nemertes
RESEARCH
Independence. Integrity. Insight.

The Evolving Threat Landscape: **Protecting Your Mobile and Virtual Environment from Emerging Security Threats**

John Burke
Principal Research Analyst
Nemertes Research
www.nemertes.com

Agenda

- About Nemertes
- Security and Compliance Trends
- Addressing the Evolving Security Threat Landscape
- Conclusion and Recommendations

Independence. Integrity. Insight.

Nemertes:
Bridging the Gap Between Business & IT

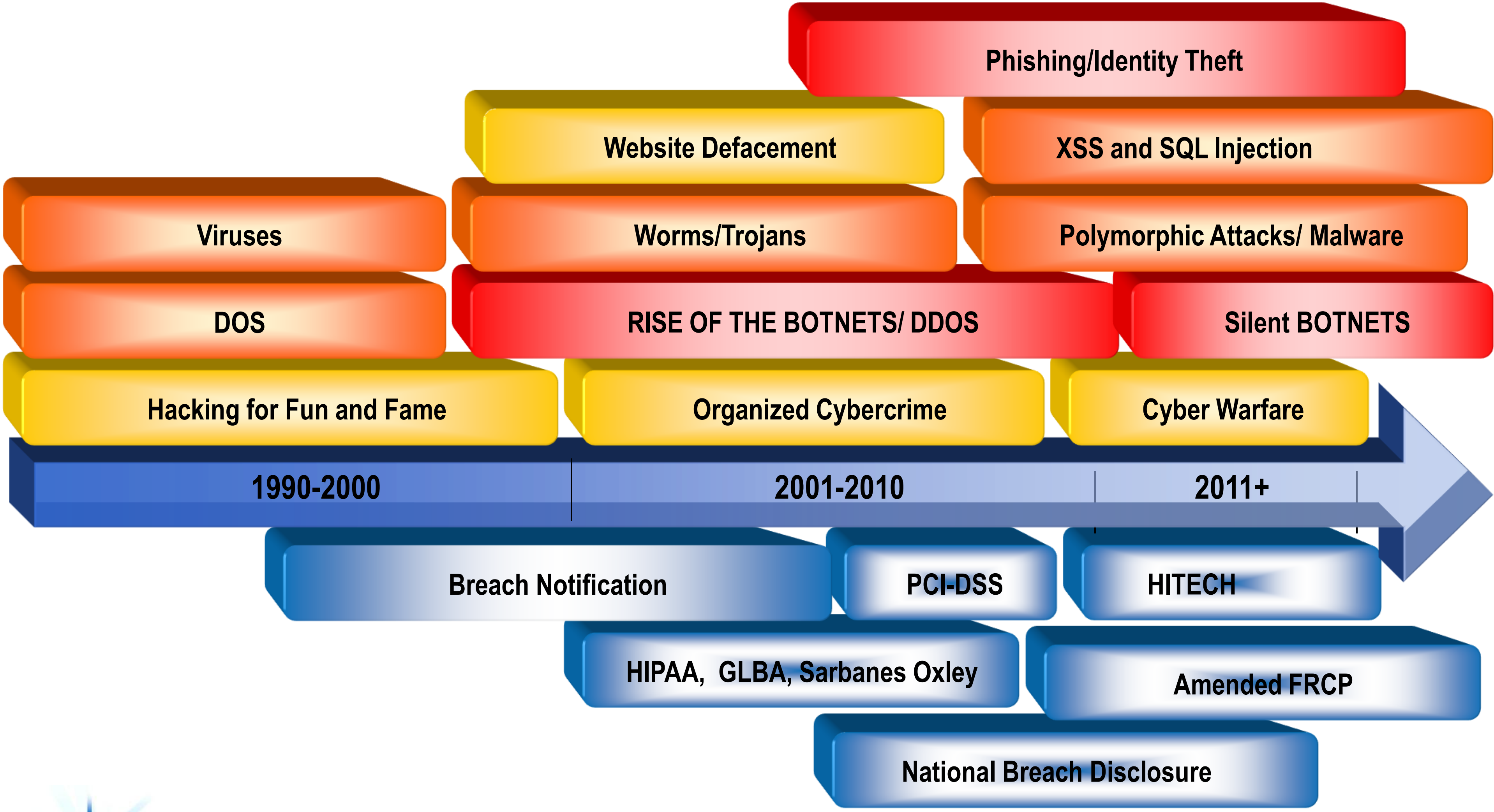
- Quantifies the business impact of emerging technologies
- Conducts in-depth interviews with IT professionals

- Advises businesses on critical issues such as:
  - Unified Communications
  - Social Computing
  - Data Centers & Cloud Computing
  - Security
  - Next-generation WANs

