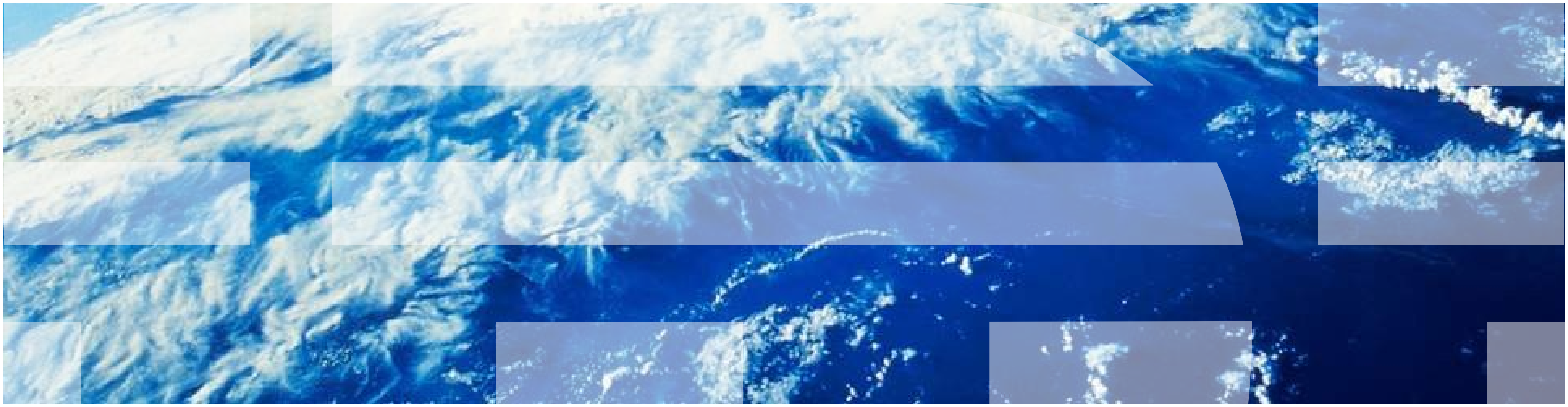
Christian Fahlke
GMT Channel Leader Internet Security Systems
IBM Central & Eastern Europe, Middle East and Africa (CEEMEA)

May 20th, 2009

Securing a Dynamic Infrastructure

IT Virtualization – new challenges



© 2009 IBM Corporation

Global market forces are impacting us all

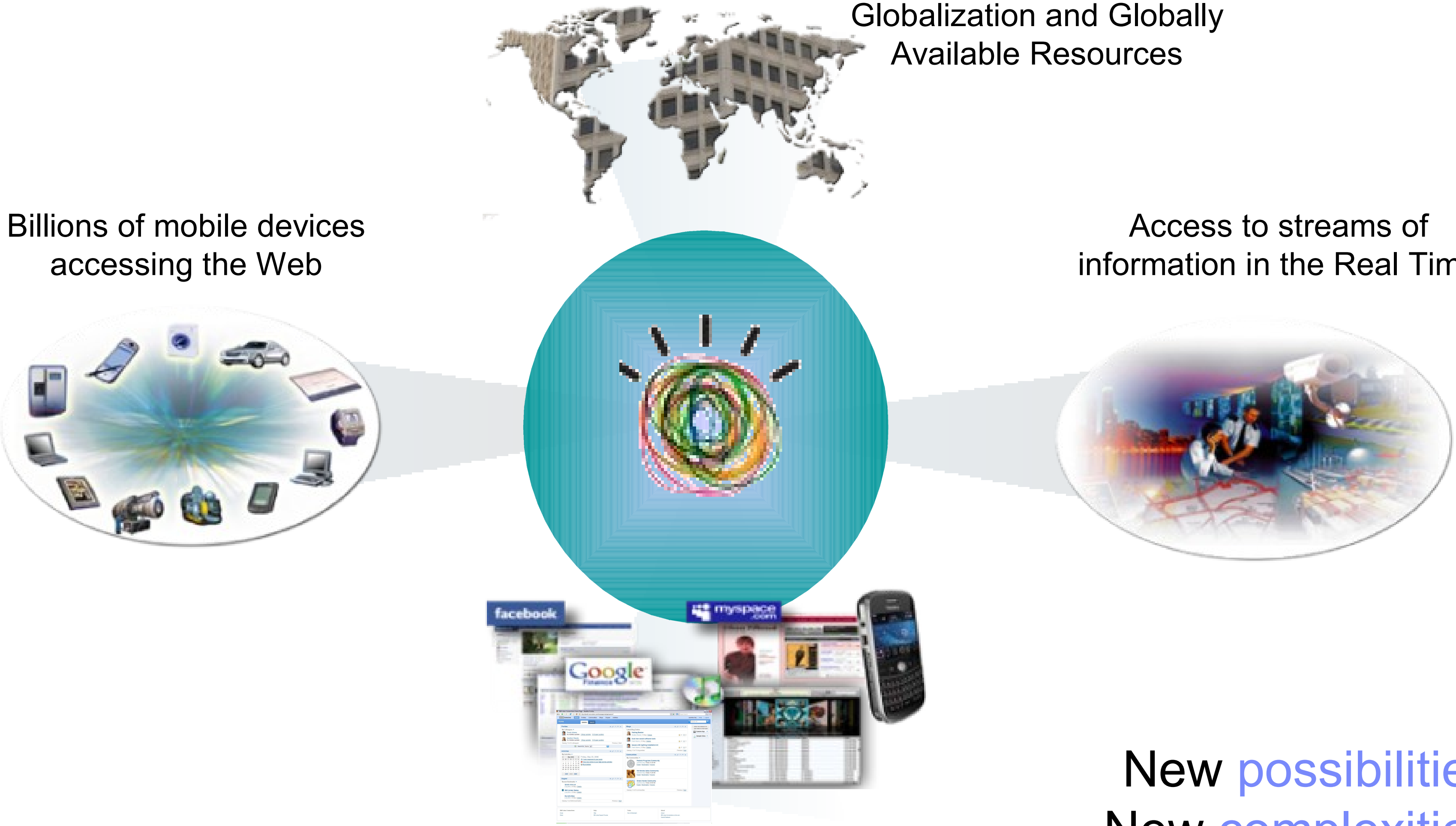
- Reality of living in a globally integrated world
  - Widespread impact of economic downturn and uncertainty
  - Energy shortfalls and erratic commodity prices
  - New customer demands and business models
  - Information explosion and risk/opportunity growth
- Businesses are under increasing pressure to effectively:
  - Manage operational cost and complexity
  - Deliver continuous and high-quality service
  - Address security risks intensified by innovation, emerging technologies, data/information explosion, etc.

