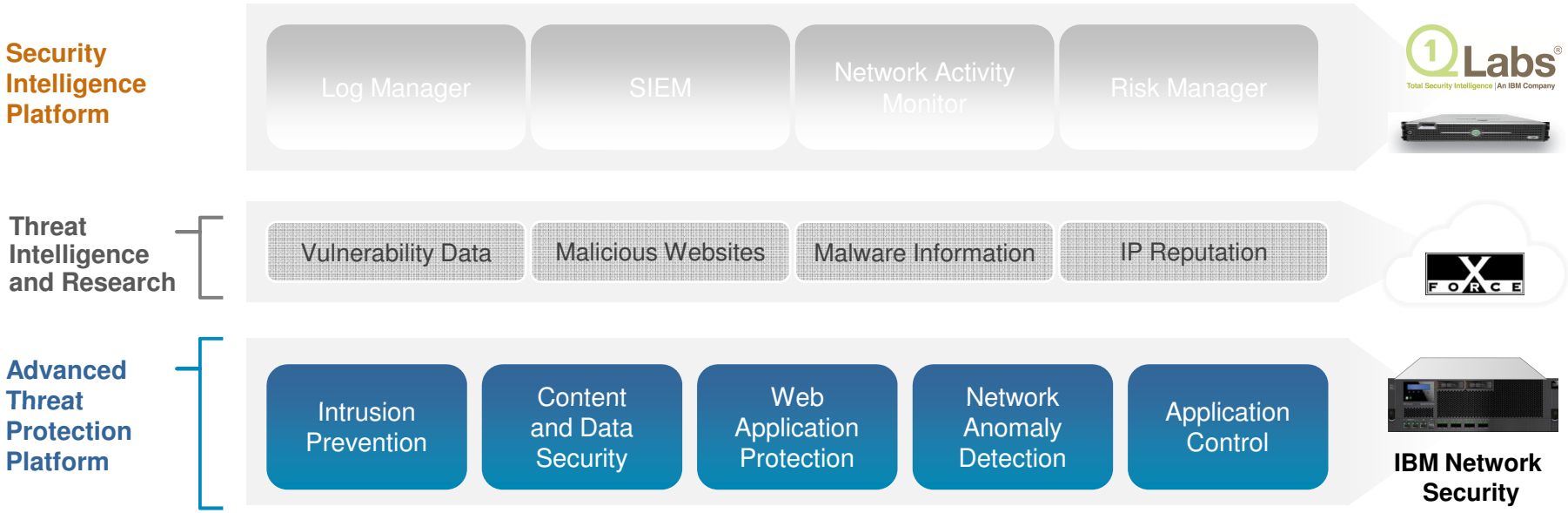
IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

Combatting today´s changing threats
IBM's Extensible Approach to Threat Prevention

Bart Bruijnesteijn, IBM Security

The Advanced Threat Protection Platform



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

At the Core: IBM Security Network Intrusion Prevention System

GX Series

Adaptive Threat Protection

Ahead-of-the-threat extensible protection backed by the power of X-Force®

How does Adaptive Threat Protection Work?

How it Works

- Deep inspection of network traffic
- Identifies & analyzes >200 network and application layer protocols and data file formats

What it Prevents

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal

Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

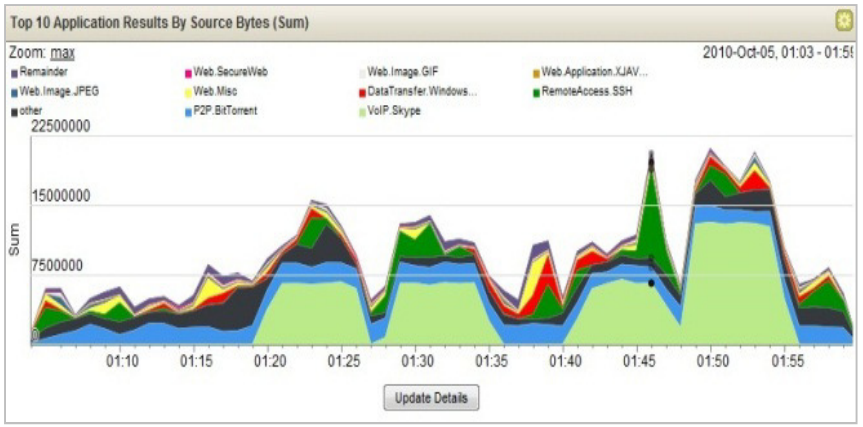
X-Force Threat Intelligence: The IBM Differentiator

X-Force Threat Intelligence Cloud

- **X-Force database** - extensive catalog of vulnerabilities
- **Web filter database** – malicious or infected websites
- **IP Reputation** – botnets, anonymous proxies, bad actors
- **Application Identification** – web application information
- **Vulnerability Research** – latest vulnerabilities and protections
- **Security Services –** manage IPS for 3000+ Customers

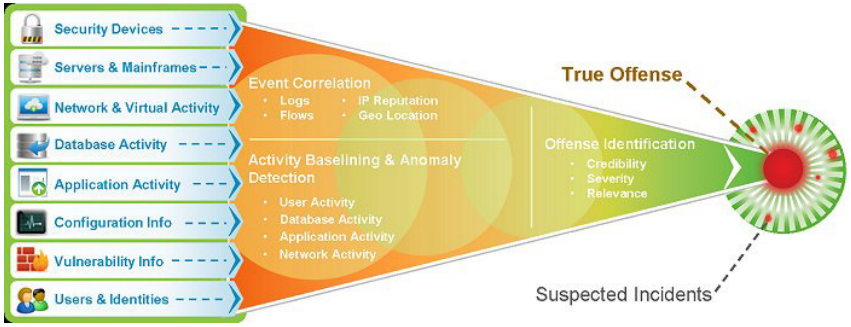
Expanding Capabilities with QRadar Network Anomaly Detection

- **QRadar Network Anomaly Detection** is a purpose built version of QRadar for IBM's intrusion prevention portfolio



- The addition of QRadar's behavioral analytics and real-time correlation helps better detect and prioritize stealthy attacks

- Supplements visibility provided by IBM Security Network Protection's Local Management (LMI)



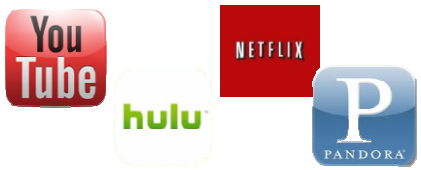
- Integration with IBM Security Network Protection including the ability to send network flow data from XGS to QRadar

Next Generation Challenges Require Next Generation Security

Stealth Bots • Targeted Attacks
Worms • Trojans • Designer Malware

SOPHISTICATED ATTACKS

Increasingly sophisticated attacks are using multiple attack vectors and increasing risk exposure



STREAMING MEDIA

Streaming media sites are consuming large amounts of bandwidth

SOCIAL NETWORKING

Social media sites present productivity, privacy and security risks including new threat vectors

URL Filtering • IDS / IPS
IM / P2P • Web App Protection
Vulnerability Management

POINT SOLUTIONS

Point solutions are siloed with minimal integration or data sharing

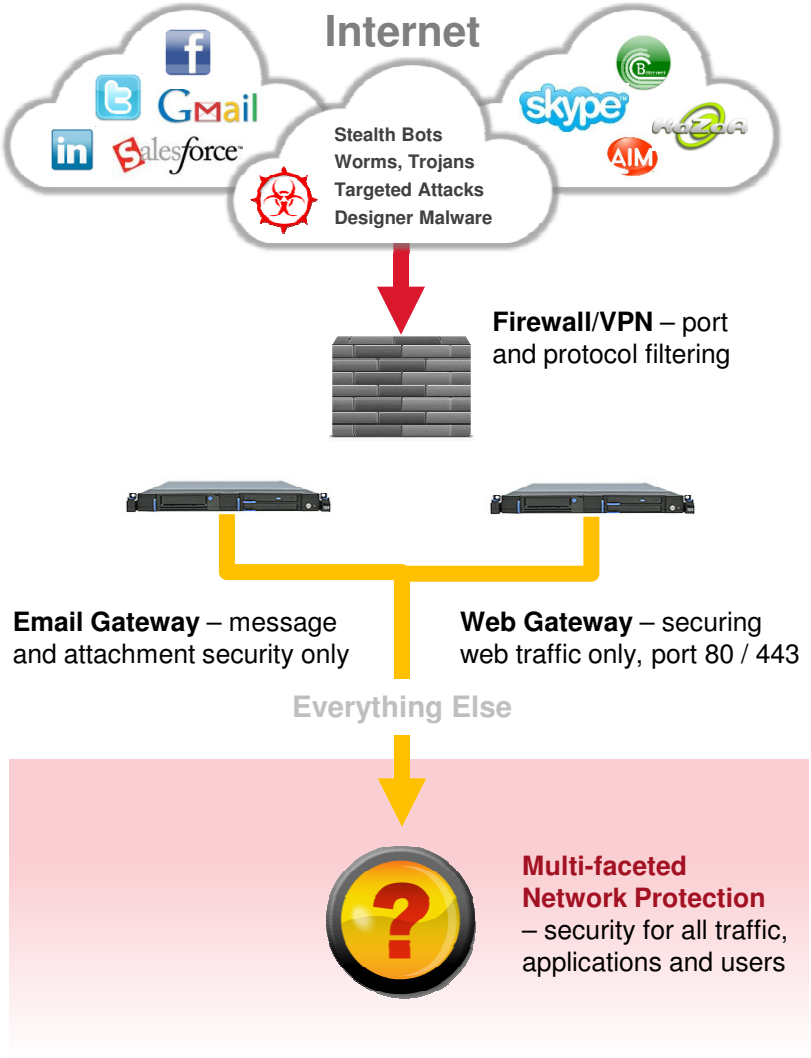
Network Defense: Traditional solutions not up to today's challenges