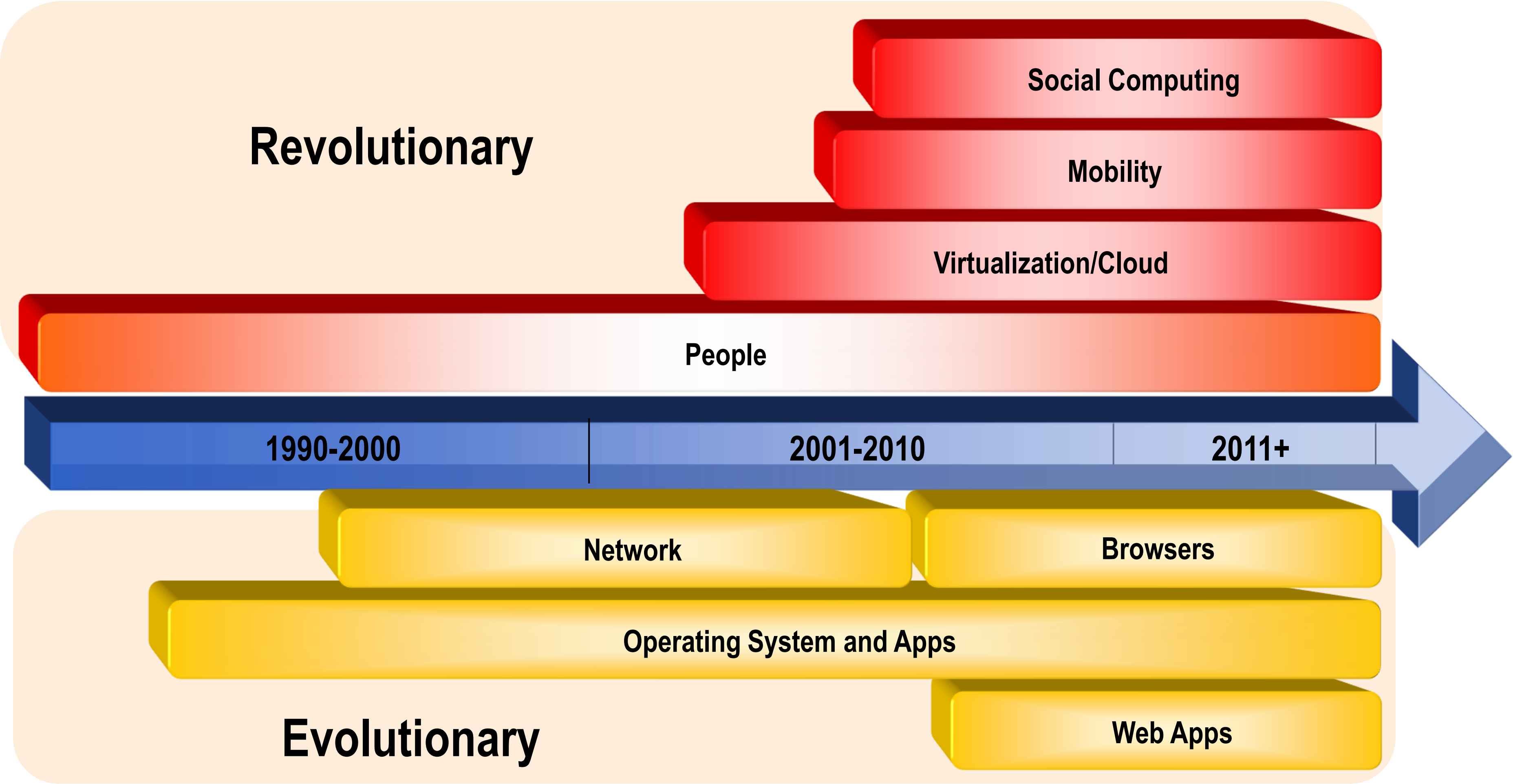
- Cost models, RFPs, Architectures, Strategies

Security and Compliance Trends

The Evolving Threat Landscape



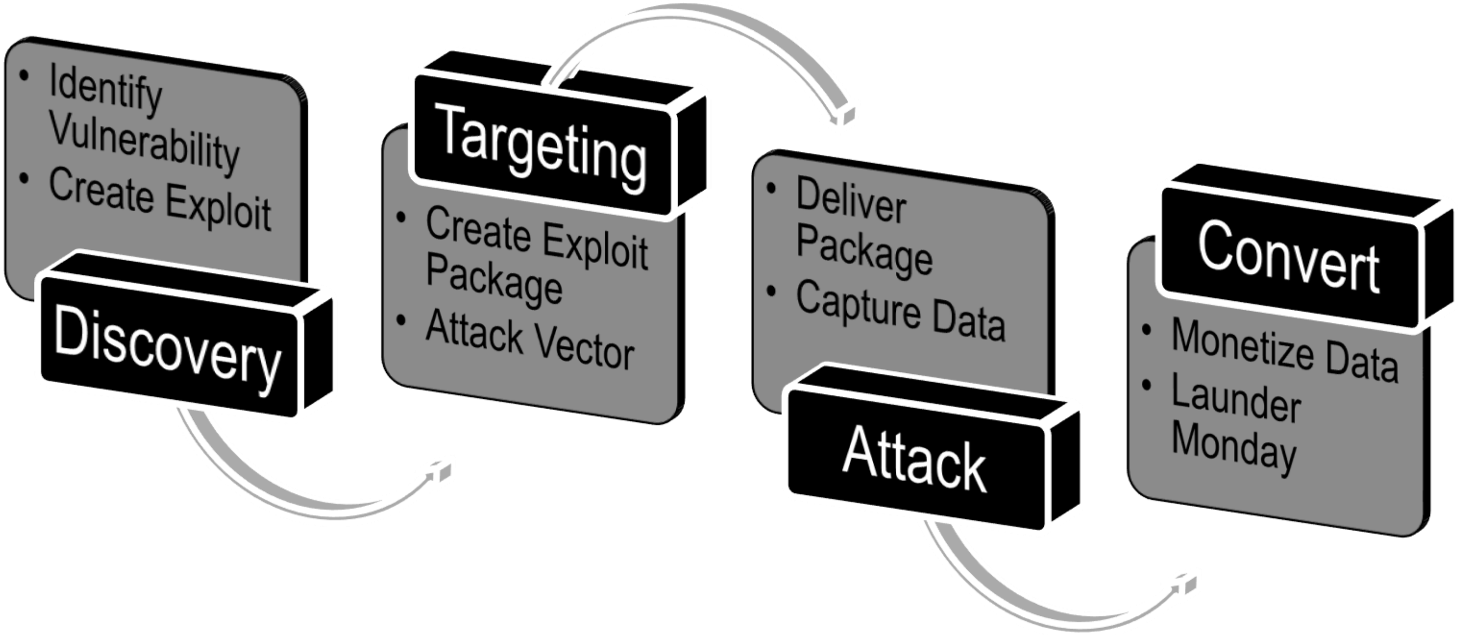
The Evolving Vulnerability Landscape



Independence. Integrity. Insight.

