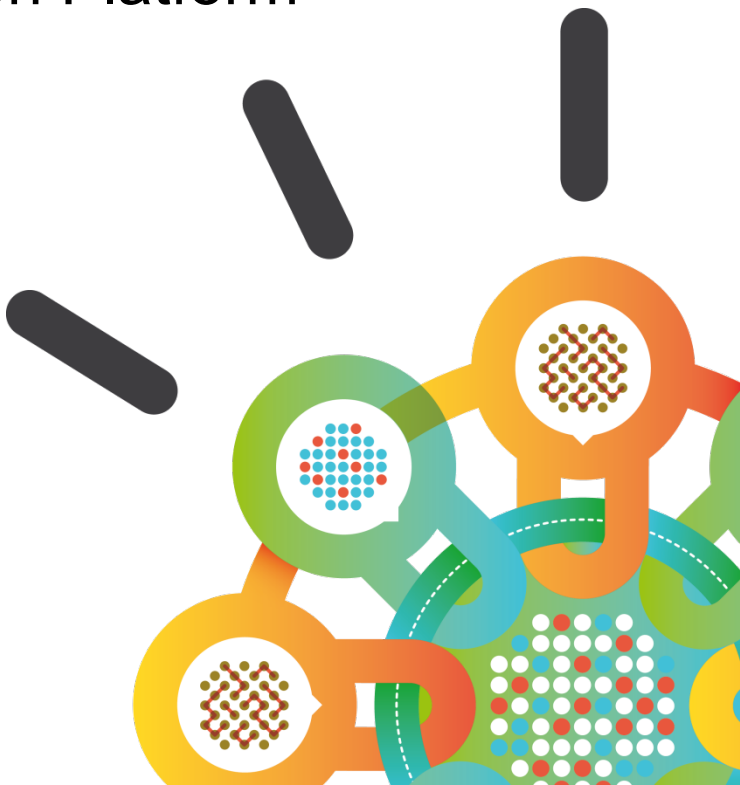
Security Intelligence.
Think Integrated.

Network IPS – The Next Generation

…and IBM's Advanced Threat Protection Platform

September 2012

Simon Smith
Client Technical Professional
simon.smith@uk.ibm.com



Disclaimer

Please Note:

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.

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

DATA EXPLOSION

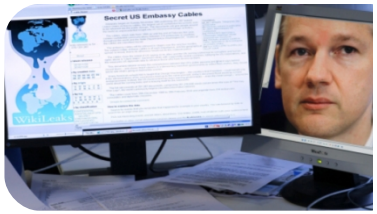
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

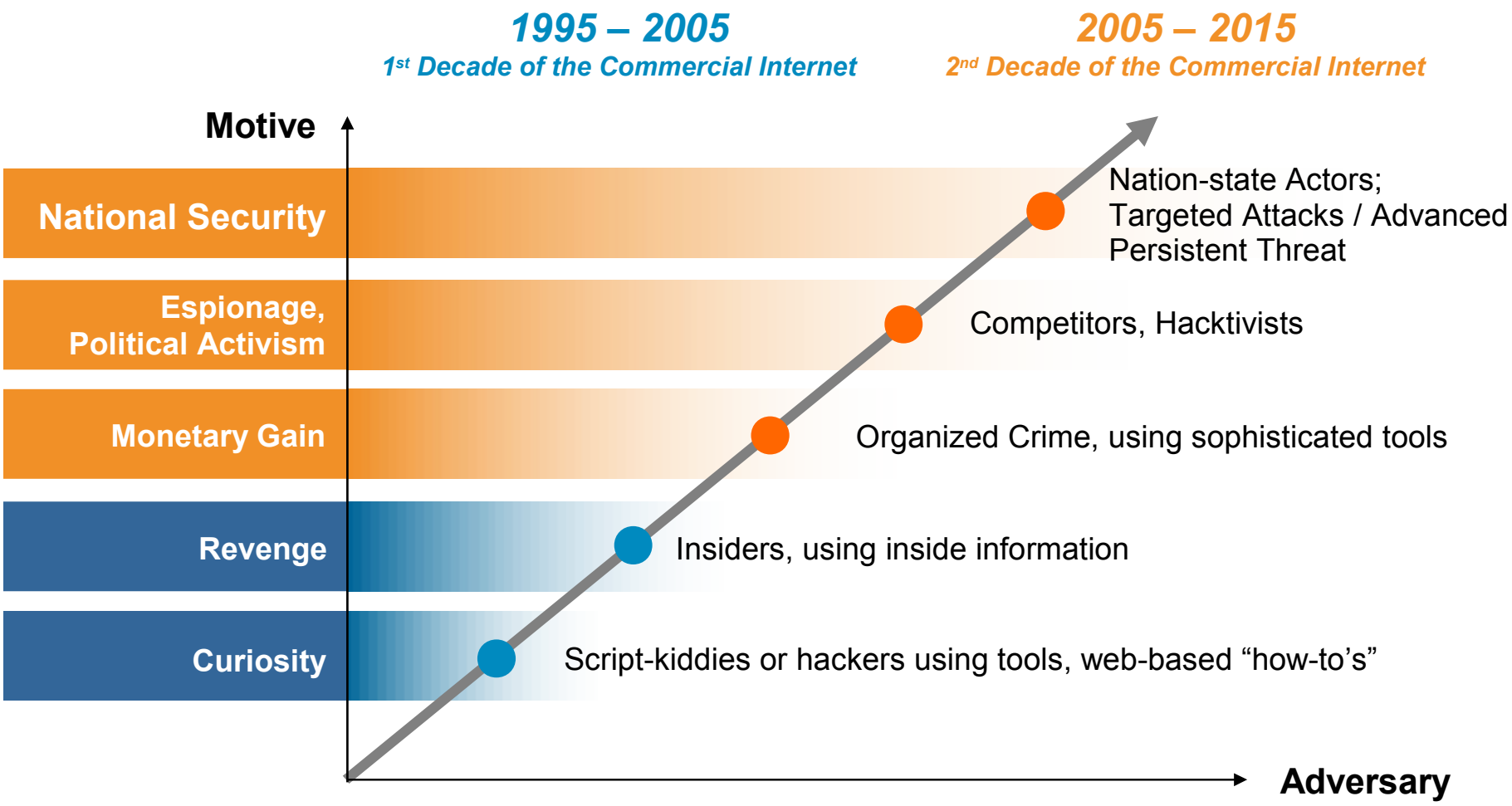
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more



ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cybercrime to terrorism to state-sponsored intrusions

Advanced Threats: The sophistication of Cyber threats, attackers and motives is rapidly escalating



