IBM Forum Segrate - Milano

18 settembre:
Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

IBM Advanced Threat Protection Platform

Fabio Panada IBM Security Tech Sales Leader

Advanced Threats is one of today's key mega-trends

Advanced Threats

Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence

Advanced Persistent Threats
Stealth Bots Targeted Attacks
Designer Malware Zero-days

Enterprise Customers

Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed

Mobile Computing

Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility

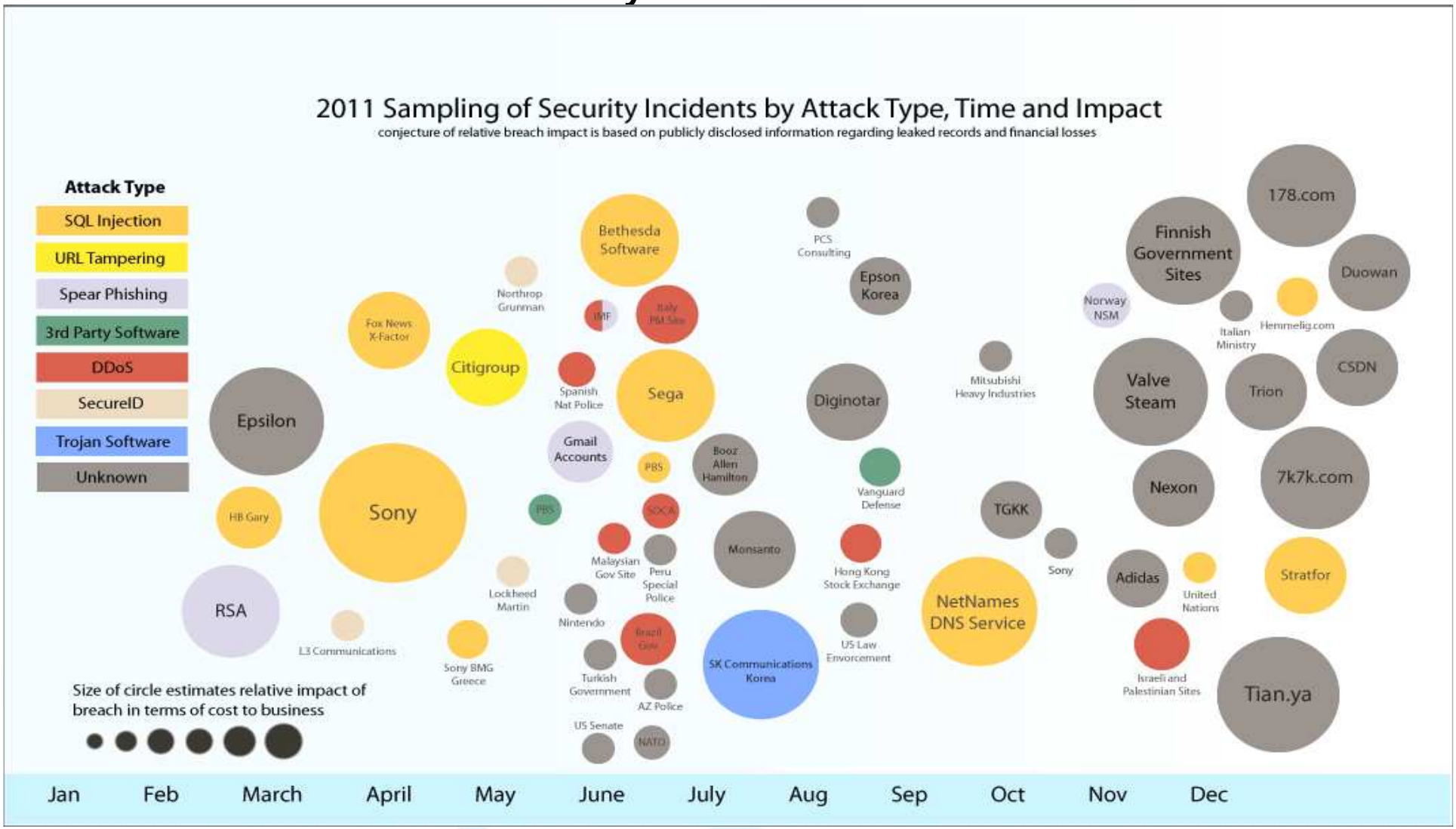
Regulation and Compliance

Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures

GLBA
FFIEC
PCI Security Standards Council
Sarbanes-Oxley
Financial and Accounting Disclosure Information

