7 Kasım 2012 - Çırağan Palace Kempinski

IBM Connected 2012 Istanbul

Learn. Collaborate. Innovate.

NEW GENERATION INTRUSION PREVENTION SYSTEMS

Hakan TURGUT
IBM Security Systems Bölge Yöneticisi
Türkiye, Doğu Avrupa, Rusya ve CIS Ülkeleri

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

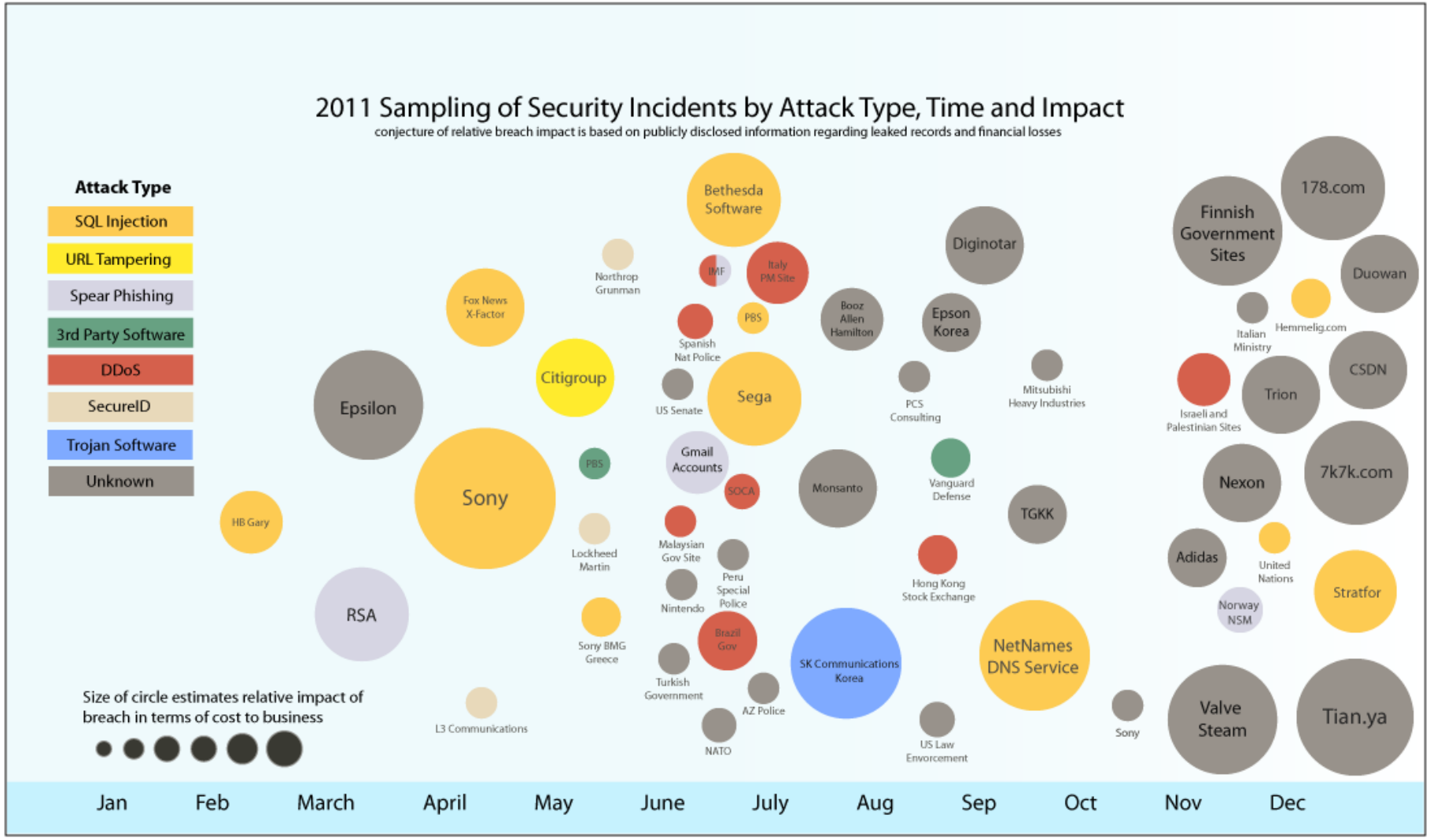
Social media sites present productivity, privacy and security risks including new threat vectors

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

POINT SOLUTIONS

Point solutions are siloed with minimal integration or data sharing

Proof points: Targeted attacks shake businesses & governments



Source: 2011 Year-End X-Force Trend and Risk Report.

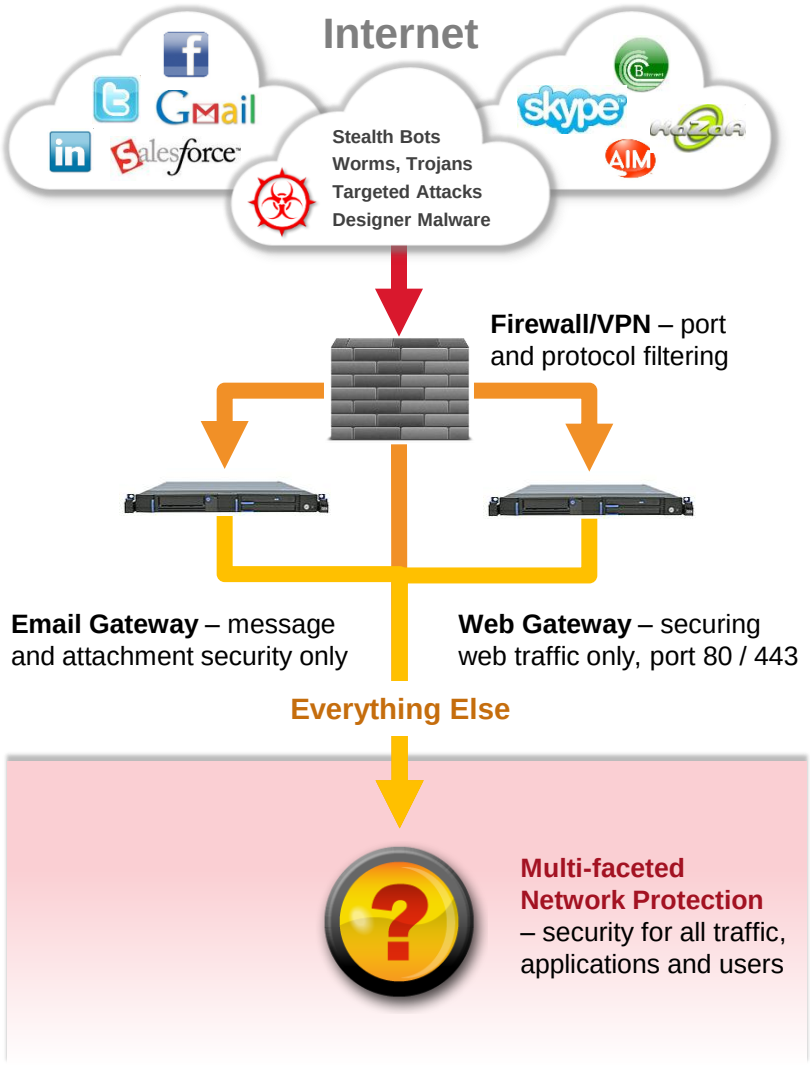
Network Defense: Traditional solutions not up to today's challenges

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



The Need to Understand the Who, What, and When

- Server
- Network
- Geography
- Reputation
- User or Group

- 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

Where do you stand?

