2010 2011 2012 2013

Who Moved My Cheese?

Why The Security Industry Has Been Turned Upside Down

John N. Stewart
jns@cisco.com

Vice President
Chief Security Officer

FIRST Conference 2010

Challenge Questions…

Why do we think its possible to fully protect something when we don’t fully know what it is?

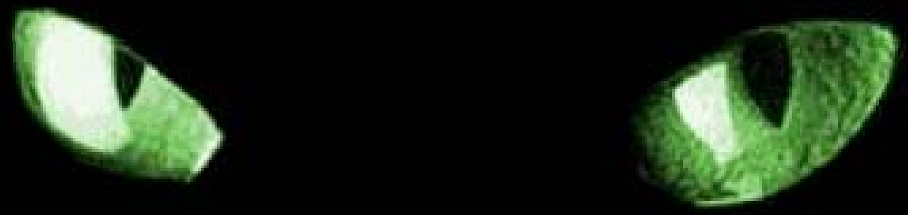
Is ROI the right question?

How come it takes so much money and sophistication to protect something and only a little to penetrate it?

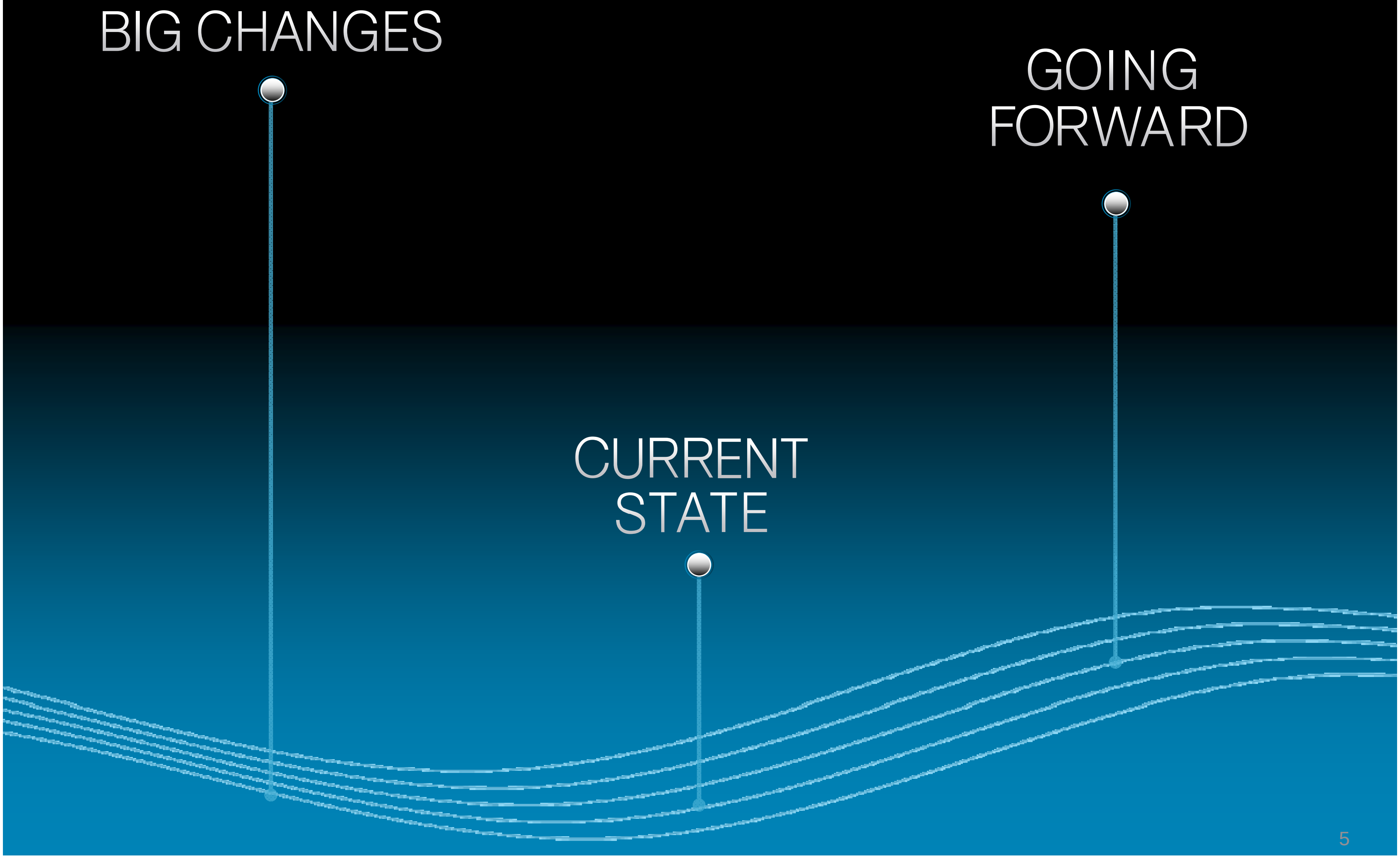
Why do we build critical systems that are so fragile?

In the Spirit of Fading Perimeter….

YOUR E-MAIL PASSWORD SHOULDN'T BE THE SAME AS YOUR DRAWBRIDGE PASSWORD.
9/15



What is our adversary thinking…
right…
now…?