Cyber breaches are having a growing impact

"The Year of the Security Breach" – IBM's X-Force® R&D



Cloud Breaches 2011

Top 3 Vulnerabilities

- SQL Injections Attacks
- Cross Site Scripting
- Phishing and Malware

43 percent of current cloud users **reported a security incident** in the last 12 months

Customer Business Pains

- Need to stop known threats and zero-day attacks to spread on the network
- Impossibility to install patches to fix vulnerabilities
- Applications need to be protected agains abuse & misuse
- Network Anomaly Detection for enhanced analisys
- Reduce manual effort of security operations and compliance reporting
- Protection against both Client and Server Based Attacks
- Control applications utilization (who, what, why)

Implications

- Loss of confidential information including company confidential or client information
- Average cost of a security breach is $7.2 Million*
- Average cost per compromised record is $214*
- Additional lost revenues from interruption of business operations or brand damage
- Decreased productivity due to decreased availability or service quality of business critical infrastructure
- Increased cost and complexity trying to keep pace with changing security risks

*Source: Ponemon Institute

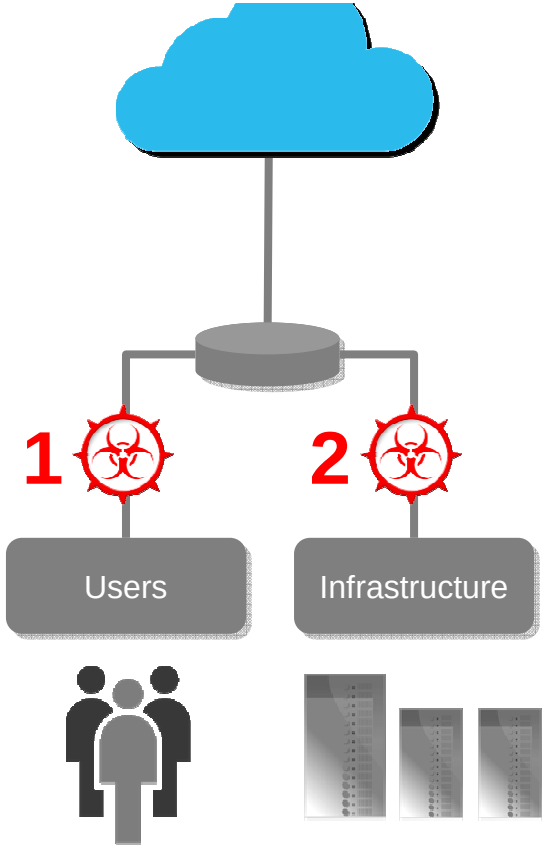
Client and Server Based Attacks to the network

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

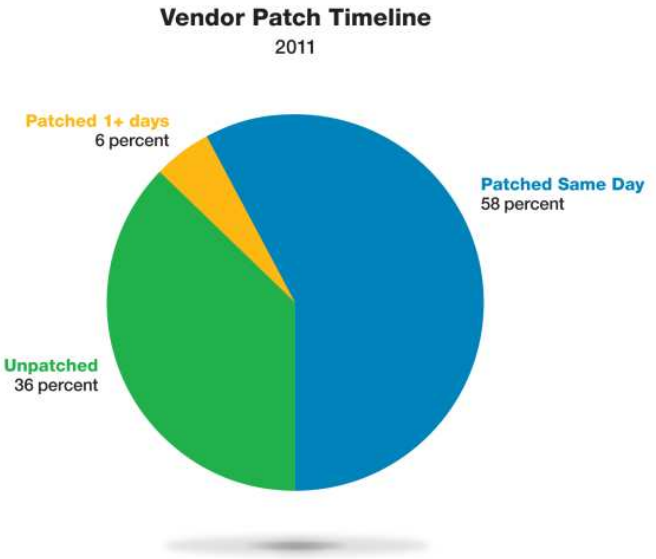
Network Intrusion Prevention Solutions that Fit Customers' Needs