Techniques used by attackers are bypassing traditional defenses

Advanced

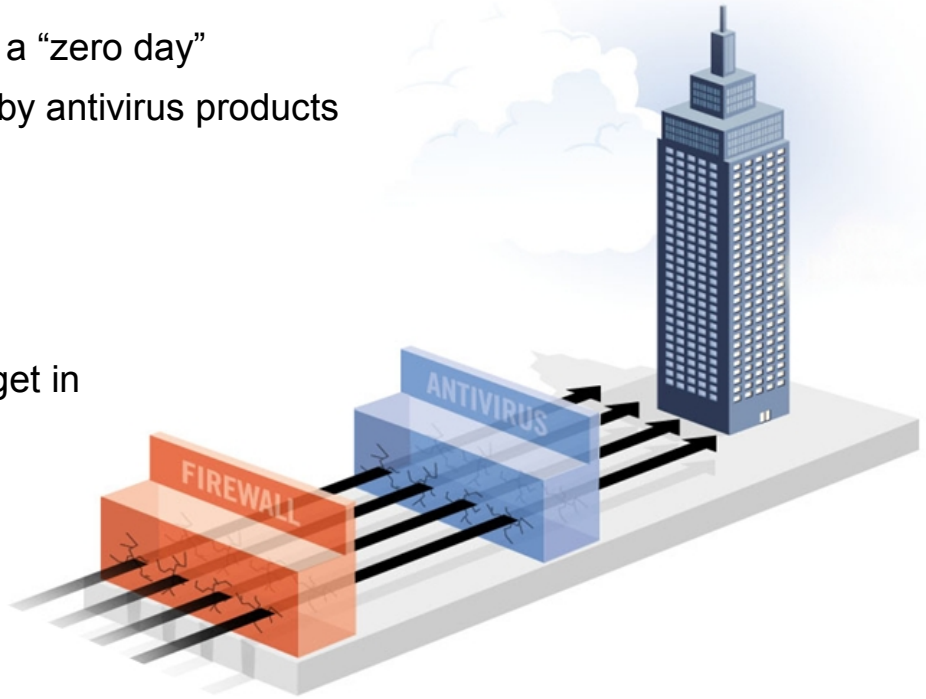
- Using exploits for unreported vulnerabilities, aka a “zero day”
- Advanced, custom malware that is not detected by antivirus products
- Coordinated attacks using a variety of vectors

Persistent

- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in
- Resistant to remediation attempts

Threat

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are actually “out to get you”



These methods have eroded the effectiveness of traditional defenses including firewalls, intrusion prevention systems and antivirus - ***leaving holes in the network***

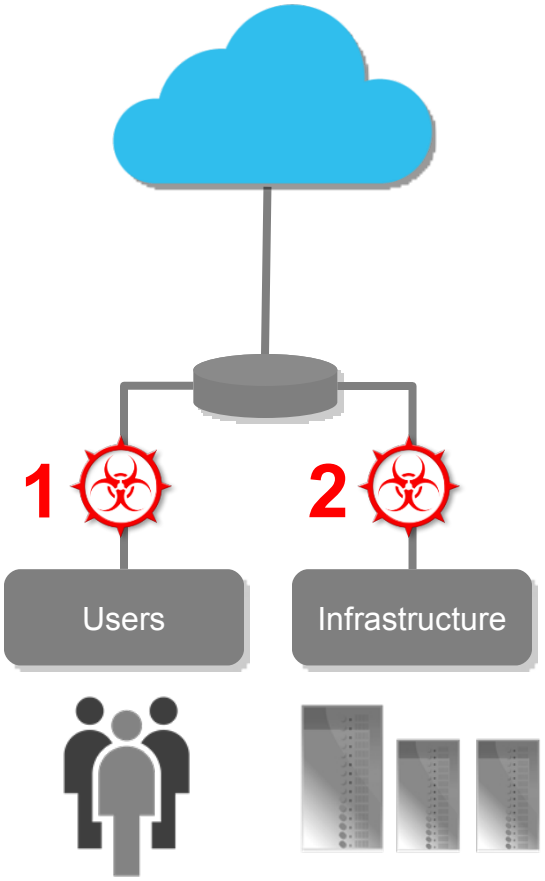
Closer look at the attack vectors of today's threats

1. User Attacks (Client-side)

- **Drive-by Downloads:** User browses to a malicious website and/or downloads an infected file using an unpatched browser or application
- **Targeted Emails:** Email containing an exploit or malicious attachment is sent to an individual with the right level of access at the company

2. Infrastructure Attacks (Server-side)

- **SQL Injection:** Attacker sends a specially crafted message to a web application, allowing them to view, modify, or delete DB table entries
- **General Exploitation:** Attacker identifies and exploits a vulnerability in unpatched or poorly written software to gain privileges on the system



Despite the growing number of techniques used to gain access, one fact remains constant:
a remote attacker must gain access over the corporate network

IBM Advanced Threat Protection

Our strategy is to protect our customers with advanced threat protection at the network layer - by strengthening and integrating network security, analytics and threat Intelligence capabilities

1. Advanced Threat Protection Platform

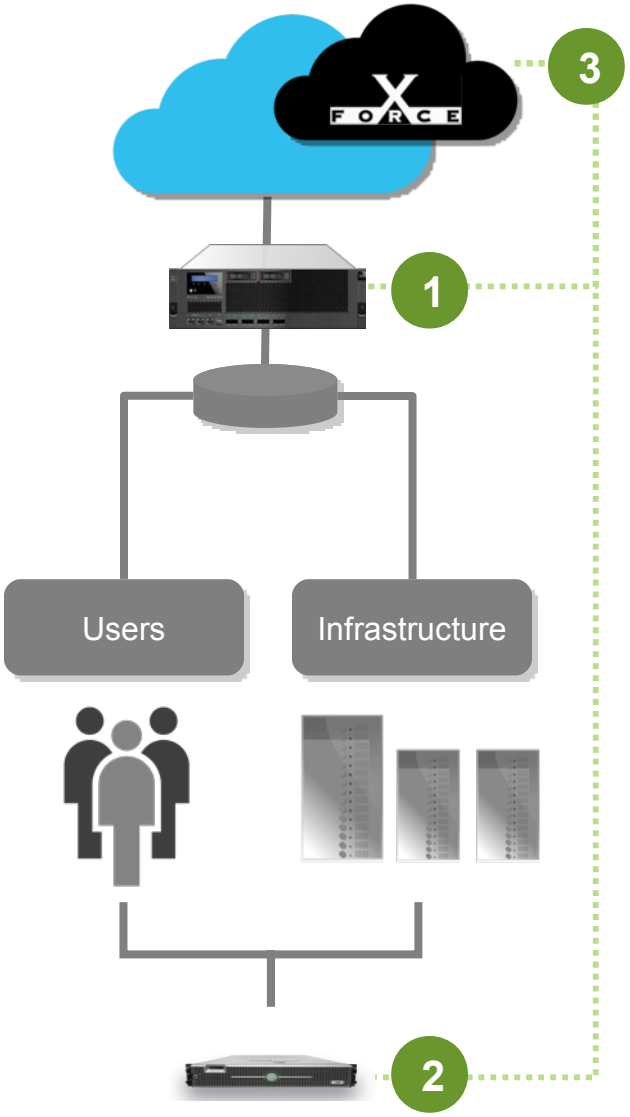
Evolves Intrusion Prevention to become a Threat Protection Platform – providing packet, content, file and session inspection to stop threats from entering the network