BIG CHANGES

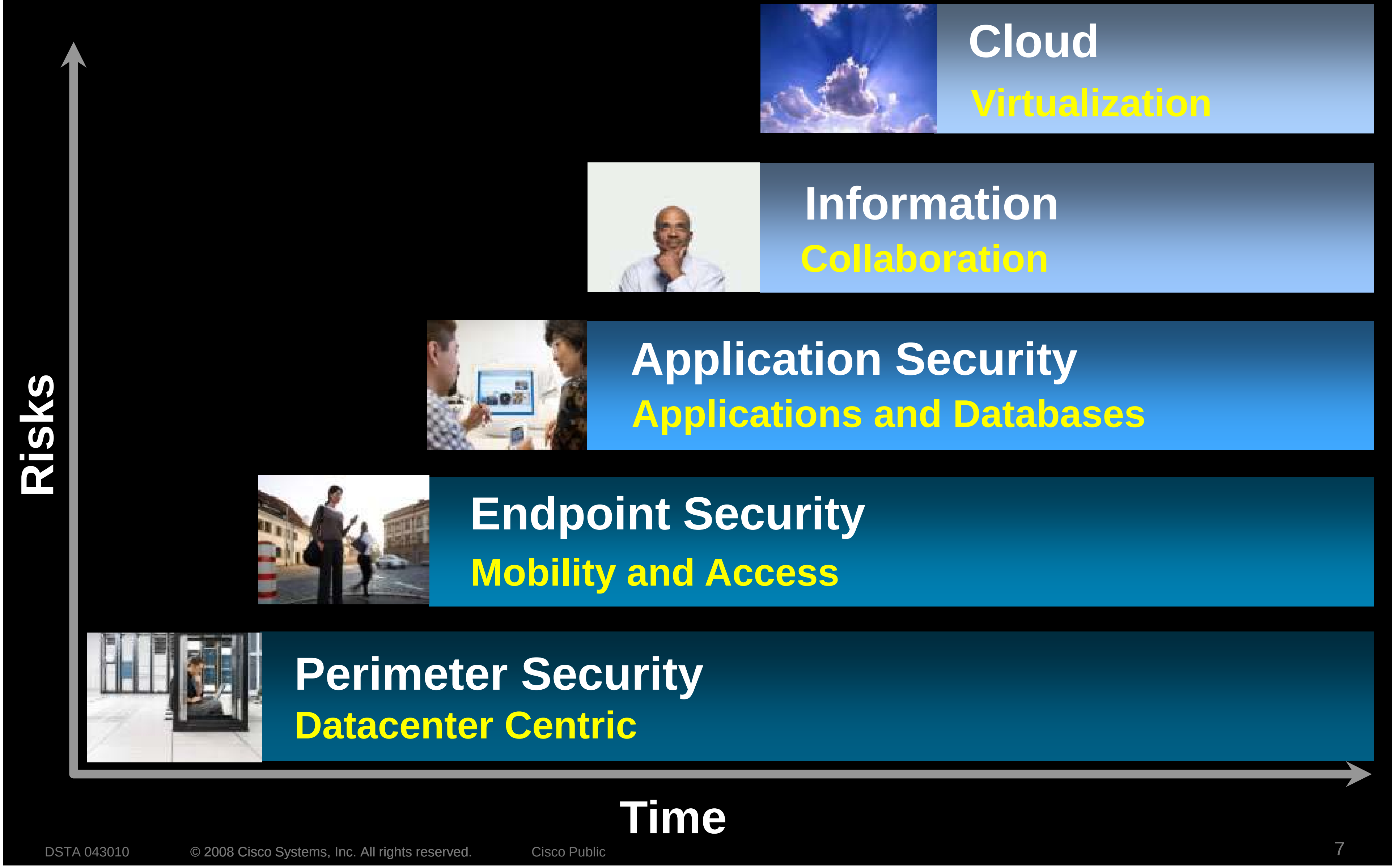
GOING FORWARD

CURRENT STATE

BIG CHANGES

Significant Security Challenge

Transitions



Cloud
Virtualization

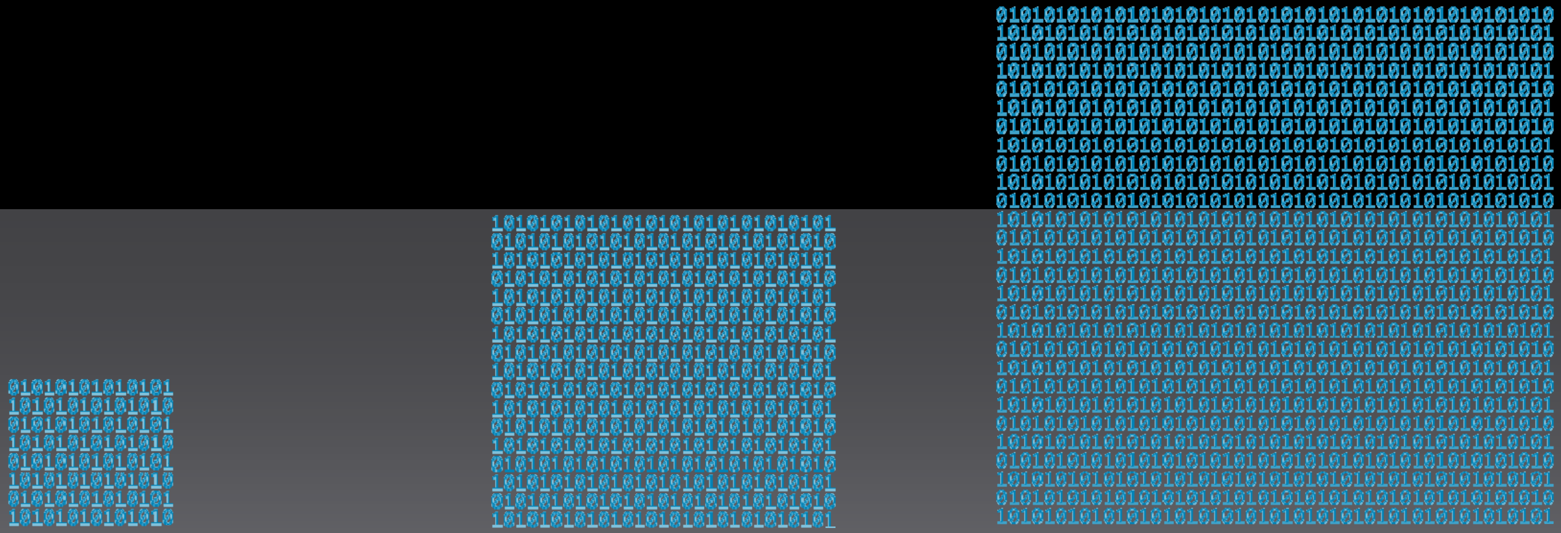
Information
Collaboration

Application Security
Applications and Databases

Endpoint Security
Mobility and Access

Perimeter Security
Datacenter Centric

Global Flow of Information



5 Exabytes per month

1.4 Billion DVDs crossing the Network

2007

21 Exabytes per month

4.8 Billion DVDs crossing the Network

2010

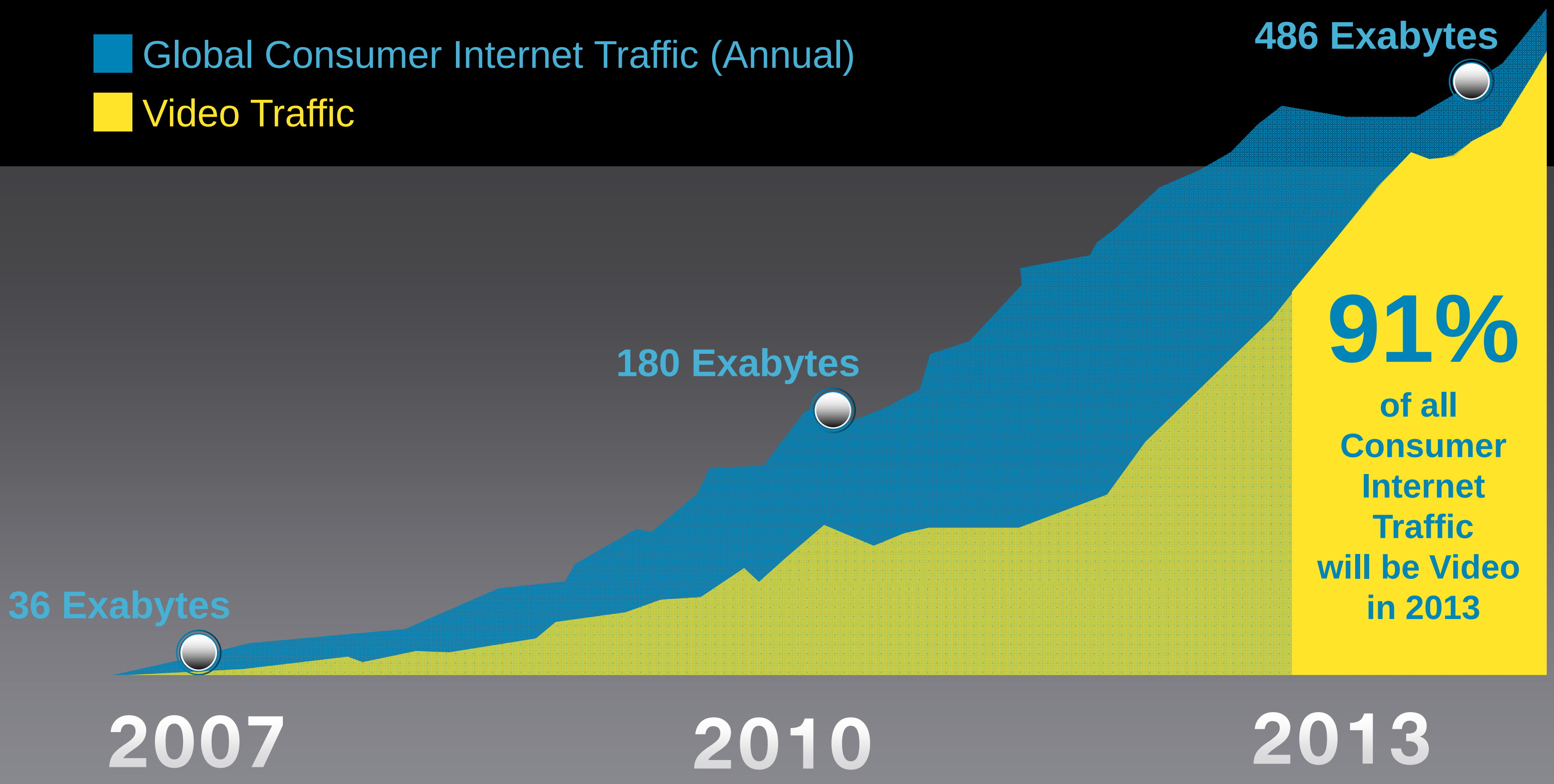
56 Exabytes per month

12.8 Billion DVDs crossing the Network

2013

Source: Cisco Visual Networking Index

Video Will Dominate the Information Flow