- **Block threats before they impact your organization**
- **Uncompromising security backed by X-Force®**
- **Inspected throughput from 200 Mbps to 20Gbps+**
- **Protection for up to 8 network segments**
- **Scale from remote offices to the network core**

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**

IBM Virtual Patch Technology

- **36%** of all vulnerabilities disclosed during the 2011 had no vendor-supplied patches available to remedy the vulnerability
- Shielding a vulnerability from exploitati independent of a software patch
- Enables a responsible patch management process that can be adhered to without fear of a breach
- IBM is a MAPP (Microsoft Active Protections Program) partner



Source: IBM X-Force® Research and Development

Source: IBM X-Force Trend & Risk Report 2011

Java 0-Day Exploited in the Wild

27 August 2012

- **Java 0-Day Exploited in the Wild**

  Zero-Day Season is Not Over Yet
  Oracle Java Runtime Environment sandbox code execution

  New Java zero-day vulnerability has been spotted in the wild. We have seen this unpatched exploit being used in limited targeted attacks. Most of the recent Java run-time environments i.e., JRE 1.7x are vulnerable. In my lab environment, I was able to successfully exploit my test machine against latest version of FireFox with JRE version 1.7 update 6 installed.

Description:

Oracle Java Runtime Environment could allow a remote attacker to execute arbitrary code on the system. By persuading a victim to visit a specially-crafted Web site containing a malicious Java applet, an attacker could exploit this vulnerability to bypass sandbox restrictions to download and execute arbitrary code outside the sandbox.

28 August 2012

- **IBM Raising Internet Threat Level to AlertCon 2**

The Java exploit (CVE-2012-4681) continues to become more wide spread and, with the inclusion of this code in the Blackhole Exploit Kit, we have decided to raise our Internet Threat Level to AlertCon 2 in an effort to bring increased awareness of this situation to our customers. Customers using our Proventia series of network sensors can enable Java_Possibly_Malicious_Applet.

We encourage you to work with your vendor to find the best coverage for this exploit. Customers who can not disable Java, due to application requirements, may want to consider turning off the plugin in your browsers, which should still allow your desktop applications to run properly.

29 August 2012

New 'Reliable' Java Attack Spreading Fast, Uses Two Zero-Day Bugs

Hundreds of domains serving up attack, tens of thousands of new victim machines since Java exploit was added to BlackHole toolkit

Aug 29, 2012 | 03:43 PM |

By **Kelly Jackson Higgins**
Dark Reading

Widespread attacks are under way using a weaponized reliable Java exploit that relies on not one, but two zero-day exploits.

The Java exploit was originally used for targeted attacks to push remote access Trojans onto a victim's machine when it first went public, but this week was hurriedly added to the popular BlackHole crimeware kit, making it easily available to all types of cybercriminals. "When it got merged into BlackHole, it started to push malware of a more traditional type, like banking Trojans [and] Zeus variants," says Patrik Runald, director of security research for Websense.

At least 100 domains are now serving up the exploit, according to estimates by Websense and other researchers, 83 percent of which are located in the U.S., according to Websense. And so far, the number of infected hosts is in the tens of thousands range, according to Seculert's latest data.

30 August 2012

IBM Internet Security Systems
Ahead of the threat.™

ALERTCON 2

Name:	Oracle Java Runtime Environment Sandbox Code Execution
Public disclosure/ In the wild date:	August 27, 2012
Aliases:	Oracle JRE 1.7.0 Update6
Risk:	High
CVE:	CVE-2012-4681
Description:	The Java Runtime Environment (JRE) versions 7 update 6 and possibly other versions contain a vulnerability that can be exploited for sandbox evasion and remote code execution in the context of the current user.

ISS Coverage

Product	Content Version
Proventia Network IDS Proventia Network IPS Proventia Network MFS Proventia Server (Linux) RealSecure Network RealSecure Server Sensor	32.082
Proventia Desktop Proventia Server IPS (Windows)	2796

Propagation Techniques	ISS Protection	Available
remote exploit	Java Sandbox Code Execution* Java Possibly Malicious Applet	30 Aug 2012 09 Aug 2011

31 August 2012

Home > News > Security > Security Fixes and Improvements

August 31st, 2012, 08:57 GMT · By Eduard Kovacs

Java Users Still Not Safe, Experts Report New Vulnerability to Oracle (Exclusive)

Researchers from Polish firm Security Explorations – the ones who were the first to report the vulnerabilities which led to the now-infamous Java zero-day – have just reported another similar bug to Oracle. This means that Java users are still exposed, even if they've applied the patch released by the company.

31 August 2012

Security Experts: Java Should Be Disabled Unless Necessary

Security researchers say Java's popularity as an attack vector means it should be disabled unless it is needed

Aug 31, 2012 | 12:06 PM |

By **Brian Prince, Contributing Writer**
Dark Reading

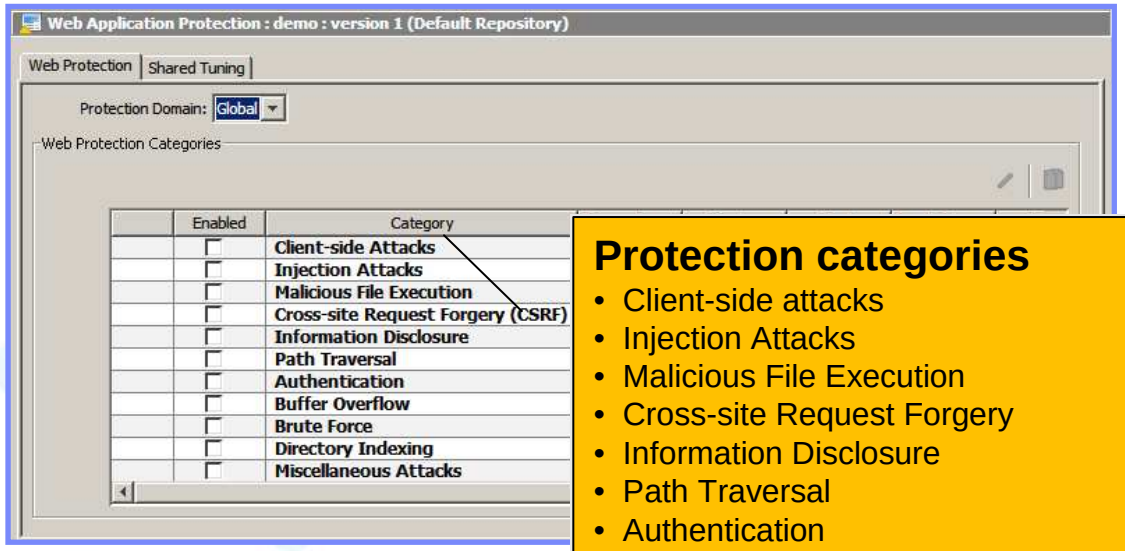
Since the acquisition of Sun Microsystems a few years ago, Oracle has found itself tasked with protecting a technology that has increasingly come under the gun from attackers -- Java. According to security researchers, Java's popularity as an attack vector means it's time for organizations to disable it unless there is a strong use case.

"As it happens, very few websites rely on Java for dynamic content," says Tod Beardsley, Metasploit engineering manager at Rapid7. "Java isn't relied on nearly as much as Javascript and Flash. Most people can disable their Java browser plug-in and not really notice the difference."

The bugs at the center of much of the latest drama are CVE-2012-4681, which Oracle patched Thursday amid growing anxiety. However, there is a report that researchers from security vendor Security Explorations have found a vulnerabilityin the update that can be exploited to escape the Java sandbox and execute code.

Web Application Protection and Appscan

- ✓ **Network analyst creates a virtual patch by turning on IBM Security IPS Web application protection policy**
- ✓ **Network analyst enables protection categories in the policy based on the types of discovered vulnerabilities with AppScan**

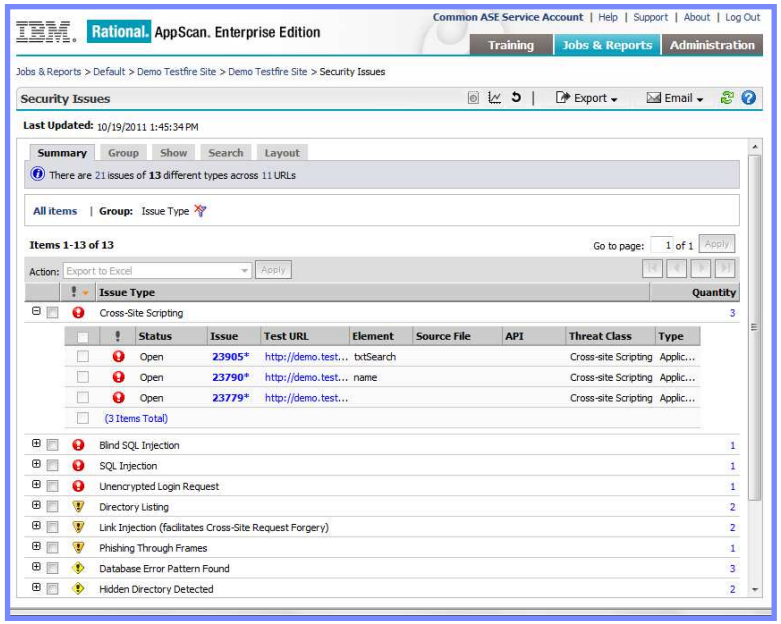


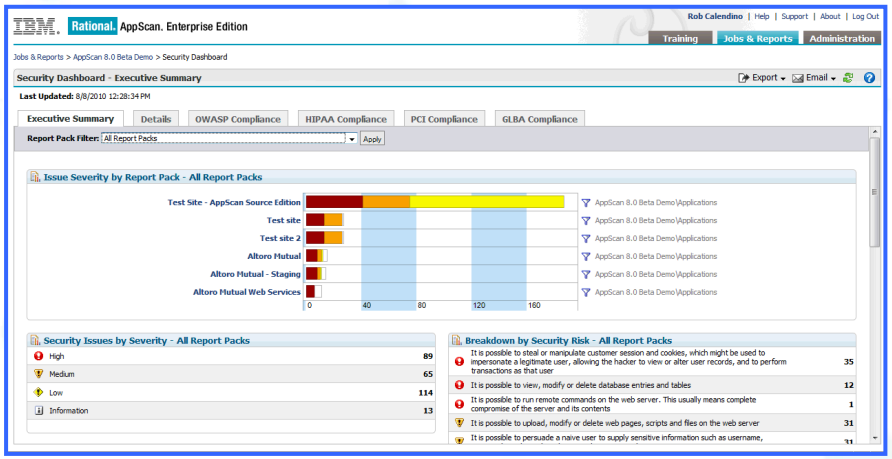
Protection categories

- Client-side attacks
- Injection Attacks
- Malicious File Execution
- Cross-site Request Forgery
- Information Disclosure
- Path Traversal
- Authentication
- Buffer Overflow
- Brute Force
- Directory Indexing
- Miscellaneous Attacks

Check your applications for security vulnerabilities with AppScan Enterprise

- ✓ **Security analyst performs automated security assessments of new or already deployed Web applications**
- ✓ **Security analyst reviews findings and identifies vulnerabilities**
- ✓ **Application development team are notified about security vulnerabilities**





SiteProtector SecurityFusion™ module provides security intelligence

Tag Name	Status	Severity	Event Count	Source Count
HTTP_POST_SQL_UnionSelect	Detected event	Medium	3	1
HTTP_POST_SQL_UnionSelect	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_POST_XP_Cmdshell	Detected event	High	48	1
HTTP_QuikStore	Attack failure (blocked by Proventia appliance)	Medium	5	1
HTTP_repeated_character	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_Server_ID	Detected event	Low	21986	2
HTTP_Share_Point_XSS	Detected attack (vuln not scanned recently)	Medium	1	1
HTTP_Shells_Perl_Exe	Detected attack (vuln not scanned recently)	Medium	4	1
HTTP_testcgi	Attack failure (blocked by Proventia appliance)	High	1	1
HTTP_Translate_F_SourceRead	Attack failure (blocked by Proventia appliance)	Medium	48	1
HTTP_Twiki_Image_Include_CmdExec	Attack failure (blocked by Proventia appliance)	High	2	1
HTTP_Unify_UploadServelet	Attack failure (blocked by Proventia appliance)	High	1	1
HTTP_Unix_Passwords	Detected event	High	12	1
HTTP_URL_BackslashDotDot	Detected attack (vuln not scanned recently)	High	42	1
HTTP_URL_dotpath	Detected event	Low	4	1
HTTP_URL_Many_Slashes	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_URL_repeated_char	Detected event	Medium	1	1
HTTP_URL_Repeated_Dot	Detected attack (vuln not scanned recently)	Medium	12	1
HTTP_URLscan	Detected event	Medium	2	1
HTTP_Webplus	Attack failure (blocked by Proventia appliance)	Medium	1	1
HTTP_Windows_Executable	Attack failure (blocked by Proventia appliance)	High	168	1
SQL_Injection	Attack likely successful (vulnerable)	High	73	2
XPath_Injection	Attack likely successful (vulnerable)	Medium	438	1

