Security Intelligence.
Think Integrated.

IBM Security Network Protection Solutions

Pre-emptive protection to keep you Ahead of the Threat®

October 22, 2014
Cambridge, MA

Paul Griswold
Program Director, Strategy & Product Management
Infrastructure Security
IBM Security Systems

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.

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.

Infrastructure - Network

Area of Focus

Guard against attacks using an Advanced Threat Protection Platform with insight into users, content and applications

Portfolio Overview

IBM Security Network Protection (XGS)

Next-generation network protection to safeguard both computing infrastructure and users from today's most serious threats

IBM Security Intrusion Protection (GX)

Industry-leading intrusion protection focused on protecting computing infrastructure

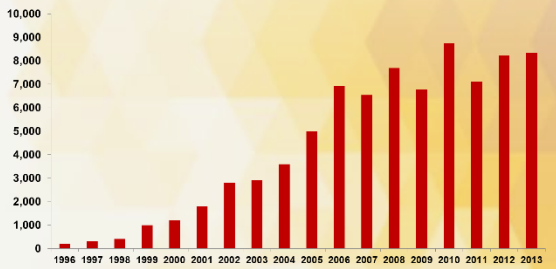
IBM Security SiteProtector

Central management of security devices to control policies, events, analysis and reporting for your business

Increasing attack surface and threat sophistication

Increasing Number of Vulnerabilities

Growth in Vulnerabilities
1996 - 2013

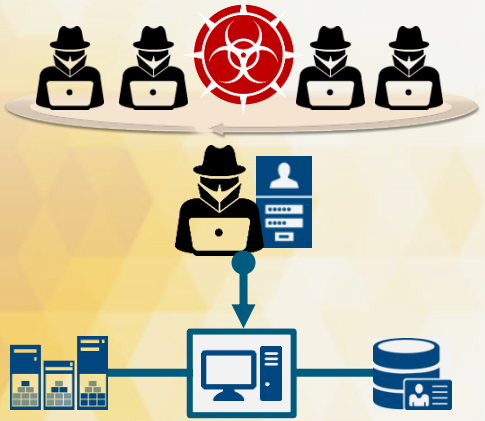


- Vulnerabilities increasing
- Overall attack surface is growing
- Patches cannot be instantly implemented or do not exist

Zero-day Attacks and Constantly Mutating Threats

- Attacks constantly mutating to evade signatures
- Increasing number of zero-day exploits

Multi-faceted Threats and APTs



- Well coordinated attacks by well coordinated teams
- Attackers exploiting users to gain access
- Traditional security tools unable to detect or assess the extent of the breach

Average cost of a breach is $5.9M and compliance pressures continue to grow

 Source: 2014 Cost of a Breach Study: United States, Ponemon Institute

Today's point product solutions defend against yesterday's attacks

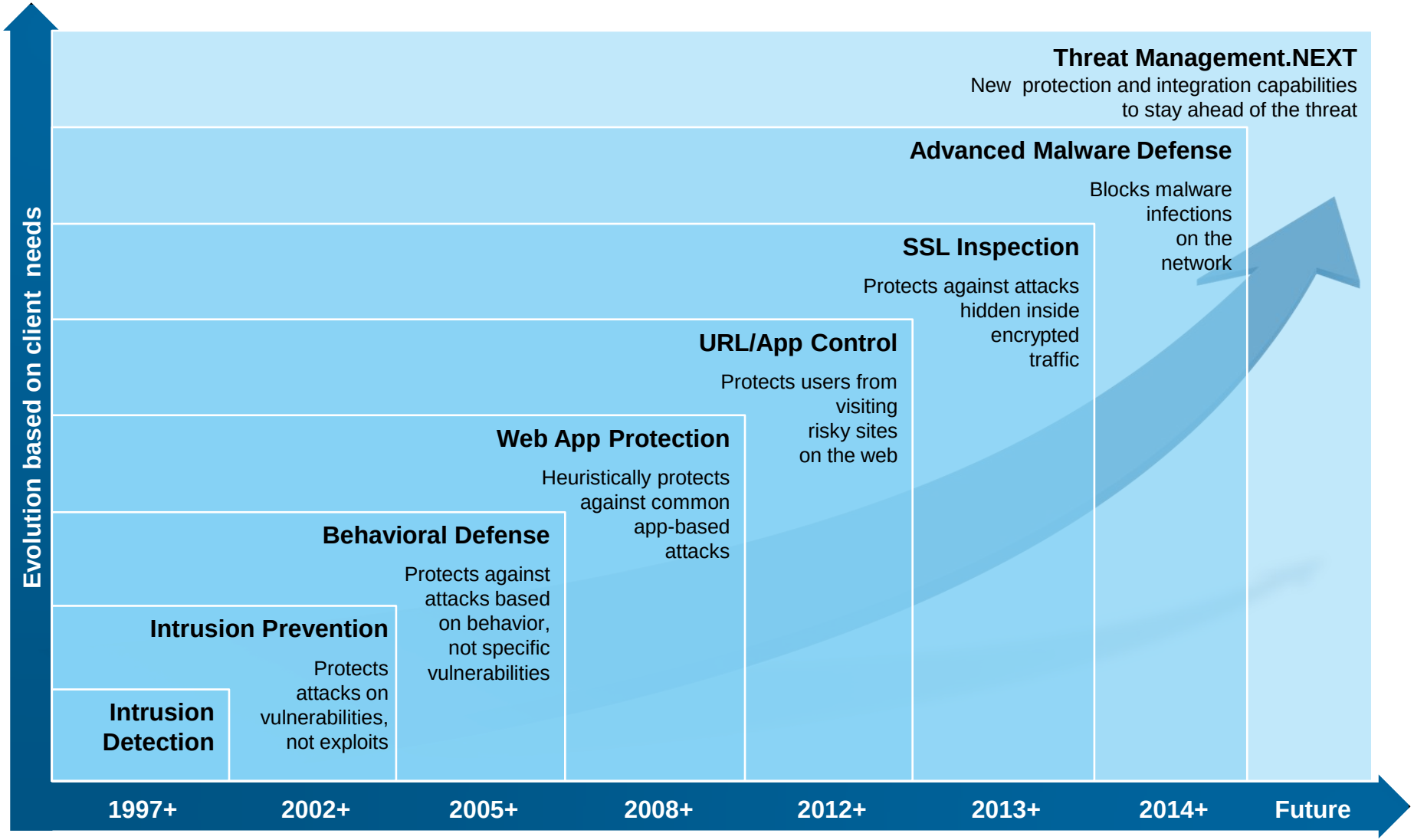
Broad Attacks
Indiscriminate malware, spam and DoS activity

