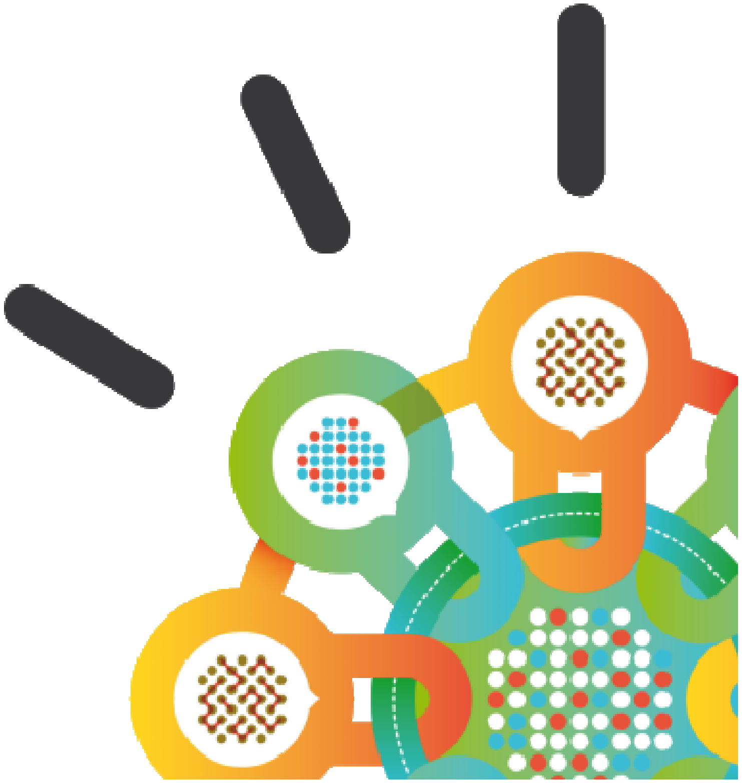
Security Intelligence.
Think Integrated.

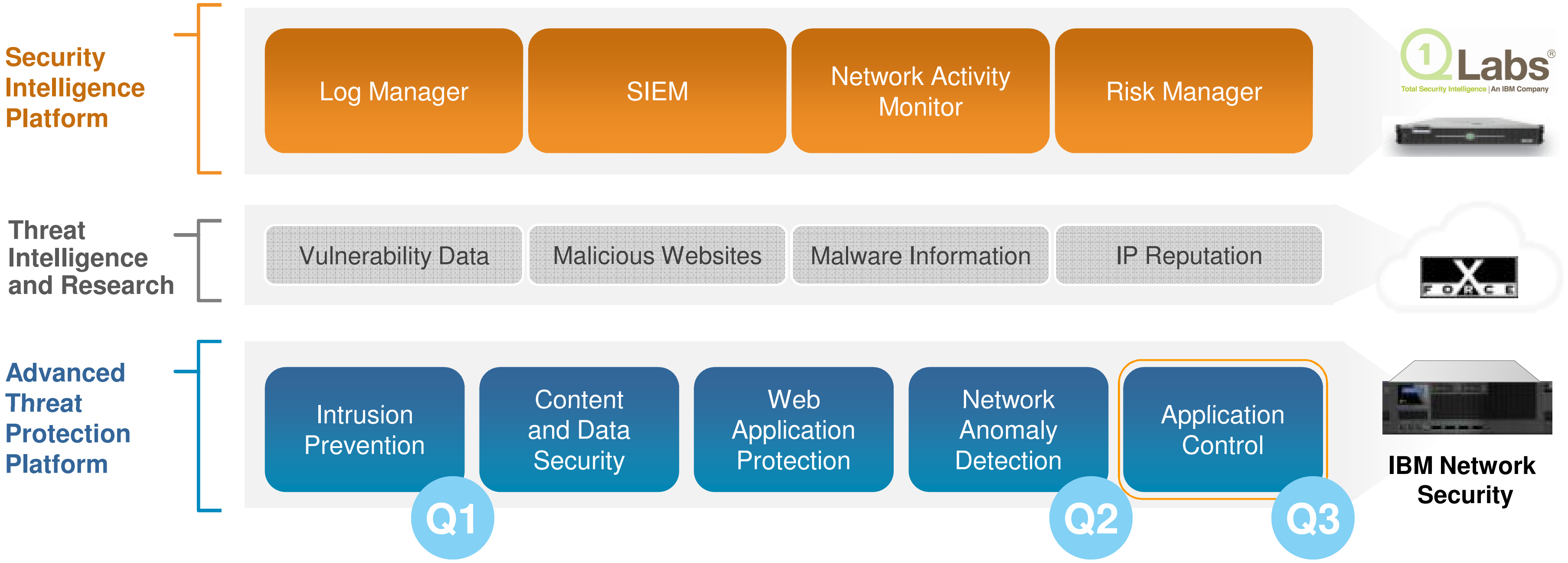
Introducing IBM’s Advanced Threat Protection Platform