> "We have seen more change in the last 10 years than in the previous 90."
>
> Ad J. Scheepbouwer,
> CEO, KPN Telecom

The planet is getting instrumented, interconnected and intelligent.

© 2009 IBM Corporation

Welcome to the **smart planet**… *and a smarter infrastructure*



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.

© 2009 IBM Corporation

Managing risks introduced by new opportunities

Emerging technology

- Virtualization and cloud computing increase infrastructure complexity and can reduce visibility to overall risk posture.
- Web 2.0 and SOA style composite applications introduce new challenges with the applications being a vulnerable point for breaches and attack.

Data and information explosion

- Data volumes are doubling every 18 months.*
- Storage, security, and discovery around information context is becoming increasingly important.

Wireless world

- Mobile platforms are developing as new means of identification.
- Mobile security technology is less mature than the security used to protect PCs.

Supply chain

- The chain is only as strong as the weakest link… partners need to shoulder their fair share of the load for compliance and the responsibility for failure.

Clients expect privacy

- An assumption or expectation now exists to integrate security into the infrastructure, processes and applications to maintain privacy.

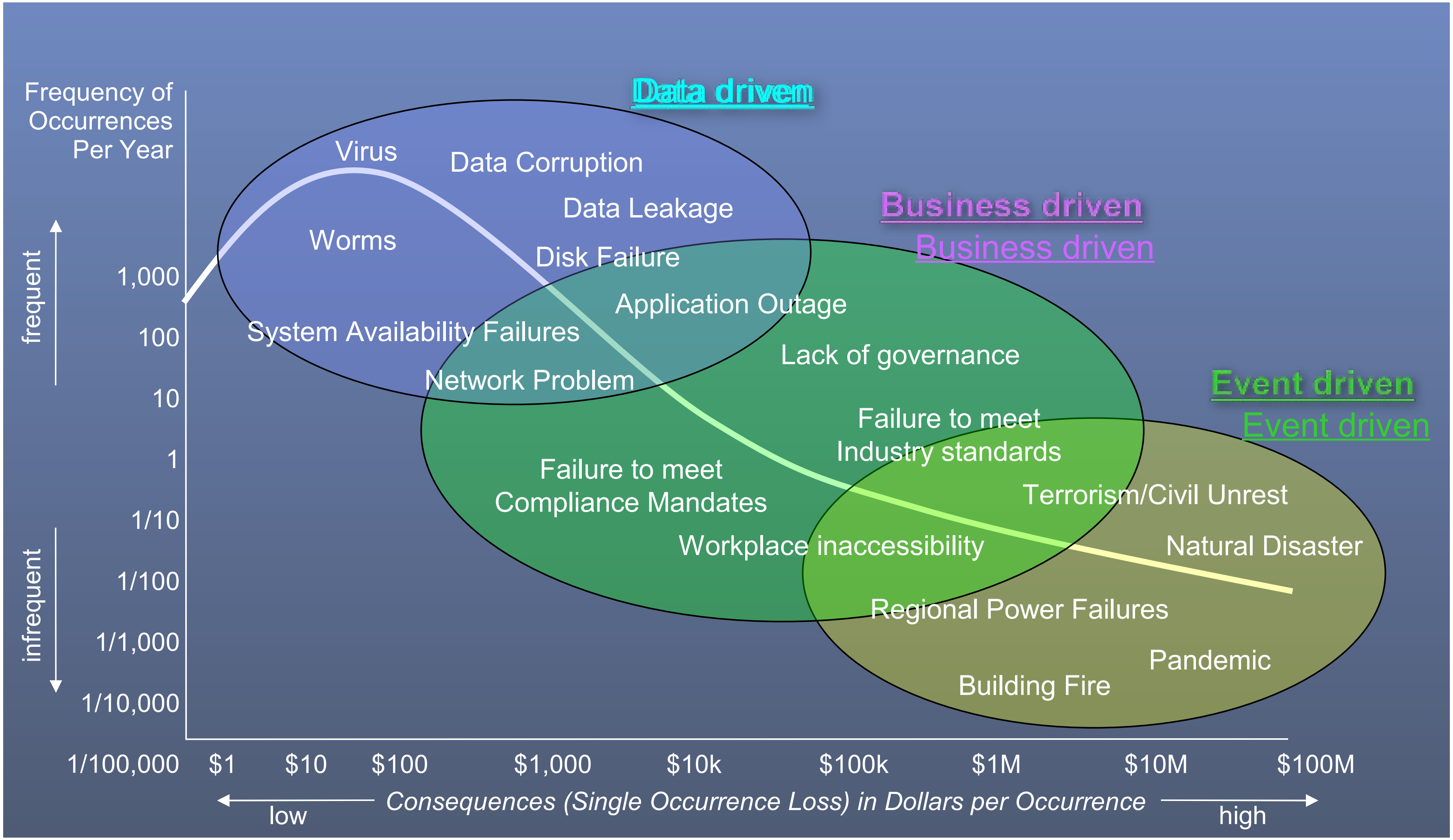
Compliance fatigue

- Organizations are trying to maintain a balance between investing in both the security and compliance postures.