2. QRadar Security Intelligence Platform

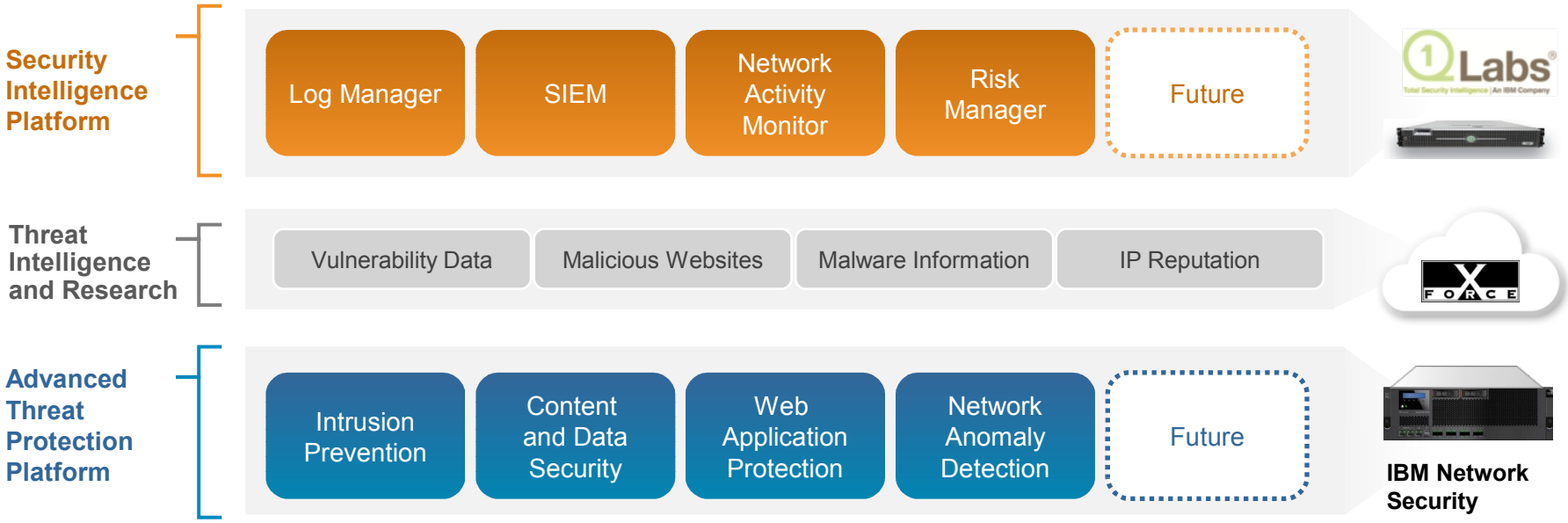
Builds tight integration between the Network Security products, X-Force intelligence feeds and QRadar Security Intelligence products with purpose-built analytics and reporting for threat detection and remediation

3. X-Force Threat Intelligence

Increases aperture of threat intelligence information and feedback loops for our products. Leverages the existing X-Force web and email filtering data, but also expands into additional IP Reputation data sets



IBM's vision for Advanced Threat Protection



Advanced Threat Protection Platform

Ability to prevent sophisticated threats and detect abnormal network behavior by leveraging an extensible set of network security capabilities - in conjunction with real-time threat information and Security Intelligence

Expanded X-Force Threat Intelligence

Increased coverage of world-wide threat intelligence harvested by X-Force and the consumption of this data to make smarter and more accurate security decisions across the IBM portfolio

Security Intelligence Integration

Tight integration between the Advanced Threat Protection Platform and QRadar Security Intelligence platform to provide unique and meaningful ways to detect, investigate and remediate threats

IBM's vision for Advanced Threat Protection

Security Intelligence Platform

- Log Manager
- SIEM
- Network Activity Monitor
- Risk Manager
- Future

X-Force Labs

Threat Intelligence and Research

- Vulnerability Data
- Malicious Websites
- Malware Information
- 3 IP Reputation

X-Force

Advanced Threat Protection Platform

- 1 Intrusion Prevention
- Content and Data Security
- Web Application Protection
- 2 Network Anomaly Detection
- 4 Future

IBM Network Security

1. IBM Security Network IPS powered by X-Force
2. **2Q12:** QRadar Network Anomaly Detection
3. **2Q12:** X-Force IP Reputation Intelligence for QRadar
4. **Future:** What's next?

Network Intrusion Prevention that fits your needs

IBM Security Network Intrusion Prevention (IPS)

- Delivers Advanced Threat Detection and Prevention to stop targeted attacks against high value assets before they impact the organization
- Proactively protects systems with IBM Virtual Patch® technology.
- Protects web applications from threats such as SQL Injection and Cross-site Scripting attacks
- Integrated Data Loss Prevention (DLP) monitors data security risks throughout your network
- Provides Ahead of the Threat® protection backed by world renowned IBM X-Force Research

IBM Security SiteProtector

- Provides central management of security devices to control policies, events, analysis and reporting

IBM Security Network IPS Models									
	Remote	Perimeter			Core				
Model	**GX4004-200**	**GX4004**	**GX5008**	**GX5108**	**GX5208**	**GX7412-5**	**GX7412-10**	**GX7412**	**GX7800**
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	4	4	4	8	8	8	4

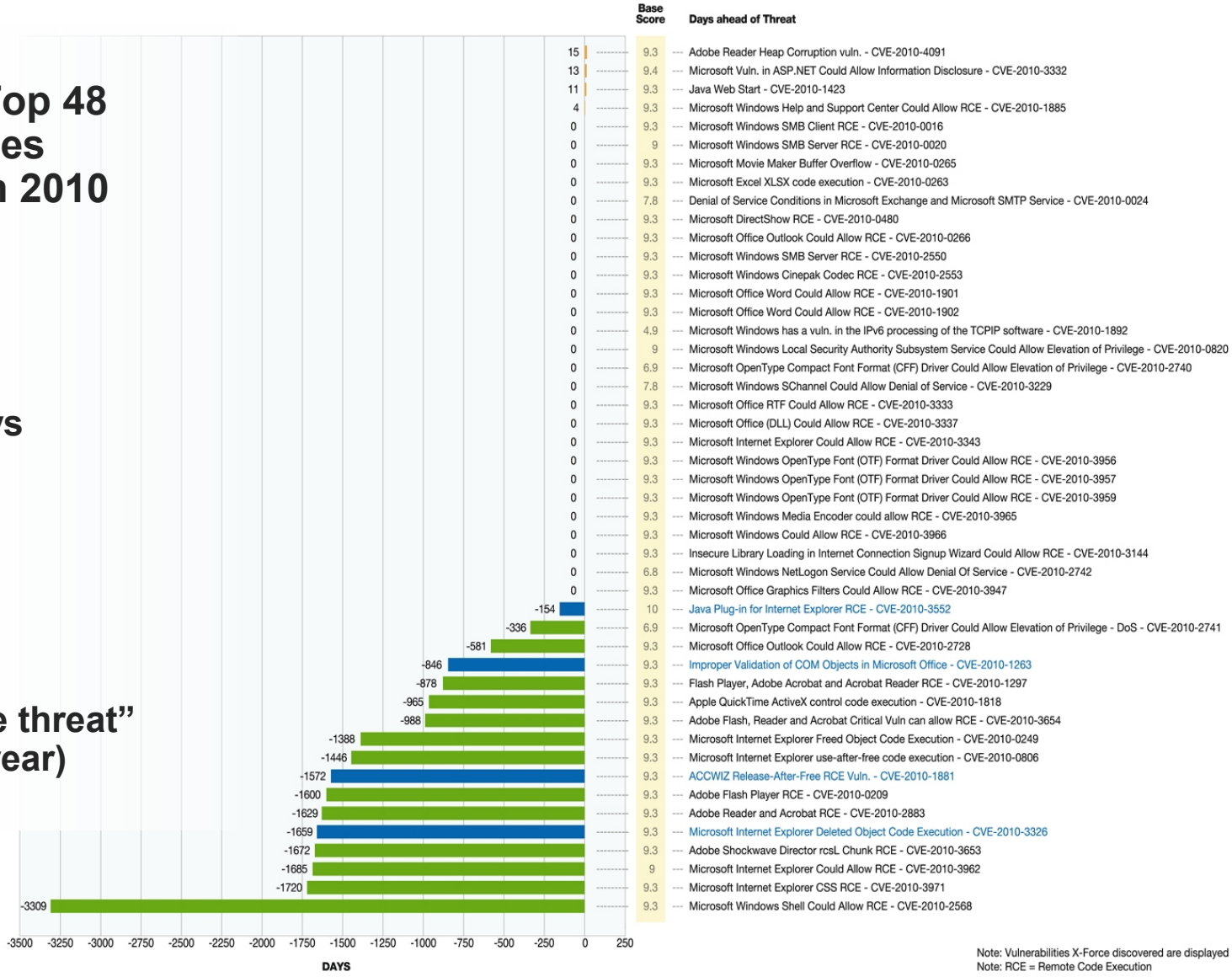
Keeping our customers “Ahead of the Threat”