Introducing IBM’s Extensible Approach to Threat Prevention

Paul Kaspian
Senior Product Marketing Manager
IBM Security Systems



The Advanced Threat Protection Platform



Security Intelligence Platform

Log Manager | SIEM | Network Activity Monitor | Risk Manager

Threat Intelligence and Research

Vulnerability Data | Malicious Websites | Malware Information | IP Reputation

Advanced Threat Protection Platform

Intrusion Prevention | Content and Data Security | Web Application Protection | Network Anomaly Detection | Application Control

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

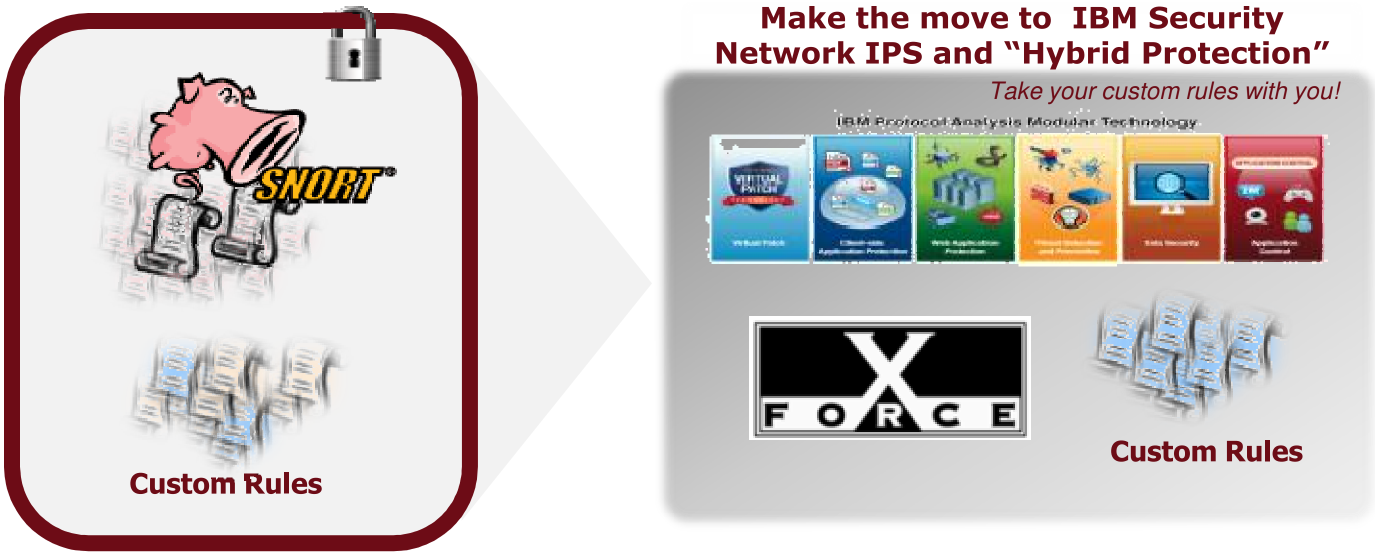
Increased coverage of world-wide threat intelligence harvested by X-Force and the consumption of this data to make smarter and more accurate security decisions across the IBM portfolio

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

Q1 2012: The Introduction of Hybrid Protection

- Simplify your IPS strategy and deployment by migrating your custom SNORT rules to IBM Security Network IPS appliances
- Hybrid protection combines market leading X-Force Protocol Analysis with the ability to create and import custom SNORT rules
- Proven protection beyond traditional IPS including protection from advanced threats such as browser attacks, data leakage, and malicious web applications designed to evade most security technologies



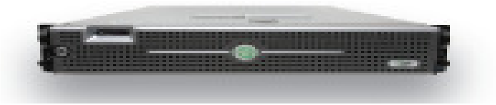
Make the move to IBM Security Network IPS and "Hybrid Protection"

Take your custom rules with you!

