Managed Security Services

Securing a Smarter Planet

Globalization and Globally Available Resources

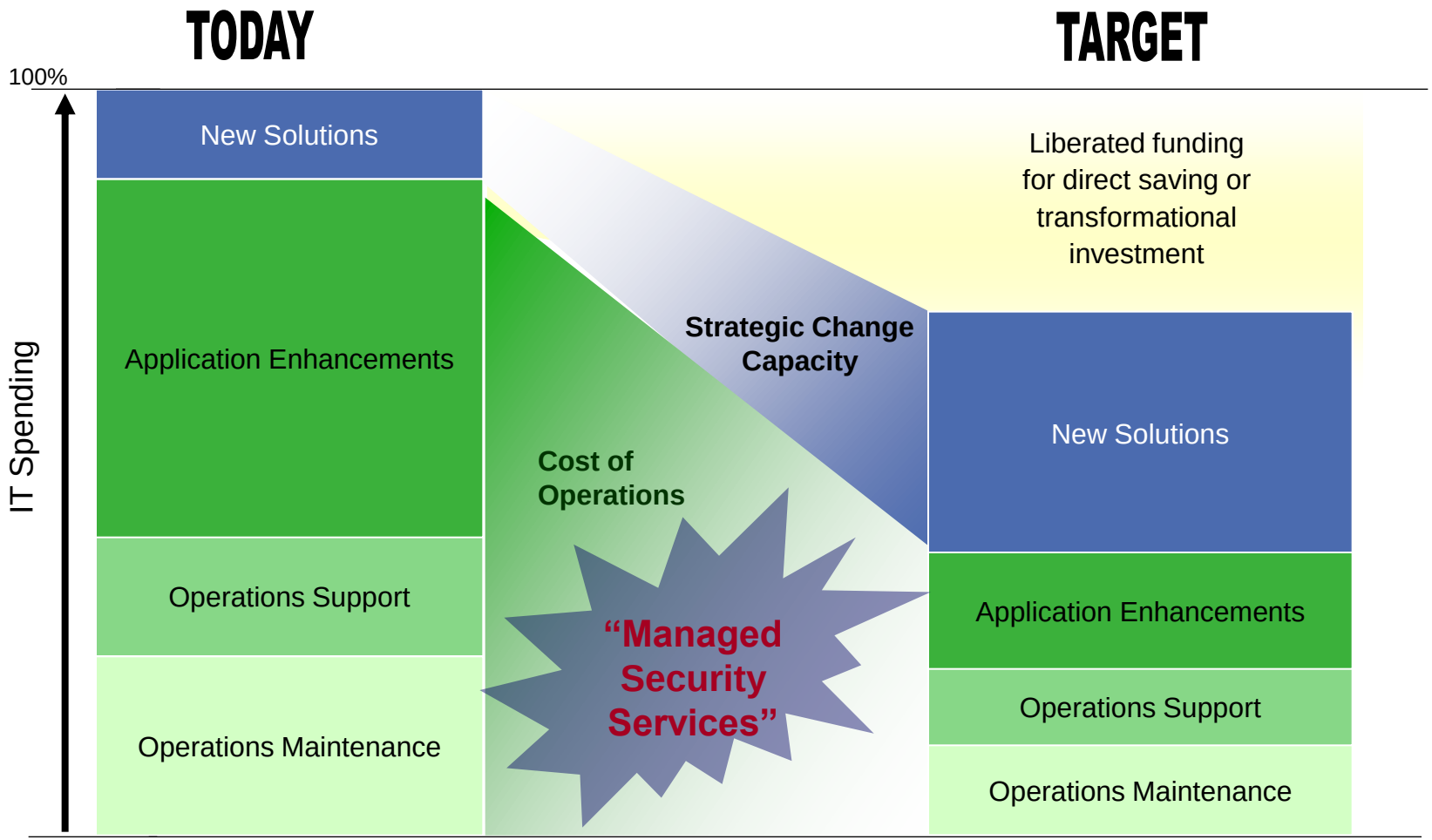
Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

New Forms of Collaboration

New possibilities.
New complexities.
New risks.

