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.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
The challenging state of network security

**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

**POINT SOLUTIONS**
Point solutions are siloed with minimal integration or data sharing

Stealth Bots • Targeted Attacks
Worms • Trojans • Designer Malware

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

Optimizing the World’s Infrastructure
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

**Stealth Bots, Worms, Trojans**

**Targeted Attacks, Designer Malware**

**Network Defense**

- **Optimizing the World’s Infrastructure**
The Need to Understand the Who, What, and When

Who
172.29.230.15, 192.168.0.0 /16

What
80, 443, 25, 21, 2048-65535

Controls

Security

Access Control

Web Category Protection

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
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

- 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
  - 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

- 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
InformationWeek IT Pro Ranking: IPS and IDS

<table>
<thead>
<tr>
<th>Network IPS/IDS Overall Vendor Performance</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM/ISS</td>
<td>75%</td>
</tr>
<tr>
<td>Cisco Systems</td>
<td>74%</td>
</tr>
<tr>
<td>Check Point Software Technologies</td>
<td>74%</td>
</tr>
<tr>
<td>McAfee/NitroSecurity</td>
<td>72%</td>
</tr>
<tr>
<td>HP/TippingPoint</td>
<td>71%</td>
</tr>
<tr>
<td>Juniper Networks</td>
<td>71%</td>
</tr>
<tr>
<td>Intel/McAfee</td>
<td>71%</td>
</tr>
<tr>
<td>Snort</td>
<td>68%</td>
</tr>
</tbody>
</table>

IBM/ISS leads our vendor evaluation survey of network IPS/IDS vendors, earning an overall performance rating of 75%. Cisco Systems and Check Point Software Technologies are just behind at 74%. IT pros also evaluated HP, Intel, Juniper Networks and Snort.

When it comes to IPD/IDS features, IBM topped the competition for attack blocking and centralized management—two categories where open source stalwart Snort fared the worst.

- IBM Ranked #1 in 11 out of 12 Feature Evaluations:
  - 1 Gbps or higher throughput
  - Ability to block real-time attacks
  - Centralized management
  - DDoS detection/protection
  - Flexibility of signature and policy tuning
  - Full packet capture
  - Log export to SIEM
  - Low false positives/false negatives
  - Provides sufficient analysis without dropping packets
  - Robustness of community for rules and signatures
  - Speed of signature updates

- Ranked #2 in Pre-built compliance settings

Published August 2012
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

“We were able to detect the Trojan “Poison Ivy” within the first three hours of deploying IBM Security Network Protection”  
– Australian Hospital

---

**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

---

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
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

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

- 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

PCTY2012
No Download No Sharing
No Youtube and Facebook during office hours
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

Stealth Bots
Worms, Trojans
Targeted Attacks
Designer Malware

Proven Security
Ultimate Visibility
Complete Control

PCTY2012
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
Acknowledgements, disclaimers and trademarks

© Copyright IBM Corporation 2012. All rights reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs or services do not imply that they will be made available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM’s sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information concerning non-IBM products and services was obtained from a supplier of those products and services. IBM has not tested these products or services and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products and services. Questions on the capabilities of non-IBM products and services should be addressed to the supplier of those products and services.

All customer examples cited or described are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer and will vary depending on individual customer configurations and conditions. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

IBM, the IBM logo, ibm.com, Tivoli, the Tivoli logo, Tivoli Enterprise Console, Tivoli Storage Manager FastBack, and other IBM products and services are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml.