Welcome
– Inside the developers studio

Paul Cooper

IBM Security Solutions

Business Unit Executive, ANZ

19 May 2011

The IBM
SecurityStudio Tackling the illusion of absolute security

Today's Topics - Morning

Session Topic	Time	Presenter
Introduction	9:00-9:05	Paul Cooper, Business Unit Executive, IBM Security Solutions ANZ
Welcome to the lab	9:00-9:10	Paul Jensen, Security Development Manager, Gold Coast, IBM Australia
Keynote – The Future Direction of IBM Security Solutions	9:15–9:50	Glen Gooding, IBM Security Solutions Executive, Asia Pacific
Managing Security and Identity In The Cloud	9:50–10:10	Neil Readshaw, Senior Software Engineer, Gold Coast Security Development Labs, IBM Australia
Morning Tea	10.10-10.30	
Next Generation of Protection from IBM – preview of major new security product from IBM	10:30-11:00	Dr Paul Ashley, Software Development Manager, Gold Coast Security Development Labs, IBM Australia
User-Centric Identity: practical use cases around access to social media and cloud applications	10:50–11:30	Shane Weeden, Senior Software Engineer, Gold Coast Security Development Labs, IBM Australia
How to Include Distributed Endpoints in Your Early Warning System	11:30-11:50	Matthew Prince, Senior IT Security Specialist, IBM Australia
Access Management Landscape – Fraud and Mobility	11:50-12:10	Chris Hockings, AP Team Leader Software Advanced Technology (SWAT), IBM Australia
Lunch	12:00-12:30	

Today's Topics - Afternoon

Session Topic	Time	Presenter
Is Your Organisation ready for the mobile device explosion? Roundtable discussion	12:45-13:30	Glen Gooding - facilitator
Who is looking after the safety of your database?	13:30-14:00	Scott Henley, Security Architect, IBM Australia
Afternoon Tea	14:00-14:15	
Gold Coast Security Labs 5-Minute Technical Showcase		
1. Addressing common security pitfalls of virtualised infrastructure	14:15-14:20	Andrew Sallaway, Gold Coast Security Development Labs, IBM Australia
2. Enhancing user convenience through smart card single sign-on	14:20-14:25	Jenny Wong, Gold Coast Security Development Labs, IBM Australia
3. breaking the sound barrier of intrusion prevention	14:25-14:30	Glen Leeder, Gold Coast Security Development Labs, IBM Australia
4.What's happening in web security on the Gold Coast	14:30-14:35	Simon Canning, Gold Coast Security Development Labs, IBM Australia
5. Managing large number of emerging threats in the application space	14:35-14:40	Steven Schmidt, CISSP, CISA A/NZ Technical Sales Specialist, IBM Australia
Closing remarks	14:40-15:00	Paul Cooper, Business Unit Executive, IBM Security Solutions ANZ

The IBM
SecurityStudio Tackling the illusion of absolute security

The Future Direction of IBM Security Solutions

Glen Gooding

AP Lead Security Tiger Team

19 May 2011

The IBM SecurityStudio Tackling the illusion of absolute security

Agenda

- Gold Coast Security Development
- A Unique Point of View on Security
- Vision and Strategy
- IBM security – in action today
- Questions and Answers

3 Key Take Aways

Principles of Secure by Design

How IBM helps customers to achieve Compliance, reduce Complexity and lower Costs

The elements of the Security Framework

A perspective that evolves with realization of the smarter planet

The planet is getting more
Instrumented, **Interconnected** and **Intelligent**.

1 trillion

By next year, an estimated 2 billion people will be on the Web... and a **trillion** connected objects – cars, appliances, cameras, roadways, pipelines – comprising the "Internet of Things."

90%

Nearly **90%** of innovation in automobiles is related to software and electronics systems. 30-60% of the value is in the software.

162 million

Almost **162 million** smart phones were sold in 2008, surpassing laptop sales for the first time.