IBM can help you gain operational efficiencies and IT capacity -- to save money and increase investments in new solutions



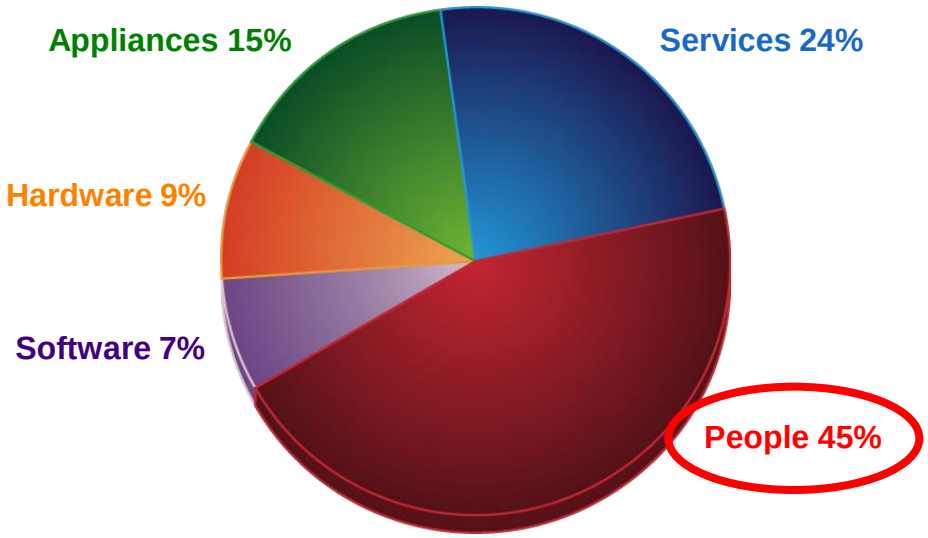
The Security Complexity & Cost Challenge

IT Security Priorities

Security Solution	Spend Priority
Access/ID	5
Firewall	3
Endpoint Firewall	7
Virtual Private Network (VPN)	6
Intrusion Detection Service (IDS)	1
Antivirus	11
Anti-spam	12
Spam Filtering	10
Web Filtering	13
Patching	8
Security Information Management	2
Vulnerability Assessment (VA)	9
Other	4

Source: Customer interviews

% of IT Spend



- Enterprises are looking to reduce security complexity
- Enterprises require integrated solutions that reduce total cost of protection and improves their security posture
- “People” consume the largest percent of IT spend

IBM delivers a new approach for sustainable business through manageable security

Designed to:

- **Enable innovation through secured, end-to-end infrastructure and platforms**
- **Reduce number and complexity of required security controls**
- **Reduce redundant security expenses**
- **Improve organizational and operational agility and resiliency**
- **Leverage industry expertise to help unify policy management**
- **Deliver needed visibility, control and automation**

5

Managed Security Services Portfolio Overview

Managed Security Services

- Managed Firewall Services
- Managed IPS and IDS Services
- Managed UTM Services
- Managed Protection Services for Networks and Servers
- Managed Secure Web Gateway

MSS Cloud Computing

- Vulnerability Management Services
- Security Event Management Services
- Secure Log Management Services
- IBM ISS X-Force® Threat Analysis Services
- Managed E-mail Security
- Managed Web Security

Multiple Device Types & Vendors Supported

What is the Virtual-SOC?

Virtual-SOC is the integrated security architecture enabling IBM to deliver market-leading Managed Security Services by combining advanced analysis and correlation capabilities, artificial intelligence, industry-leading security expertise and SLAs, and a high impact Web-based management portal in a single unified system.

Allows You To:

- Optimize Resources
- Reduce Complexity
- Enforce Security Policy
- Improve Overall Security Posture
- Demonstrate Compliance

Total Cost of Ownership Reducing Complexity, Improving Employee Productivity, Infrastructure Optimization

