410,455** Windows client systems
- **36,109** Windows servers
- **24,000** *NIX servers
- **1200+** vulnerability assessment products

Size estimates of scale and volume of events and logs

- **1.5 – 2 TB** per month /major security service
- **200 – 750GB** total / minor security service

Your security team sees…



Clarity…

Insights…

Everything

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated there.

Stream Keynote: Security Intelligence

Pulse2013

Optimizing the World's Infrastructure