Approximately 70% of the digital universe is created by individuals, **but enterprises are responsible for 85%** **of the security, privacy, reliability, and compliance.**

Security enables us to address these risks and innovate confidently

Safe Adoption of new Forms of technology

Protection of digital identities and Privacy

New Business Models like outsourcing and teleworking

Adoption of virtualization and cloud computing

Addressing compliance complexity

Information availability and integrity for real time decision making

Today's Security Concerns

- **Greater complexity and increased attack surface**

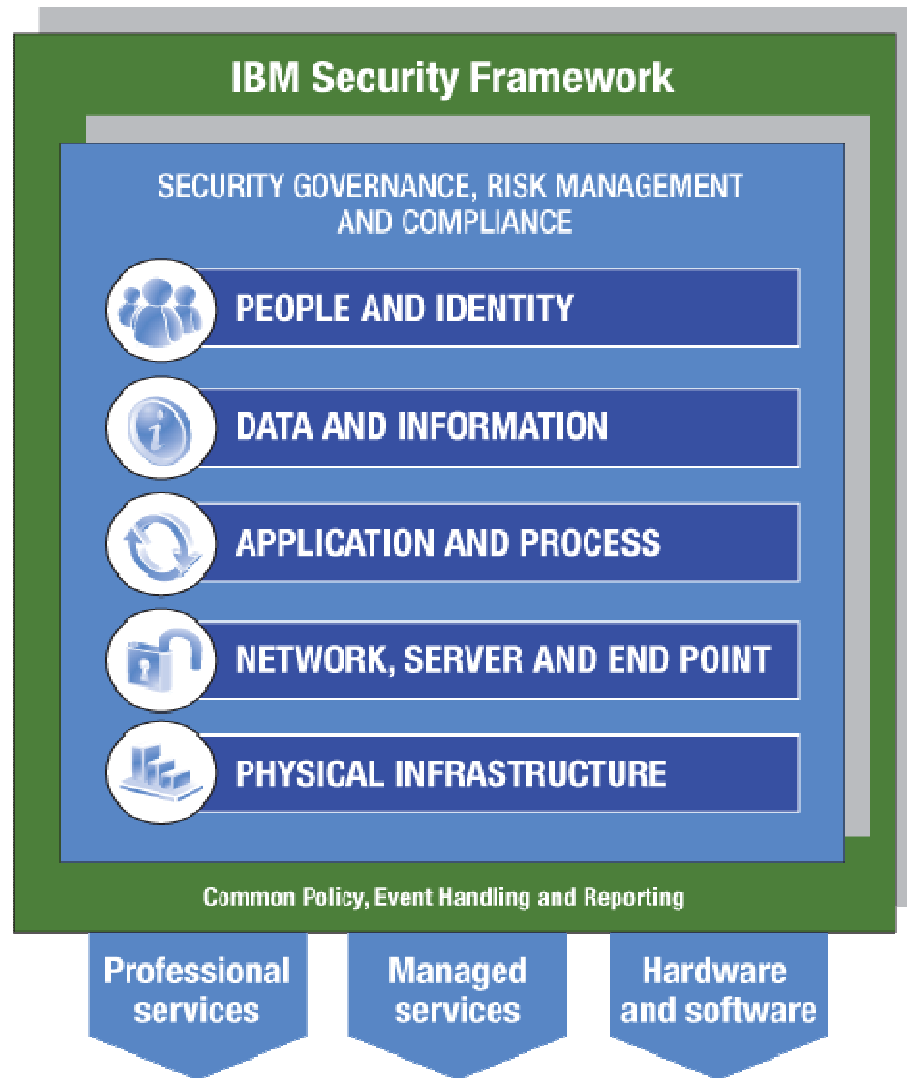|	
• **Growing threat to critical infrastructure/national security**	• **Growing threat to online services**
• **Emergence of a sophisticated market for software flaws**	• **New level of complexity in malware not seen before**