Current Limitations

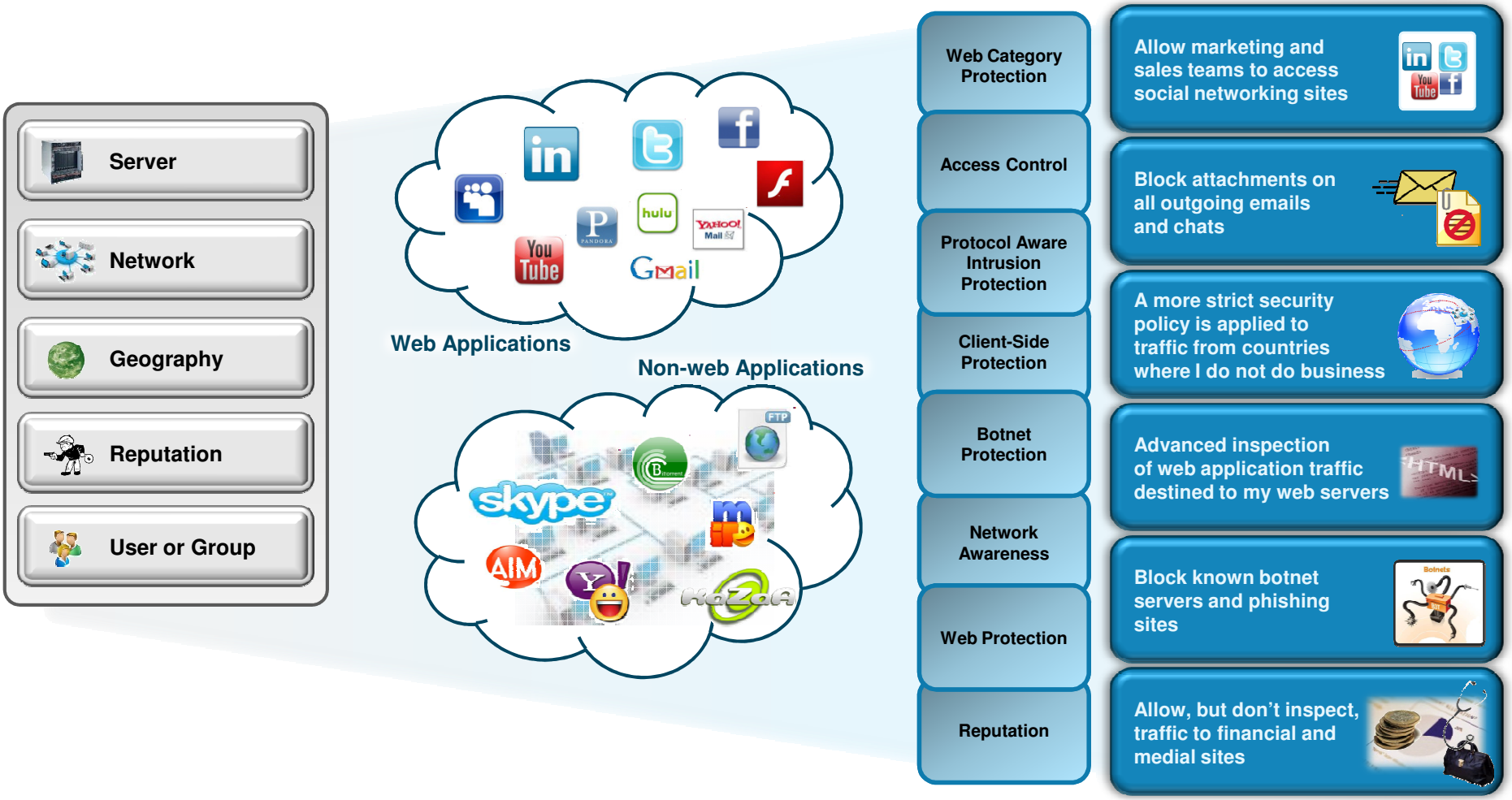
- Threats continue to evolve and standard methods of detection are not enough
- Streaming media sites and Web applications introduce new security challenges
- Basic "Block Only" mode limits innovative use of streaming and new Web apps
- Poorly integrated solutions create "security sprawl", lower overall levels of security, and raise cost and complexity

Requirement: Multi-faceted Protection

- 0-day threat protection tightly integrated with other technologies i.e. network anomaly detection
- Ability to reduce costs associated with non-business use of applications
- Controls to restrict access to social media sites by a user's role and business need
- Augment point solutions to reduce overall cost and complexity



Protecting Today's Networks from Tomorrow's Threats



Who → 172.29.230.15, 192.168.0.0 /16

What → 80, 443,25, 21, 2048-65535

Controls → ?

Security

IBM Security Network Protection

PROVEN SECURITY	NEW WITH XGS ULTIMATE VISIBILITY	NEW WITH XGS COMPLETE CONTROL
Extensible, 0-Day protection powered by X-Force®	Understand the Who, What and When for all network activity	Ensure appropriate application and network use

IBM Security Network Protection XGS 5000
builds on the proven security of IBM intrusion prevention solutions by delivering the addition of next generation *visibility* and *control* to help balance security and business requirements

Proven Security: Extensible, 0-Day Protection Powered by X-Force®

- **Next Generation IPS** powered by X-Force® Research protects weeks or even months "ahead of the threat"
- **Full protocol, content and application aware** protection goes beyond signatures
- **Expandable protection modules defend against emerging threats** such as malicious file attachments and Web application attacks

"When we see these attacks coming in, it will shut them down automatically."

– Melbourne IT

[The IBM Threat Protection Engine] "defended an attack against a critical government network another protocol aware IPS missed"

– Government Agency

IBM Security Network Protection XGS 5000

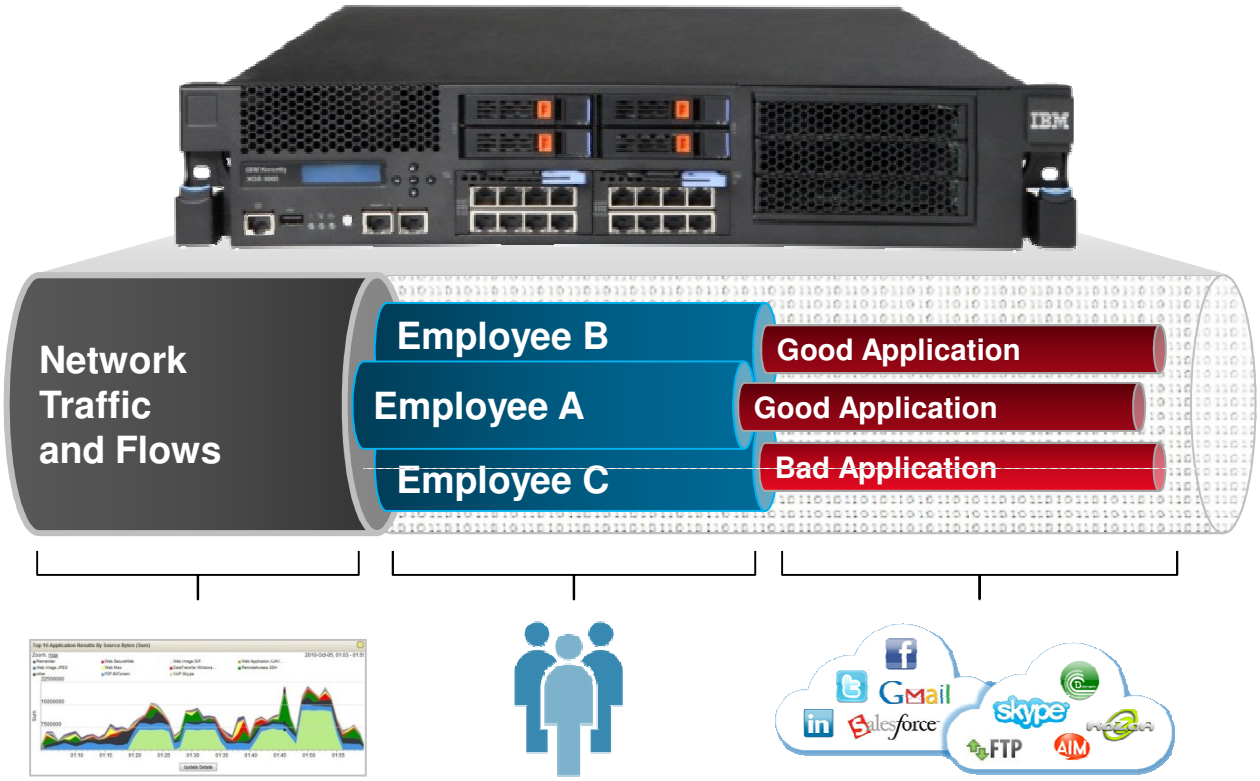
IBM Security Threat Protection

- Vulnerability Modeling & Algorithms
- Stateful Packet Inspection
- Port Variability
- Port Assignment
- Port Following
- Protocol Tunneling
- Application Layer Pre-processing
- Shellcode Heuristics
- Context Field Analysis
- RFC Compliance
- Statistical Analysis
- TCP Reassembly & Flow Reassembly
- Host Response Analysis
- IPv6 Tunnel Analysis
- SIT Tunnel Analysis
- Port Probe Detection
- Pattern Matching
- Custom Signatures
- Injection Logic Engine

- Backed by X-Force®
- 15 years+ of vulnerability research and development
- Trusted by the world's largest enterprises and government agencies
- True protocol-aware intrusion prevention, not reliant on signatures
- Specialized engines
  - Exploit Payload Detection
  - Web Application Protection
  - Content and File Inspection

Ultimate Visibility: Understanding Who, What and When

- **Immediately discover** which applications and web sites are being accessed
- **Quickly Identify misuse** by application, website, user, and group
- **Understand who and what** are consuming bandwidth on the network
- **Superior detection of advanced threats** through integration with QRadar for network anomaly and event details



Network Flow Data provides real time awareness of anomalous activities and QRadar integration facilitates enhanced analysis and correlation

Complete Identity Awareness associates valuable users and groups with their network activity, application usage and application actions

Application Awareness fully classifies network traffic, regardless of address, port , protocol, application, application action or security event

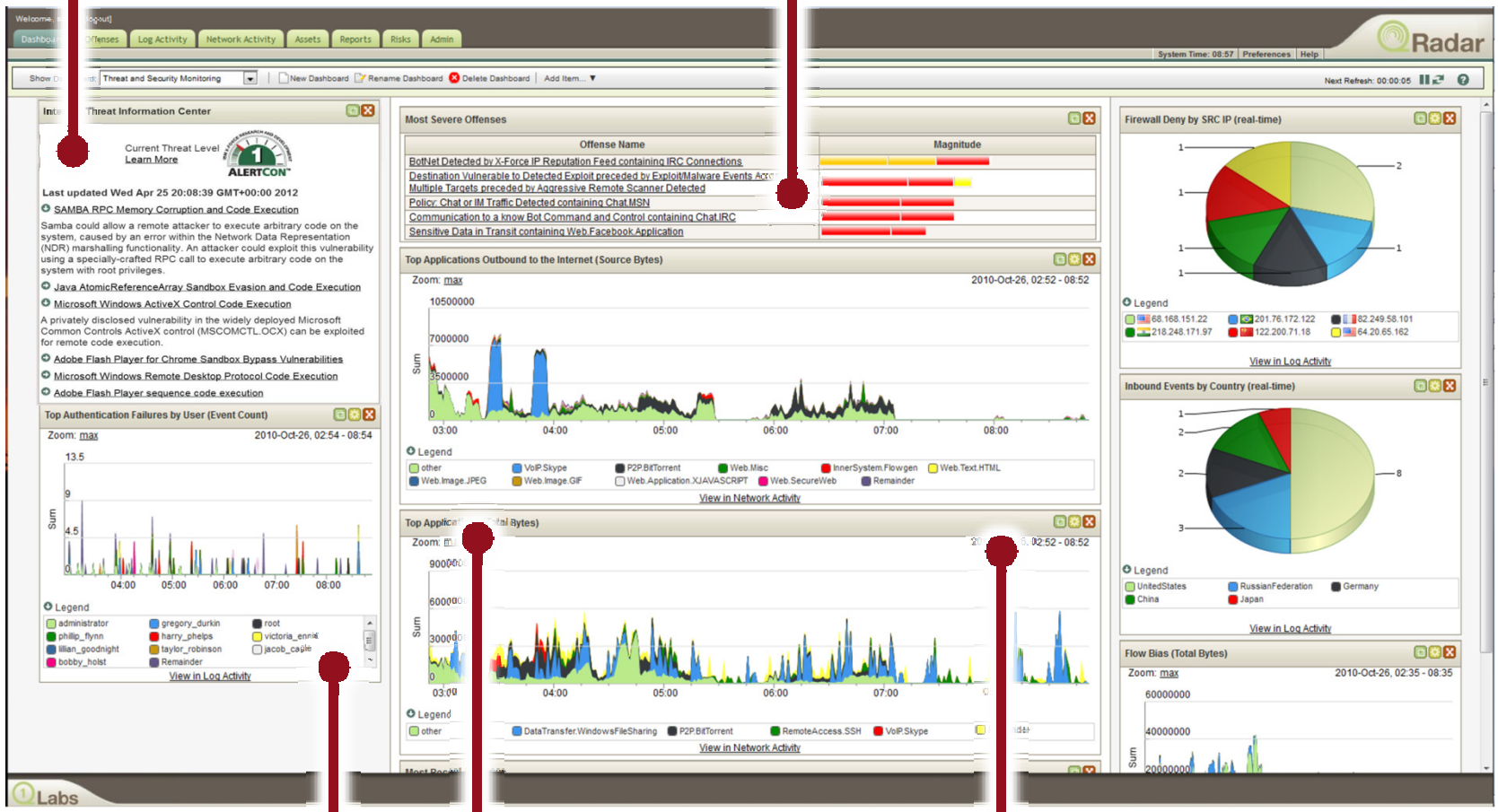
"We were able to detect the Trojan "Poison Ivy" within the first three hours of deploying IBM Security Network Protection"

– Australian Hospital

Increase Security ● Reduce Costs ● Enable Innovation

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

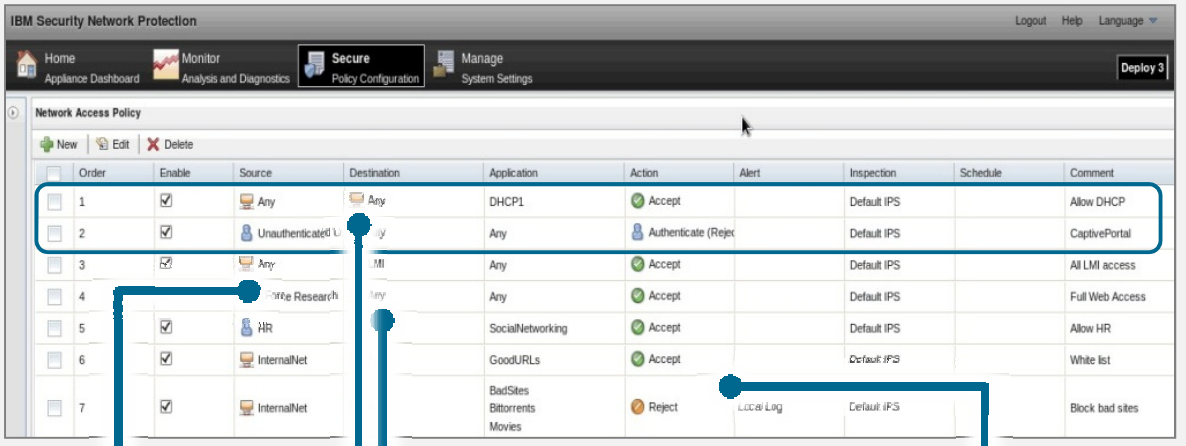
Inbound Security Events

Complete Control: Overcoming a Simple Block-Only Approach

- **Network Control** by users, groups, systems, protocols, applications & application actions
- **Block evolving, high-risk sites** such as Phishing and Malware with constantly updated categories
- **Comprehensive up-to-date web site coverage** with industry-leading 15 Billion+ URLs ***(50-100x the coverage comparatively)***
- **Rich application support** with 1000+ applications and individual actions

"We had a case in Europe where workers went on strike for 3 days after Facebook was completely blocked…so granularity is key."