91% of all Consumer Internet Traffic will be Video in 2013

Source: Cisco Visual Networking Index

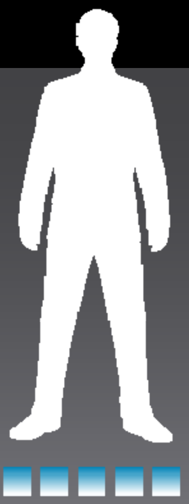
World of Connected Devices

Total 500 Million

1/10th of a Device per Person on Earth

2007

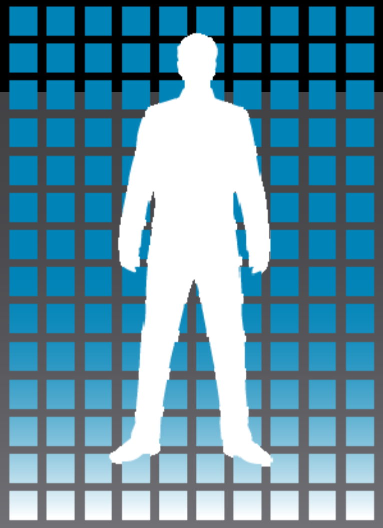
Total 35 Billion



5 Devices per Person on Earth

2010

Total 1 Trillion



140 Devices per Person on Earth

2013

Source: Forrester Research, Cisco

World of Applications

TOTAL MOBILE APPS	iPHONE APPS ALONE	APPS WORLDWIDE
3,000	160,000	1,500,000
2007	2010	2013

Source: Apple, Windows Mobile, Cisco Analysis (Forecast of 2013 assuming consistent growth trends)

Increase in Security Threats

624,000

2007

2,600,000

2010

5,700,000
(projected)