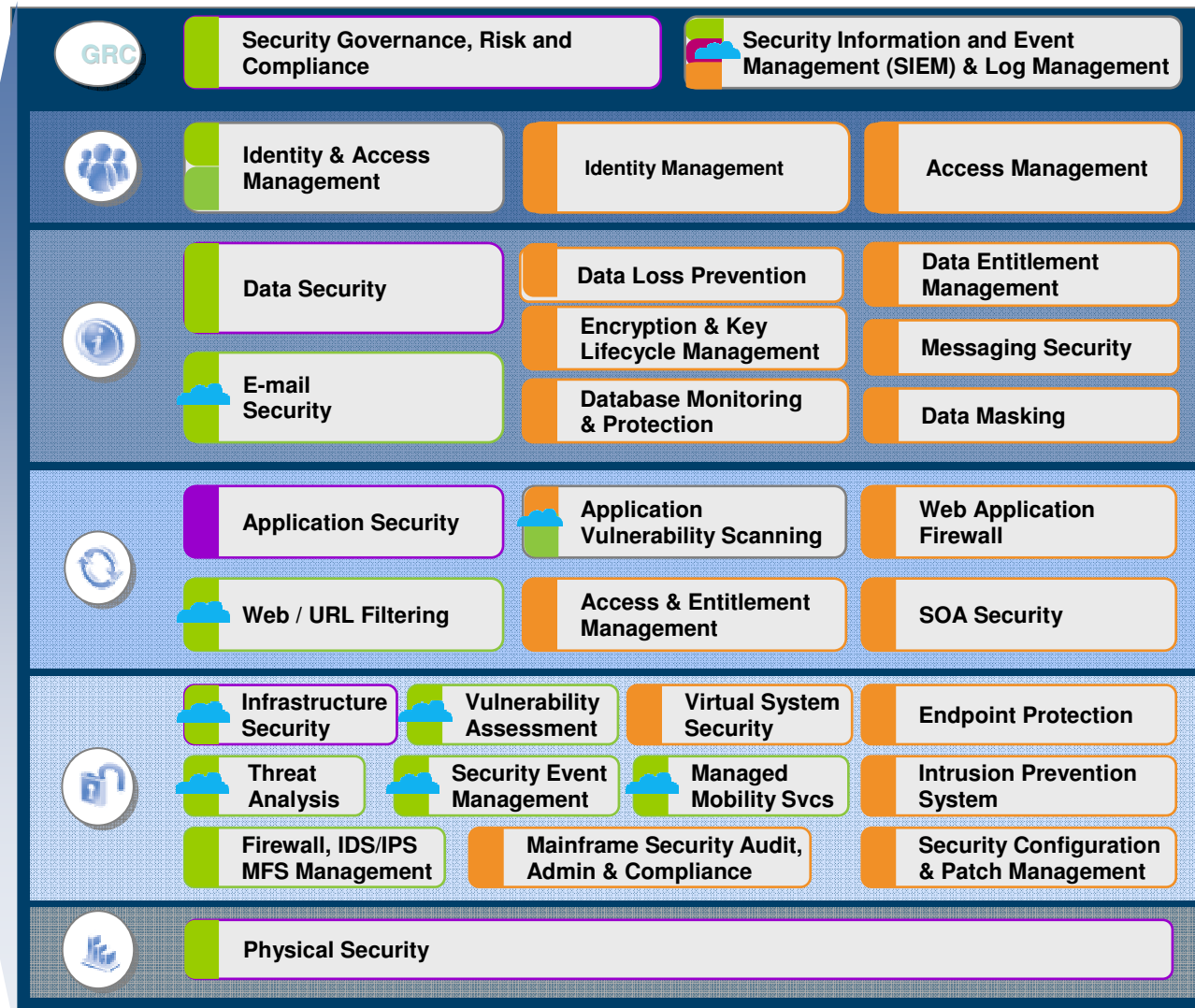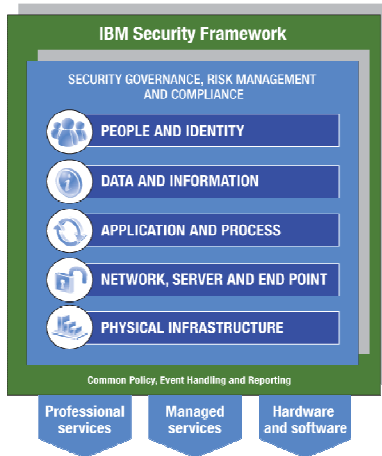- **Compliance regulations & industry codes of practice will increase system complexity**

Our strategy?: IBM Security Framework

Our strategy?: Be comprehensive, leverage partners

Professional Services

Managed Services

Products

Cloud Delivered

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software

GRC

Security Governance, Risk and Compliance

Security Information and Event Management (SIEM) & Log Management

Identity & Access Management | Identity Management | Access Management

Data Security | Data Loss Prevention | Data Entitlement Management

| | Encryption & Key Lifecycle Management | Messaging Security |

E-mail Security | Database Monitoring & Protection | Data Masking

Application Security | Application Vulnerability Scanning | Web Application Firewall

Web / URL Filtering | Access & Entitlement Management | SOA Security

Infrastructure Security | Vulnerability Assessment | Virtual System Security | Endpoint Protection

Threat Analysis | Security Event Management | Managed Mobility Svcs | Intrusion Prevention System

Firewall, IDS/IPS MFS Management | Mainframe Security Audit, Admin & Compliance | Security Configuration & Patch Management

Physical Security

TREND MICRO | symantec. | FIDELIS | DS³ | JUNIPER NETWORKS | Check Point SOFTWARE TECHNOLOGIES LTD. | CISCO | Blue Coat | RAPID7 | websense ESSENTIAL INFORMATION PROTECTION | VERDASYS. | MODULO Solutions for GRC

IBM security – one of the largest players in the world

| 9 Security Operations Centers | + | 9 Security Research Centers | + | 11 Security Solution Development Centers | + | 133 Monitored Countries | + | 900+ Professional Services Security Consultants | + | 600+ field security specialists | + | 4,500 Security Delivery Experts | + | 400+ security operations analysts |

Zurich, CH
Delft, NL
Ottawa, CA   Toronto, CA   Brussels, BE   Herzliya, IL
Boulder, US
Almaden, US   TJ Watson, US   Tokyo, JP
Costa Mesa, US   Detroit, US   Haifa, IL   Bangalore, IN   Tokyo, JP
Austin, US   Raleigh, US   Pune, IN   Taipei, TW
Atlanta, US   Bangalore, IN
Atlanta, US   Atlanta, US   Singapore, SG
Brisbane, AU
New Delhi, IN   Gold Coast, AU
Hortolândia, BR   Perth, AU

- 20,000+ Devices under Contract
- 3,700+ MSS Clients Worldwide
- 9 Billion+ Events Managed Per Day

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

Our strategy?: Research = Intelligence = Security

**The mission of the
IBM Internet Security Systems™
X-Force® research and development
team is to:**

- **Research and evaluate threat and protection issues**

- **Deliver security protection for today's security problems**

- **Develop new technology for tomorrow's security challenges**

- **Educate the media and user communities**

X-Force Research

10B	analyzed Web pages & images
150M	intrusion attempts daily
40M	spam & phishing attacks
46K	documented vulnerabilities

Millions of unique malware samples

**IBM builds technology for
tomorrow based on IBM Research**

- Identify mission-critical enterprise assets and very sensitive data.

- Build fine-grained perimeters

- Monitor fine-grained perimeters and close the loop

- End-to-end security

- Secure by design

Our strategy?: Security for the Business and IT

VISIBILITY
Monitor in real-time

CONTROL
React quickly & effectively

AUTOMATION
Achieve efficiency

Business

Defines the need (compliance, threat) and needs the reports

GRC
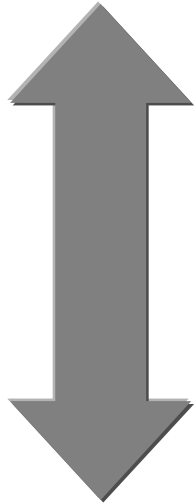
Buys the technology and deploys the control