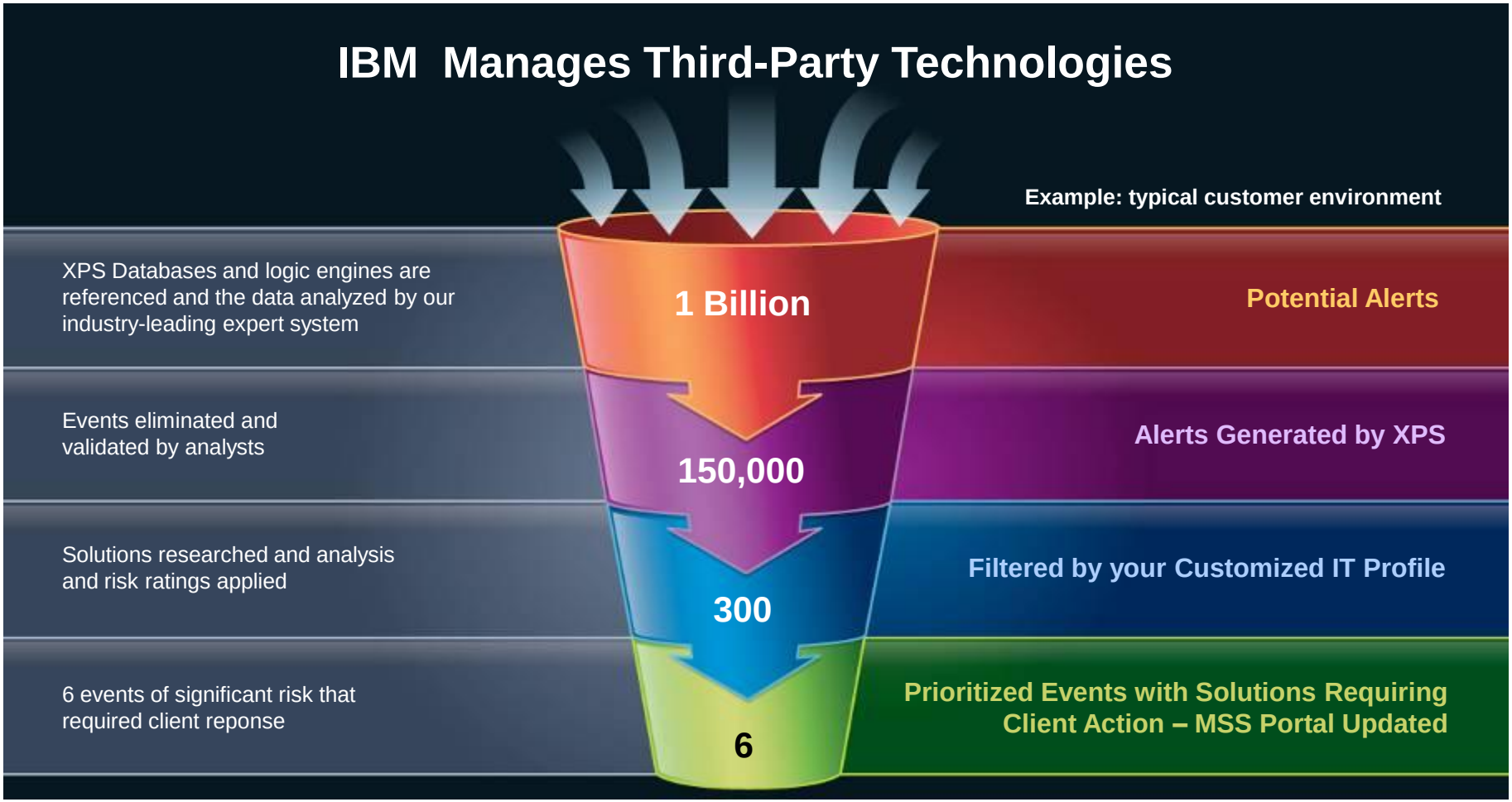
- **Open vendor architecture**
- **Consolidated security views**
  - Managed Security Services
  - Security Enablement Services
- **Powerful query & reporting options**
- **Automated event/ log analyses**

- **Unlimited event/ log archive**
- **Granular permissions system**
- **Guaranteed availability**
- **Integrated trouble ticketing & workflow**
- **Integrated IBM Internet Security Systems X-Force® intelligence**

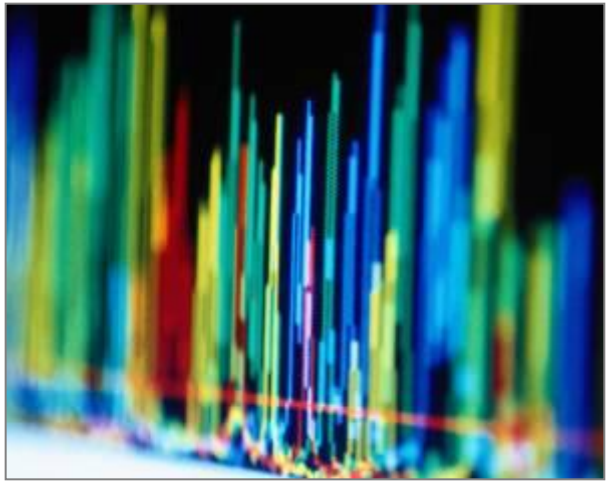
Virtual-SOC Portal

Virtual-SOC Integrated Services Architecture:

Client Example



Why IBM MSS



Guaranteed Protection

- Industry's leading performance-based service level agreement (SLA) with a cash-back payment*
- Designed to provide protection from known and unknown threats

Lower Total Cost of Ownership

- Reduced complexity
- Infrastructure Optimization
- Optimized Employee Productivity

Demonstration of Compliance

- A cornerstone of many clients' internal and regulatory controls for SOX, PCI, GLBA, HIPAA, etc.
- Enhanced process controls that clients can leverage to meet and maintain compliance
- Provides efficiencies in on-going compliance maintenance

*Attack must be confirmed by IBM Security Services Org

IBM global security reach

9 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 30,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 4 Billion+ Events Per Day

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

12

Thank you!

BACKUP CHARTS

The Power of Integrated Services

"MSS in Action"

Managed Protection Services with Vulnerability Management Services

1

Scan network to detect vulnerabilities.

2

Use the Virtual-SOC portal to request application of patch updates to protect entire network or individual servers.

3

Upon receipt of the patch request, an IBM ISS SOC analyst will implement an IPS rule, if applicable; to block access to the specific vulnerability and apply protection for the system until it is patched.

The Power of Integrated Services

"MSS in Action"

Managed Intrusion Detection/Prevention Service with the Managed Firewall Services

The Power of Integrated Services

"MSS in Action"

Security Event & Log Management Services & Managed Intrusion Detection/Prevention Services or Managed Firewall Services

1

IBM ISS provides the ability to manage, monitor, or view all of the customer's firewall, IDS and IPS devices.

2

IBM ISS provides customers with a consolidated security view and full reporting capabilities.

3

Customers can access secure log/event archival of all aggregated security events for up to 7 years.

4

Customer can leverage combined trouble ticketing capabilities to track issue resolution transparently across managed and unmanaged devices.

The Power of Integrated Services

"MSS in Action"

X-Force® Threat Analysis Service and Vulnerability Management Services

1

Schedule automated scans to identify OS's, applications, and their respective vulnerabilities.

2

Scan results dynamically reconfigure the customer's XFTAS alerting preferences, providing real-time alert notifications for actionable vulnerabilities.

3

Remediation workflow management features of the VMS service allow for generation of tickets for vulnerable assets with powerful grouping and prioritization capabilities.

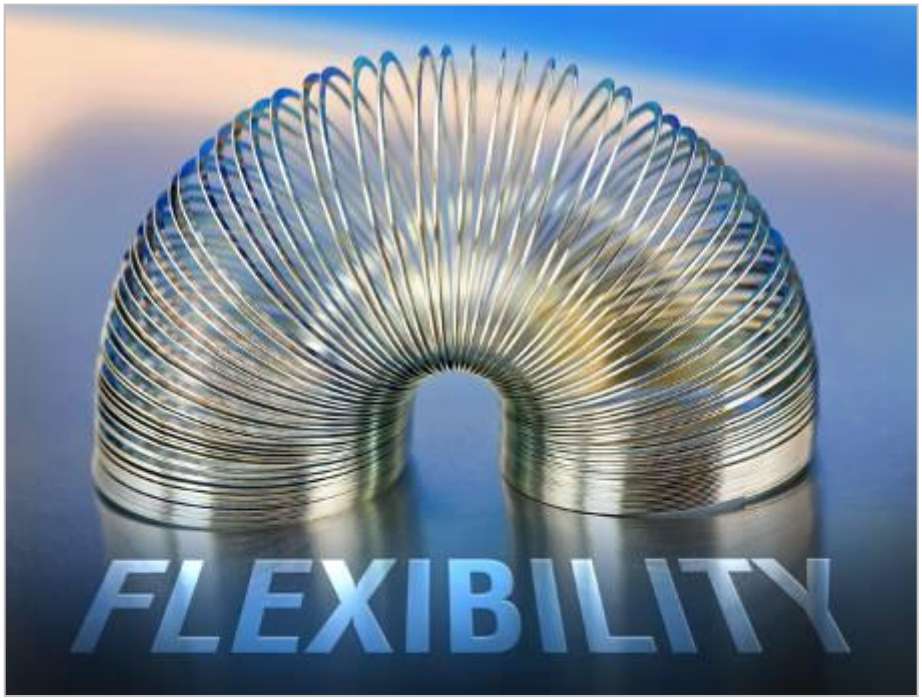
4

Validated remediation tasks have been completed by re-scanning of vulnerable assets.