**Source: Pyramid Research, October 2007*

© 2009 IBM Corporation

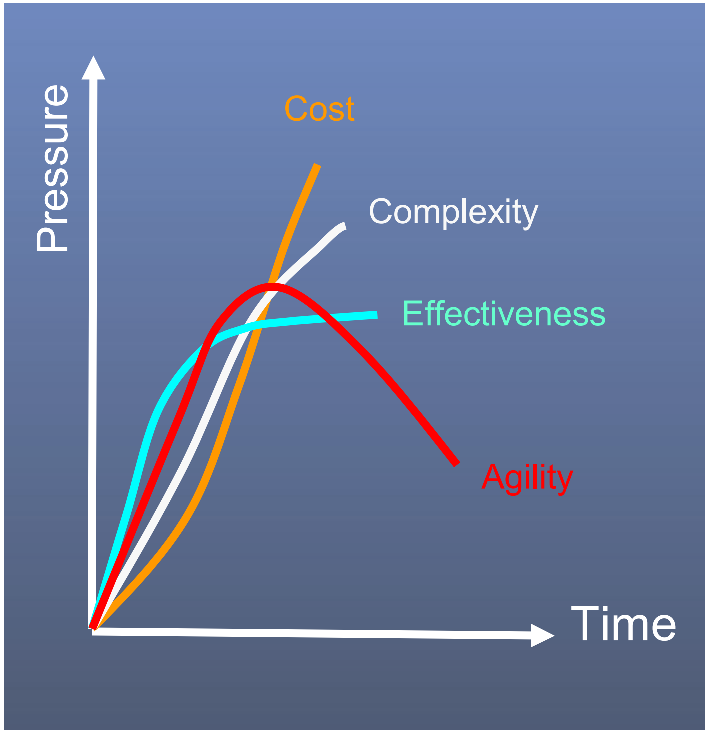
Not all risks are created equal…



© 2009 IBM Corporation

…neither are all Security solutions

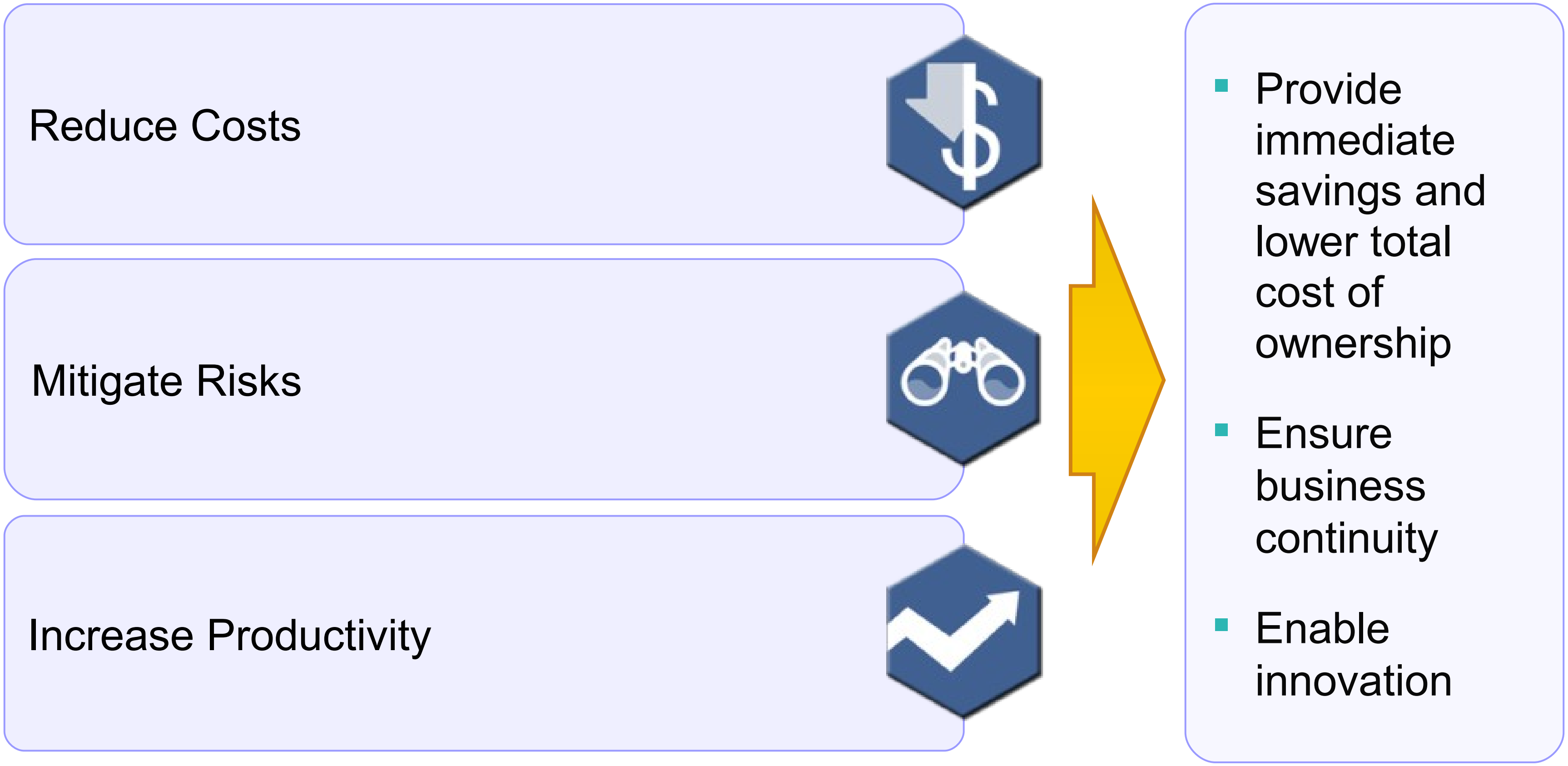
- Find a balance between effective security and cost
  - The axiom… never spend $100 dollars on a fence to protect a $10 horse
- Studies show the Pareto Principle (the 80-20 rule) applies to IT security*
  - 87% of breaches were considered avoidable through reasonable controls
- Small set of security controls provide a disproportionately high amount of coverage
  - Critical controls address risk at every layer of the enterprise
  - Organizations that use security controls have significantly higher performance*



*Sources: W.H. Baker, C.D. Hylender, J.A. Valentine, 2008 Data Breach Investigations Report, Verizon Business, June 2008
ITPI: IT Process Institute, EMA December 2008

© 2009 IBM Corporation

IBM Security Solutions –why do our customers invest into virtualisation



Reduce Costs

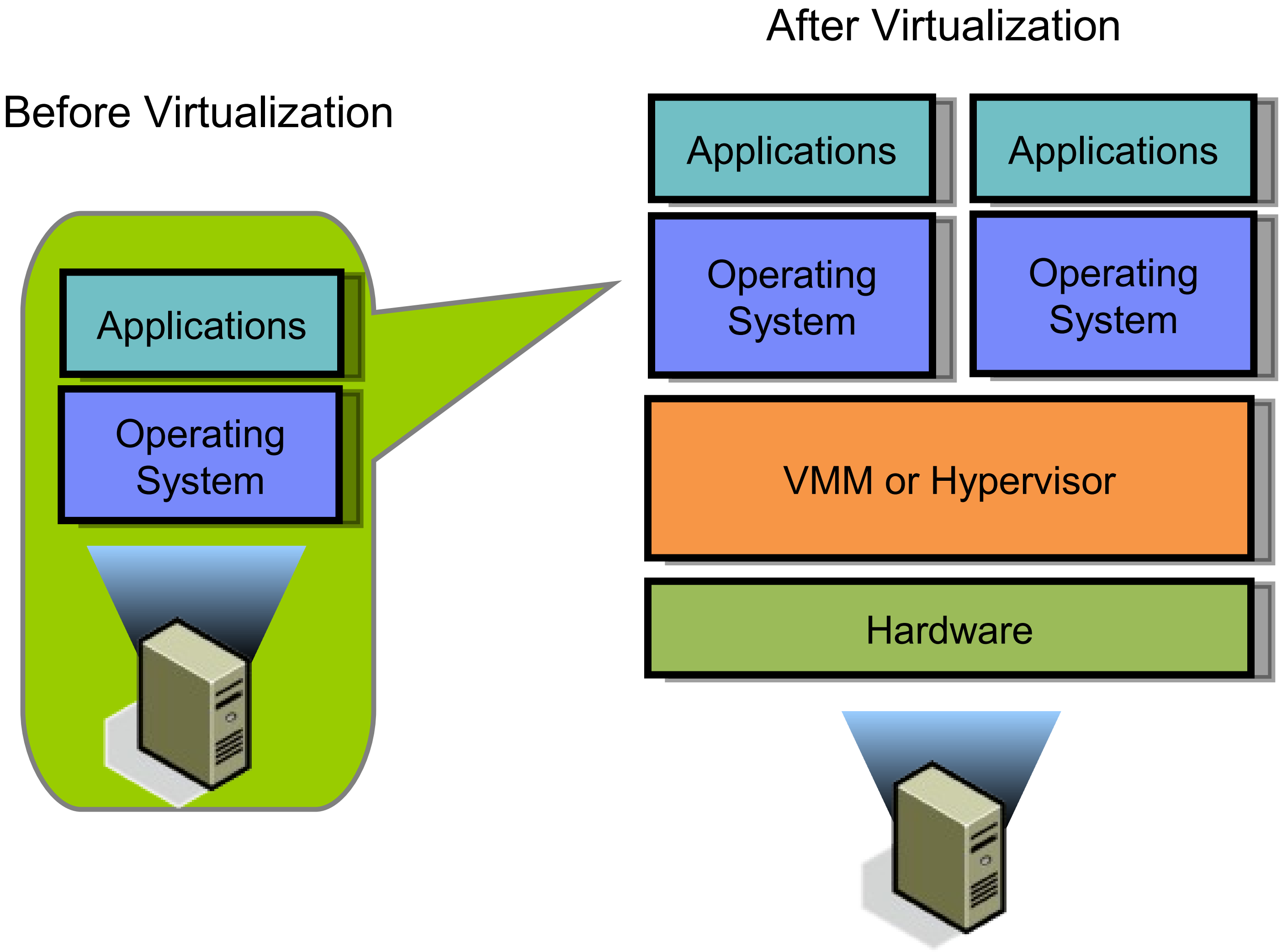
Mitigate Risks

Increase Productivity

- Provide immediate savings and lower total cost of ownership
- Ensure business continuity
- Enable innovation

© 2009 IBM Corporation

Basics: Virtualization Architecture



Before Virtualization

Applications

Operating System

After Virtualization

Applications

Applications

Operating System

Operating System

VMM or Hypervisor

Hardware

© 2009 IBM Corporation

What does Virtualization Change?

- Everything
  - Dynamic, fluid data-center
  - Resource pools
  - Commoditization of everything
  - Increased efficiency

- Nothing
  - Virtual IT is still IT…

    Security

    Management

    Complexity

    heterogeneity

© 2009 IBM Corporation

Virtualization and Enterprise Security

- Virtualization != Security
  - Standard servers are as secure as standard VMs
- Partitioning divides VMs, but does not secure them
- Same principles apply
  - Defense in depth
  - Network design and segmentation
  - Unified security management

© 2009 IBM Corporation

Threat Landscape

- New Swath of Availability Attacks
  - Owning a single guest
  - Breaking out of the guest
  - Compromise of Virtual Console/Management
    - Provision my own evil guest(s)
    - Adjust resource quotas
    - Shut OFF guest(s)
  - Compromise of the VMM/Hypervisor
    - IsGameOver()

© 2009 IBM Corporation

Organizational Ownership?

- Who owns the Virtual [Fill in the Blank] ?

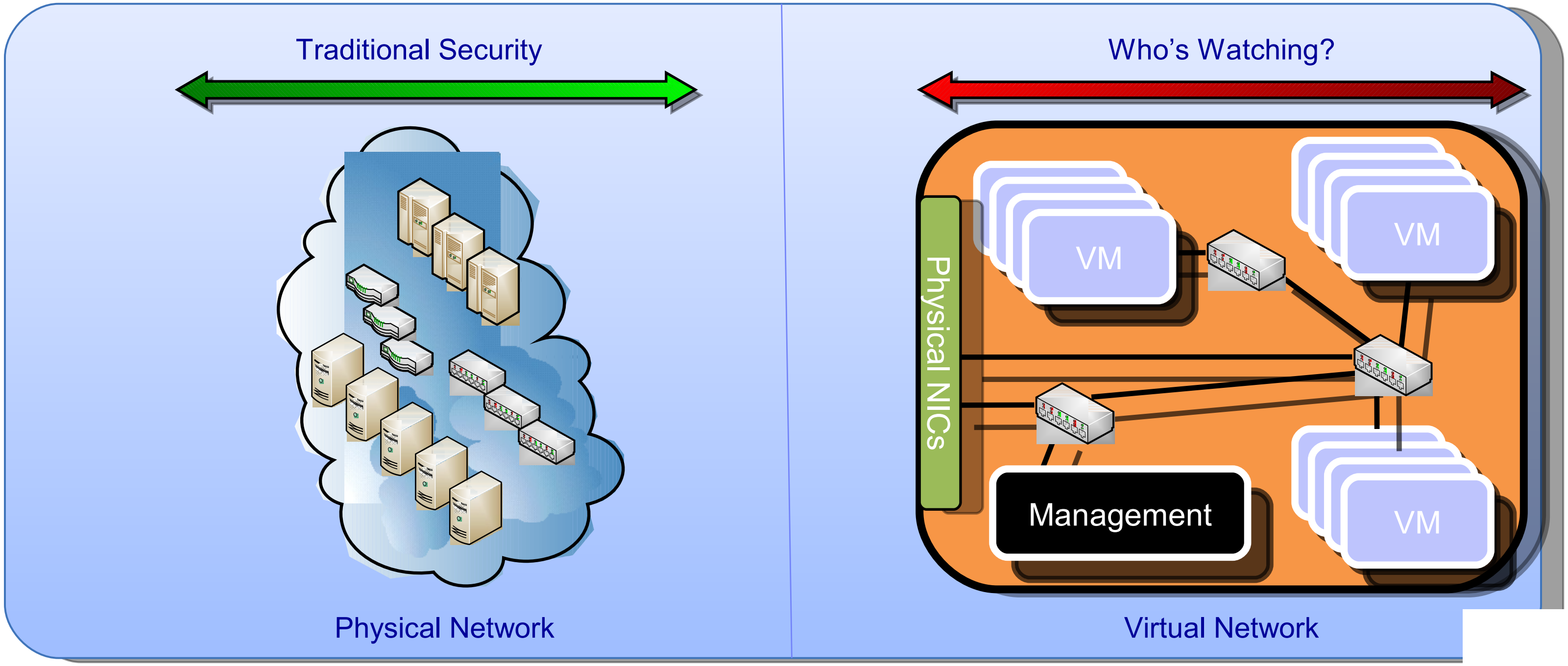
Network Admin

Server Admin

Application Owners

Data Custodians

?



New Operational Challenges

- Find the Server…
  - Live Migration makes servers harder to track
- Configuration/Patch Management
  - Pause/Offline features impact:

      Audits

      Scanning

      Patching
- Image Management
  - Storage
  - Version Control

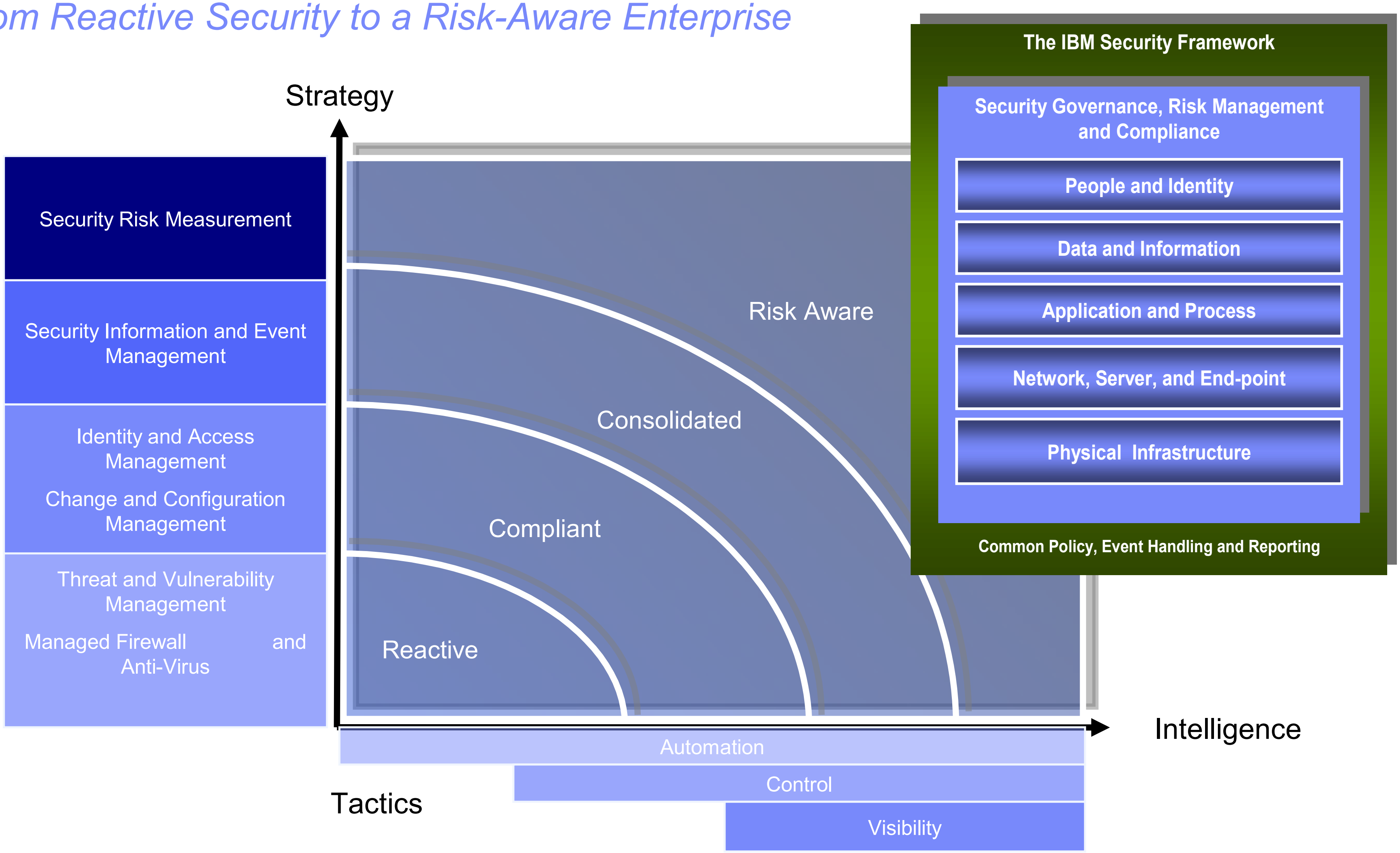
© 2009 IBM Corporation

What Can I Do?

© 2009 IBM Corporation

The IBM Security Framework

From Reactive Security to a Risk-Aware Enterprise



Strategy
Security Risk Measurement
Security Information and Event Management
Identity and Access Management
Change and Configuration Management
Threat and Vulnerability Management
Managed Firewall and Anti-Virus
Risk Aware
Consolidated
Compliant
Reactive
Intelligence
Tactics
Automation
Control
Visibility
The 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

© 2009 IBM Corporation

The Security Optimization Approach

- Redefine and Simplify Risk Management **Re-evaluating priorities to balance risk in light of evolving challenges**
- Establish a Total Security Framework and Solutions Portfolio **Leveraging innovation and integration in consideration of holistic security and IT infrastructure**
- Simplify the Security Risk Lifecycle **Aligning with business processes to ensure continuous improvement**
- Join with a Transformative Security Partner to Achieve these New World Imperatives **Adding world-class expertise for success today – and in the future**