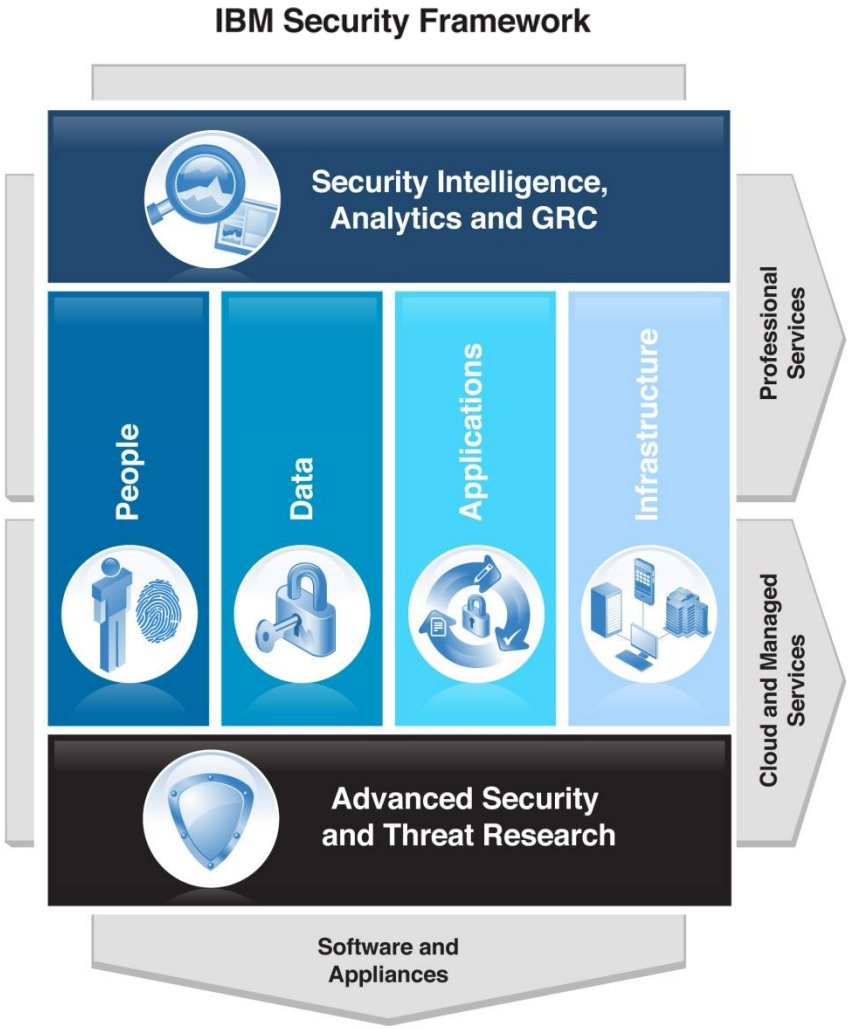
Compliance	**1. Have you assessed your security risks?**
	2. Do you leverage an industry standard to measure security effectiveness?
	3. Do you have a common set of controls for compliance?
	4. Are you retaining critical records and logs for security forensics?
Internal and External Threats	**5. Do you leverage the latest research on threats?**
	6. Who has access to your data, applications and systems?
	7. How do you handle incident response and disaster recovery?
	8. Have you classified and encrypted sensitive data?
	9. Do you know what authorized users are doing with your data?
	10. Is security built into new initiatives, such as cloud computing?

IBM Can Help – the IBM Security Framework

IBM Security Systems

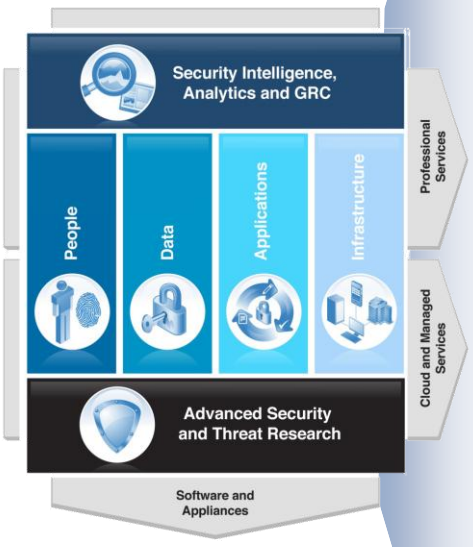
- Only vendor in the market with end-to-end coverage of the security foundation
- $1.8B investment in innovative technologies
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise



IBM Security – Delivering Intelligence, Integration and Expertise

= IBM addresses



- Security Governance, Risk & Compliance
- SIEM (Security Intelligence, Enterprise Compliance)
- Identity and Access Management
- Identity Management
- Access Management
- Data Security
- Data Loss Prevention
- Encryption and Key Lifecycle Management
- Messaging Security
- E-mail Security
- Database Monitoring and Protection
- Data Masking
- Application Security
- App Vulnerability Scanning
- Web Application Firewall
- App Source Code Scanning
- Web / URL Filtering
- Access and Entitlement Management
- SOA Security
- Infrastructure Security
- Vulnerability Assessment
- Mainframe Security
- Threat Assessment
- Web/URL Filtering
- Intrusion Prevention System
- Firewall, IDS/IPS, MFS, End Point Mgmt.
- Security Event Management
- Virtual System Security

- ✓ X-Force Research & Development
- ✓ T.J. Watson & 8 other security research centers
- ✓ IBM Kassel content security team
- ✓ Managed Security Services
- ✓ 2,000+ security engineers in 11 centers

Who is Attacking Our Networks?

Attacker Types and Techniques 2011 H1

Off-the-Shelf tools and techniques

- Indiscriminate
- Lack sophisticated technical skills
- Use tool chest of exploit and malware kits
- Botnet builders
- Financially motivated malware activity
- Spam and DoS

Sophisticated

- Cyberwar

Broad

- Financially motivated targeted hacks
- DDoS attacks
- LulzSec and Anonymous (hacktivists)

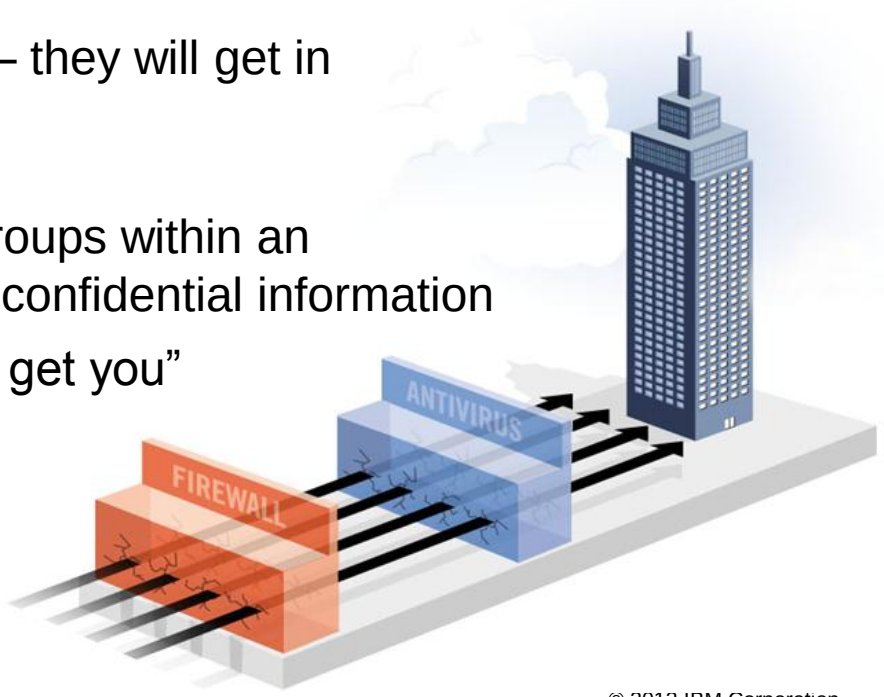
- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulns
- Unprecedented attack techniques