Multi-faceted Targeted Attacks
Advanced, persistent, organized, and politically or financially motivated

Tactical Approach *Compliance-driven, Reactionary*	Strategic Approach *Intelligence-driven, Continuous*
▪ Rely on pattern matching to find specific instances of attacks	▪ Block entire classes of attacks, including mutations
▪ Rely on other add-on products like proxies and application firewalls	▪ Protect against user-focused and application-level attacks
▪ Targets only certain types of broad attacks	▪ Protect against advanced malware and persistent threats
▪ Solution provider obtains their research from third parties	▪ Offer industry-leading security research and development
▪ Piece-part solution	▪ Seamlessly integrate with an entire portfolio of industry-leading security solutions

The history of IBM Security Network Protection

Evolving beyond intrusion prevention to provide greater value



IBM is uniquely positioned to offer integrated protection

IBM Security Network Protection solutions and integrations

Smarter Prevention

Trusteer Apex Endpoint Malware Protection

NEW *Java Lockdown Protection - granular control of untrusted code, cloud-based file inspection, and QRadar integration*

IBM Security Network Protection XGS

NEW *Advanced Threat Quarantine integration from QRadar and third-party products, inclusion of Trusteer intelligence into XGS*

Security Intelligence

IBM Security QRadar Security Intelligence

NEW *Data Node appliance, new flow and event APIs, and QRadar Vulnerability Manager scanning improvements*

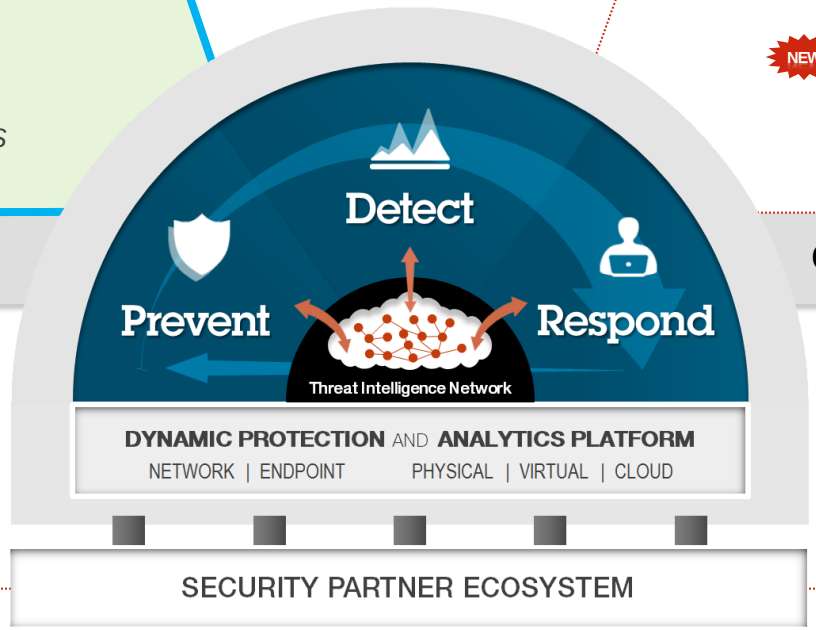
Continuous Response

IBM Security QRadar Incident Forensics

NEW *Integrated forensics module with full packet search and visual reconstruction of relationships*

IBM Emergency Response Services

NEW *Increased global coverage and expertise related to malware analysis and forensics*



Open Integrations

Ready for IBM Security Intelligence Ecosystem

NEW *New functionality from partners including FireEye, TrendMicro, Damballa and other protection vendors*

Global Threat Intelligence

IBM X-Force Threat Intelligence

NEW *New real-time sharing of Trusteer threat intelligence from 100M+ endpoints with X-Force*