© 2009 IBM Corporation

Security Optimization Process Overview

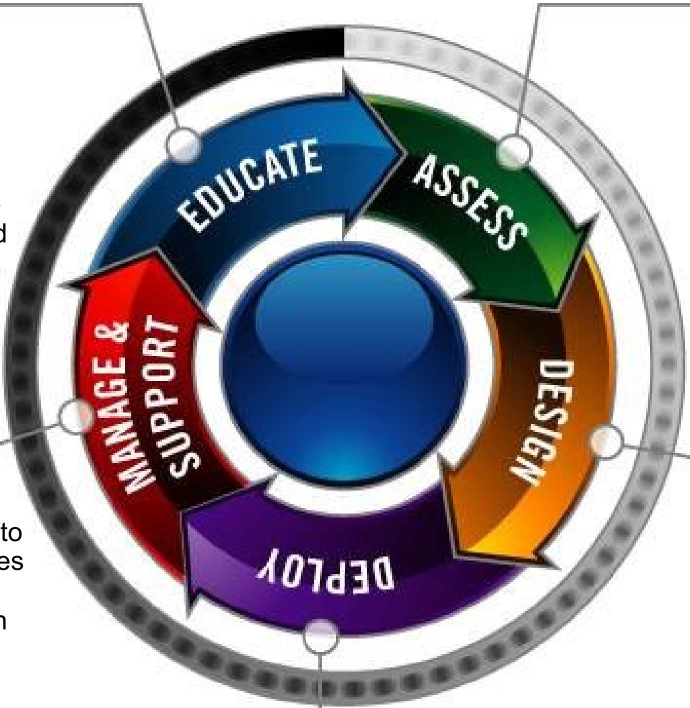
A proven integrated lifecycle methodology that improves the enterprise's ability to control and manage risk

Phase 5. Educate

- Action: Education and knowledge transfer of security best practices
- Result: Improved employee understanding and skills related to security

Phase 4. Manage and Support

- Action: Management of security infrastructure/program to meet defined business objectives
- Result: Insures gaps remain closed and new gaps are not opened by providing improved protection, lowering TCO, and demonstrating compliance



Phase 1. Assess

- Action: Assess current level of security effectiveness and strengthen network and security posture by identifying vulnerabilities and weakness against best-practices
- Result: Gap analysis and resolution recommendations between current state and requirements.

Phase 2. Design

- Action: Design and documentation of policies, procedures, and architecture/solutions to ensure protection and extension of business capabilities
- Results: Creation of gap closure plan for short and long-term resolution to ensure optimization of security infrastructure

Phase 3. Deploy

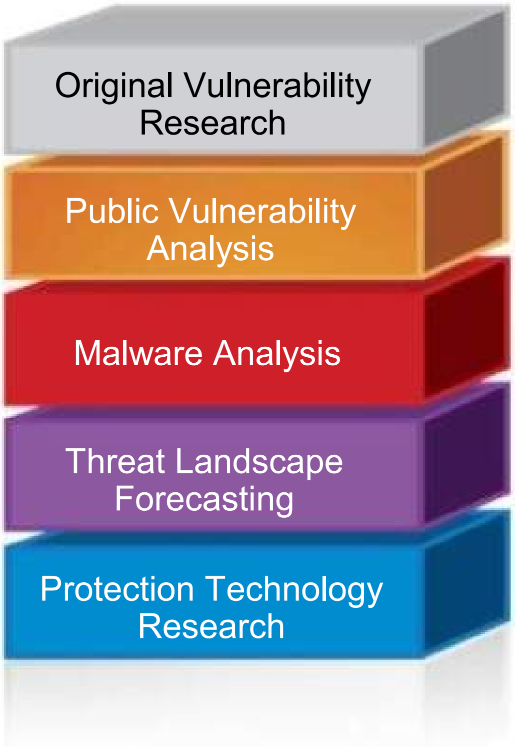
- Action: Expert deployment, implementation, tuning, and change support
- Results: Helps client execute gap closure plan, improve performance and cost savings

© 2009 IBM Corporation

Only IBM Security is backed by the IBM X-Force® research team

Research → Technology → Solutions

Research



Original Vulnerability Research

Public Vulnerability Analysis

Malware Analysis

Threat Landscape Forecasting

Protection Technology Research

Technology

X-Force Protection Engines

- Extensions to existing engines
- New protection engine creation

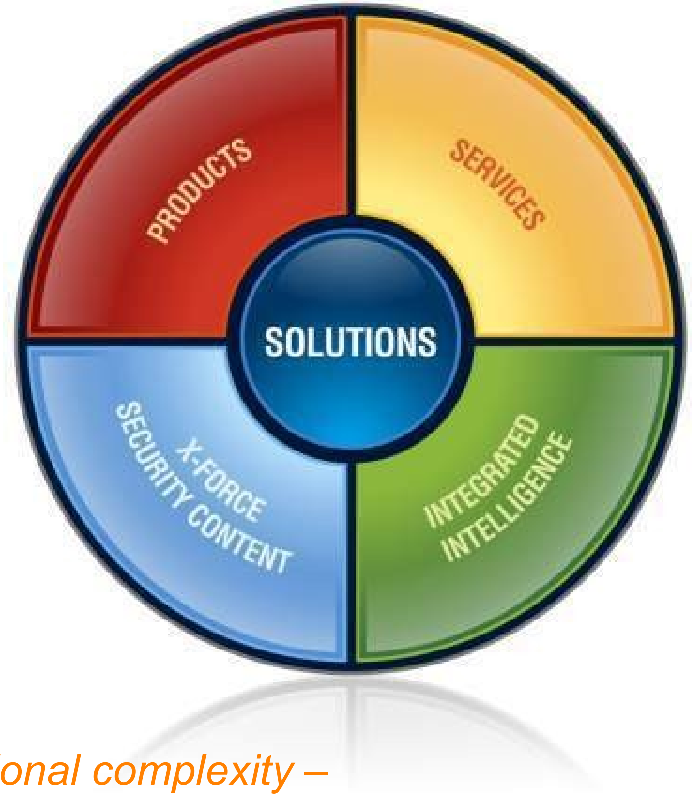
X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing

Solutions

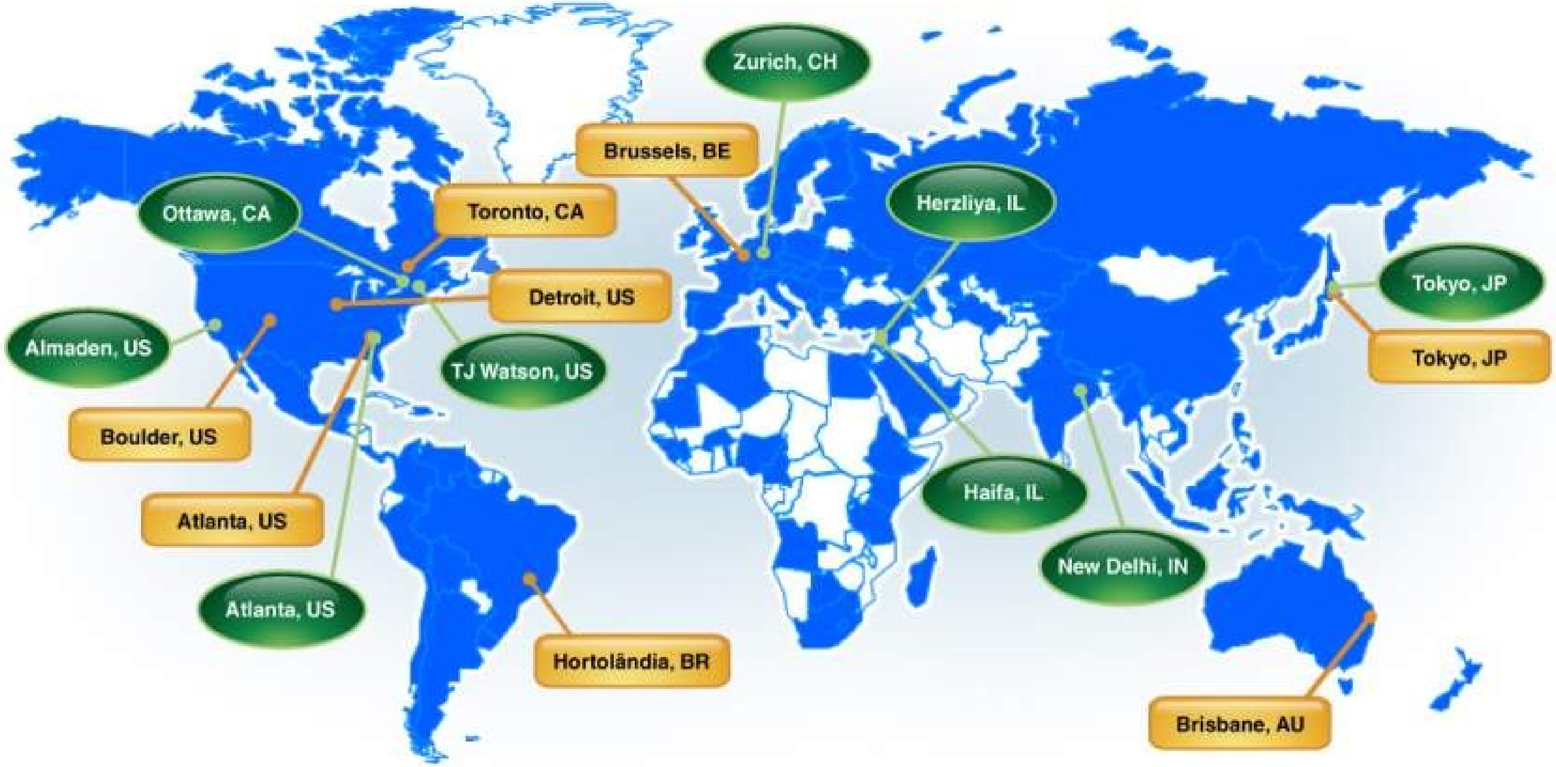


The X-Force team delivers reduced operational complexity –
helping to build integrated technologies that feature "baked-in" simplification

© 2009 IBM Corporation

IBM global security reach

8 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 2.5 Billion+ Events Per Day

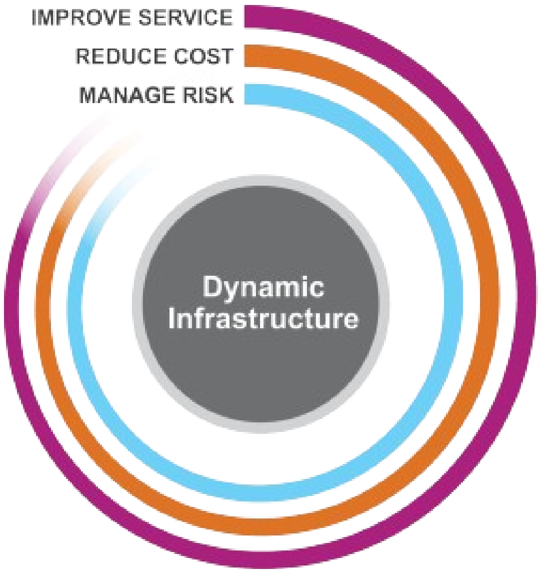


IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

© 2009 IBM Corporation

Next steps

- To learn more about security from IBM, visit: ibm.com/security
- In-depth briefings on security solutions that map to your needs
- Collaborative workshop or assessment from IBM or our Certified Business Partners
- Proof of technology / concept



© 2009 IBM Corporation

Christian Fahlke – Channel Leader
IBM Internet Security Systems

Central-, Eastern Europe, Middle East & Africa
fahl@ch.ibm.com

Thank you