- ✓ **IDS/IPS real-time malicious HTTP traffic is correlated with vulnerable application assets**
- ✓ **SiteProtector alerts network analyst when attacks are likely to succeed**
- ✓ **Network analyst takes action**

QRadar Network Anomaly Detection

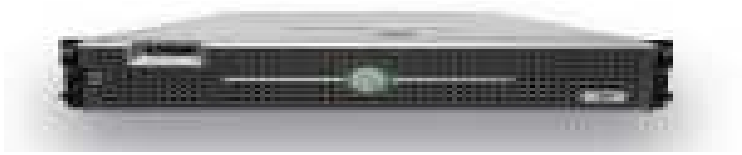
- QRadar Network Anomaly Detection
  optimized version of QRadar Network Activity Monitoring for IBM Security Network Protection solutions

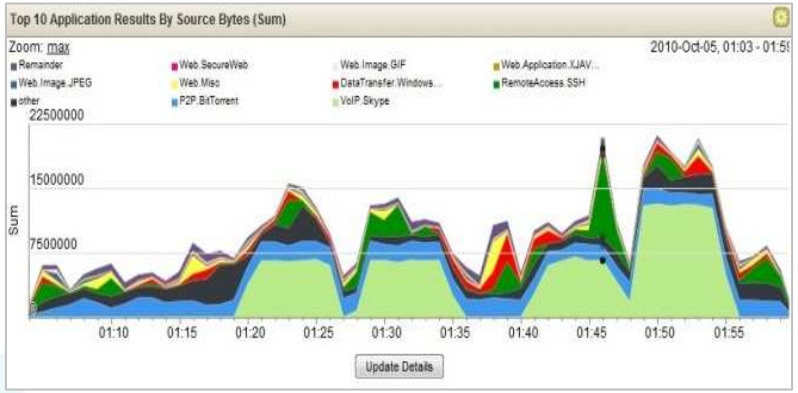
- Behavioral analytics and real-time correlation help better detect and prioritize stealthy attacks

- Integrated analysis of network flow data brings additional security intelligence to IBM Security Network Protection solutions:
  - Traffic profiling to **detect zero-day threats**
  - Correlation of threat & flow data for **enhanced incident analysis**
  - Network activity monitoring to profile **user and system behavior to improve threat intelligence and complement risk based access strategies**
  - Consolidation and correlation of data bring out the **"needle in the haystack"**
  - Network and application responsiveness to **troubleshoot connections, monitor peaks & outages, baseline for comparison,** and **distinguish anomaly types**

- Incorporates X-Force IP Reputation Feed, providing insight into suspect entities on the Internet, feeding correlation intelligence