IBM Security Network Protection

Pre-emptive protection to keep you Ahead of the Threat®

BROAD COVERAGE

Protects against a full spectrum of attack techniques

ZERO-DAY PROTECTION

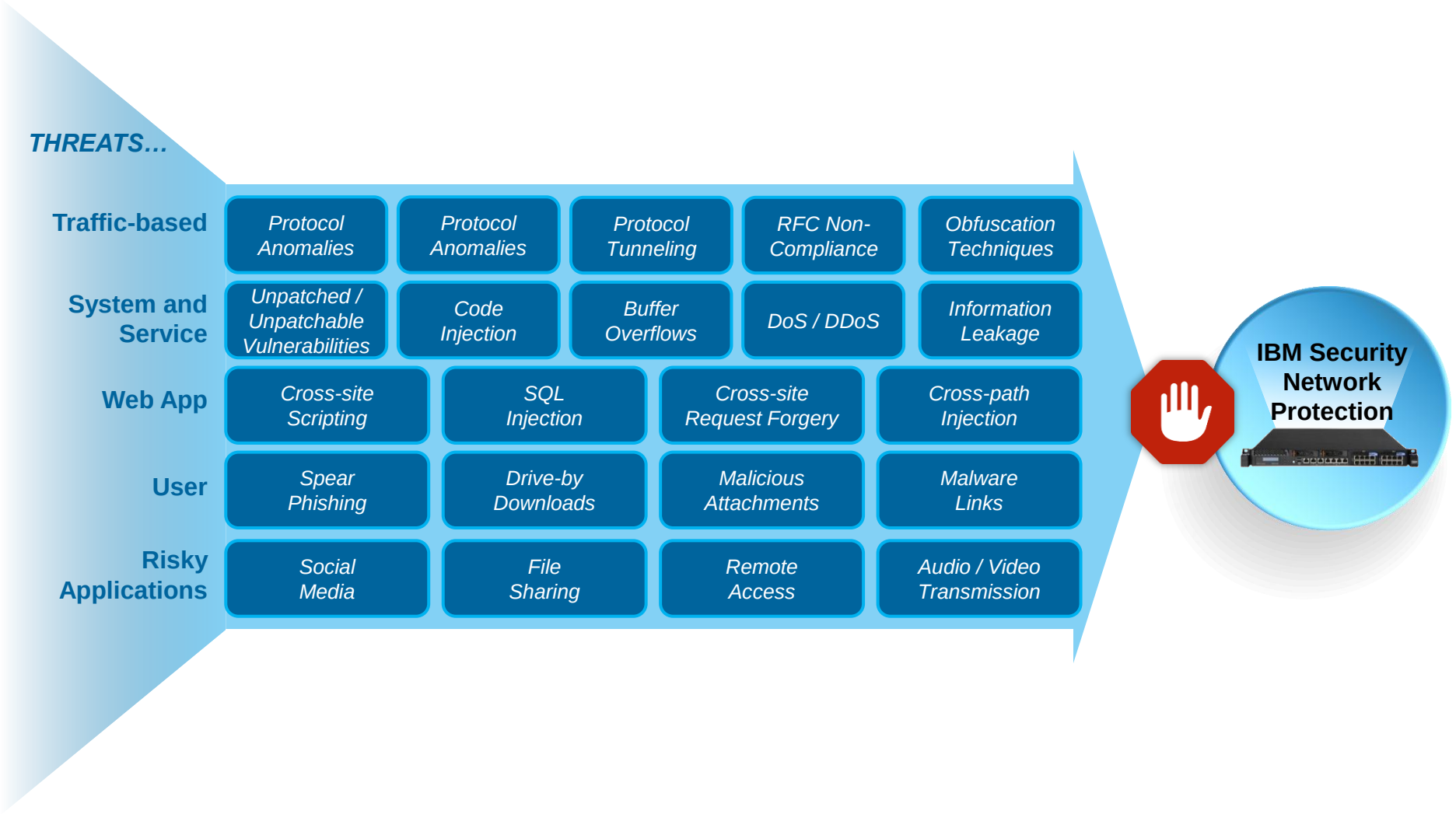
Protects against known and unknown attacks

ADVANCED INTELLIGENCE

Powered by XForce® global threat research

Broad coverage

Protects against a full spectrum of attack techniques



Broad coverage

Comprehensive protection, visibility, and control over network traffic

Deep Packet Inspection

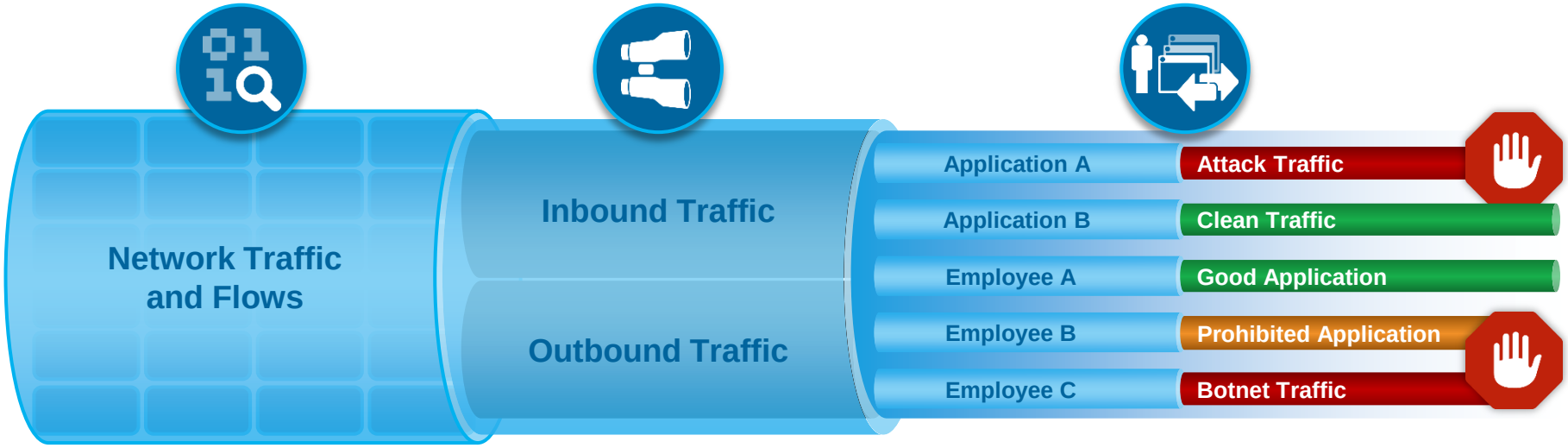
Fully classifies network traffic, regardless of address, port, or protocol