Single Criminal – “The Good Old Days”

- Key Characteristics:
  - Slow, single threaded
  - High risk for hacker



Discovery

- Identify Vulnerability
- Create Exploit

Targeting

- Create Exploit Package
- Attack Vector

Attack

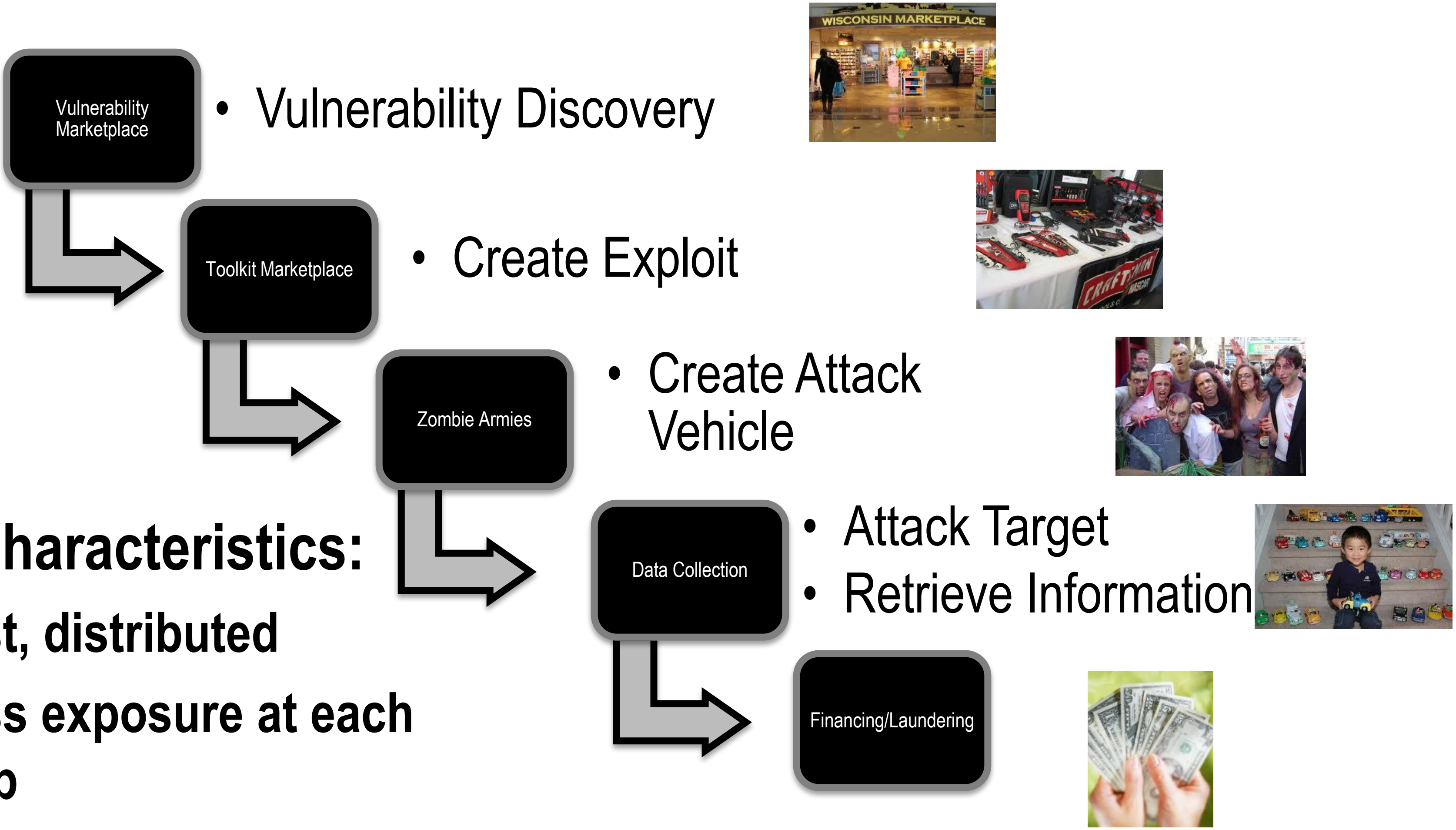
- Deliver Package
- Capture Data

Convert

- Monetize Data
- Launder Monday

Criminal Black Market

IDTHEFT $10.75 ▲2% STRM $16.32 ▲ 0.17% BOTNET $4.75 ▲ 26.2% STLNAMEX $5.6 ▲ 3% LEAKDTA $5.25 ▲ 7% LPTPTAXI $4.20 ▼3% PHISH $52.58 ▲ 0.4%



Vulnerability Marketplace

- Vulnerability Discovery

Toolkit Marketplace

- Create Exploit

Zombie Armies

- Create Attack Vehicle

Data Collection

- Attack Target
- Retrieve Information

Financing/Laundering

- **Key Characteristics:**
  - **Fast, distributed**
  - **Less exposure at each step**

Independence. Integrity. Insight.

The Changing End-User Landscape

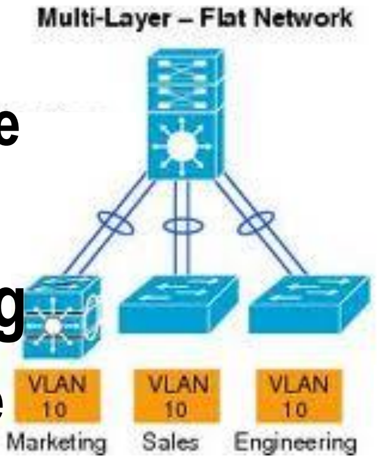
- Employee personal use of technology influences IT decisions for 46% of organizations
- About 67% of organizations have a formal telework policy
- The line between personal and work computing is blurring
- 11% of organizations have some staff using mobiles instead of PCs
- Demand for social computing is high

"If you asked from a percentage standpoint: can do 60-70% of all the work I need to do from a mobile device, but I still need that laptop for other small pieces." – CIO, very large manufacturer

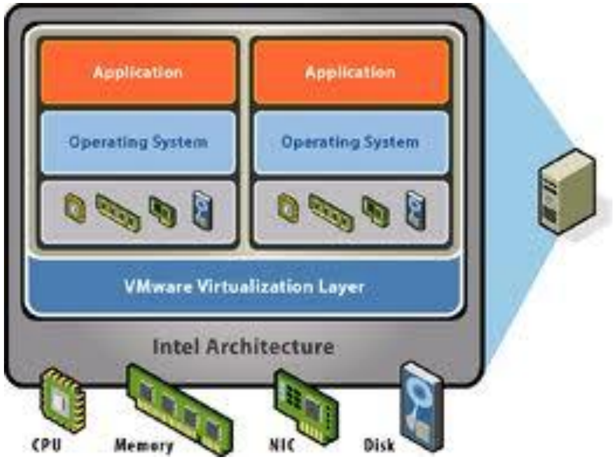
Independence. Integrity. Insight.

The Changing Data Center Landscape

- Server virtualization is ubiquitous with up to 68% of workloads virtualized (depending on company size)
- Networks are flattening as organizations move from traditional 3-tier to 2-, or 1-tier networks
  - Virtualization contributes as virtual switches create huge layer 2 networks
- Data center expansion into the cloud is coming
  - Currently < 10% organizations using Infrastructure as a Service (IaaS) with additional 27% evaluating



New Pressures on Security



- Virtualization/Cloud
- Mobility
- Social Computing

Challenges and Risks of Virtualization

- Organizational: Security staffs are not organized around virtualized environments
  - "Netsec" teams don't fully grasp "virtsec"
  - Security teams are engaged too late in the process
- Operational: Virtualization blurs separation of duties (SoD)
  - Server admins can reconfigure virtual server, storage and virtual network
- Functional: Virtualization affects network defense and compliance
  - Virtualization can put you out of compliance
    - 60% of security practitioners say it's the primary justification
  - Virtualization flattens the network, reducing defense-in-depth

Security/Compliance of Virtual Infrastructure

- VirtSec adoption is less than 20% of organizations
- Despite low adoption, there is confidence in existing security controls providing sufficient compliance and security protection
  - 51.9% of organizations rate the compliance and security of their virtual infrastructure EXCELLENT

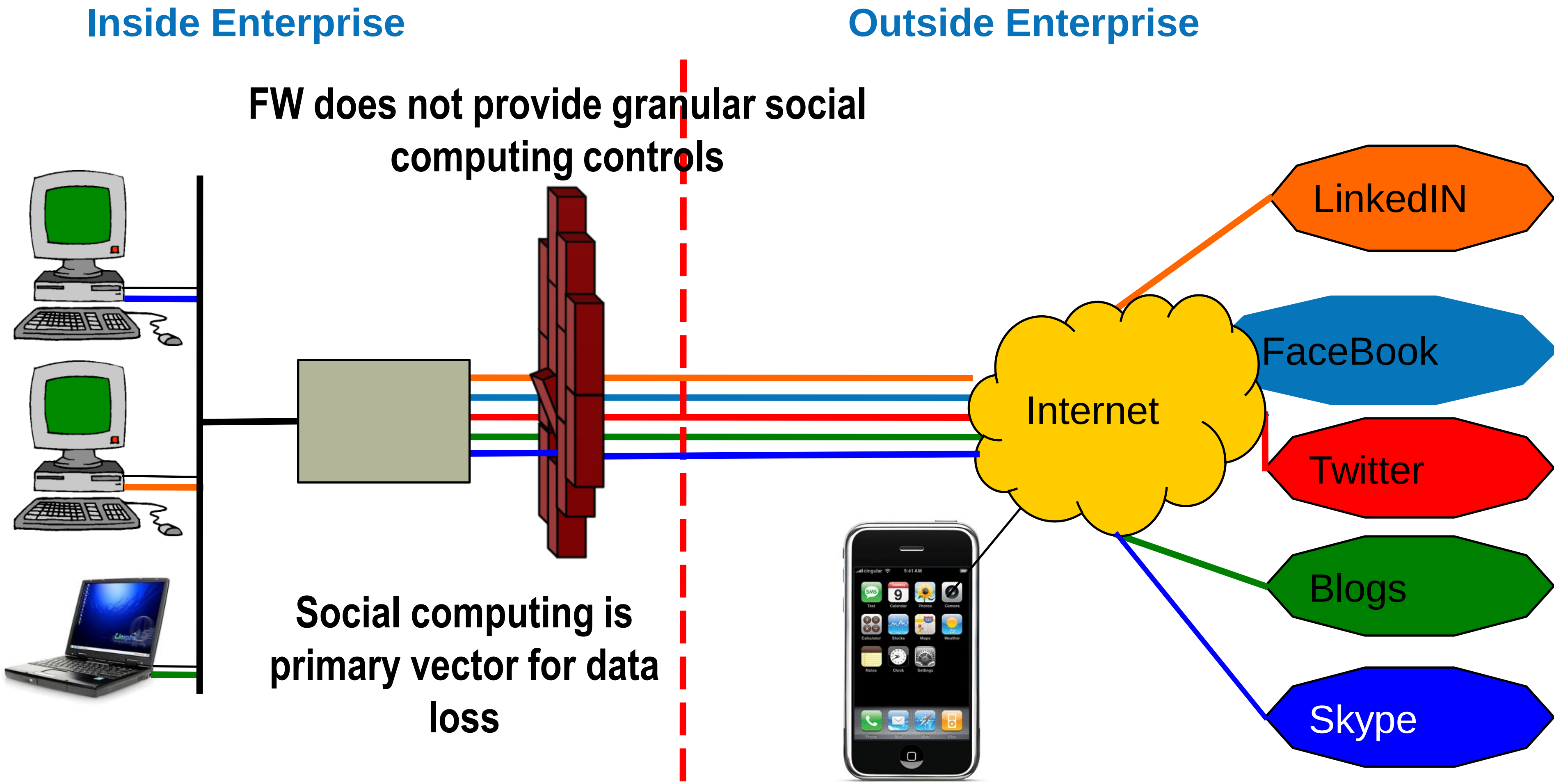
Independence. Integrity. Insight.