Targeted

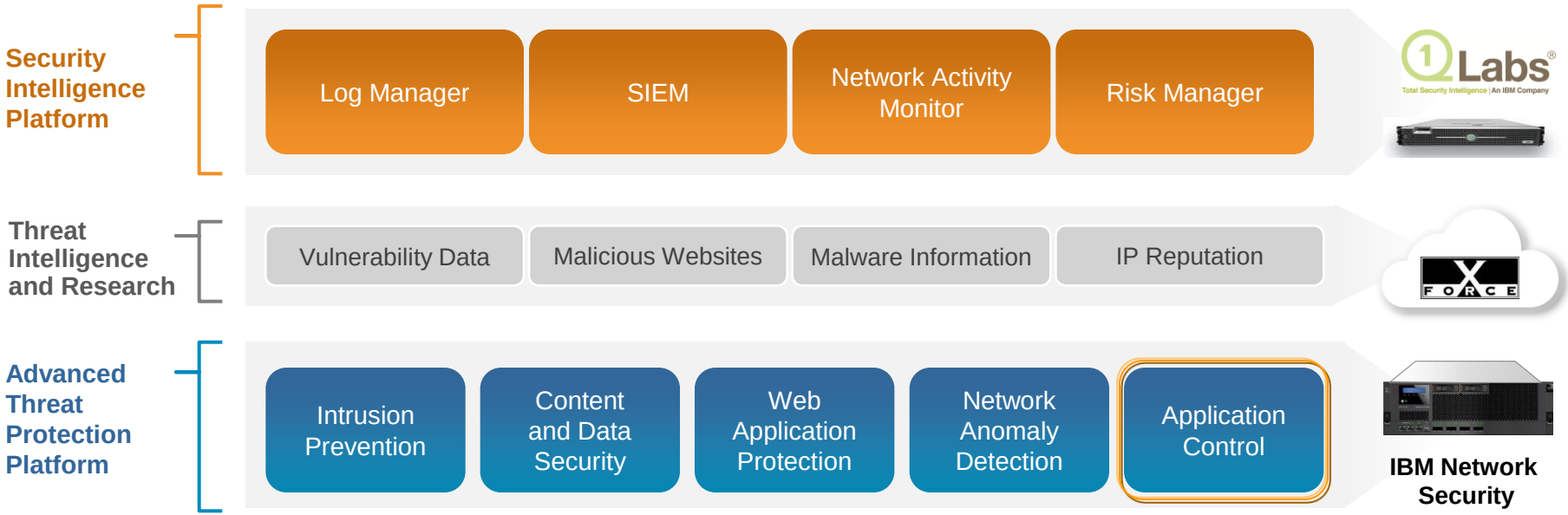
Source: IBM X-Force® Research and Development

Advanced Persistent Threats – Evolving Sophistication

1. **Advanced**
   - Exploiting unreported (zero-day) vulnerabilities
   - Advanced, custom malware is not detected by antivirus products
   - Coordinated, well researched attacks using multiple vectors
2. **Persistent**
   - Attacks last for months or years
   - Attackers are dedicated to the target – they will get in
3. **Threat**
   - Targeted at specific individuals and groups within an organization; aimed at compromising confidential information
   - Not random attacks – they are “out to get you”
4. Responding is different too:
   Watch, **Wait**, **Plan** … and call the FBI



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

Introducing **IBM Security Network Protection XGS 5000**

	NEW WITH XGS	NEW WITH XGS
PROVEN SECURITY	**ULTIMATE VISIBILITY**	**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

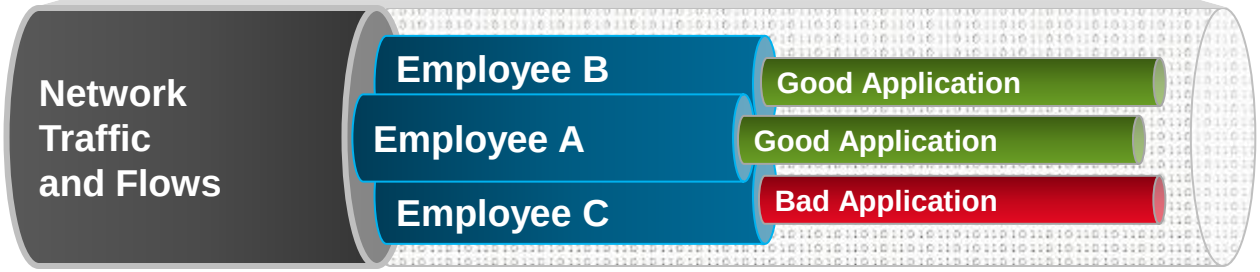
- Vulnerability Modeling & Algorithms
- Stateful Packet Inspection
- Port Variability
- Port Assignment
- Port Following
- Protocol Tunneling
- Application Layer Pre-processing
- Shellcode Heuristics
- Context Field Analysis
- RFC Compliance
- Statistical Analysis
- TCP Reassembly & Flow Reassembly
- 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

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

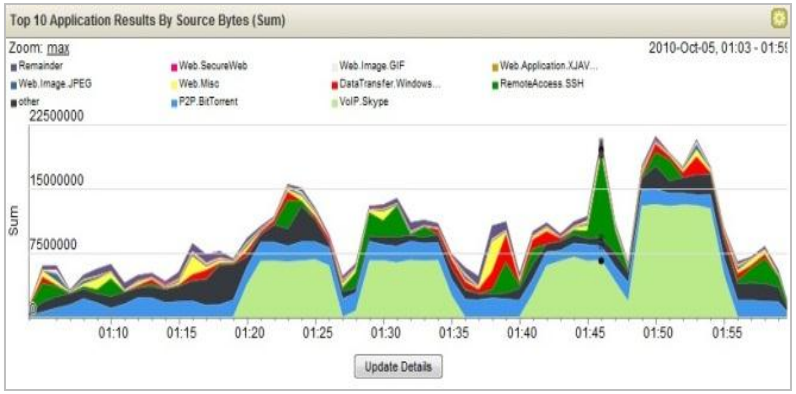
QRadar Network Anomaly Detection

- **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



IBM Security Network IPS: Core Threat Protection

Addressing Key Challenges

- Balance security and performance of critical applications
- Address changing threats with limited resources and budget
- Reduce cost and complexity of security infrastructure
- Larger organizations require security at network core

Core Capabilities

Exceeding traditional network IPS to deliver comprehensive security including:

- Web application protection
- Protection from client-side attacks
- Data Loss Prevention (DLP)
- Application control
- Virtual Patch technology