SSL Visibility

Identifies inbound and outbound traffic threats, without needing a separate appliance

Identity and Application Awareness

Associates users and groups with their network activity, application usage and actions



400+
Protocols and file formats analyzed

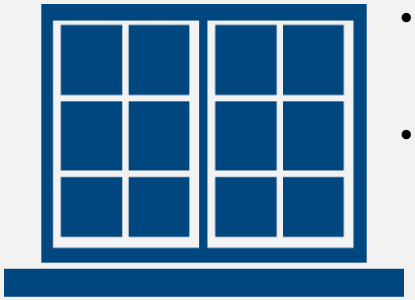
22+ Billion
URLs classified in 70 categories

2,000+
Applications and actions identified

The IBM fundamental approach to threat protection

VULNERABILITY vs. EXPLOIT

A weakness in a system



- Can be used to do something unintended
- Can be exploited in multiple ways

A method used to gain system entry

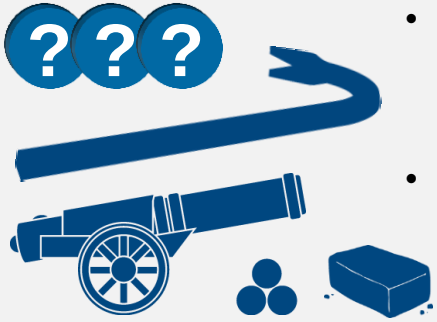
- Many different exploits can target a single vulnerability
- Not all exploits are publicly available, and mutation is common

IBM PROTECTION vs. OTHER PRODUCTS

IBM protects the vulnerability

- Stays ahead of the threat with pre-emptive protection that stops things from breaking the window

Other products only block the exploits



- Looks for methods that can break the window
- Keeping up can be challenging

IBM goes beyond pattern matching with a broad spectrum of vulnerability and exploit coverage

Exploit Signatures

Attack-specific pattern matching

Other IPS solutions stop at pattern matching

Vulnerability Decodes

Focused algorithms for mutating threats

Application Layer Heuristics

Proprietary algorithms to block malicious use

Web Injection Logic

Patented protection against web attacks, e.g., SQL injection and cross-site scripting