Q2 2012: The Introduction of QRadar Network Anomaly Detection

- **QRadar Network Anomaly Detection** is a new QRadar product that brings Increased security insight to IBM Security SiteProtector and IBM Security Network IPS
- The addition of QRadar's behavioral analytics and real-time correlation helps better detect and prioritize stealthy attacks

Total Security Intelligence | An IBM Company



Comprehensive Approach

- SiteProtector as core for command & control
- QRadar Network Anomaly Detection for enhanced analytics
- QRadar QFlow and VFlow Collectors provide network awareness via deep packet inspection
- Integrated policy management & workflows within SiteProtector facilitate a rapid response to threat and more proactive visibility

The challenging state of network 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

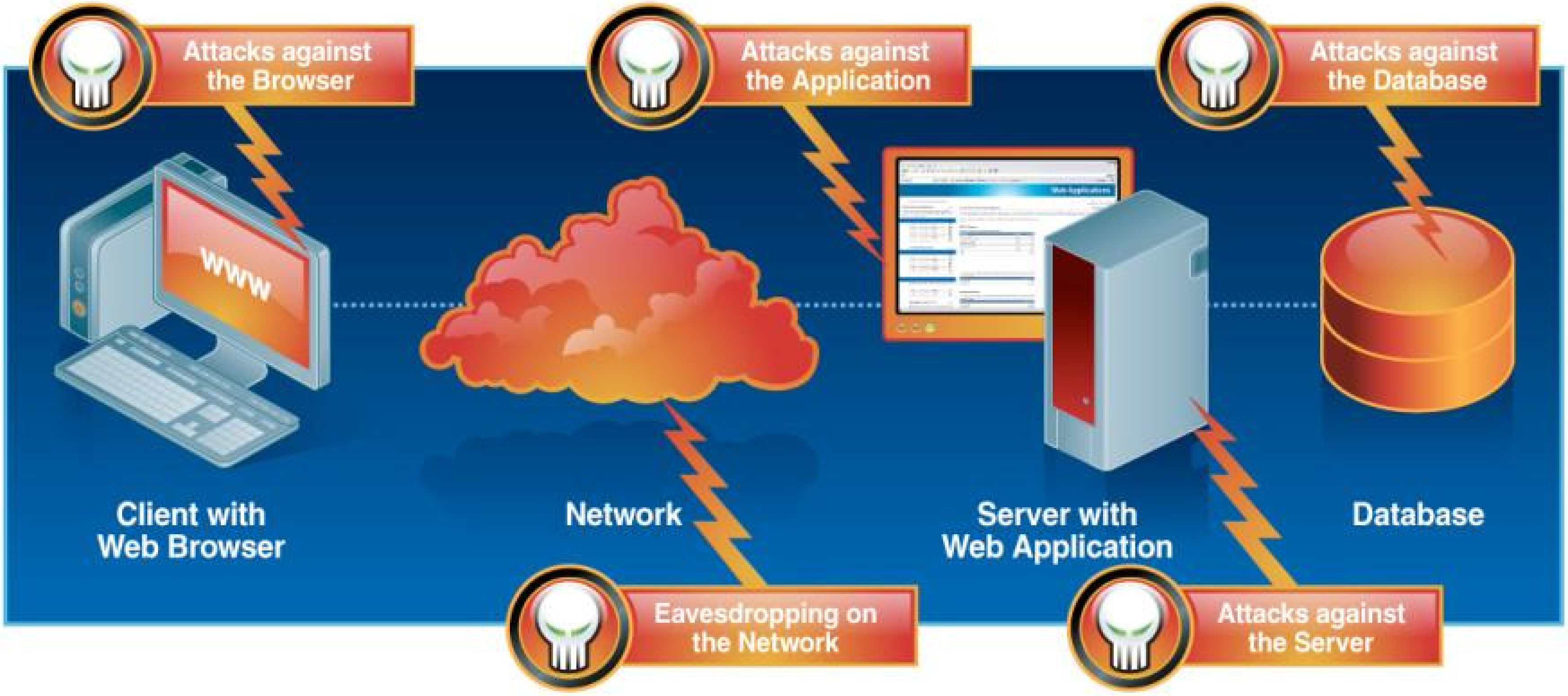
Social media sites present productivity, privacy and security risks including new threat vectors

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

POINT SOLUTIONS

Point solutions are siloed with minimal integration or data sharing

Attack Vectors


Attacks against the Browser
Attacks against the Application
Attacks against the Database
www
Client with Web Browser
Network
Server with Web Application
Database
Eavesdropping on the Network
Attacks against the Server