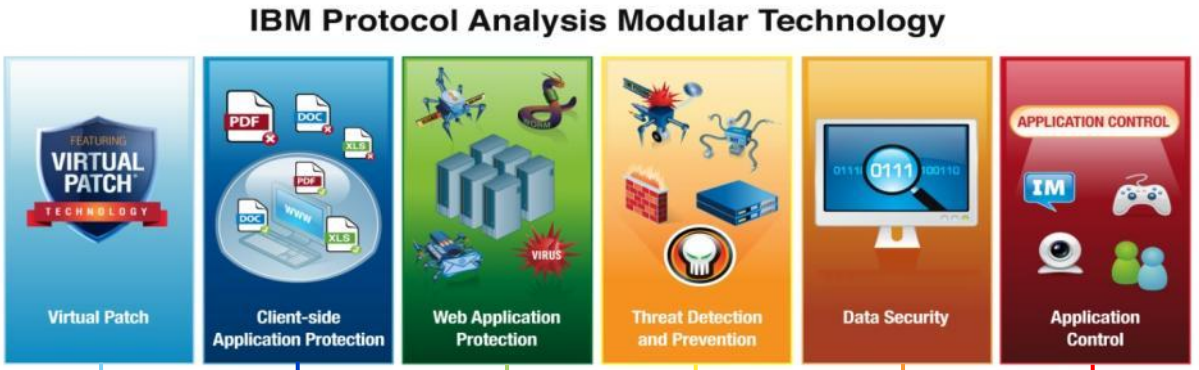
Unmatched Performance delivering up to 20Gbps+ of throughput and 10GbE connectivity without compromising breadth and depth of security

Evolving protection powered by world renowned X-Force threat research to stay “ahead of the threat”

Reduced cost and complexity through consolidation of point solutions and integrations with other security tools

The Outcome: Extensible Protection with Protocol Analysis Module

Intrusion prevention just got smarter with extensible protection backed by the power of X-Force



Virtual Patch

What It Does:
Shields vulnerabilities from 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 2009, 52% of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.

Client-Side Application Protection

What It Does:
Protects end users against attacks targeting applications used everyday such as Microsoft Office, Adobe PDF, Multimedia files and
Web browsers.

Why Important:
At the end of 2009, vulnerabilities, which affect personal computers, represent the second-largest category of vulnerability disclosures and represent about a fifth of all vulnerability disclosures.

Web Application Protection

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).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Threat Detection & Prevention

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 Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Data Security

What It Does:
Monitors and identifies 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.

Application Control

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 tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

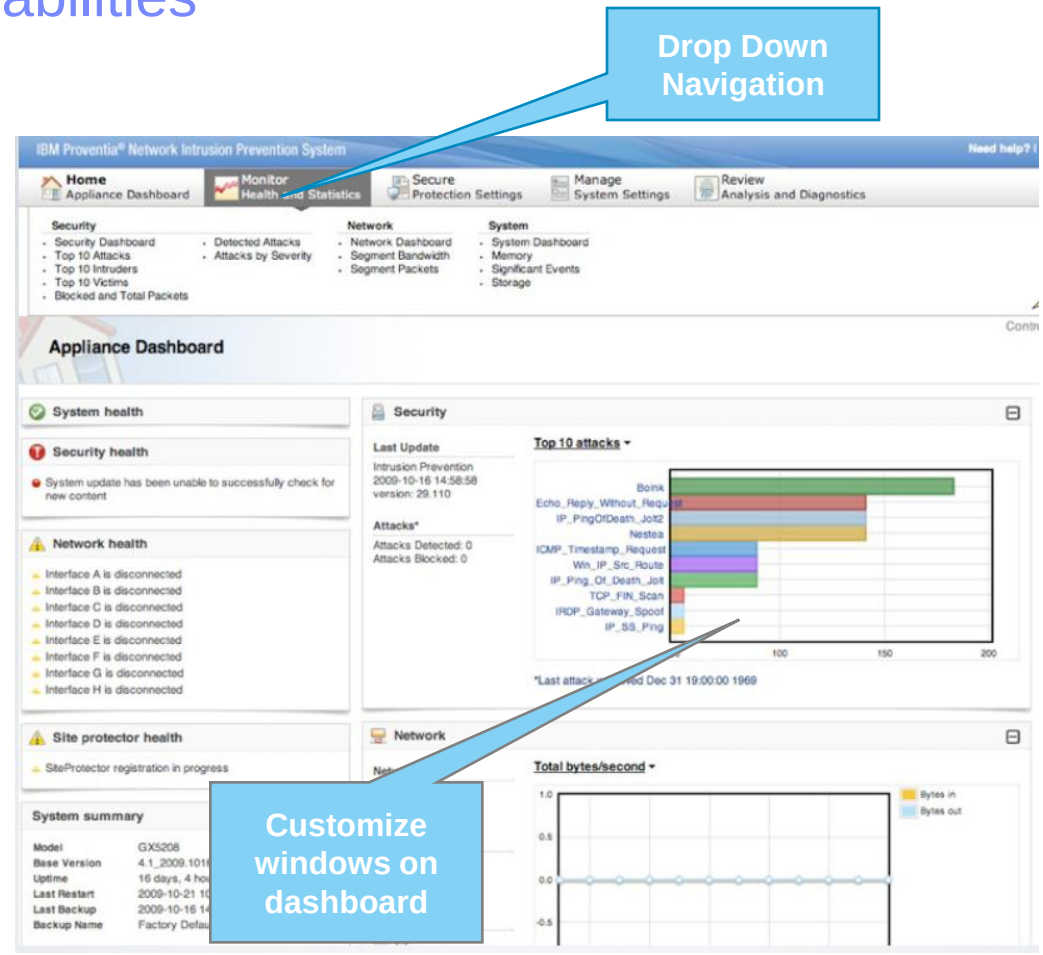
Network IPS Management Capabilities

Browser-based local management interface (LMI)

- Single view of health, protection & network statistics from a customizable dashboard
- Simplified view of data security and web application protection policies
- Patch management statistics and log evidence

Central management through IBM Security SiteProtector™ System

- Simple, powerful command and control
- Robust reporting, customized event viewing and event correlation
- Comprehensive alerting and response options
- Highly scalable to accommodate hundreds of IBM Security Network IPS appliances

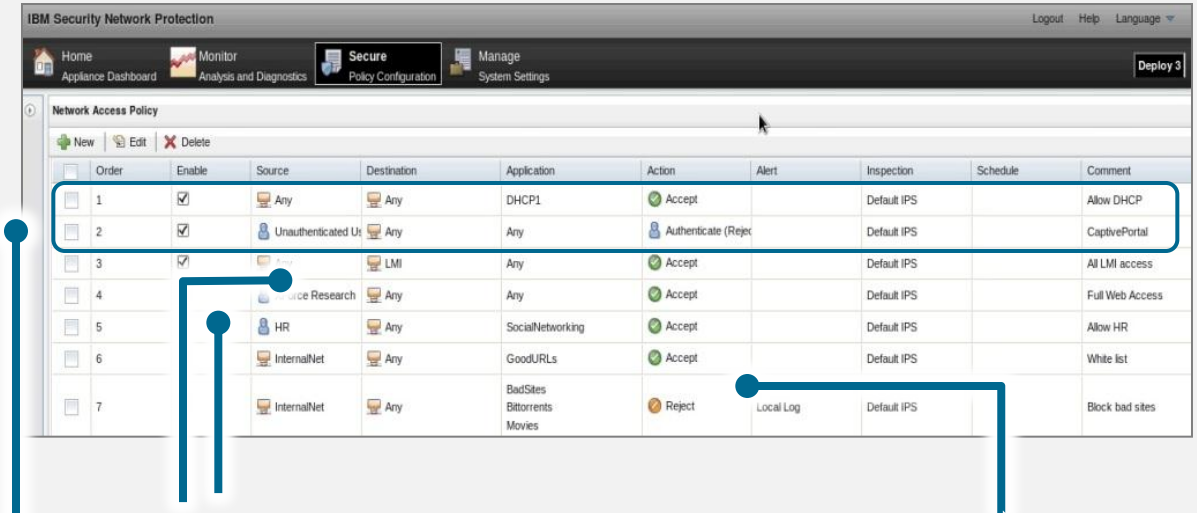


Complete Control: Overcoming a Simple Block-Only Approach

- Control network access 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."