Q1 Labs®
Total Security Intelligence | An IBM Company

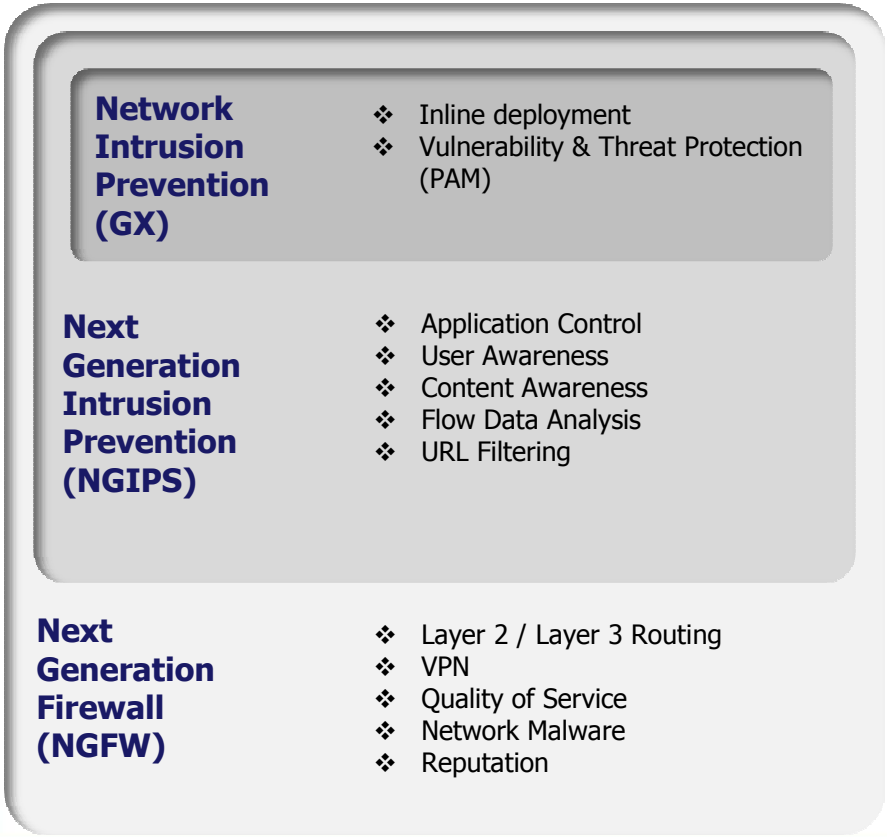




What is an NG-IPS?

According to Gartner…

- **Deployed as in-line device –** bump-in-the-wire solution
- **First-generation IPS Capabilities** – vulnerability and threat signatures; Detection and blocking at wire speed; Signature Updates
- **Application Awareness** – Identify & Enforce network security policy at the [web/network] application layer.
- **Context Awareness** –Use information from sources outside the IPS to make blocking decisions, or to modify the blocking rule base.
- **Content Awareness** – Inspect and classify inbound/outbound executables, and other similar file types, such as PDF and MS Office files. Make pass, quarantine or drop decisions in near real time.
- **Agile Engine** – Provide an upgrade path for the integration of new information feeds and new techniques to address future threats.



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

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

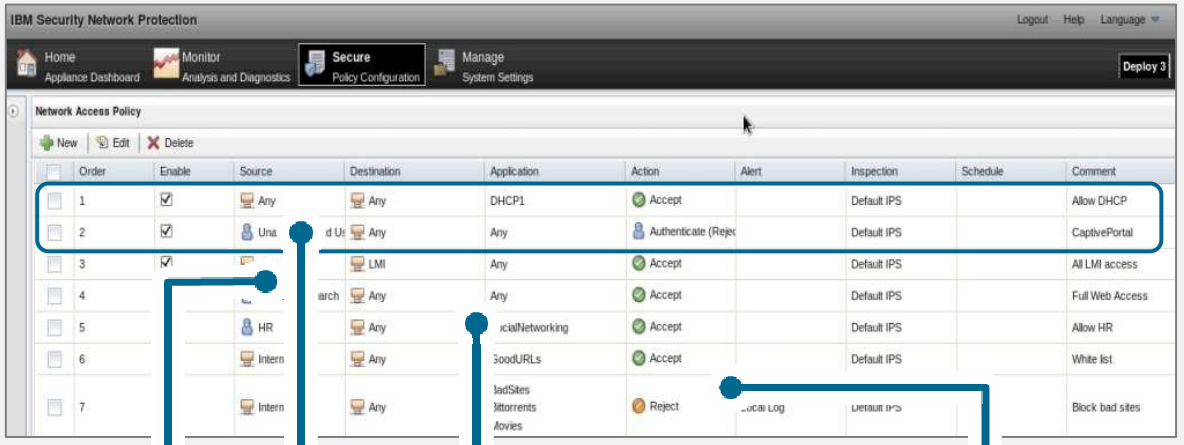
Ability to protect against the threats of today and tomorrow

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 soc networking, file shar 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