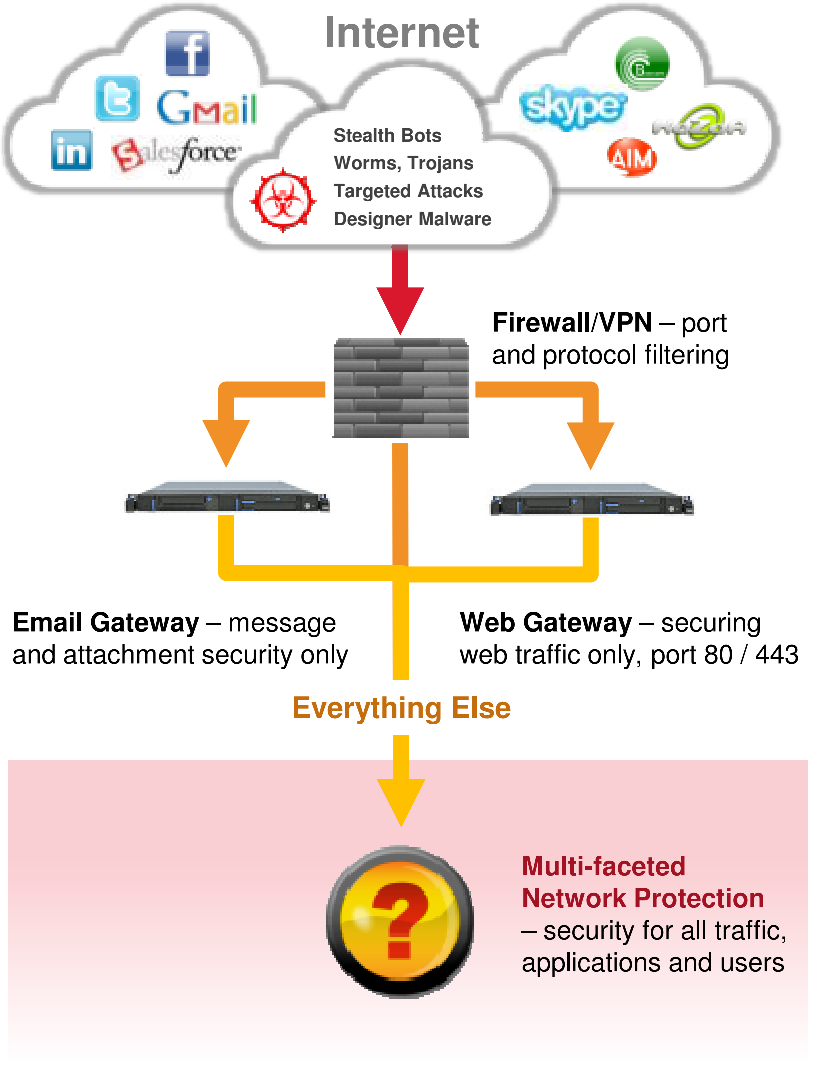
Network Defense: Traditional solutions not up to today's challenges

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



Firewall/VPN – port and protocol filtering

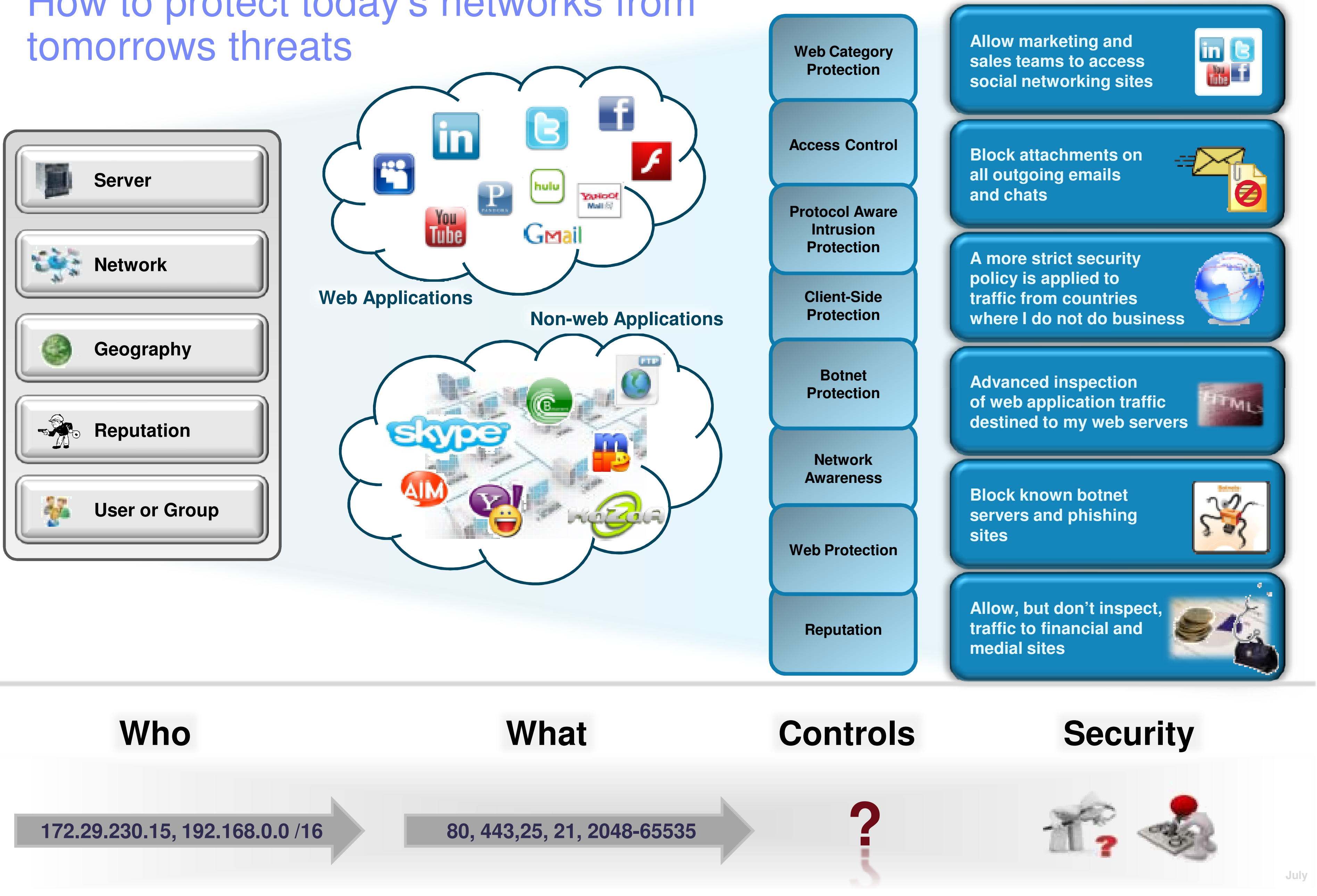
Email Gateway – message and attachment security only

Web Gateway – securing web traffic only, port 80 / 443

Everything Else

Multi-faceted Network Protection – security for all traffic, applications and users

How to protect today's networks from tomorrows threats



Server

Network

Geography

Reputation

User or Group

Web Applications

Non-web Applications

Web Category Protection

Access Control

Protocol Aware Intrusion Protection

Client-Side Protection

Botnet Protection

Network Awareness

Web Protection

Reputation

Allow marketing and sales teams to access social networking sites

Block attachments on all outgoing emails and chats

A more strict security policy is applied to traffic from countries where I do not do business

Advanced inspection of web application traffic destined to my web servers

Block known botnet servers and phishing sites

Allow, but don't inspect, traffic to financial and medial sites

Who

172.29.230.15, 192.168.0.0 /16

What

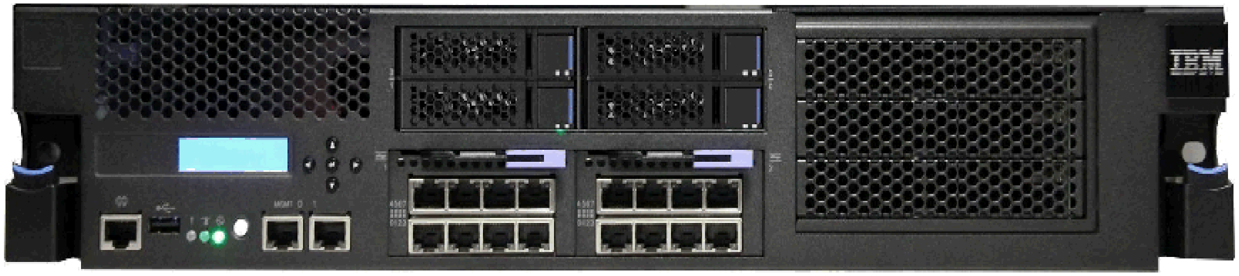
80, 443,25, 21, 2048-65535

Controls

?

Security

Introducing **IBM Security Network Protection XGS 5000**



PROVEN SECURITY

Extensible, 0-Day protection powered by X-Force®

+

NEW WITH XGS

ULTIMATE VISIBILITY

Understand the Who, What and When for all network activity

+

NEW WITH XGS

COMPLETE CONTROL

Ensure appropriate application and network use

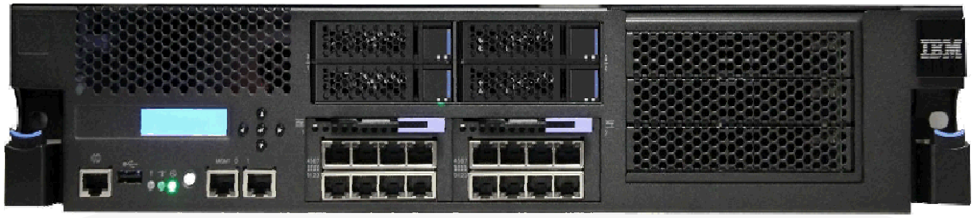
IBM Security Network Protection XGS 5000
builds on the proven security of IBM intrusion prevention solutions by delivering the addition of next generation *visibility* and *control* to help balance security and business requirements