– SecureDevice



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 control policies

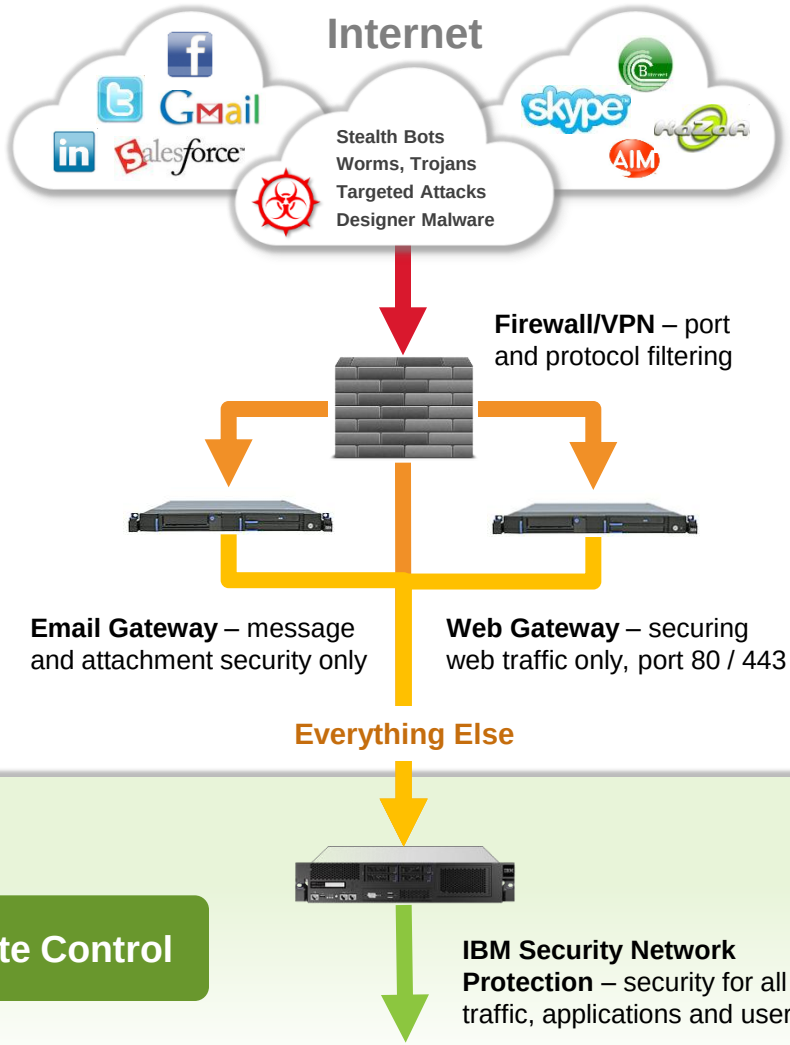
The XGS 5000: A Critical Part of Your Network Defense

Better than a Next Generation Firewall

- 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

Better than a Signature-based 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**

IBM X-Force® Threat Information Center

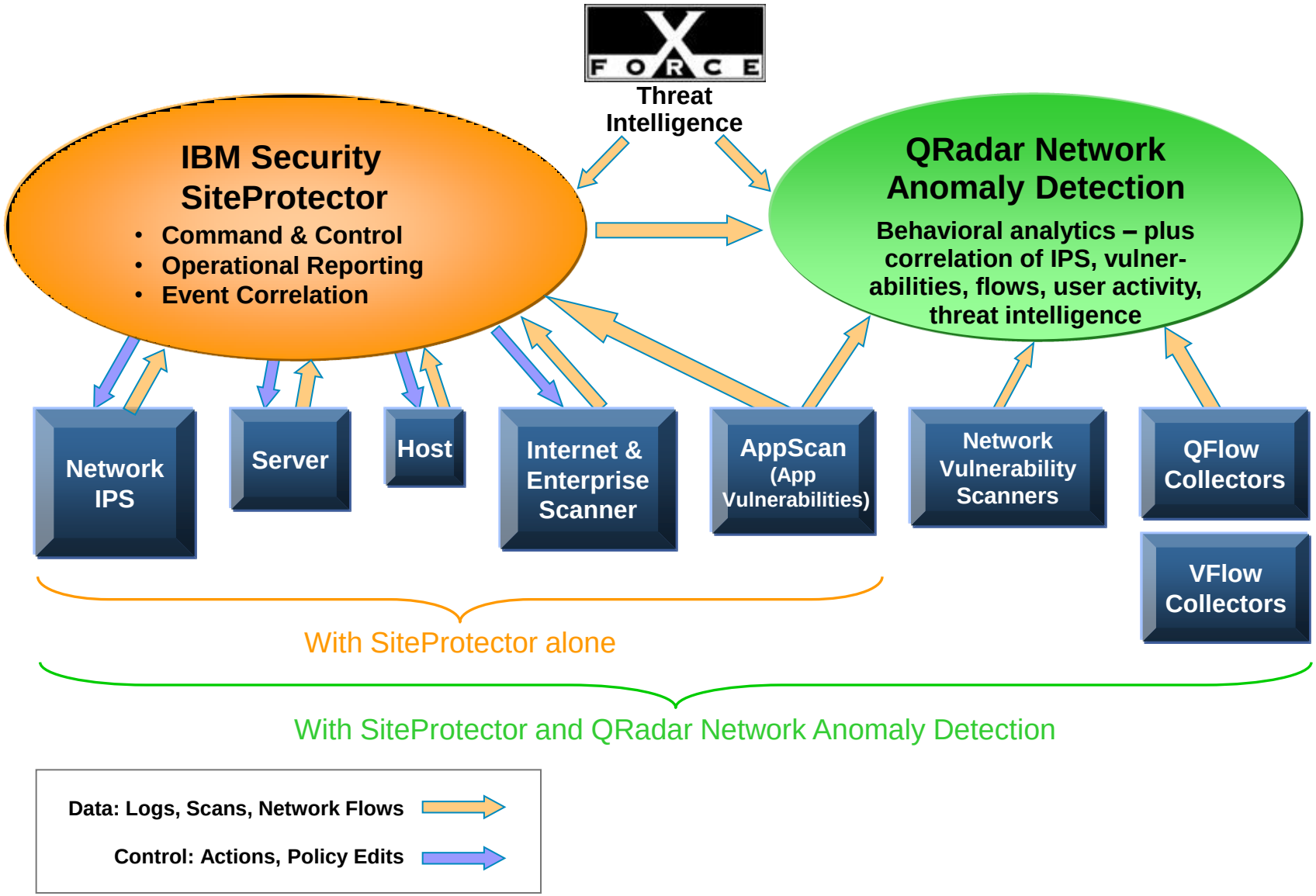
Real-time Security Overview w/ IP Reputation Correlation

Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

Enhanced Detection through Anomaly Detection, Correlation & Flow Analysis



Key Benefits

1) Gain superior network visibility

- Delivers deep insight into network, user and application behavior
- Enhances situational awareness to improve an organization's overall security posture