Flexible Service Options

What You Get

- Multiple service levels to fit business goals
- Dynamic outsourcing:
  - **Anytime:** Peak hours, off-peak hours, days, nights, weekends
  - **Anyhow:** In-house, outsourced or a combination of both
  - **Anywhere:** Multiple devices, globally, remotely
- Traditional and performance-based SLAs
- Vendor and device agnostic services
- Traditional managed service options, cloud-based, Security as a service delivery options (Security enablement services)



MSS - Lower Total Cost of Ownership

Reduced Complexity

- **Consolidates multi-vendor environments for easier management and operational focus**
  - ISS, CheckPoint, Cisco, Juniper, Symantec, McAfee, TrendMicro, 3com and more…
- **Allows organizations to consolidate and efficiently manage global operational footprints**
  - Globally distributed resources, regional/remote offices, mobile workforce, independent security management, centralized framework
- **Simplifies information overload… Security Event and Log Data**
  - Example: Firewalls & IDS
    - Over 150GB of data per week
    - Generate over 250,000 alerts
    - Complex environments can generate over 250,000,000 events and logs a day

MSS - Lower Total Cost of Ownership

Infrastructure Optimization

- **Aggressive elimination of malicious traffic resulting in maximized network uptime, availability, and bandwidth**
  - Preemptive protection, integrated vulnerability management and security intelligence, expert deployment and configuration
  - Proactive risk management vs. reactive..."Ahead of the Threat”
- **Integrated services delivery allows for the seamless integration of disparate security technologies from multiple vendors together with built in security intelligence allows for improved decision making and maximization of infrastructure investment**
  - Integrated X-Force security intelligence
  - Virtual patching
  - V-SOC XPS automated correlation, normalization and prioritization for both managed and unmanaged devices
  - Integrated trouble ticketing and workflow for faster, automated remediation

MSS - Lower Total Cost of Ownership

Infrastructure Optimization

- **Simplification of on-going security management, allows for re-allocation of cost savings**
  - V-SOC portal presents single view for overall security management of disparate security technologies from multiple vendors for both managed and unmanaged devices
  - V-SOC XPS automates many of the management functions that would other have to be performed manually
  - Integrated ticketing and workflow for faster, automated remediation
  - Unlimited security log and event storage in a forensically sound manner for easy retrieval for security investigation and forensics

- **Improved evaluation, configuration and deployment of new security technologies, improves speed to protection and optimizes security capabilities**
  - Expert deployment and policy configuration and tuning to meet your specific business objectives
  - Utilization of best security practices for compliance
  - Vendor agnostic capabilities

- **Global, yet local capabilities and scalability for optimization of existing infrastructure**
  - Consistent delivery of services from global SOCs with localized language and local resources
  - We have a VSOC in Hortolandia - Brazil

MSS - Helps Demonstrate Compliance

- A cornerstone of many clients' internal and regulatory controls for SOX, PCI, GLBA, HIPAA, etc.
  - Collecting, monitoring, archiving logs for access control policy violations (24/7/365)
  - Reporting for system policies and change control
  - Documented best practices in security infrastructure management
  - Integrated delivery of security technologies required by many regulations such as firewall, intrusion detection systems, vulnerability management, security event and log management, etc.
- Enhanced process controls that clients can leverage to meet and maintain compliance
  - IBM ISS MSS follows security best practices in accordance to ISO and COBIT standards
    - *The same standards from which government and industry regulations are written*
  - Physical security, network security, facilities continuity, infrastructure security, fire protection, disaster recovery, security and privacy policies, certified processes and procedures
  - IBM holds some of the industry's top certifications by which clients can leverage
    - *SAS70 Type II attested*
    - *AICPA SysTrust certified for security, availability, & confidentiality*
- Provides efficiencies in on-going compliance maintenance
  - Save time and money maintaining compliance while improving your security posture!

Security Expertise: X-Force Research & Development

**The IBM X-Force®
research and development team: the world's leading enterprise security organization**

- The core of all IBM Security products and services
- Focuses on analyzing and researching threats and vulnerabilities to develop preemptive protection technologies
- Integrates with IBM MSS for global threat monitoring
- Maintains the most comprehensive vulnerability DB in the world, and analyzes each and every one to determine impact against threats