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

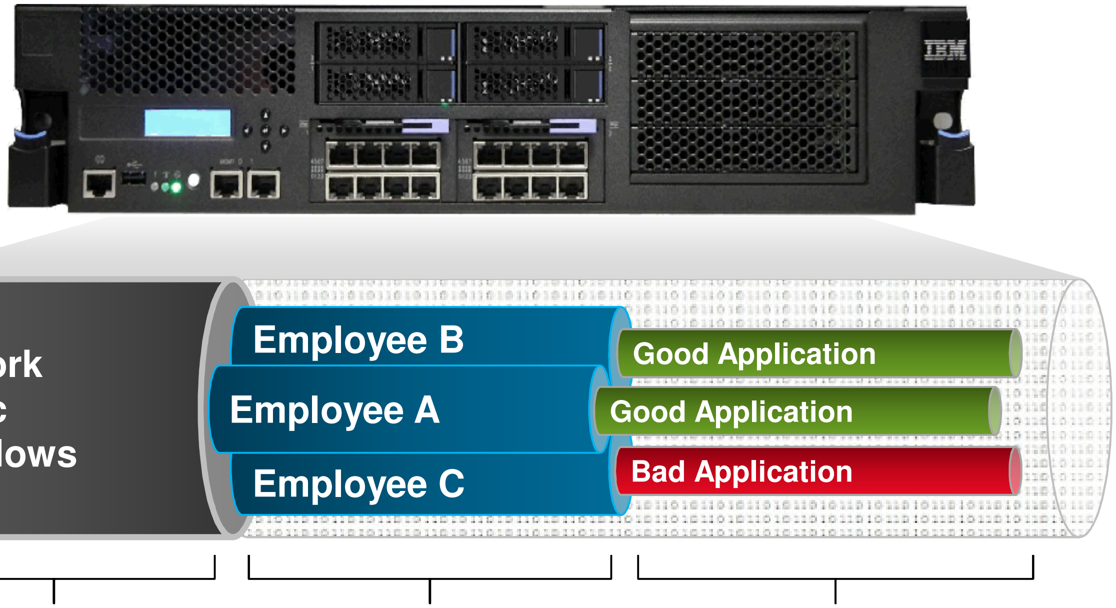
– Specialized engines

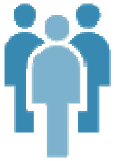
- Exploit Payload Detection
- Web Application Protection
- Content and File Inspection

Ability to protect against the threats of today and tomorrow

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

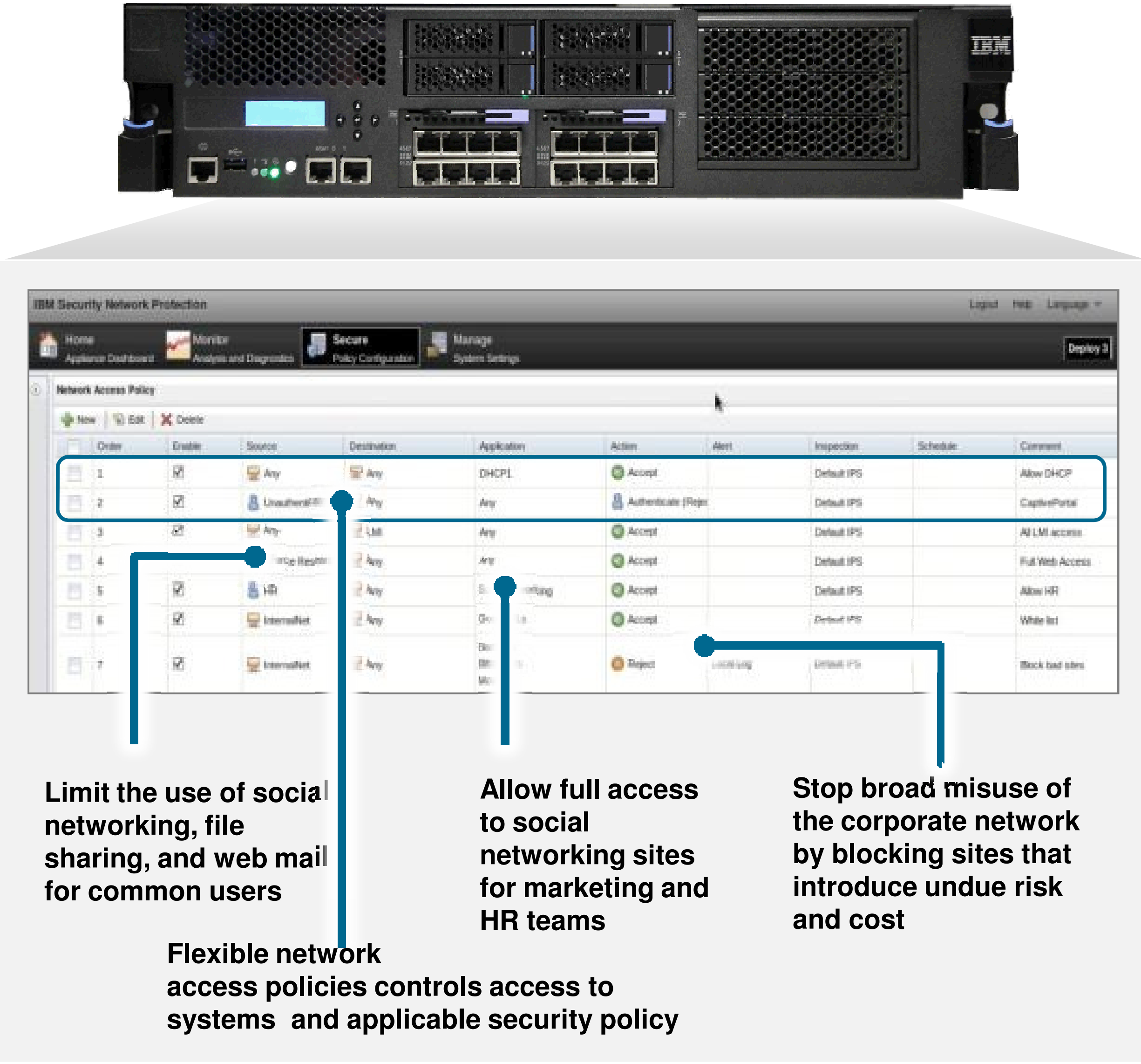
Application Awareness fully classifies network traffic, regardless of address, port , protocol, application, application action or security event

> *“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

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



IBM Security Network Protection

Network Access Policy

☐	Order	Enable	Source	Destination	Application	Action	Alert	Inspection	Schedule	Comment
☐	1	☑	Any	Any	DHCP1	Accept		Default IPS		Allow DHCP
☐	2	☑	Unauthenti[illegible]	Any	Any	Authenticate (Rejec		Default IPS		CaptivePortal
☐	3	☑	Any	LMI	Any	Accept		Default IPS		All LMI access
☐	4		[illegible]e Res[illegible]	Any	Any	Accept		Default IPS		Full Web Access
☐	5	☑	HR	Any	S[illegible]rking	Accept		Default IPS		Allow HR
☐	6	☑	InternalNet	Any	Go[illegible] L[illegible]	Accept		Default IPS		White list
☐	7	☑	InternalNet	Any	Bo[illegible] Bit[illegible] Mo[illegible]	Reject	Local Log	Default IPS		Block bad sites

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

> *"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*

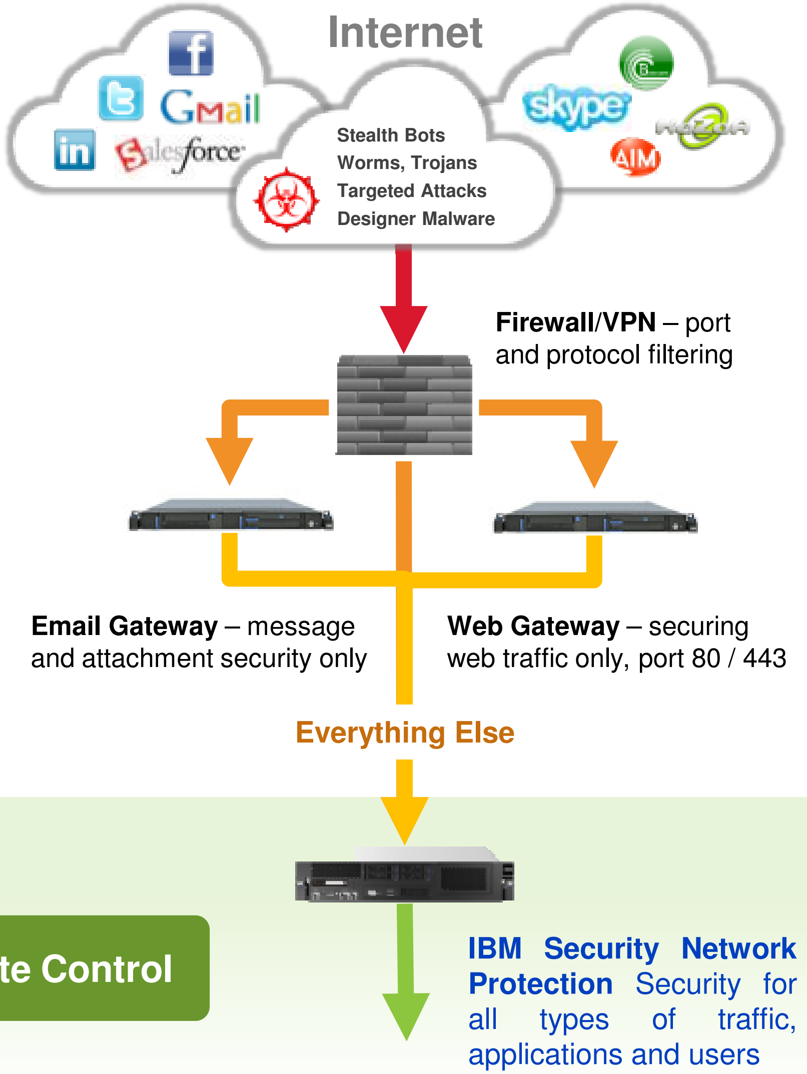
The XGS 5000: The Best Solution for Threat Prevention