XGS – Introducing Advanced Controls

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

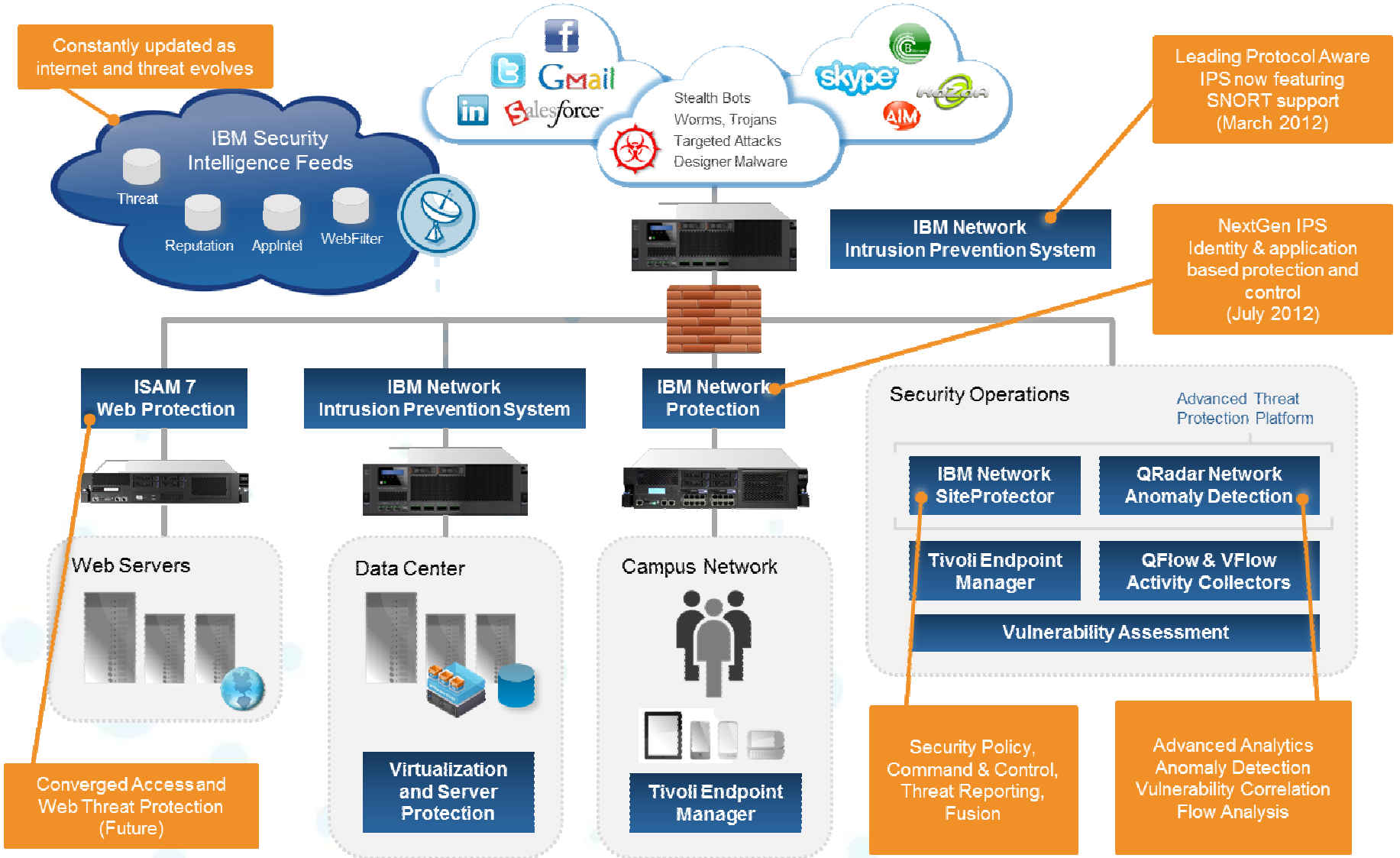
Web Applications

Non-web Applications

Web Category Protection	Allow marketing and sales teams to access social networking sites
Access Control	Block attachments on all outgoing emails and chats
Protocol Aware Intrusion Protection	A more strict security policy is applied to traffic from countries where I do not do business
Client-Side Protection	Advanced inspection of web application traffic destined to my web servers
Botnet Protection	Block known botnet servers and phishing sites
Network Awareness	
Web Protection	Allow, but don't inspect, traffic to financial and medial sites
Reputation	

Who	What	Controls	Security
172.29.230.15, 192.168.0.0 /16	80, 443,25, 21, 2048-65535	?	

Advanced Threat Protection Platform



IBM Internal & Business Partner Use Only

ibm.com/security