2013

Source: Symantec and Cisco Analysis

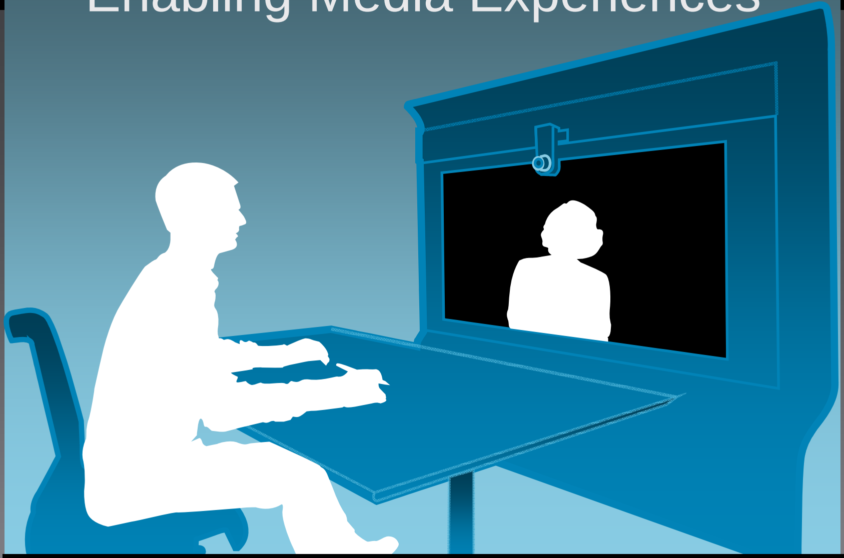
And Beyond…

PEOPLE TO PEOPLE

High-Bandwidth Pipes

Rich/Real-Time Interaction

Enabling Media Experiences



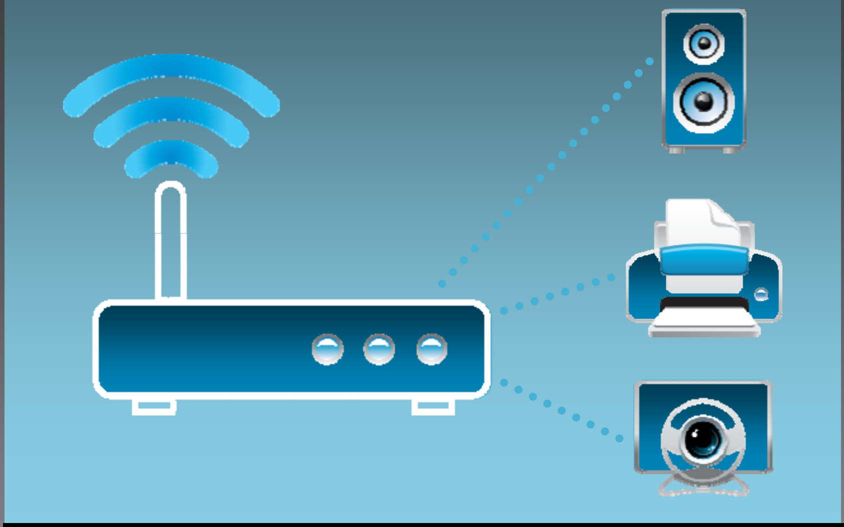
“Video is the killer app”

THINGS TO THINGS

Low-Bandwidth and Low-Power

Wireless Sensors Everywhere

Non-Stop Flow of Data



“SmartGrid is the anchor use case”

Business Internet ❯ **Consumer Internet** ❯ **Industrial Internet**

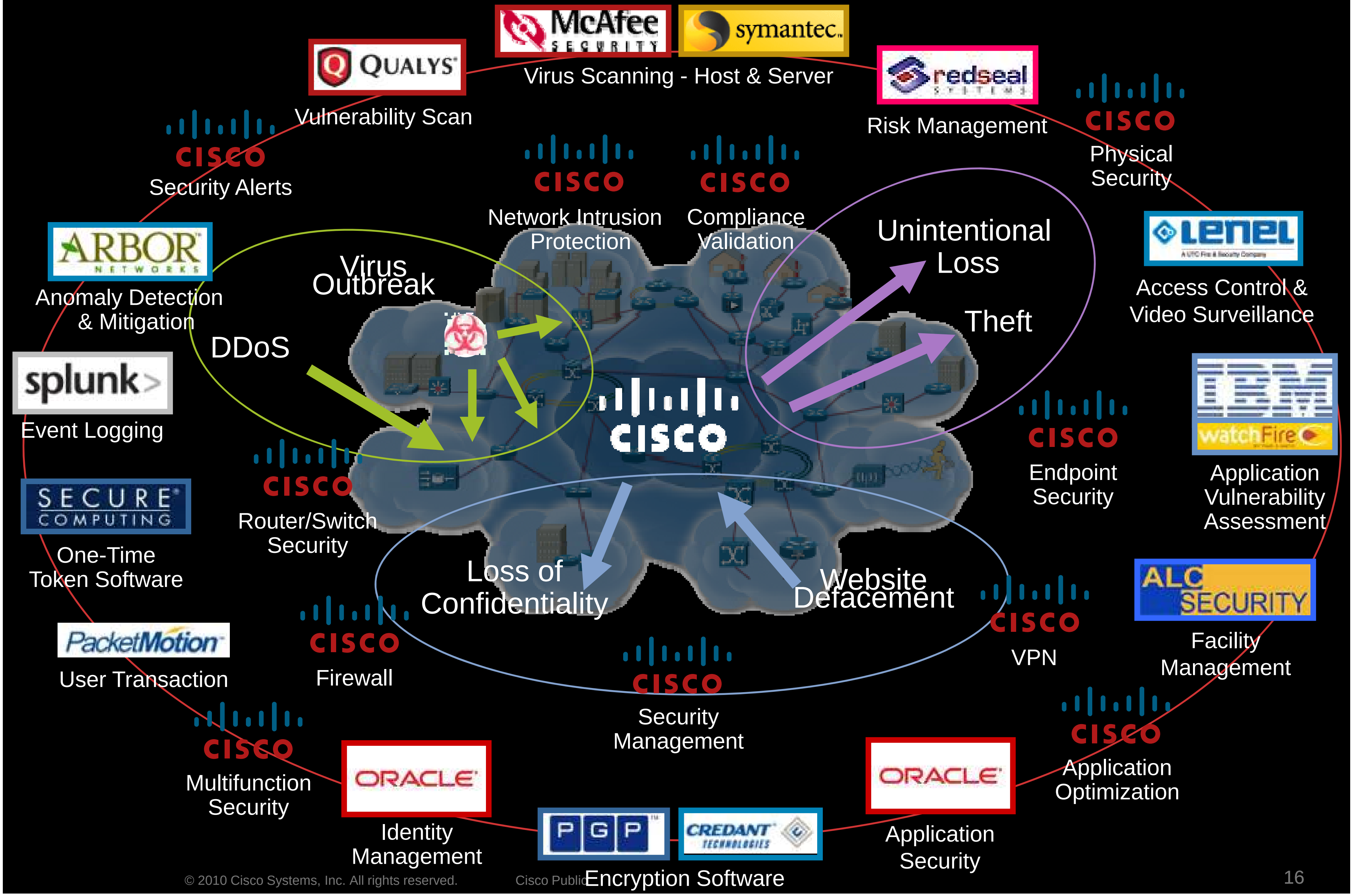
CURRENT STATE

Asymmetric Problems in Assurance…

Expensive To Protect, Trivial To Shake Confidence

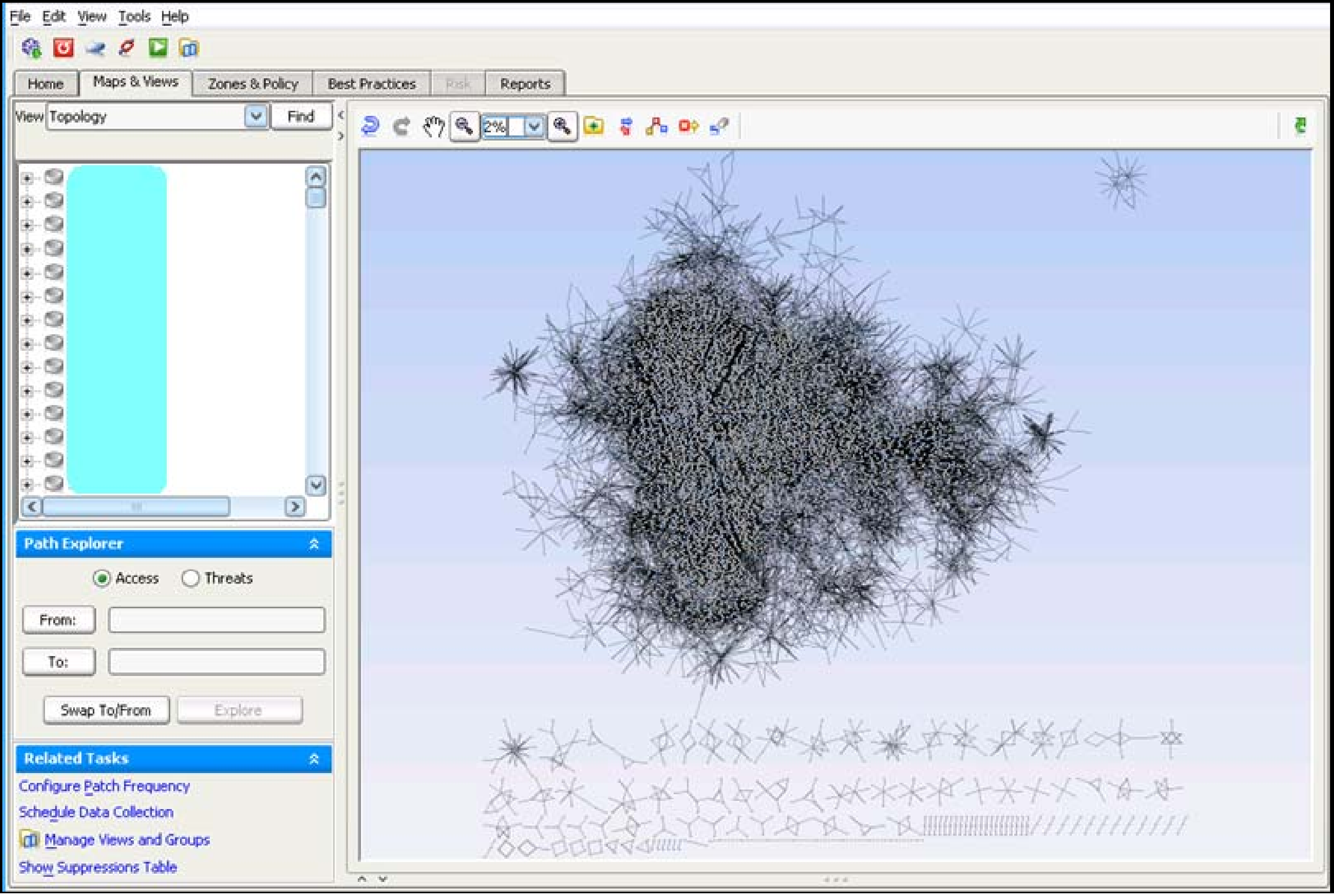
- We spend an amazing amount protecting, and it is trivial to circumvent
- Complexity is the enemy, and the opportunity
- Our adversaries use our practice against us, especially when it is fixed