2) Reduce the time-to-detection and business impact of security breaches

- Helps detect threats that might otherwise be missed for months or years
- Aids in limiting the impact of breaches and protecting sensitive information

3) Investigate and resolve security incidents faster and more thoroughly

- Enables security professionals to perform forensic investigations more quickly & accurately
- Helps to quickly assess the scope of any breach including required mitigation

4) Reduce manual effort of security operations and compliance reporting

- Helps distinguish true threats from false positives, saving significant time
- Scores each incident and intelligently presents data in an easy-to-use way
- Automates many data gathering and reporting activities for regulatory compliance

Key Capabilities

Anomaly detection and network behavioral analysis

- Analyzes network flows, IPS alerts and user activity in real-time, monitoring for and alerting on any observed activity that falls outside of “normal” behavior
- Determines baseline levels of activity along virtually any dimension of interest – offering a high degree of granularity and flexibility – and then triggers alerts as appropriate
- Learning period and trigger period can both be set through straightforward parameters
- Anomaly detection capabilities can account for both seasonality and growth trends

Real-time correlation of IPS, network traffic, vulnerability, user activity data, and threat intelligence

- Correlates an extensive set of data to identify and prioritize threats
- Incorporates IBM X-Force IP Reputation Data Feed, providing insight into suspect entities on the Internet based on knowledge of 15 billion IP addresses and images

Key Capabilities (continued)

Network flow analysis for deep visibility and insight

- Network flow analysis of NetFlow and similar data, as well as QFlow data collected by QRadar QFlow and VFlow Collectors (optional add-on products)
- QFlow data includes Layer 7 application content captured for detection and forensic purposes; can be correlated with IPS alerts, user activity and vulnerabilities
- With deep packet inspection capabilities, QFlow also provides visibility into threats such as traffic disguised as other applications

Automated dashboards and reports

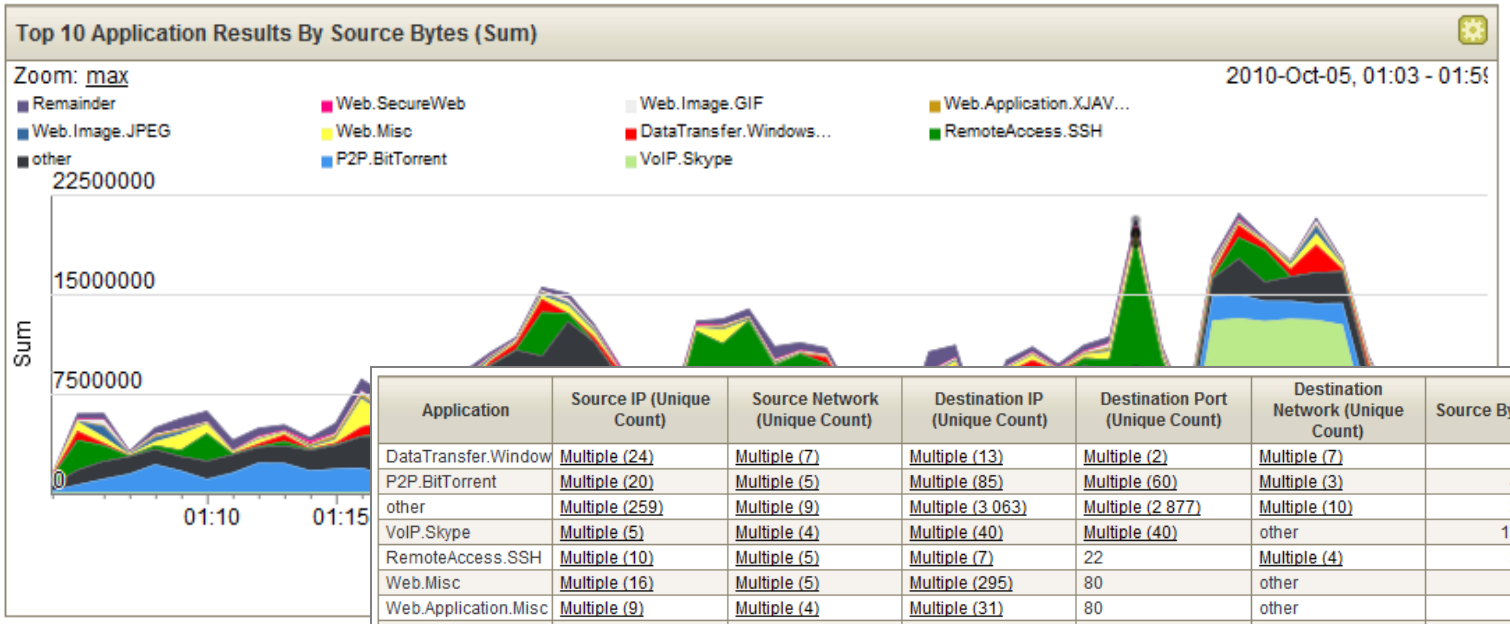
- Numerous report templates and dashboards delivered out-of-the-box; easily create custom reports & dashboards or modify existing report & dashboards
- Reports can be run ad hoc, or automatically run hourly, daily, weekly, etc.

Workflow management to track threats and ensure resolution

- Creates and manages offenses (incidents) which contain a complete summarization of the problem and all contextual data; integrates with external systems
- Mark offenses for follow up, close offenses, receive email notification when offenses are updated, and more

Flow Analytics and Anomaly Detection

- **Network traffic doesn't lie.** Attackers can stop logging and erase their tracks, but can't cut off the network (flow data)
- Helps detect day-zero attacks that have no signature
- Detects anomalies that might otherwise get missed
- Provides definitive evidence of attack
- Enables visibility into all attacker communications

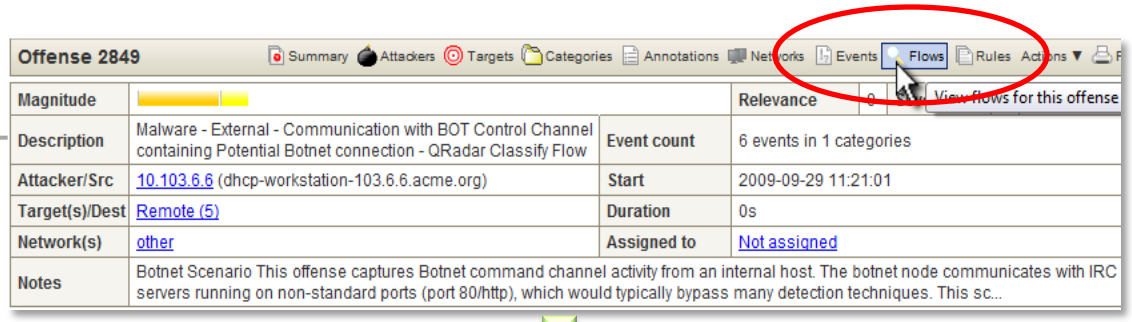


Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204

Example: Detecting Stealthy Threats

Potential Botnet Detected?

This is as far as many solutions can go



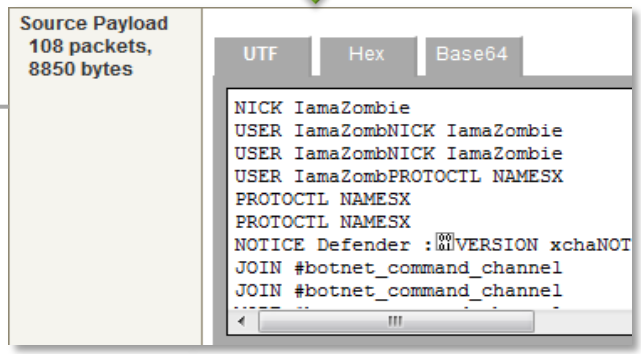
IRC on port 80?