– IBM Business Partner



Limit the use of social networking, file sharing, and web mail for common users

Allow full access to social networking sites for marketing and HR teams

Stop broad misuse of the corporate network by blocking sites that introduce undue risk and cost

Flexible network access policies controls access to systems and applicable security policy

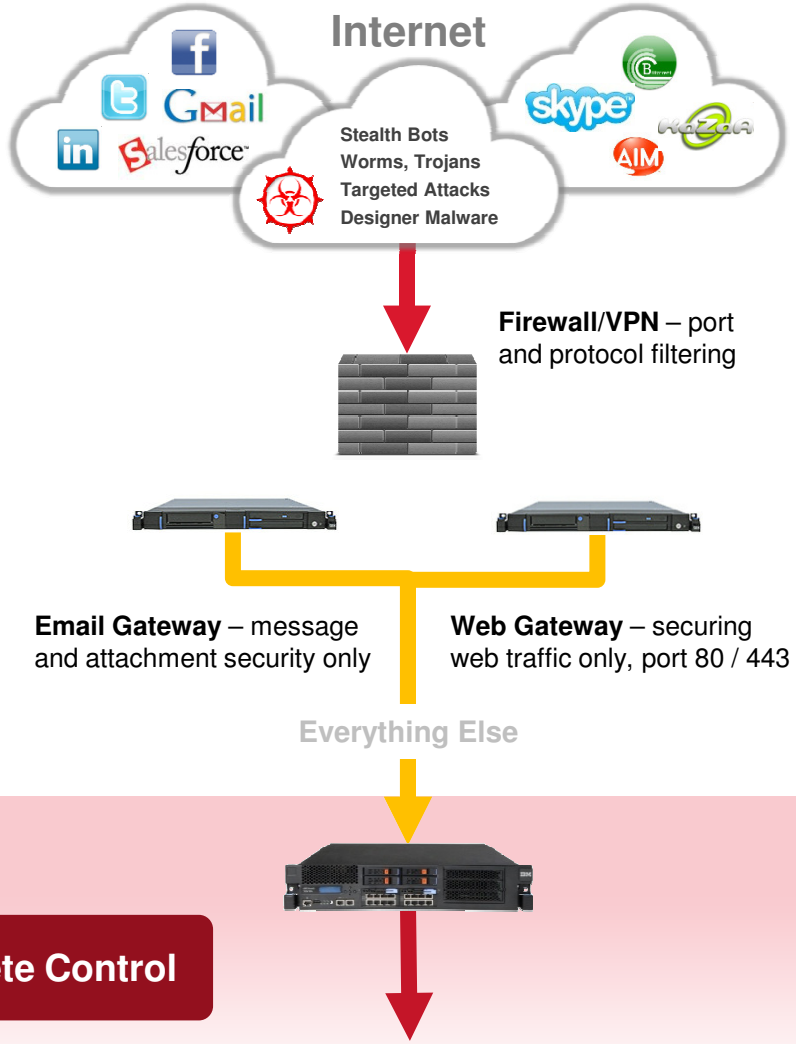
The XGS 5000: The Best Solution for Threat Prevention

Better Network Control

- Natural complement to current Firewall and VPN
- Not rip-and-replace – works with your existing network and security infrastructure
- More flexibility and depth in security and control over users, groups, networks and applications