IT Operations

Mitigate the risks

People & Identity

Network Server & Endpoint

Data & Info

Application & Process

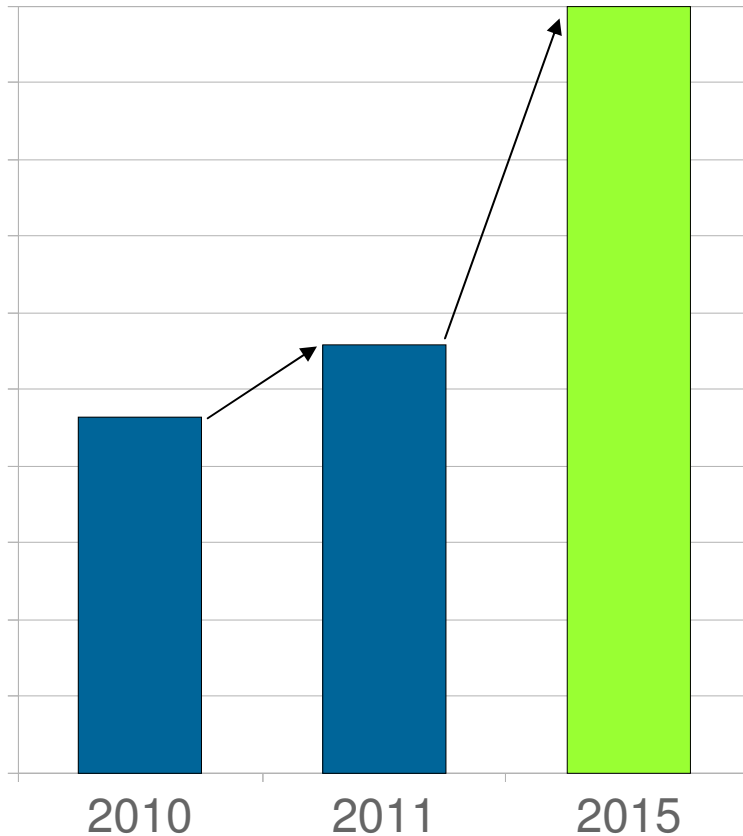# Our strategy?: Security for your Industry
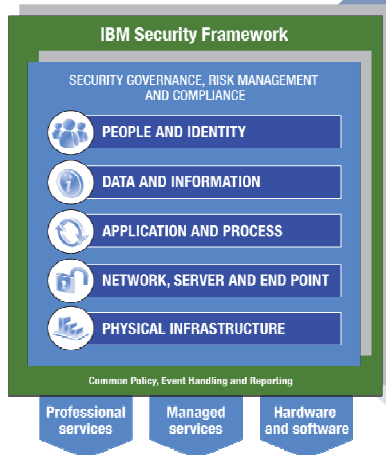
IBM understands emerging challenges facing industries

Health Care – Energy & Utilities

Our strategy?: Security is a growth play!

IBM Security – Vision 2015

2010   2011   2015

RESEARCH
Security & Privacy
X-Force

STG
Security Server
(RACF)
Crypto cards

GBS
Security & Privacy
Practice

IBM
Security Solutions

SWG
AIM/DataPower
IM/Guardium/Optim
Lotus/Protector
Rational/AppScan
Tivoli/ISS/Big Fix

GTS
Professional Services
Managed Services

IBM Security acquisitions *(1999 – 2010)*:

DASCOM   access360   DATAPOWER   consul   INTERNET SECURITY SYSTEMS   ENCENTUATE   watchfire   OUNCE LABS   Guardium   princeton softech   BIGFIX
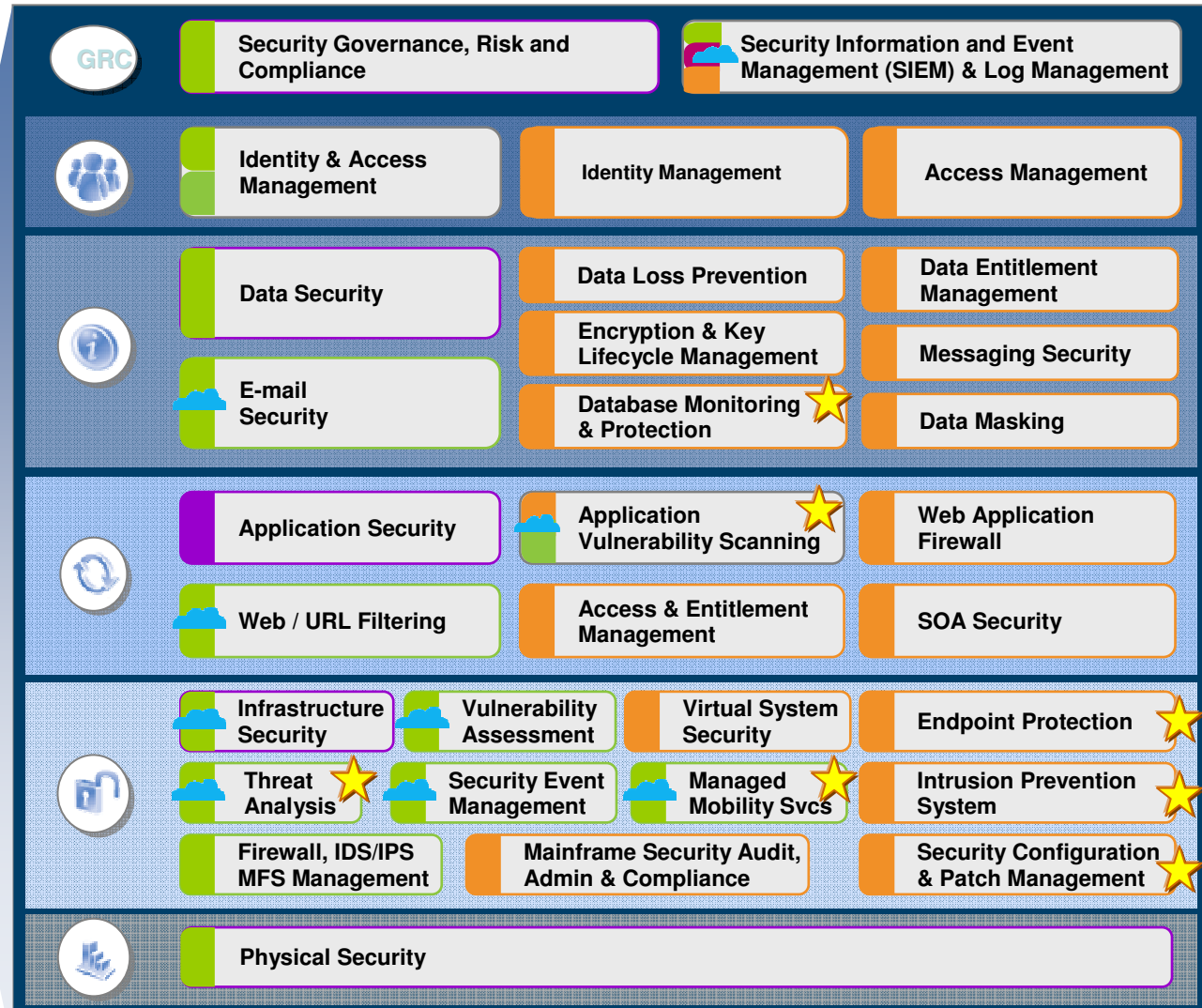
Key Themes Driving 2011 Announcements

Key Themes from Customers:

- Proliferation of "smart" devices

- Securing cloud…

- … security as a Cloud-based service

- Cybersecurity and the advancement of threats

- Application vulnerabilities and attacks

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

IBM Security Solutions Announcements at a Glance

Professional Services

Managed Services

Products

Cloud Delivered

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software

GRC

| Security Governance, Risk and Compliance | Security Information and Event Management (SIEM) & Log Management |

| Identity & Access Management | Identity Management | Access Management |

Data Security	Data Loss Prevention	Data Entitlement Management
	Encryption & Key Lifecycle Management	Messaging Security
E-mail Security	Database Monitoring & Protection	Data Masking

| Application Security | Application Vulnerability Scanning | Web Application Firewall |
| Web / URL Filtering | Access & Entitlement Management | SOA Security |

Infrastructure Security	Vulnerability Assessment	Virtual System Security	Endpoint Protection
Threat Analysis	Security Event Management	Managed Mobility Svcs	Intrusion Prevention System
Firewall, IDS/IPS MFS Management	Mainframe Security Audit, Admin & Compliance		Security Configuration & Patch Management

| Physical Security |

The IBM SecurityStudio Tackling the illusion of absolute security

Identity & Access Management – in action today

- **Improve service**:
  - Enabling collaboration via role-based portals with access to services and applications.
  - Increasing market reach for services with federated access

- **Reduce costs**:
  - Centrally managing accounts, groups, policies, credentials, and access rights throughout the user lifecycle.
  - Automating the on-boarding and off-boarding of users
  - Decreasing help desk calls relating to password resets
  - Make it easier to integrate identity context

- **Support compliance efforts**:
  - Validating user identities, monitoring user activity, facilitating strong authentication deployments via step-up authentication
  - Centralizing and automating compliance reporting

Enabling Innovation

- *Cloud*

- *Multi Factor Authentication*

- *Identity and Access Governance*

Data & Information Security – in action today

- **Prevent data breaches & fraud**
  - Cybercriminals & rogue insiders
  - Protect customer & HR data, corporate secrets (IP)

- **Assure data governance**
  - Prevent unauthorized changes to financial data by privileged users

- **Reduce audit costs**
  - Automated, continuous controls
  - Unified heterogeneous policies
  - Simplified audit processes
  - *… without performance impact or changes to databases or applications*

- 92% of all breached records originate in database servers *(2010 Data Breach Report)*

- SQL injection plays a role in 79% of records compromised *(2010 Data Breach Report)*

- 3 of 4 organizations can't prevent privileged insiders from reading or tampering with data in their databases *(Independent Oracle User Group)*

- 85% of organizations ship unmasked production data to developers & outside parties *(Independent Oracle User Group)*

Application Security – in action today

- Trend now is to focus on application security early in the development cycle

- Addressing regulatory compliance around sensitive data accessed from applications

- Proactively reducing greatest area of IT business risk

- Enabling productivity gains from automation of vulnerability management for applications

- Application vulnerabilities are the **greatest source of risk** for organizations
  - **55% of all vulnerabilities** are Web application vulnerabilities

- 76 percent of CEO's feel that **reducing potential security flaws** within business-critical applications is the most important aspect of their data protection program.

- **Cost of data breach**:
  - *$204 – Cost of companies per compromised record*
  - *$6.6 Million – Average cost per data breach "incident"*

Network, Server and Endpoint security – in action today

- Protecting networks : Mitigate network based threats and prevent data loss

- Protecting Servers: Mitigate threats against servers, prevent data loss

- Protecting Endpoints: Effective management can cut total cost of ownership for secure desktops by 42%

- Protecting Hypervisors: Effective security controls built around your ever increasing VM farm

- Addressing threat and compliance risks to your data and infrastructure requires innovation and focus on two dimensions:
  - Need continuous security content updates
  - Scalable, modular protection and management platforms
  - Defense in depth

Enabling Innovation

- Protect the <u>whole</u> 10GbE segment TWICE with innovations achieving speed

- Innovations of security content to match the threat landscape

- Innovation of integrations that matter, saving customers time & money !

Introducing Tivoli Endpoint Manager
– Smarter, Faster Endpoint Management

Capabilities

- Security Configuration Management
- Vulnerability Management
- Asset Management
- Network Self Quarantine
- Multi-Vendor Endpoint Protection Management
- Anti-Malware & Web Reputation Service

- Network Asset Discovery
- Endpoint HW, SW Inventory
- Patch Management
- Software Distribution
- OS Deployment
- Remote Desktop Control
- Software Use Analysis
- Power Management

Investments in R&D to extend BigFix technology to secure Android-based smart phones and smart meters.