IBM Security QRadar QFlow detects a covert channel

First Packet Time	Protocol	Source IP	Source Port	Destination IP	Destination Port	Application	ICMP Type/Co	Source Flags
11:19	tcp_ip	10.103.6.6	48667	62.64.54.11	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	50296	192.106.224.13	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	51451	62.181.209.20	80	IRC	N/A	S,P,A
11:19	tcp_ip	10.103.6.6	47961	62.211.73.232	80	IRC	N/A	F,S,P,A

Irrefutable Botnet Communication

Layer 7 flow data contains botnet command control instructions



Application layer flow analysis can detect threats others miss

Example: Complex Threat Detection

Offense 3063 Summary | Attackers | Targets | Categories | Annotations | Networks | Events

Magnitude		Relevance	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Proceeded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan	Event count	1428 events in 3 cate
Attacker/Src	202.153.48.66	Start	2009-09-29 16:05:01
Target(s)/Dest	Local (717)	Duration	1m 32s
Network(s)	Multiple (3)	Assigned to	Not assigned
Notes	Vulnerability Correlation Use Case Illustrates a scenario involving correlation of vulnerability data with I China (202.153.48.66) sweeps a subnet using the Conficker worm exploit (CVE 2008-4250). The first s		

Sounds Nasty…

But how do we know this?

The evidence is a single click away.

Network Scan

Detected by QFlow

Buffer Overflow

Exploit attempt seen by Snort

	Event Name	Source IP	Destination IP	Destination Port	Log Source	Low Level Category
	Network Sweep - QRadar Classify Flow	202.153.48.66	Multiple (716)	445	Flow Classification E	Network Sweep
	NETBIOS-DG SMB v4 srvsvc NetrpPathConon	202.153.48.66	Multiple (8)	445	Snort @ 10.1.1.5	Buffer Overflow

Port	Service	OSVDB ID	Name	Description	Risk / Severity
445	unknown	49243	Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution	Microsoft Windows Server Service contains a flaw that may allow a malicious user to remotely execute arbitrary code. The issue is triggered when a crafted RPC request is handled. It is possible that the flaw may allow remote code execution resulting in a loss of integrity.	3

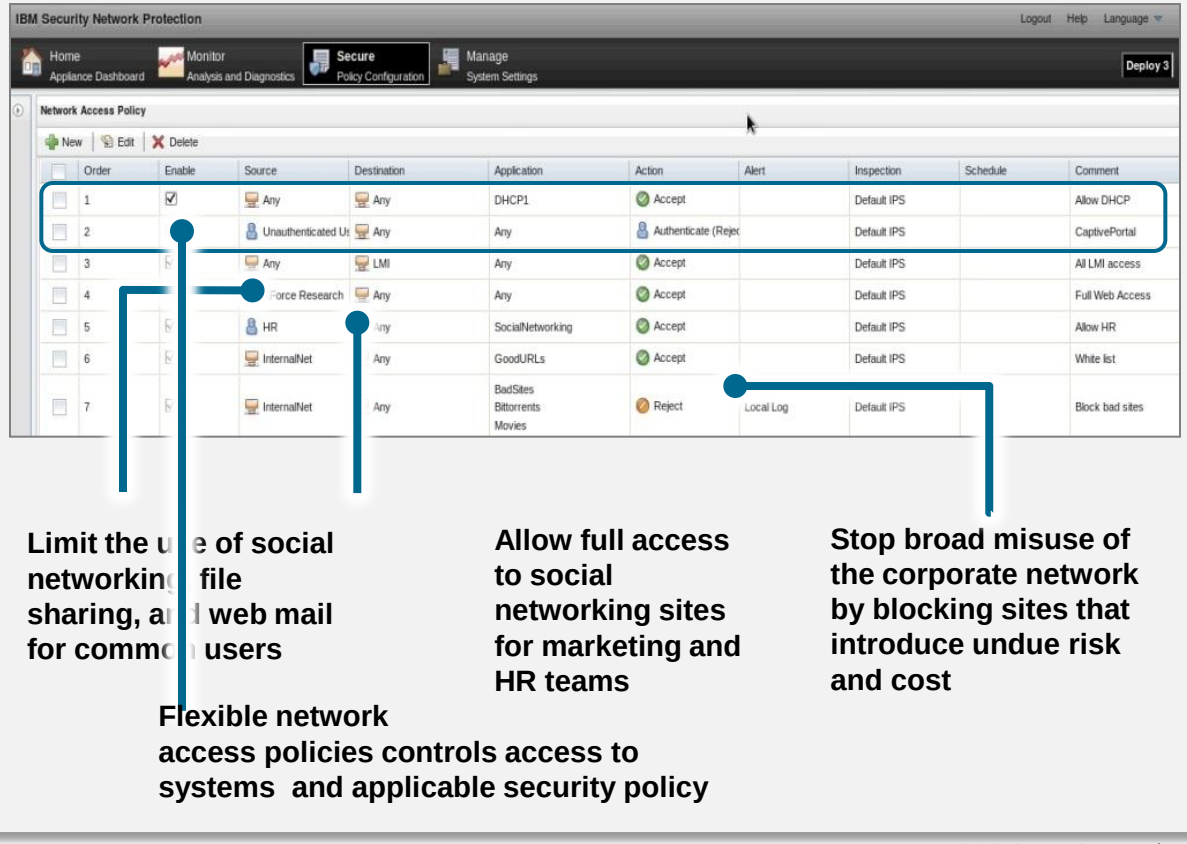
Targeted Host Vulnerable

Detected by Nessus

Total Security Intelligence:
Convergence of Network, Event and Vulnerability data

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

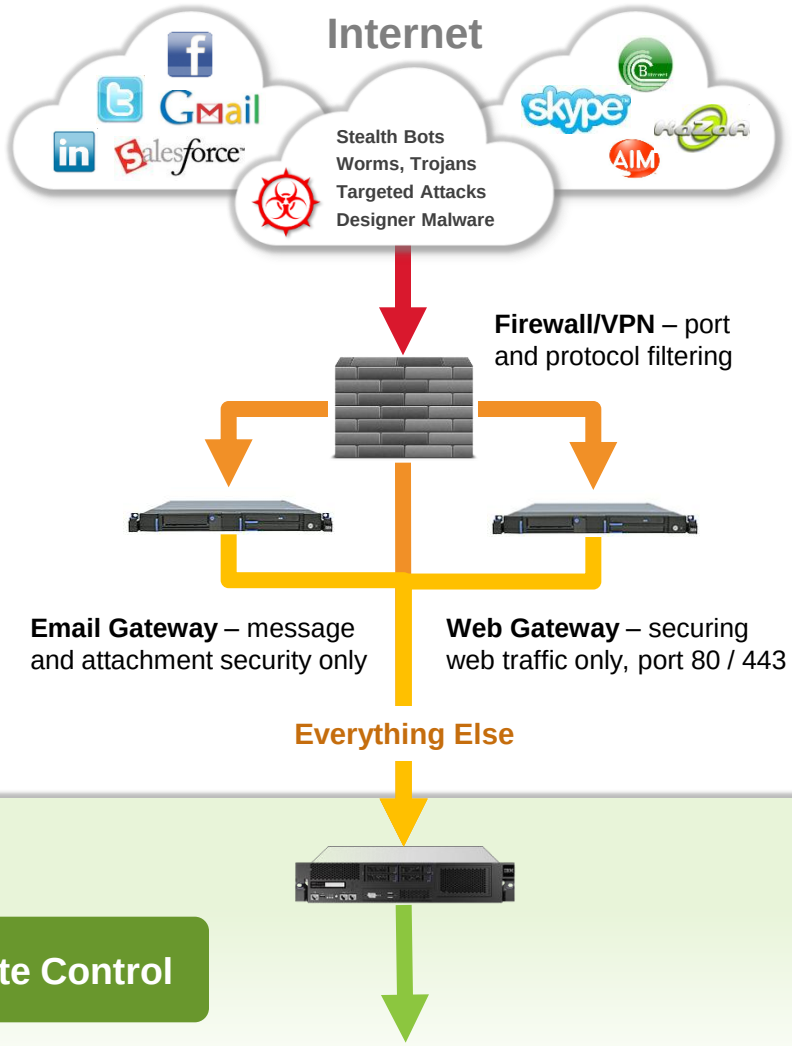
The XGS 5000: The Best Solution for Threat Prevention