Out of the Top 48 vulnerabilities disclosed in 2010

100%
within 15 Days

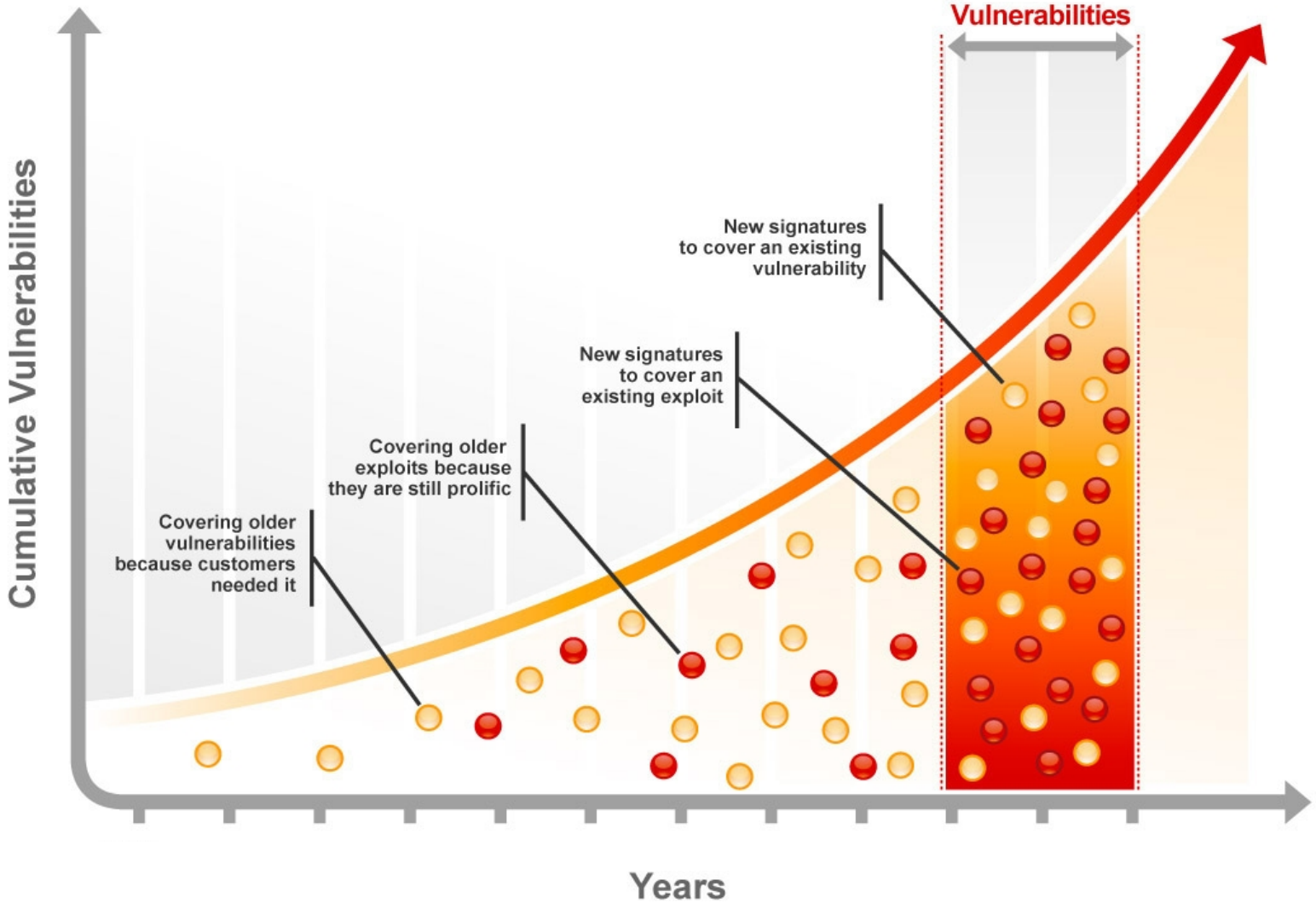
89%
same day

35%
“Ahead of the threat” (average 1+ year)