Better Threat Protection

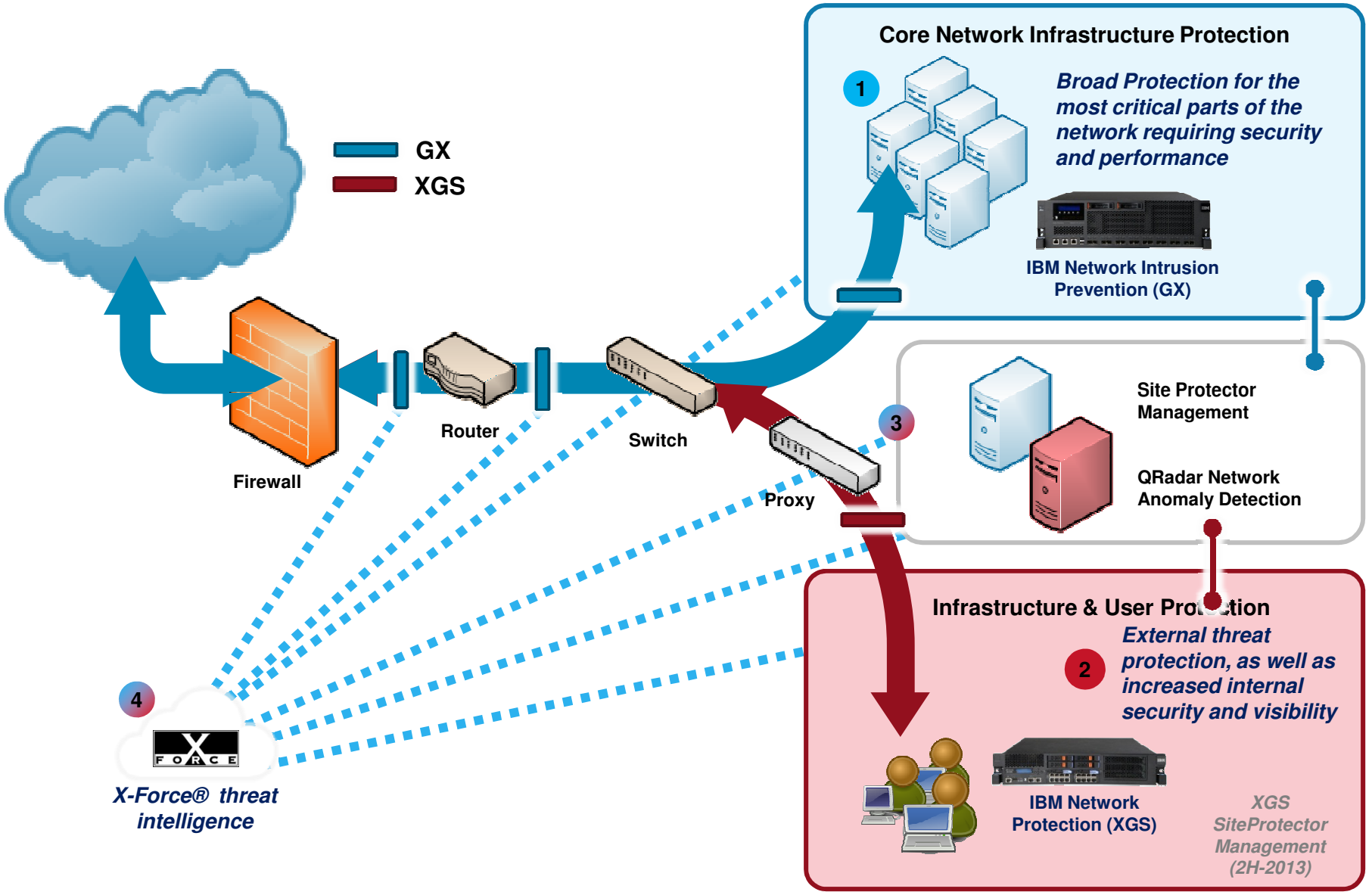
- True Protocol aware Network IPS
- Higher level of overall security and protection
- More effective against 0-day attacks
- Best of both worlds – true protocol and heuristic-based protection with customized signature support



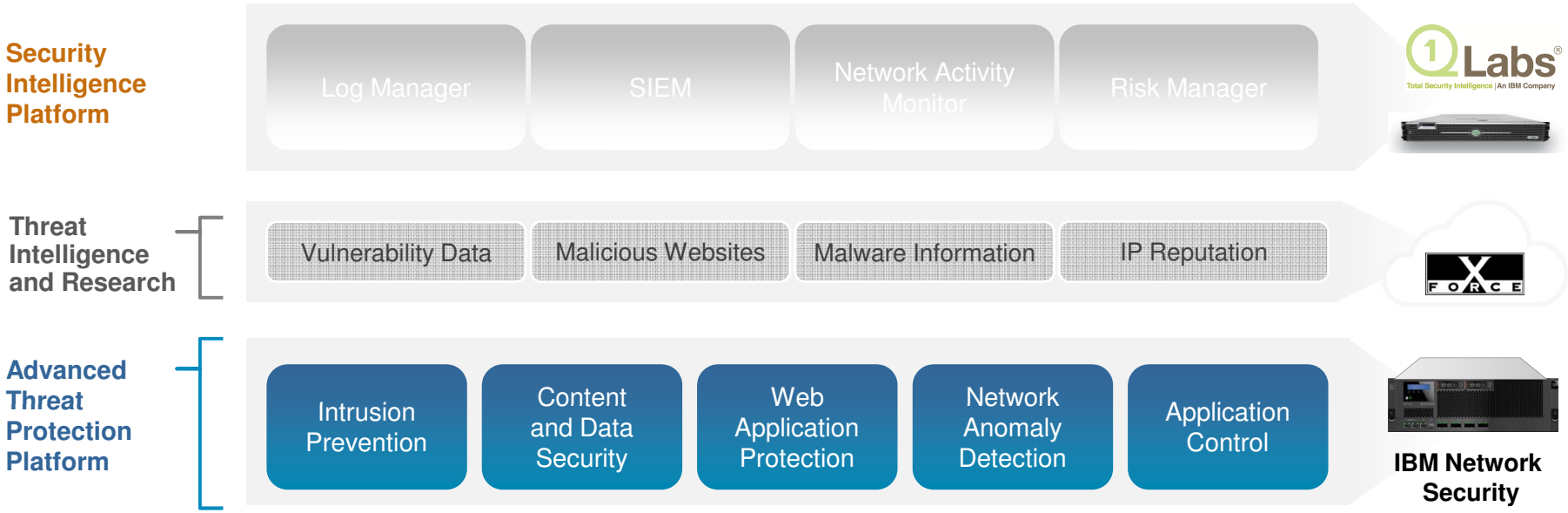
IBM Security Network Protection XGS 5000