Shellcode Heuristics

Behavioral protection to block exploit payloads

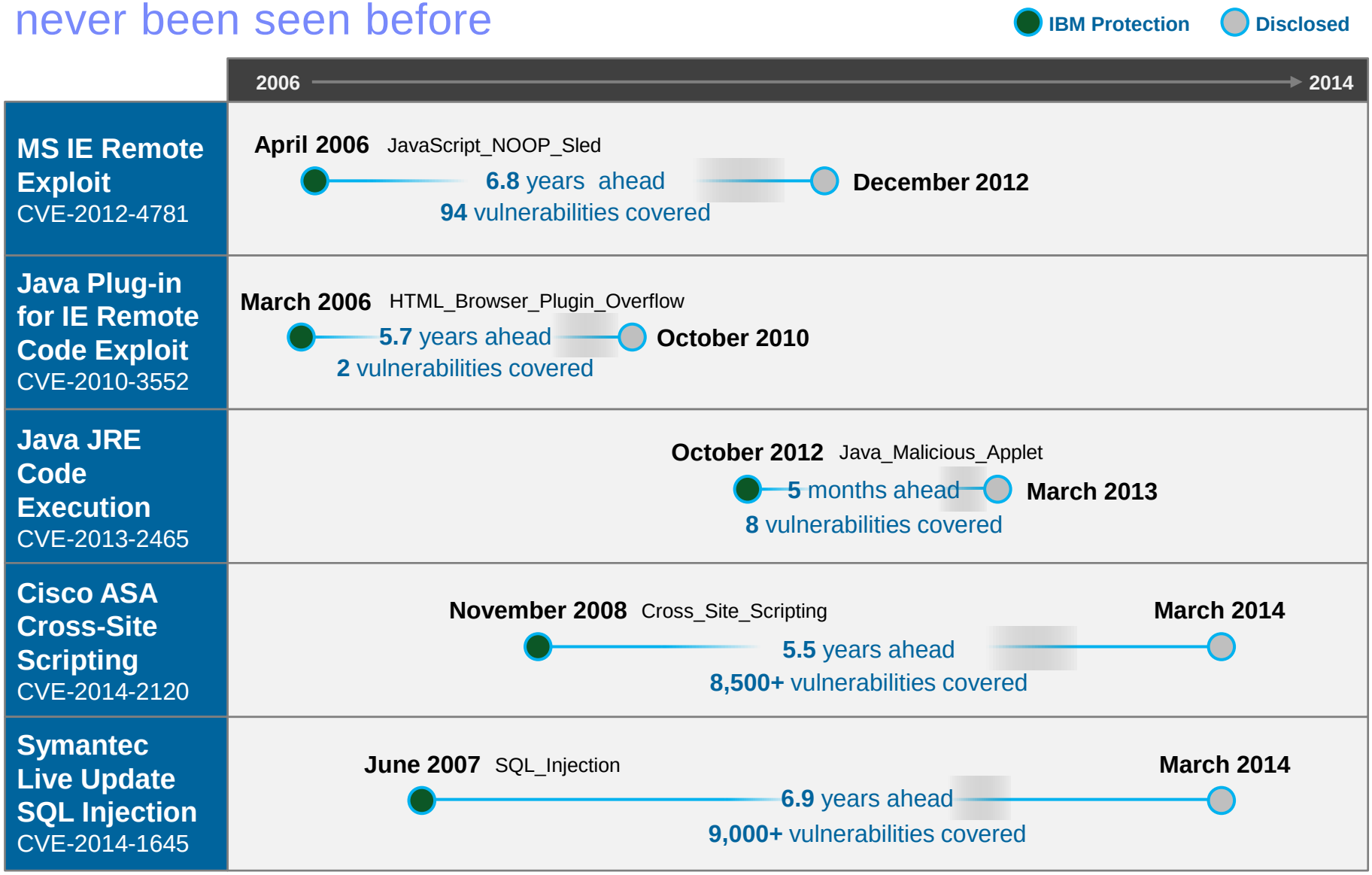
Content Analysis

File and document inspection and anomaly detection

Protocol Anomaly Detection

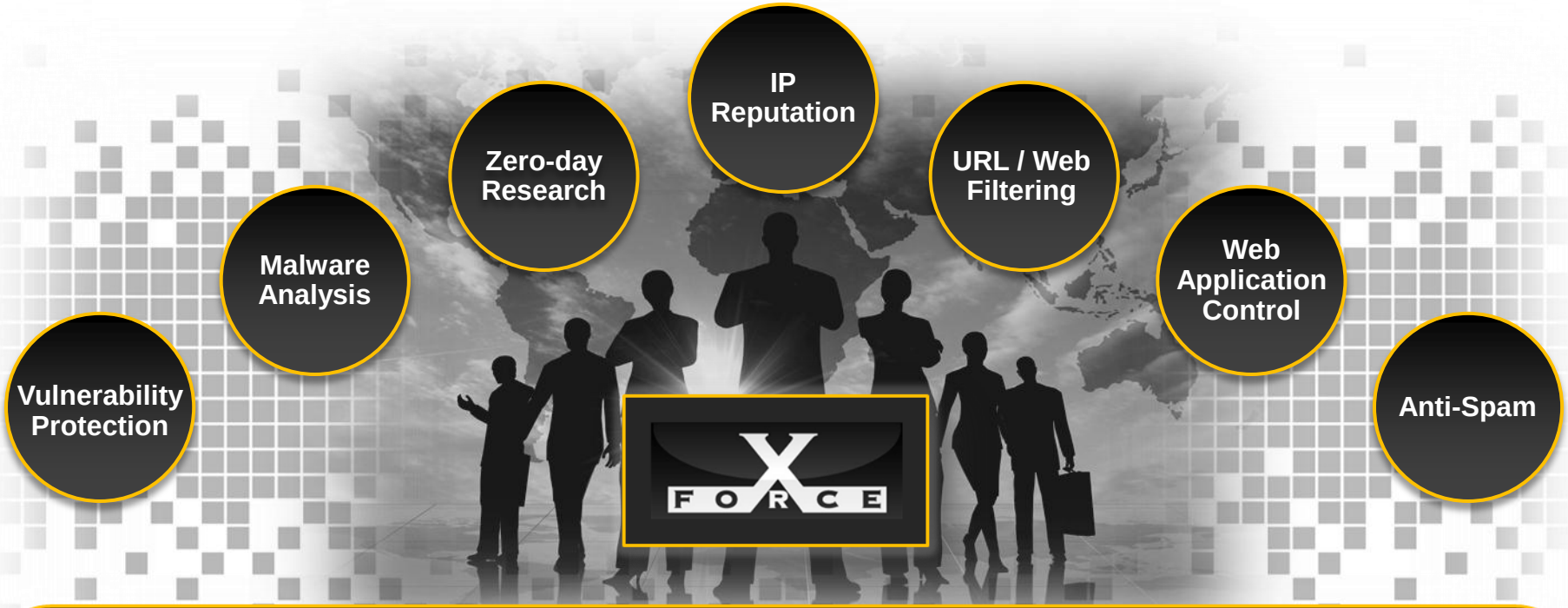
Protection against misuse, unknown vulnerabilities, and tunneling across 230+ protocols

Behavioral-based detection blocks attacks that have never been seen before



IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

XGS = X-Force in a box

Coverage

20,000+ devices under contract

3,700+ managed clients worldwide

15B+ events managed per day

133 monitored countries (MSS)