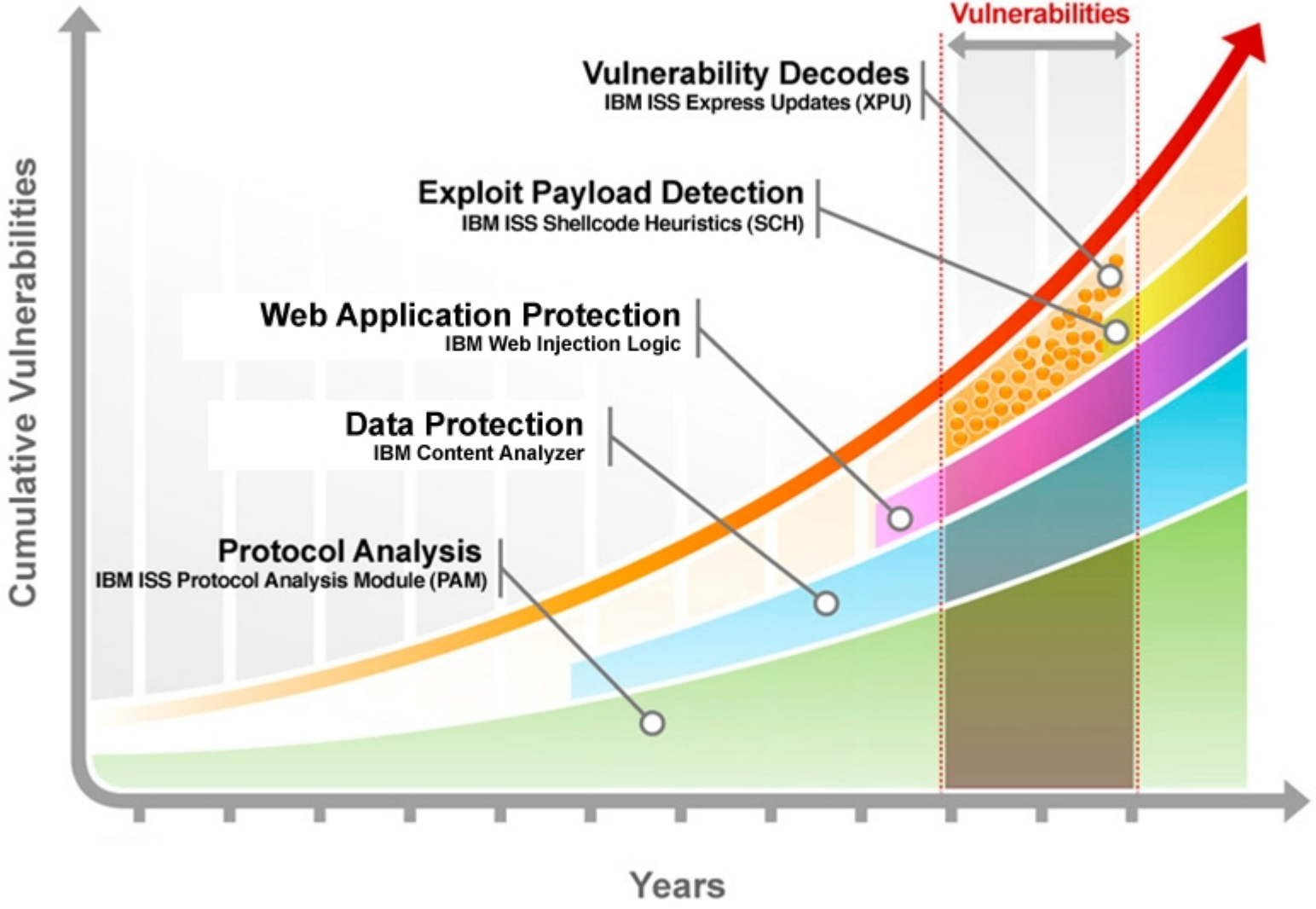


Note: Vulnerabilities X-Force discovered are displayed in blue
Note: RCE = Remote Code Execution

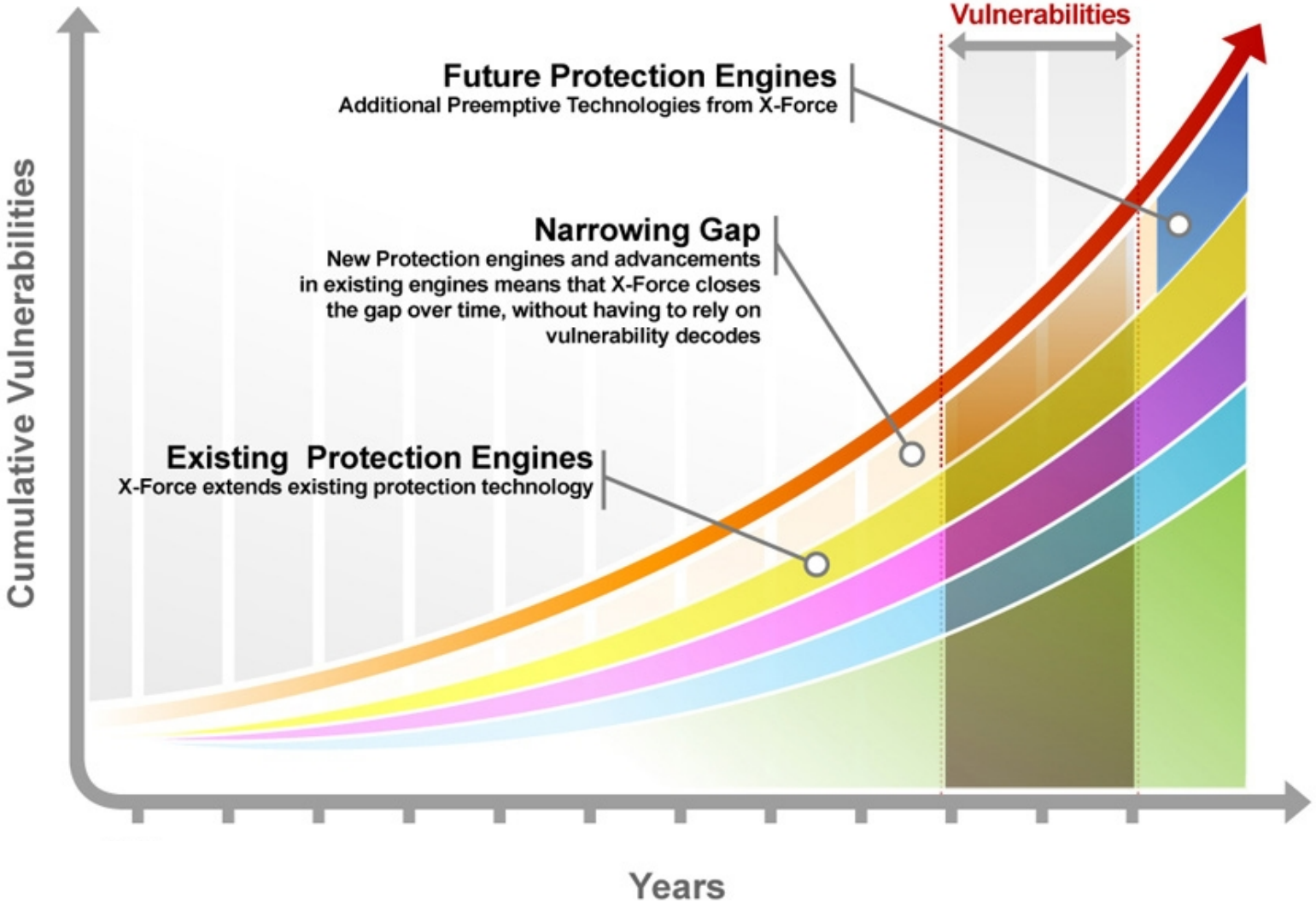
Signature-based protection alone is unsustainable