Report
Assess
Enforce
Remediate

IBM Tivoli Endpoint Manager
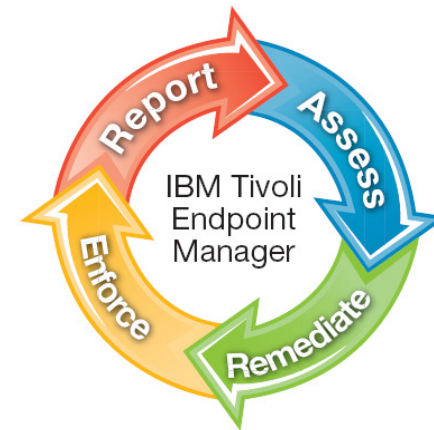
Solution Features

- Single intelligent agent for continuous endpoint self-assessment and policy enforcement

- Real-time visibility and control from a single management console

- Manage physical and virtual endpoints regardless of location, connection type or status

- Support heterogeneous platforms – Windows, UNIX, Linux and Mac operating systems

Announcing Managed Mobile Security Services – Securing Client Mobility from the Cloud

Designed to provide expert monitoring and management of policy enforced mobile connectivity to corporate and enterprise-wide assets.

Built upon the Juniper mobile security technology, this solution incorporates design and deployment capabilities along with managed services to accelerate time to value and drive established security measures to mobile endpoints.

Key Benefits

- Combines leading mobile security technology with comprehensive deployment and management services

- Allows businesses to **regain control over data** stored and disseminated to mobile smartphones, including Symbian, iOS, Android, Blackberry, and Windows Mobile

- Helps organizations **reduce the impact of lost devices** by offering location identification and remote lock/wipe functionality

Core Capabilities

Design and implementation

Broad mobile platform support

Secure, policy based connectivity

Deep security technology

Backed by IBM's industry leading MSS

The IBM®
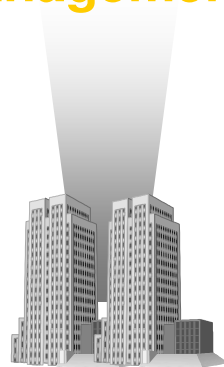**SecurityStudio** Tackling the illusion of absolute sec

IBM Cloud-based Services

From the Cloud – IBM Security Operations Centers
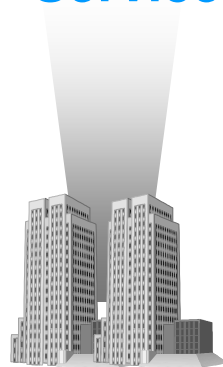
Security Event and Log Management

Vulnerability Management Service

Managed Web and Email Security Service

X-Force Threat Analysis Service

Subscription service

Cloud based

Monitoring and management

Offsite management of logs and events from IPS's, Firewalls and OSs

Proactive discovery and remediation of vulnerabilities
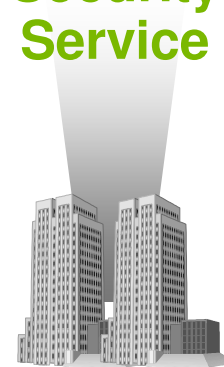
Protection against spam, worms, viruses, spyware, adware, and offensive content

Customized security intelligence based on threat information from X-Force research and development team

To the Customer – Offloading Security Tasks on the Ground

The IBM
SecurityStudio Tackling the illusion of absolute security

24

Summary: IBM has a unique perspective on security

Trusted Partner	Security Company	Solution Provider	The Company
Helping customers build smarter cities, smarter grids, new data centers, trusted passport systems and more	40+ years as leading provider of software and services across a vast array of security product and services segments	A leading provider of software and hardware solutions around the world	400,000 employees across 130 countries with private data to protect

IBM Security Solutions

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software