Mobility: Vulnerability on The Move!

- Targeted attacks emerging for Apple IOS and Android
- Employee ownership raises significant liability and security issues
  - Policies around sensitive data leakage
  - Remote wipe options
- Primary vector for data loss
- Increasing use of mobile device as security token raises the exploit value
- Most security management systems are blind to mobile devices

Independence. Integrity. Insight.

Risk Points for Social Computing



FW does not provide granular social computing controls

Social computing is primary vector for data loss

Enterprise is blind to mobile user social computing activities

Social Networking Compliance Issues

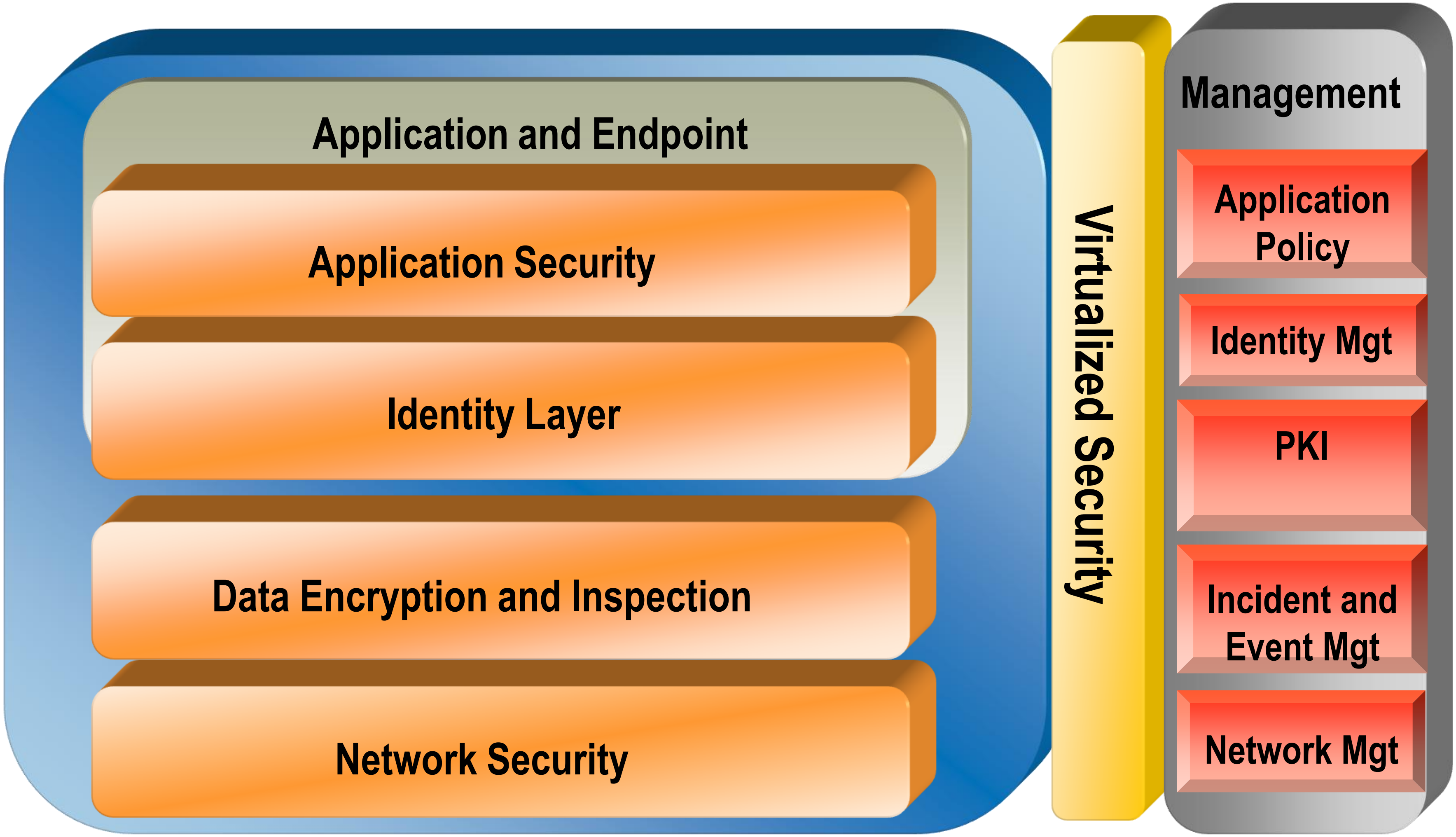
Area	Regulations	Requirement
Privacy	HIPAA, GLBA, PCI, FERPA,HITECH, State breach notification laws	Prevention of breach of Personally Identifiable (PII) or Protected Health (PHI) Information
Financial Regulations	SEC(17a-3,4), 206(4), FINRA 10-6, 2210, 3010, Comm. Rule 13	Audit and control of all external communications by investment advisors. Explicit requirements for social networking
e-Discovery	FRCP (34,37)	Discovery of Electronically Stored Information (ESI). Must be "reasonably" accessible. Retention implications for social networking