We've developed several technologies for broader threat protection

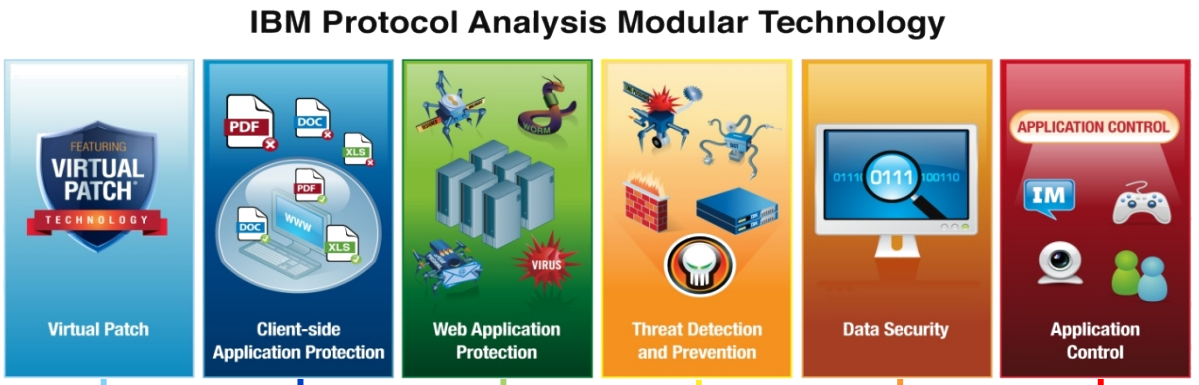


Continued advancements are necessary to stay ahead



Extensible Protection with Protocol Analysis Module

Ahead of the Threat extensible protection backed by the power of X-Force



Virtual Patch	Client-Side Application Protection	Web Application Protection	Threat Detection & Prevention	Data Security	Application Control
What It Does: Mitigates vulnerability exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach. **Why Important:** At the end of 2011, 36% of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.	**What It Does:** Protects end users against attacks targeting applications used every day such as Microsoft Office, Adobe PDF, Multimedia files and Web browsers. **Why Important:** In 2011, vulnerabilities which affect client-side applications represent one of the largest category of all vulnerability disclosures.	**What It Does:** Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery), and Directory Traversals. **Why Important:** Expands security capabilities to meet both compliance requirements and threat evolution.	**What It Does:** Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability. **Why Important:** Eliminates need of constant signature updates. Protection includes the proprietary technology such as Java bytecode exploit detection, Flash exploit detection, and Shell Code Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.	**What It Does:** Monitors, identifies, and provides control over unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist. **Why Important:** Flexible and scalable customized data search criteria; serves as a complement to data security strategy.	**What It Does:** Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunnelling. **Why Important:** Enforces network application and service access based on corporate policy and governance.

NIPS GX Firmware 4.4: Enhanced protection and flexibility with signature migration from SNORT-only alternatives

- Hybrid protection using market leading X-Force Protocol Analysis with the ability to write or import custom SNORT rules
- Reduces the TCO by enabling customers **easy migration from snort-only alternatives**
- IBM Network Protection enables customers to:
  - Export rules from SNORT-based devices
  - Migrate to IBM's PAM-based Network IPS
  - Take custom SNORT rules with them

Locked in to Signature-only IPS?

Make the move to IBM Security Network IPS

2Q12: QRadar Network Anomaly Detection

- **QRadar Network Anomaly Detection** is an optimized version of QRadar which complements SiteProtector to provide deep network visibility and real-time insight to identify and remediate threats
- Market-leading network behavioral analytics improves proficiency in proactive controls
- Integrated analysis of network flow data brings additional security intelligence:
  - Traffic profiling to **detect zero-day threats**
  - Correlation of Threat & Data flow for **enhanced incident analysis**
  - Network Activity Monitoring to **profile user and system behavior to improve threat intelligence**
- Includes support for i**dentity sources** to associate user activity with incidents; and support for **vulnerability data** to correlate attack with vulnerable assets
- Upgradeable to full QRadar SIEM

Network Behavior Awareness

Identity Awareness

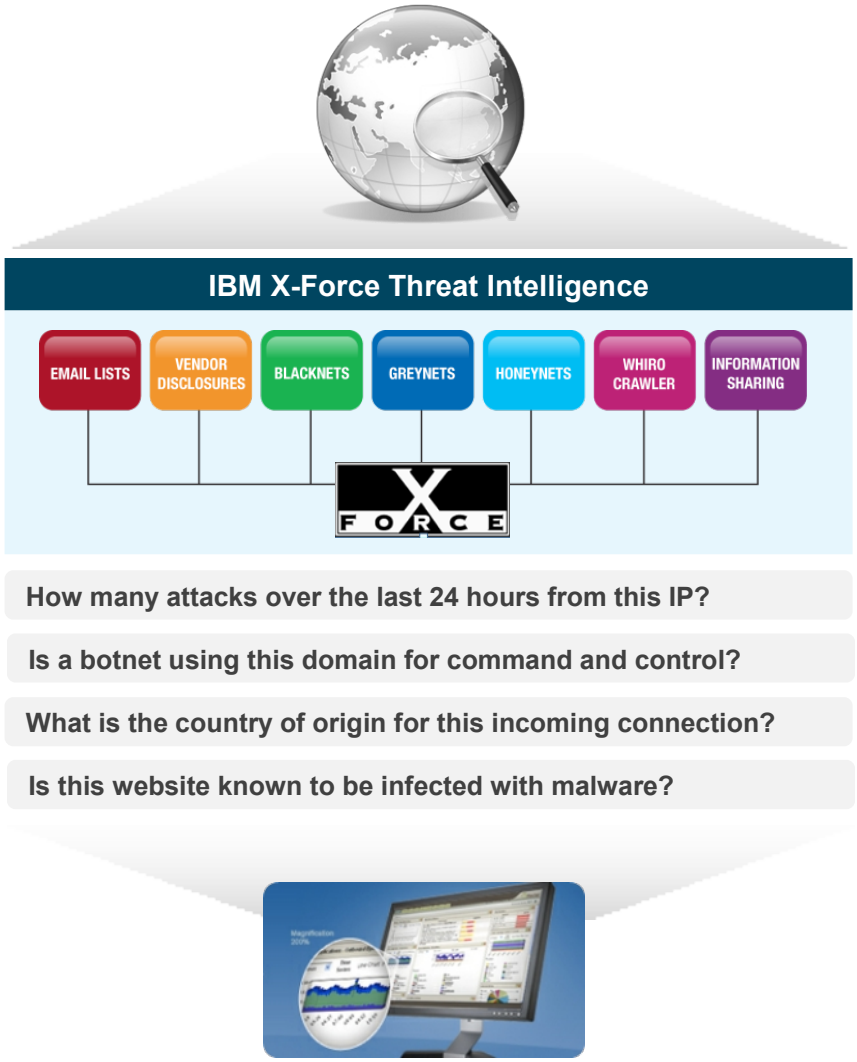
Application Awareness

Vulnerability Correlation

X-Force Reputation

2Q12: X-Force IP Reputation Feed for QRadar

- **IP Reputation** is powerful tool to determine the likelihood of a current or future attack by monitoring past behavior – using multiple network-oriented attributes
- Allows for more intelligent network security policies based on location and past behavior, as well as advanced correlation rules and protection capabilities
- Based upon continuous monitoring of the internet IP addresses and domains to refine accuracy of the IP Reputation list
- Contains information about:
  - Malicious IPs
  - Malware hosts
  - SPAM sources
  - Dynamic IPs
  - Anonymous Proxies
  - and more…



IBM X-Force® Threat Information Center

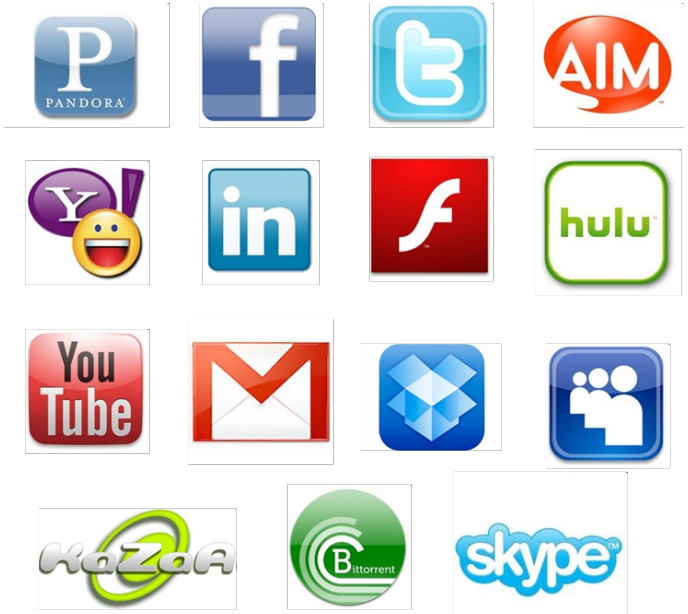
Real-time Security Overview w/ IP Reputation Correlation

Identity and User Context

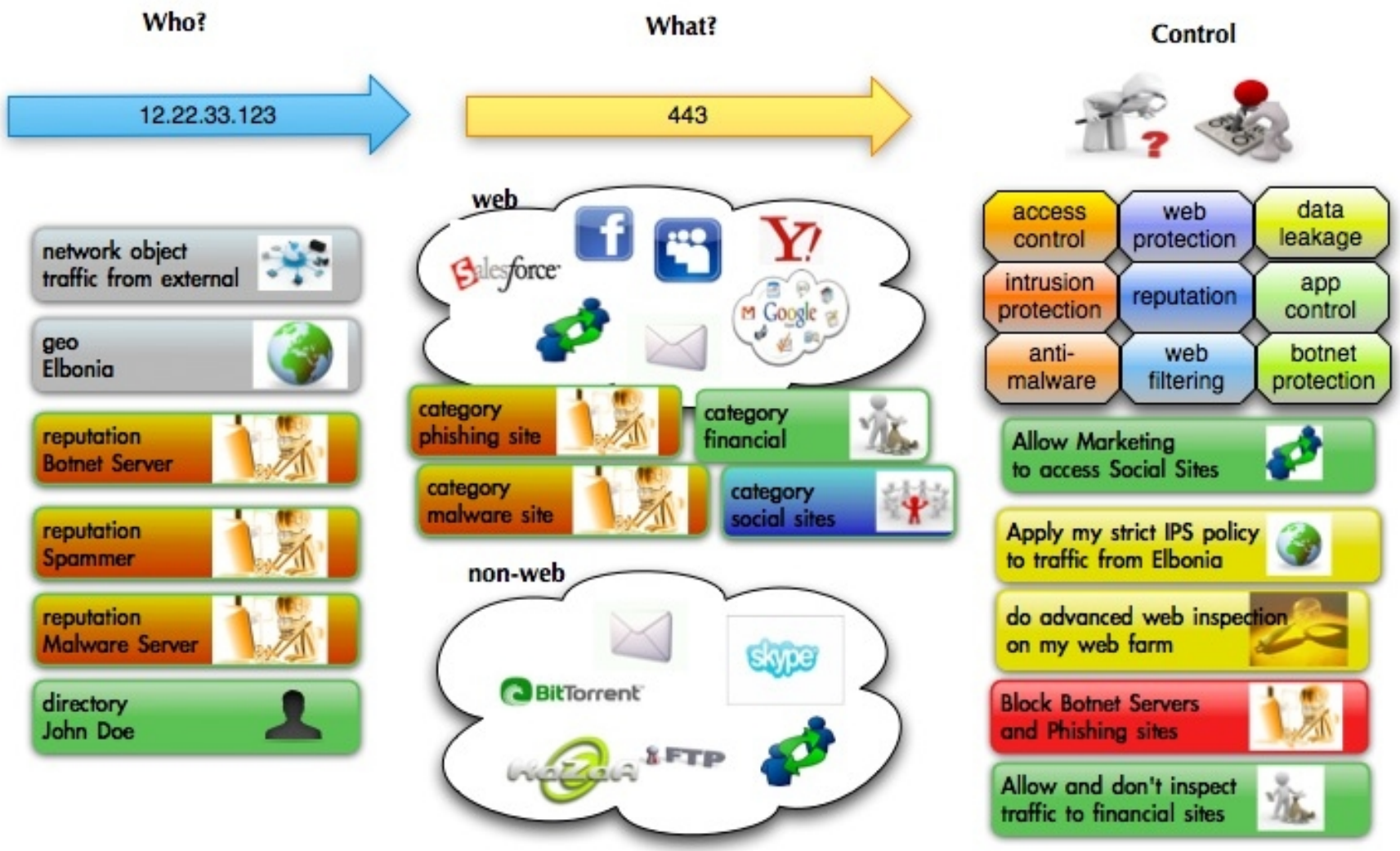
Real-time Network Visualization and Application Statistics

Inbound Security Events

What's next?