Technology Integration Is Complex

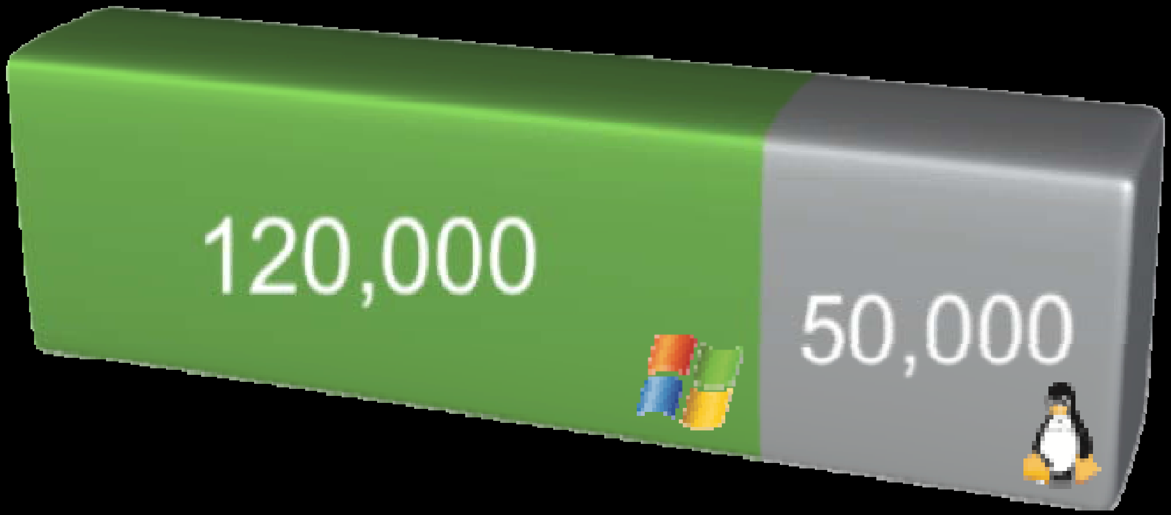


40,000 **Routers on Cisco’s network**

Network Layers are Complex



Hosts are Complex

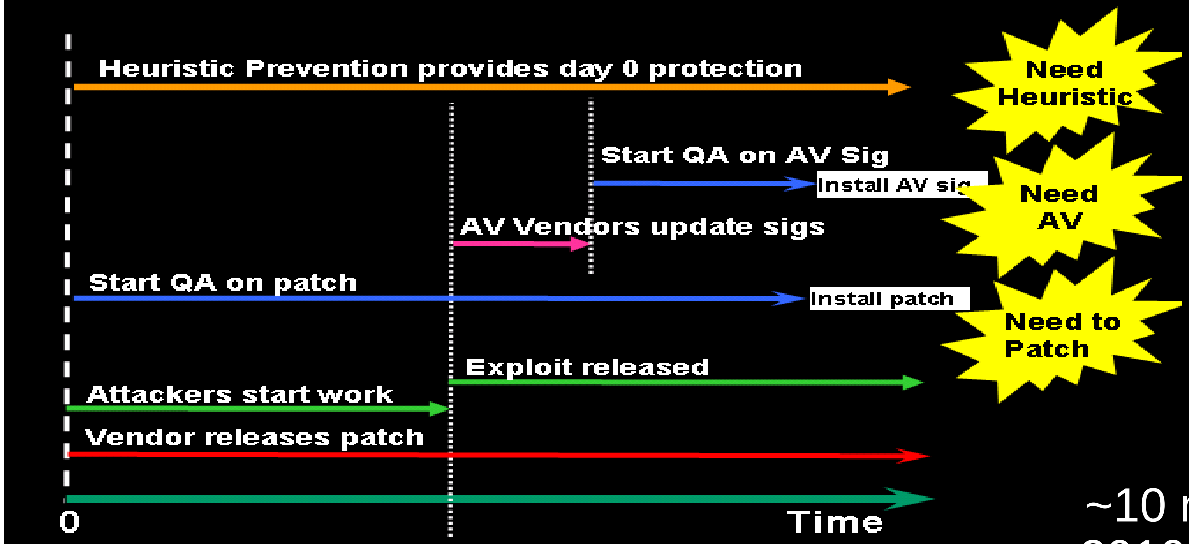


Data is Complex

2,000,000

Highly tuned IDS alerts per day

“Traditional” Practice Is Losing Effectiveness



Heuristic Prevention provides day 0 protection

Start QA on AV Sig

Install AV sig

AV Vendors update sigs

Start QA on patch

Install patch

Exploit released

Attackers start work

Vendor releases patch

0

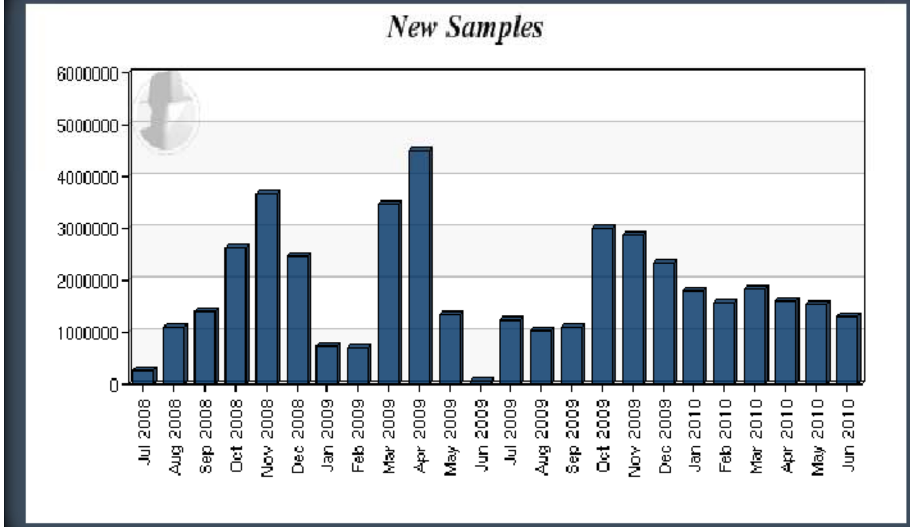
Time

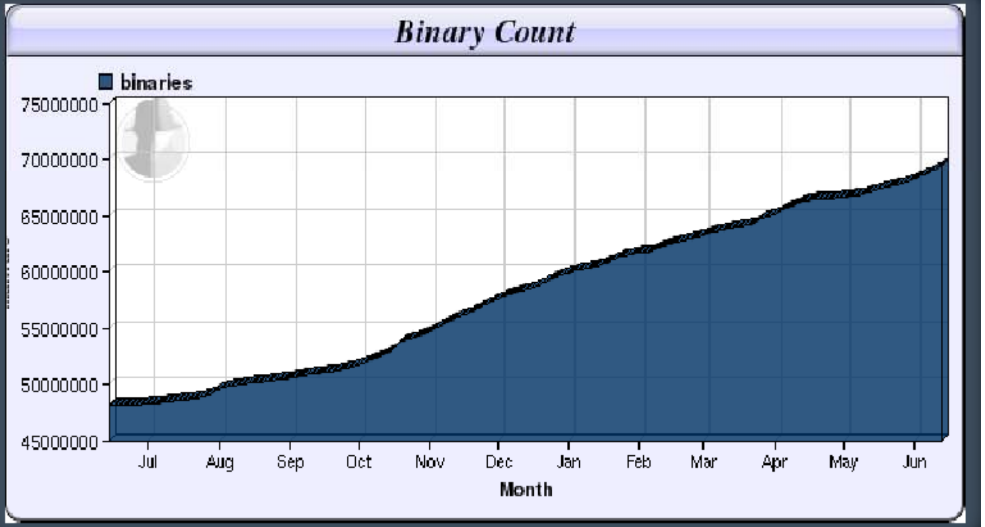
Need Heuristic

Need AV

Need to Patch

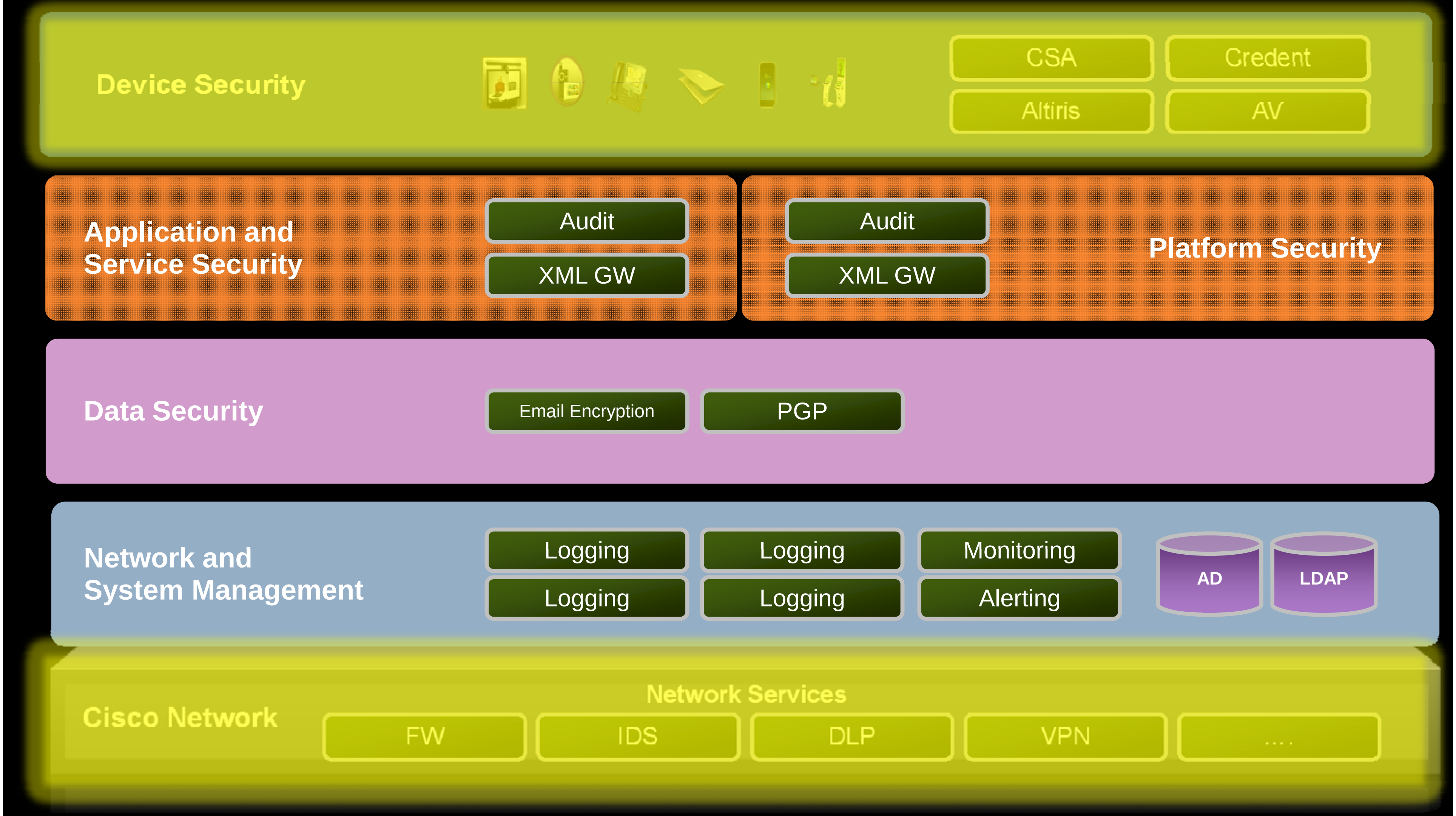
www.shadowserver.org/
14 June 2010
~10 million new hashed binaries in 2010 to date; ~70 million total seen





Where we are good is not what we need