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



Internet

Stealth Bots
Worms, Trojans
Targeted Attacks
Designer Malware

Firewall/VPN – port and protocol filtering

Email Gateway – message and attachment security only

Web Gateway – securing web traffic only, port 80 / 443

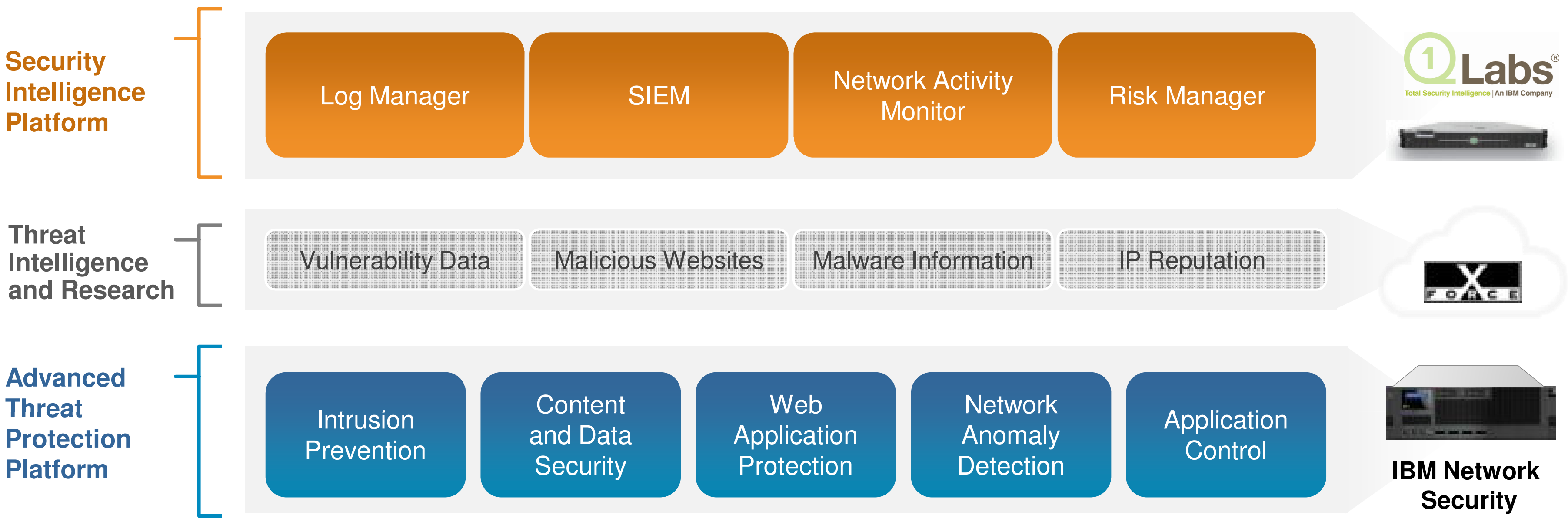
Everything Else

IBM Security Network Protection Security for all types of traffic, applications and users

IBM Security Network Protection XGS 5000

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

Part of IBM's vision for Advanced Threat Protection



Security Intelligence Platform

Log Manager

SIEM

Network Activity Monitor

Risk Manager

Threat Intelligence and Research

Vulnerability Data

Malicious Websites

Malware Information

IP Reputation

Advanced Threat Protection Platform

Intrusion Prevention

Content and Data Security

Web Application Protection

Network Anomaly Detection

Application Control

IBM Network Security

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.com/security