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

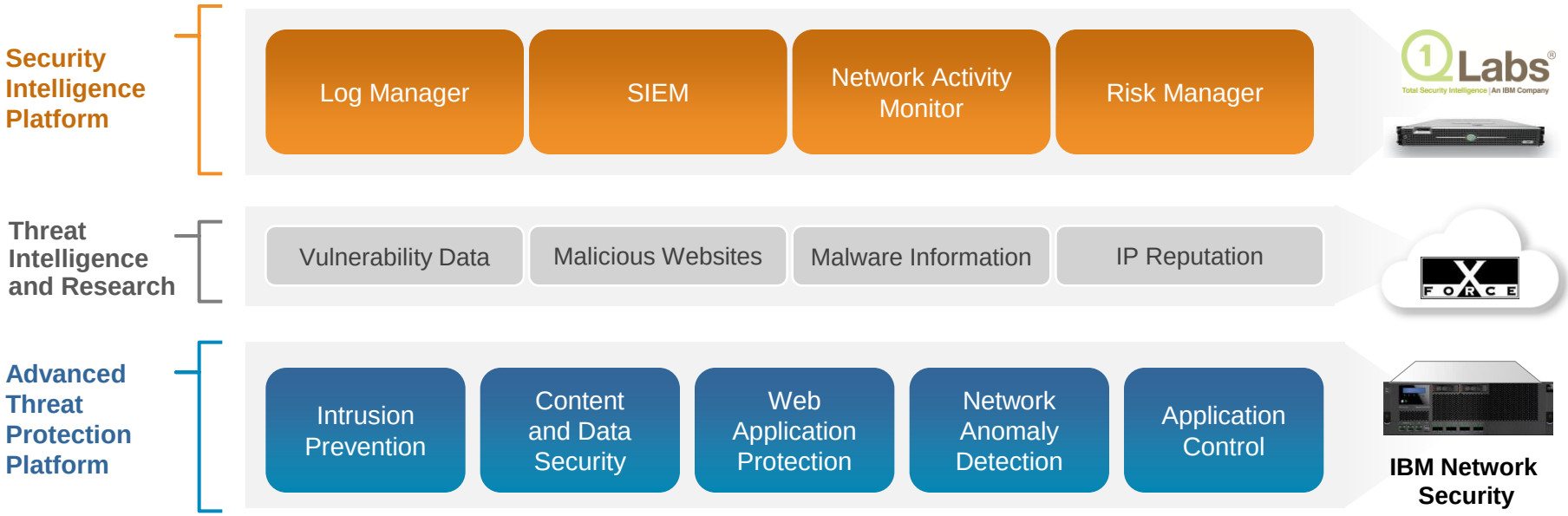
- True Protocol aware Network IPS
- Higher level of overall security and protection
- More effective against 0-day attacks
- Best of both worlds – true protocol and heuristic-based protection with customized signature support



IBM Security Network Protection XGS 5000

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

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

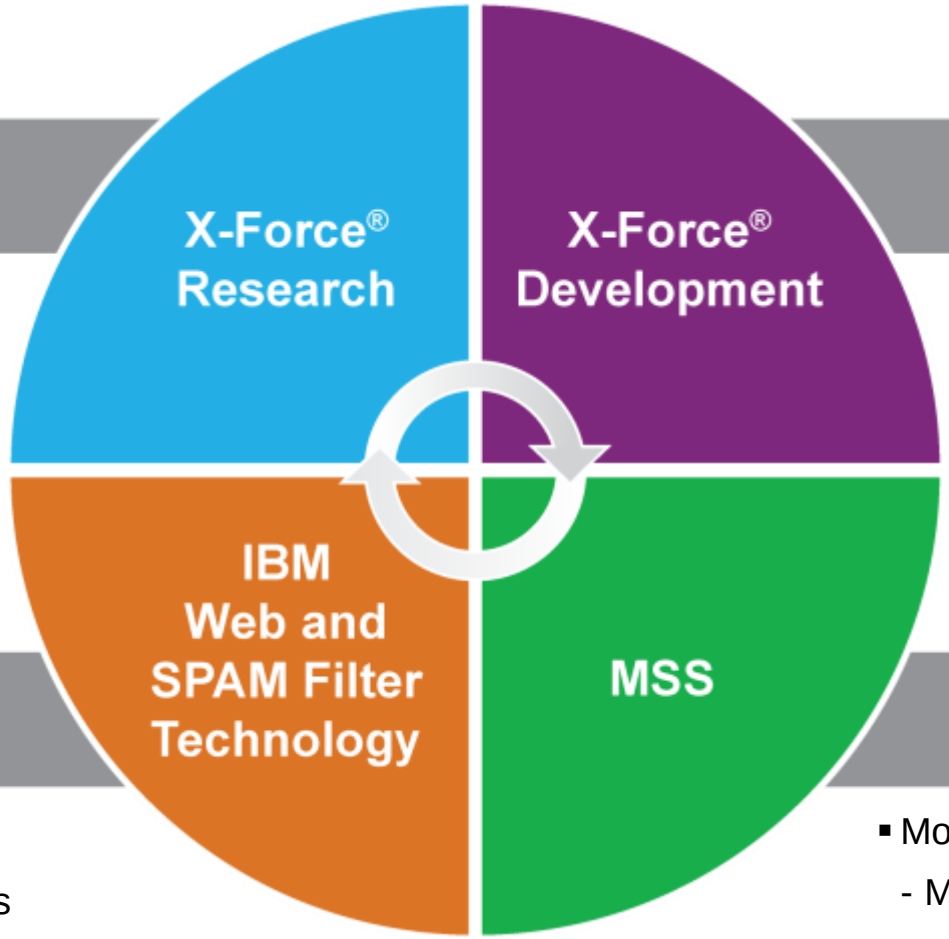
Expanded X-Force Threat Intelligence

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 X-Force Intelligence Lifecycle



New protection guidance

- Deep Crawl of Known Malicious Websites
- Analyze New Exploit Techniques
- Provide New Protection Guidance

New IPS updates

- Develop Protection
- Deliver Updates

New malicious websites

- Classify MSS Links
- Find Related Websites (Deep Crawl)
- Search for Malware
- Find New Malicious Websites
- Block All Malicious Domains

Malicious URLs

- Monitor Browsing of:
  - Million of End-users
  - Thousands of Customers
  - Hundreds of Countries
- Block Malicious Links
- Send Links to X-Force

ibm.com/security