Areas of Strength Today: Network and Device Security



Device Security

CSA

Credent

Altiris

AV

Application and Service Security

Audit

XML GW

Audit

XML GW

Platform Security

Data Security

Email Encryption

PGP

Network and System Management

Logging

Logging

Monitoring

Logging

Logging

Alerting

AD

LDAP

Cisco Network

Network Services

FW

IDS

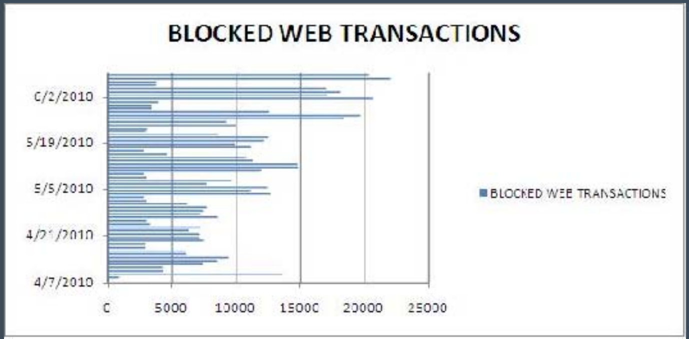
DLP

VPN

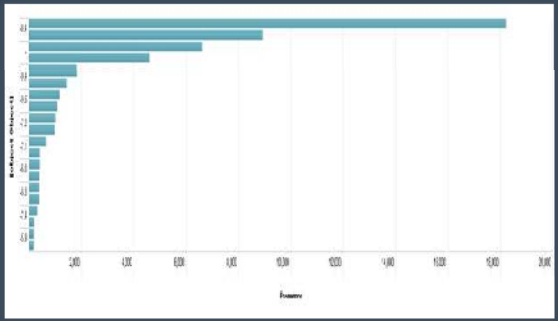
. . . .

Web Security – The Data
Malicious Transactions Blocked

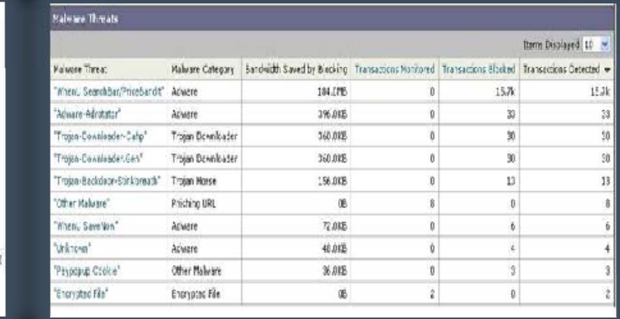
- 600,000+ including:
  - Malware downloads
  - Browser hijacking software
  - Unwanted advertisement software
  - Botnet check-ins
  - Trojan (backdoor) connections



- Average response to client = 1.4 seconds
- Average daily log data = 9Gb
- Average allowed web transactions passed = 500K/60 minutes