1,000+ security related patents

100M+ customers protected from fraudulent transactions

Depth

23B+ analyzed web pages and images

7M+ spam and phishing attacks daily

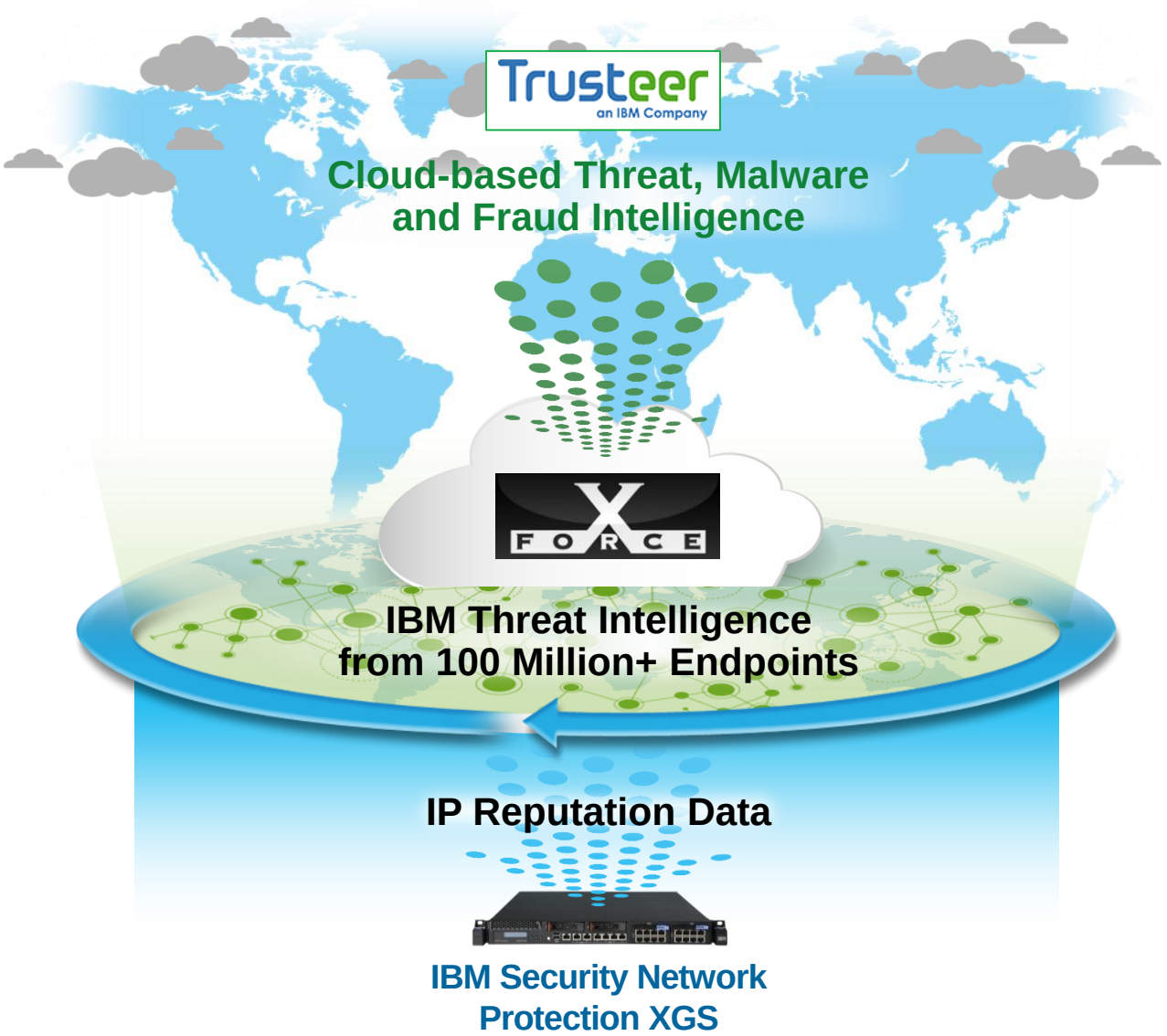
81K+ documented vulnerabilities

860K+ malicious IP addresses

1,000+ malware samples collected daily

Millions of unique malware samples

IBM Trusteer and X-Force® integration



Improved Intelligence and Security through QRadar integration

Send data flows to QRadar and as well as receive quarantine commands

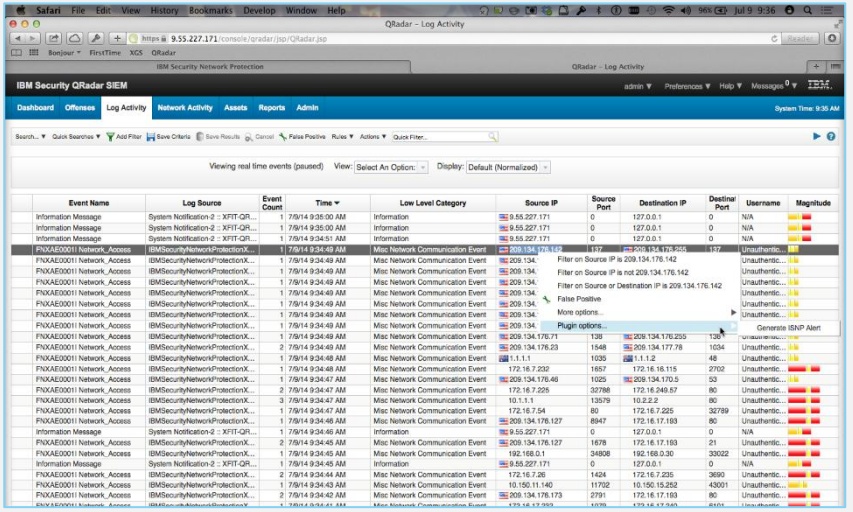
Layer 7 Flow Data to QRadar

Detect abnormal activity through network flow data generated through XGS

Identify application misuse via user and application information

Save money by reducing the need for a separate flow generation appliance

Offense-blocking from QRadar



Make QRadar Intelligence actionable by leveraging the XGS to block in-progress attacks

Reduce response time by initiating blocking within the QRadar console to stop threats quickly

Ranked #2 out of 9 vendors in recent NSS Labs testing

95.7%	Exploit block rate
97.7%	Block rate for server attacks
94.1%	Block rate for client attacks
PASS	All tests related to “stability and reliability”
PASS	All tests related to “evasions”

“[IBM’s score] speaks to the ability of the IBM IPS to perform against the types of constantly evolving threats that are often seen in today’s networks.”