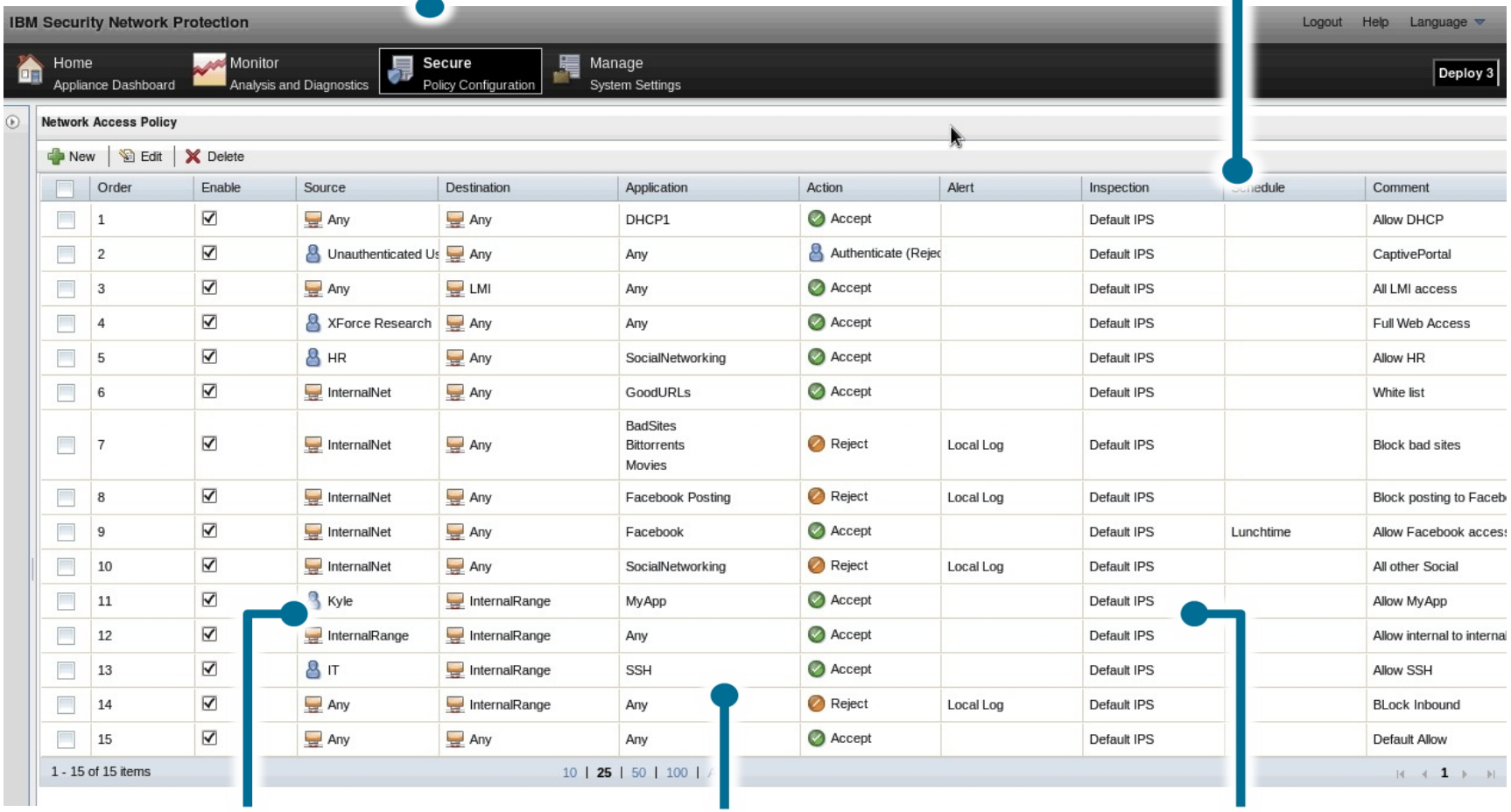


Growth of applications and user control drives security needs



Network Access Policy (NAP) - granular control by network, user, geo, reputation, app, or time-of-day

The first rule matching a given flow is processed

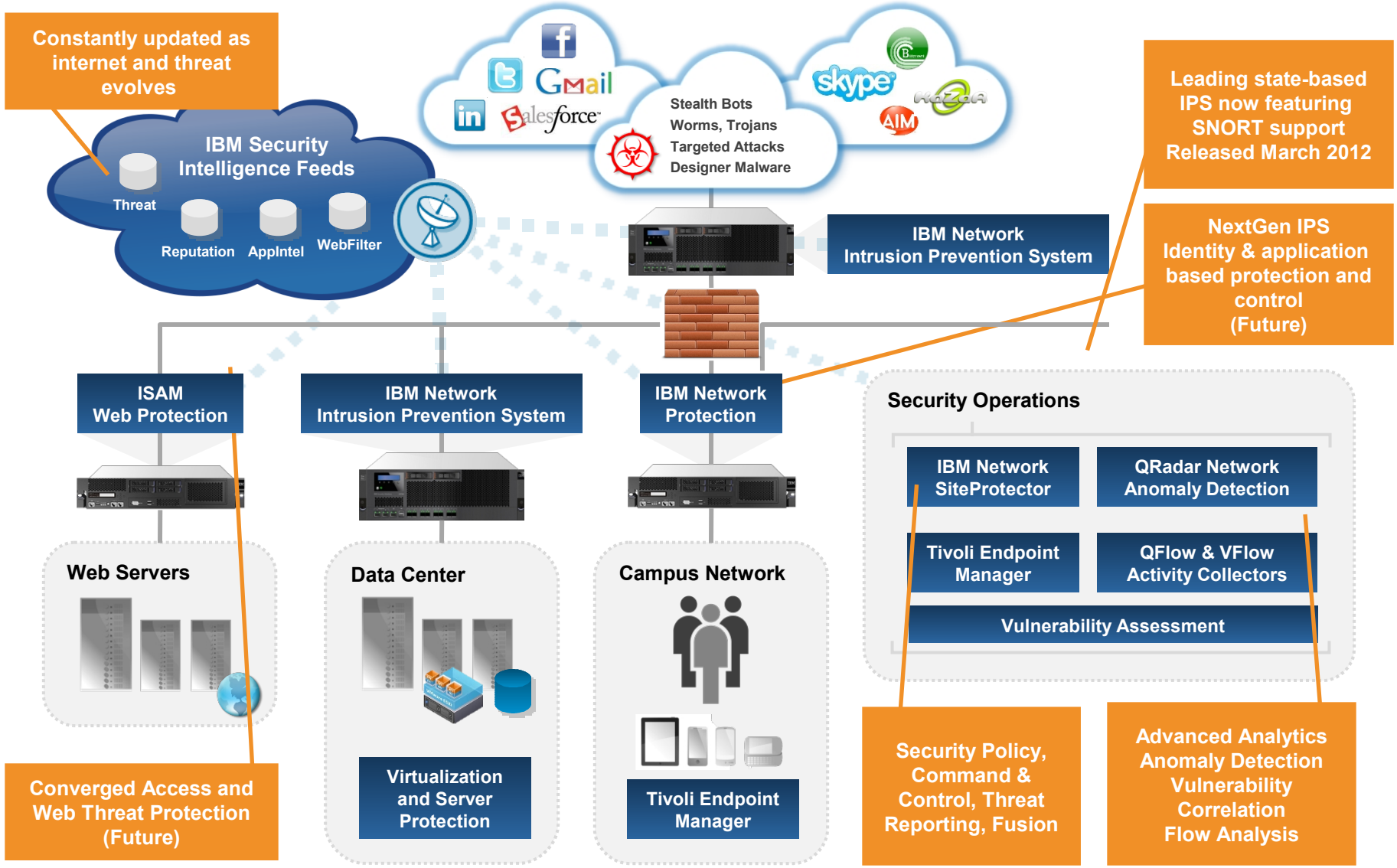


Source can be network, identity, geo, or reputation

Application can be port, app, or category

Attach a tailored security policy to any flow

Advanced Threat Protection Platform



IBM Advanced Threat Protection Platform solves key challenges

IT Security Problem	IBM ATPP Helps. . .
Incident response efforts take too long, impacting confidence in IT	Block malicious traffic
We experience too much downtime due to uncertainty over virus and malware outbreaks	Block malicious traffic
Internal executive reporting is limited, unable to demonstrate effectiveness of security systems	Report on blocked threats
IT compliance reporting is slow and manual	Provide comprehensive compliance reports
Unique network traffic patterns and unpredictable events cause planning and availability issues	Write and import custom rules and utilize freely available open source files
We don’t have efficient tools to proactively analyze network traffic to find unusual user behavior and other anomalies	Integrated analysis of network flow data and integration with SiteProtector
Lack the ability to manage user access to web and non-web applications and internet sites	Controls to manage user access at granular level and decrease bandwidth utilization

ibm.com/security