Independence. Integrity. Insight.

Addressing the Evolving Security Threat Landscape

Independence. Integrity. Insight.

Technology Architecture & Evolution



Application and Endpoint

Application Security

Identity Layer

Data Encryption and Inspection

Network Security

Virtualized Security

Management

Application Policy

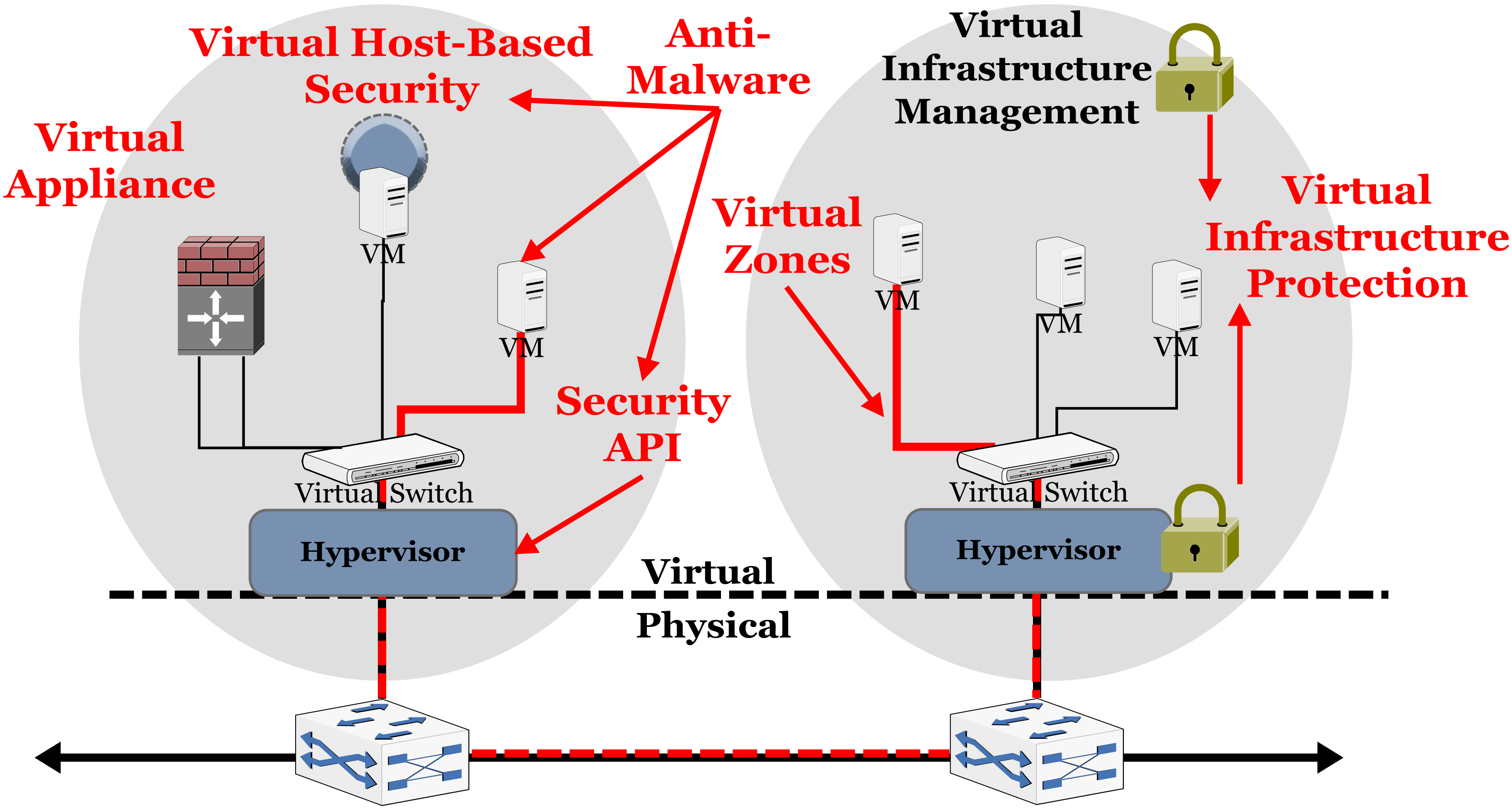
Identity Mgt

PKI

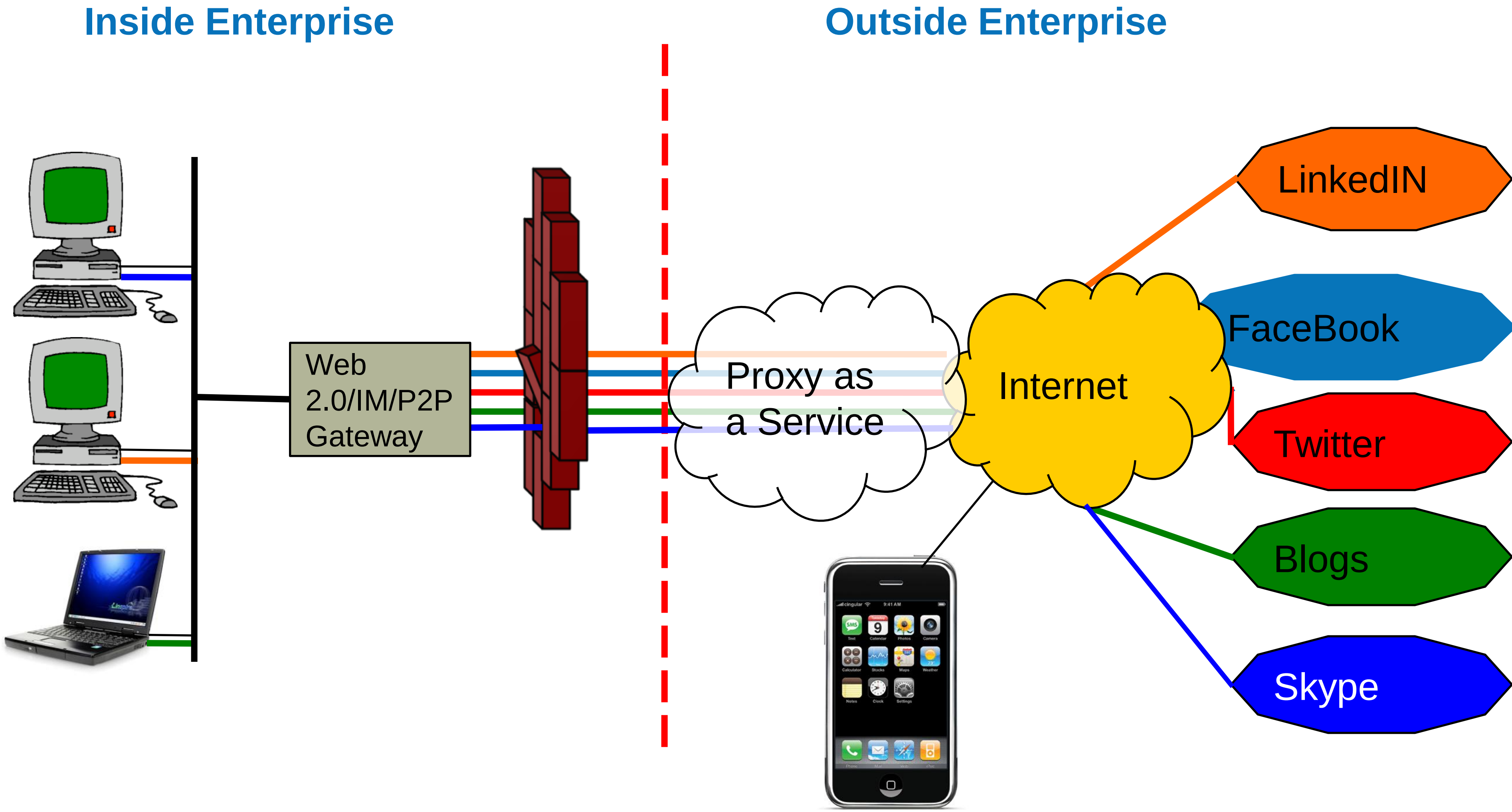
Incident and Event Mgt

Network Mgt

Virtualization Security



Securing Social Computing



10 Steps to Social Networking Compliance

- Step 1 – Take ownership
- Step 2 – Establish policy
- Step 3 – Engage compliance function early
- Step 4 – Formal education program
- Step 5 – Strong password management
- Step 6 – Content monitoring and logging
- Step 7 – Education
- Step 8 – Selective blocking of content
- Step 9 – Routine audits and review of logs
- Step 10 – Regular policy review

Independence. Integrity. Insight.

Mobility Security Touch Points

Mobile Device Management (MDM)

- Automated configuration
- OTA Updates/Backup
- Policy enforcement
- Remote wipe

Mobile Service Management (MSM)

- Carrier monitoring/SLAs
- Application monitoring
- Trouble ticket management
- Key metrics- KPI

Mobile Application Management (MAM)

- Remote OTA provisioning
- Application configuration
- OTA Updates/Backup
- Policy enforcement
- Application removal
- Application black/white lists
- Application monitoring

Risk Management

- Anti-X support
- Authentication
- Remote lock/wipe
- Key metrics- KPI
- Secure container
- Sensitive data control