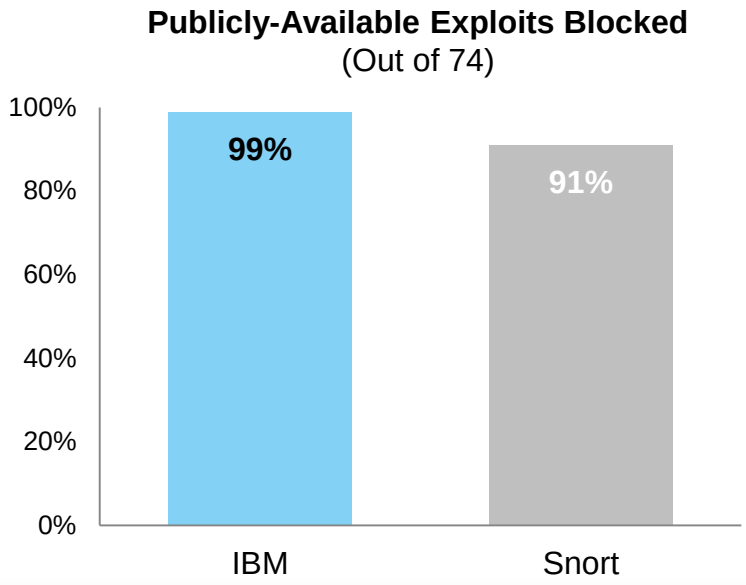
Vikram Phatak
Chairman and CEO, NSS Labs

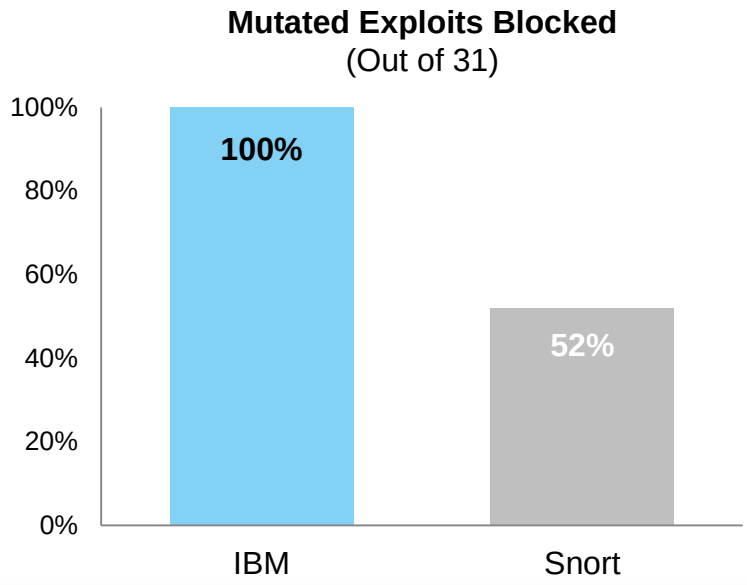
Source: NSS Labs 2013 Group IPS Test

The Tolly Report Illustrates the Benefits of Behavioral Detection

INLINE IPS SYSTEM EFFICACY

IBM IPS GX7800 vs. Snort IPS





- 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

Source: Tolly Test Report , October 2012

Simple mutations will render exploit-matching engines useless

A simple change to a variable name allows the attack to succeed, while rendering the protection of a signature matching engines useless

Original Variable Names	Mutated Variable Names
Shellcode	somecode
Block	brick
heapLib	badLib

A simple change to the HTML code in a compromised web page makes the attack invisible to signature protection

Original Class Reference

```
<html><head></head>
<body><applet
archive="jmBXTMuv.jar"
code="msf.x.Exploit.class"
width="1" height="1"><param
name="data" value=""/><param
name="jar">
```

Mutated Class Reference

```
<html><head></head>
<body><applet
archive="eXRZLr.jar"
code="msf.x.badguy.class"
width="1" height="1"><param
name="data" value=""/><param
name="jar">
```

Simply adding a comment to a web page results in an attack successfully bypassing signature IPS

Original Code	Mutated Code
`var t = unescape;`	`var t = unescape <!– Comment -->;`

XGS appliance models

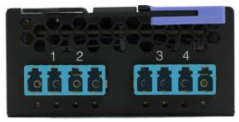
IBM Network Protection XGS			
Capabilities per Model	**XGS 3100**	**XGS 4100**	**XGS 5100**
Inspected Throughput	Up to 600 Mbps	Up to 1 Gbps	Up to 5 Gbps
Flexible Performance Levels	FPL 1: Up to 300 Mbps FPL 2: Up to 600 Mbps	FPL 1: Up to 500 Mbps FPL 2: Up to 1.0 Gbps	FPL 1: Up to 2.0 Gbps FPL 2: Up to 3.5 Gbps FPL 3: Up to 5.0 Gbps
Inspected Throughput (with SSL)	Up to 100 Mbps	Up to 400 Mbps	Up to 2.5 Gbps
Pluggable Network Interface Modules	0	1	2
Protected Segments	2	Up to 6	Up to 10

Modular Network Interfaces Help Future-Proof Investment

Seven different network modules
allow the XGS 5100 & 4100 to meet current and future connectivity needs