Proven Security | **Ultimate Visibility** | **Complete Control**

Protection for Networks, Applications and Endpoints



Part of 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

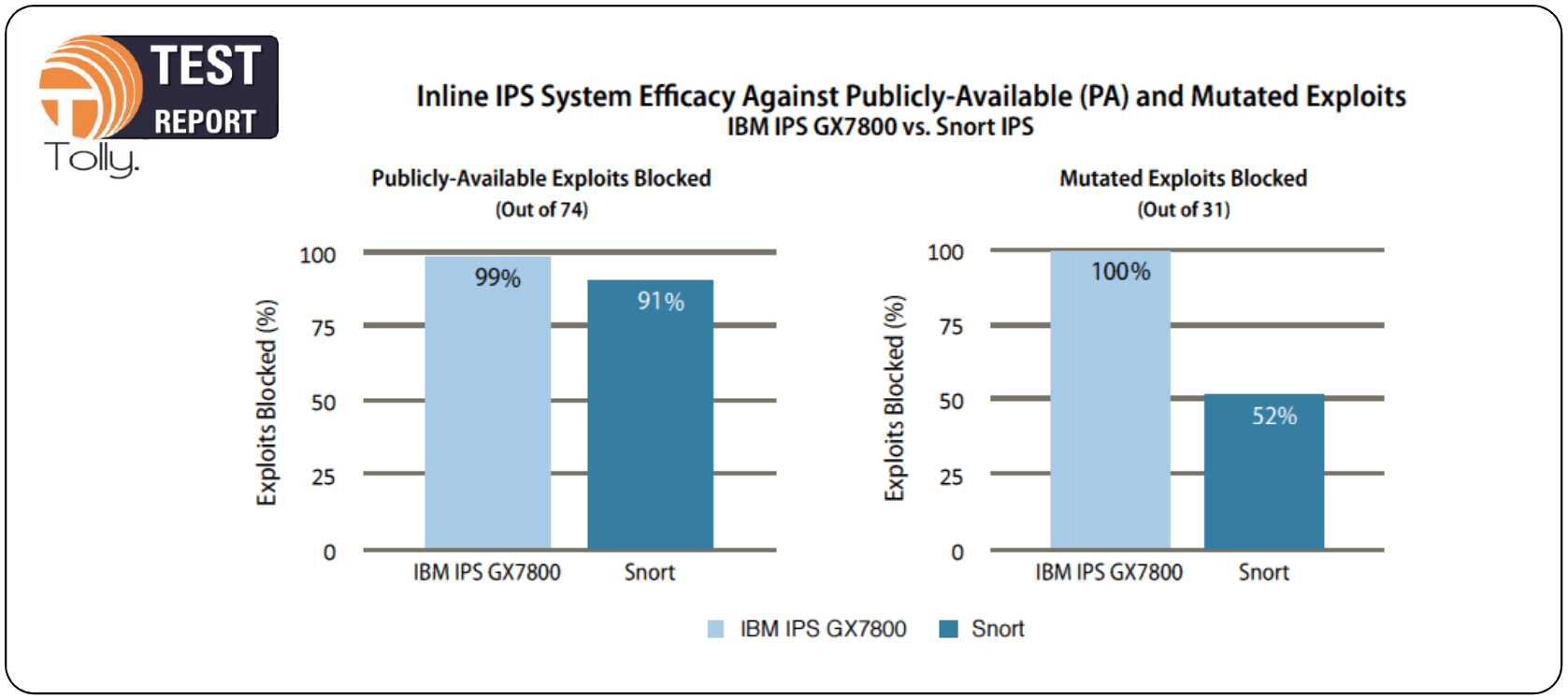
Tight integration between the Advanced Threat Protection Platform and QRadar Security Intelligence platform to provide unique and meaningful ways to detect, investigate and remediate threats

IBM Network IPS Ranked #1 in InformationWeek Report

http://reports.informationweek.com/abstract/21/8919/security/it-pro-ranking-ips-and-ids.html

"IBM, which acquired IPS vendor ISS in 2006, earned a first-place rating for both overall performance and technology-specific features."

IBM Network IPS Beats Signature-based IPS in 3rd Party Testing



- **Delivers superior protection from evolving threats with high levels of performance**
- **Stops 99% of tested, publicly available attacks**
- **Is nearly twice as effective as Snort at stopping "mutated" attacks**
- **Protects streams of 100% HTTP traffic at speeds of 20 Gbps and mixed traffic loads of 35 Gbps+**

Source: Tolly, October 2012

IBM Intrusion Prevention Solution Case Studies

EXA Corporation creates a secure and resilient private cloud

EXA has been working on a project to integrate various servers distributed across Japan. It also has been creating a hybrid cloud environment that combines external data centers and public cloud services. In this initiative, IBM Security Virtual Server Protection for VMware V1.0 and IBM Tivoli® Federated Identity Manager have been selected as vital elements to secure this cloud environment.

Addressing School System Security Challenges

"We're using IBM® network IPSs [IBM Security Network Intrusion Prevention System] at our borders of the hosting platform," says Polkinghorne. "We're using the host IPS agents on high-risk servers, and all that feeds back to a central site protector system, which is collecting the information, and doing reporting and log correlation. It's all automatic. When it picks something up, it'll sort of look and check your rule system. And if we've defined it as block this, then it'll go and block it. So when we see these attacks coming in, it'll shut them down automatically."

ibm.com/security
smartersecurity.nl