Provisioning

- Employee owned
- Allocation policies
- Activation/deactivation

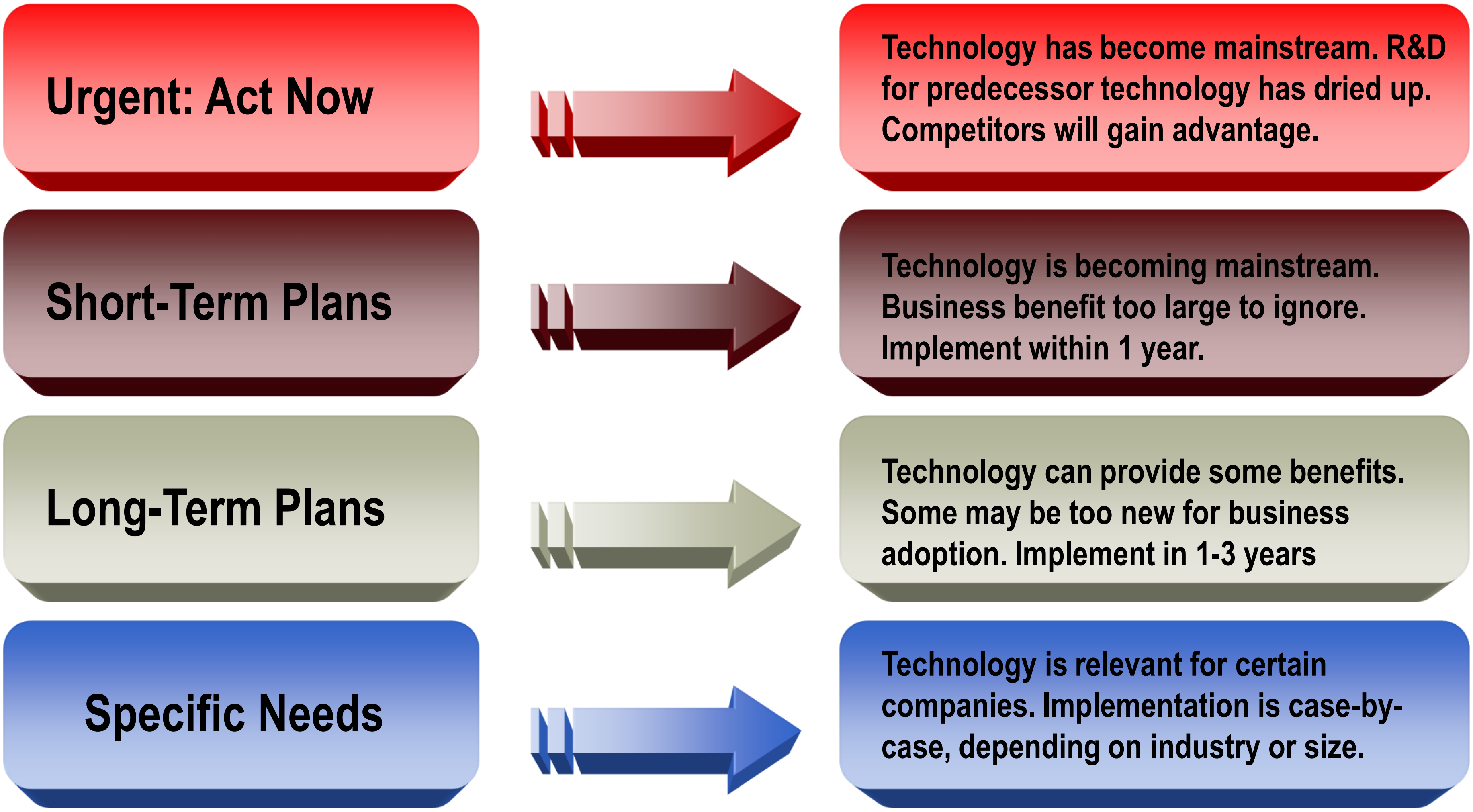
End User Support

- Remote OTA maintenance
- Remote OTA support

Independence. Integrity. Insight.

Conclusion and Recommendations

Recommendations: What Should You Be Doing?



Urgent: Act Now → Technology has become mainstream. R&D for predecessor technology has dried up. Competitors will gain advantage.

Short-Term Plans → Technology is becoming mainstream. Business benefit too large to ignore. Implement within 1 year.

Long-Term Plans → Technology can provide some benefits. Some may be too new for business adoption. Implement in 1-3 years

Specific Needs → Technology is relevant for certain companies. Implementation is case-by-case, depending on industry or size.

nemertes RESEARCH
Independence. Integrity. Insight.

Security Roadmap

- Establish a mobility policy and council
- Inventory end-user devices
- Review virtualization security controls
- Establish social networking policy

Urgent: Act Now

Independence. Integrity. Insight.

Security Roadmap

Short-Term Plans

- Complete audit of security controls for virtualization, mobility and social computing
- Implement strong configuration management for virtualization
- Implement mobility governance and security controls
- Implement social computing granular controls
- Implement VirtSec

Independence. Integrity. Insight.

Security Roadmap

- Evaluate OS choices
- Harden OS
- Implement Application Security
- Implement Virtualized Security
- Prepare for de-perimeterization
- Prepare for continuous mobility

Long-Term Plans

Independence. Integrity. Insight.

Conclusions

- The data center is undergoing transformation enabled by virtualization
  - Securing the virtual infrastructure requires a new security approach
- Mobility is transforming the way users work
  - Puts the organization at significant risk of data loss and exposure to attack
- Social computing is a here to stay – get over it!
  - Just blocking is not acceptable or effective
  - Implement granular security controls

nemertes RESEARCH
Independence. Integrity. Insight.

Thank You!