8-port RJ-45 copper
w/ built-bypass

4-port Fixed fiber (SX)
w/ built-bypass



4-port Fixed fiber (LX)
w/ built-bypass

2-port 10GbE (SR)
w/ built-bypass

2-port 10GbE (LR)
w/ built-bypass

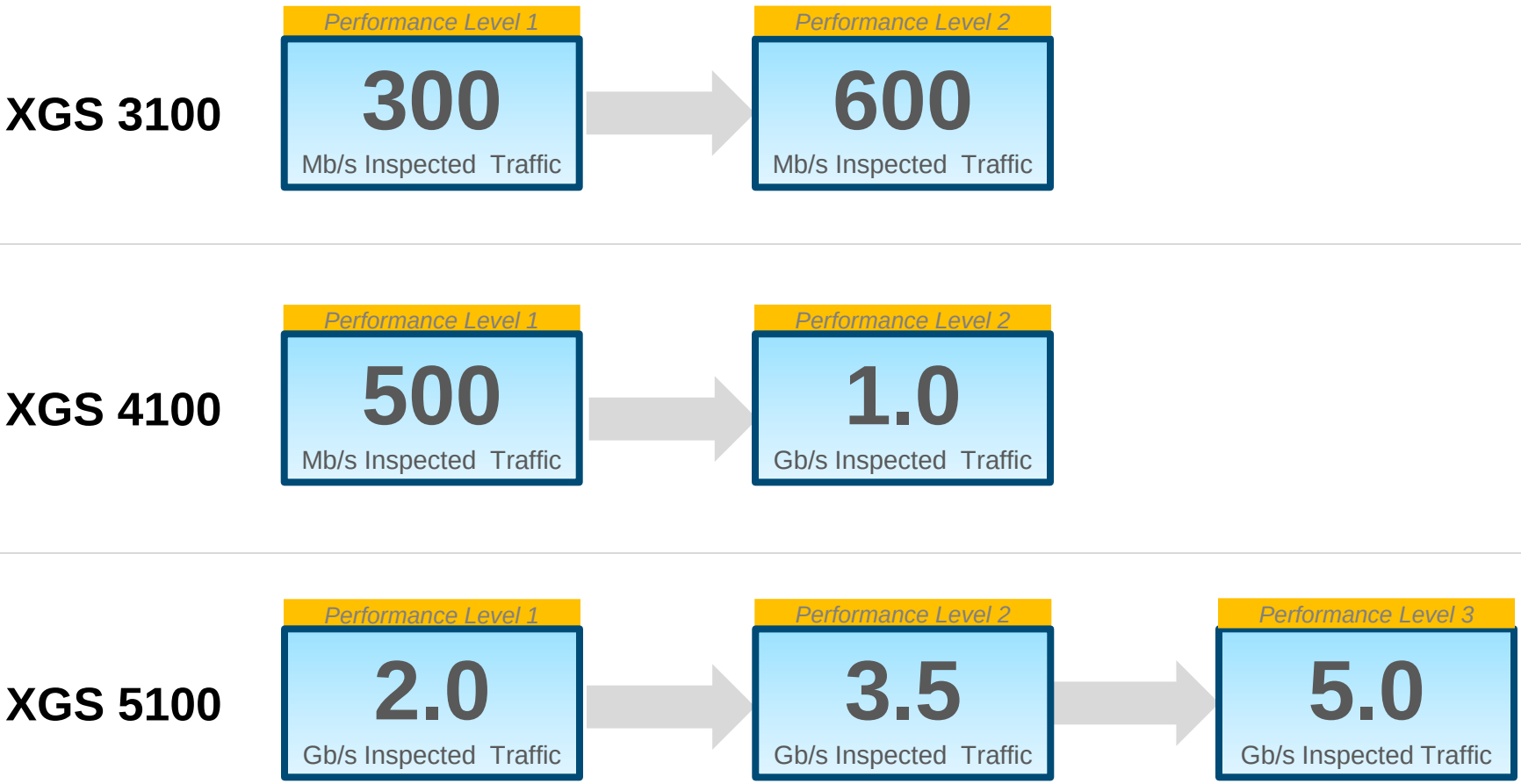
4-port SFP
(requires transcievers)

2-port 10GbE SFP+
(requires transcievers)

The XGS 5100 supports 2 NIMs,
The XGS 4100 1 NIM,
The XGS 3100 does not support NIMs.

Flexible Performance Licensing

Flexible levels of inspected throughput allow upgradable performance without the need to change hardware



XGS provides the protection needed for today's threats

Fight malware

Disrupt the attack chain including integration with Trusteer Apex and leading malware sandboxes

Protect users

Limit access to phishing messages, while blocking malicious links, drive-by downloads, and file attachments

Guard against mutated threats

By protecting the vulnerability, not looking for the exploit

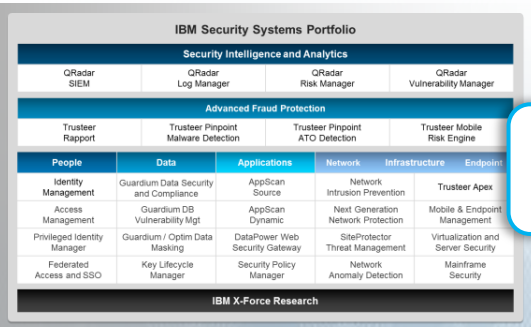
Protect against zero-day vulnerabilities

Through advanced behavioral techniques

Integrates seamlessly with QRadar

Send Layer 7 flow data to QRadar and receive quarantine commands

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework



Broadest and deepest coverage across all security domains

Worldwide research, development, and security experts

Award-winning global threat research

Intelligence. Integration. Expertise.

Learn more about IBM Security Network Protection

Visit the
IBM Security Infrastructure Protection Website

Watch the videos on the
IBM Security Infrastructure Protection Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

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.

Thank You

www.ibm.com/security