Top 10 Blocked Web-based Reputation Scoring

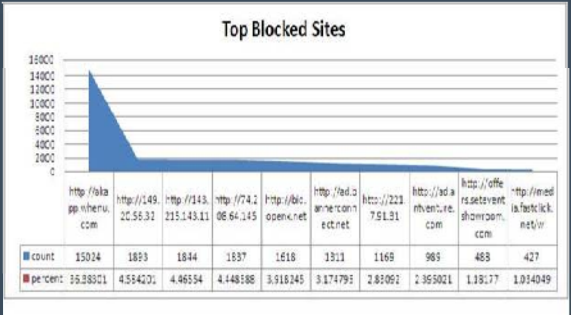


Malware Threats

Items Displayed 10

Malware Threat	Malware Category	Bandwidth Saved by Blocking	Transactions Monitored	Transactions Blocked	Transactions Detected
"WhenU.SearchBar/PriceBandit"	Adware	184.1MB	0	15.7k	15.7k
"Adware-Adrotator"	Adware	396.0KB	0	33	33
"Trojan-Downloader-Zahp"	Trojan Downloader	360.0KB	0	30	30
"Trojan-Downloader.Gen"	Trojan Downloader	360.0KB	0	30	30
"Trojan-Backdoor-Stirkoreach"	Trojan Horse	156.0KB	0	13	13
"Other Malware"	Phishing URL	0B	8	0	8
"WhenU.SaveNow"	Adware	72.0KB	0	6	6
"Unknown"	Adware	48.0KB	0	4	4
"Popup Cookie"	Other Malware	36.0KB	0	3	3
"Encrypted File"	Encrypted File	0B	2	0	2

Top Malware Threats blocked



	http://akapp.whenu.com	http://149.20.56.32	http://143.215.143.11	http://74.208.64.145	http://bic.openx.net	http://ad.bannerconnect.net	http://2217.91.31	http://adanventure.com	http://offers.seteventshowroom.com	http://media.fastclick.net/w
■ count	15024	1893	1844	1837	1618	1311	1169	989	483	427
■ percent	36.38301	4.584201	4.46554	4.448588	3.918245	3.174795	2.83092	2.395021	1.18177	1.034049

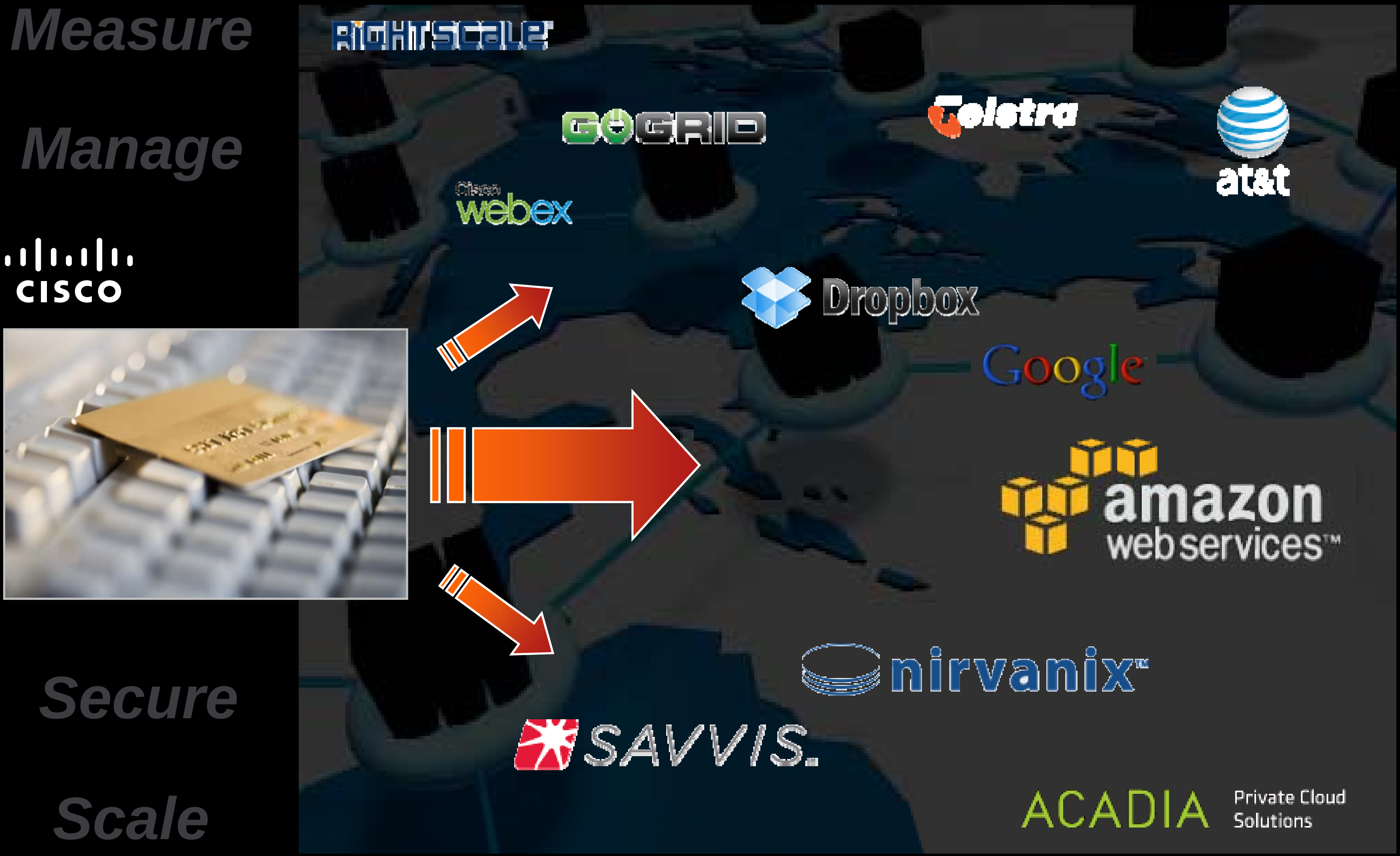
Top 10 Blocked Domains

And Data is Moving

Measure

Manage

cisco



Secure

Scale

GOING FORWARD

The best way to predict the future is to invent it.

--Alan Kay

Ask The Right Questions

You Get What You Measure, No Matter What

- Always question what you are doing –
  some things have declining investment and results

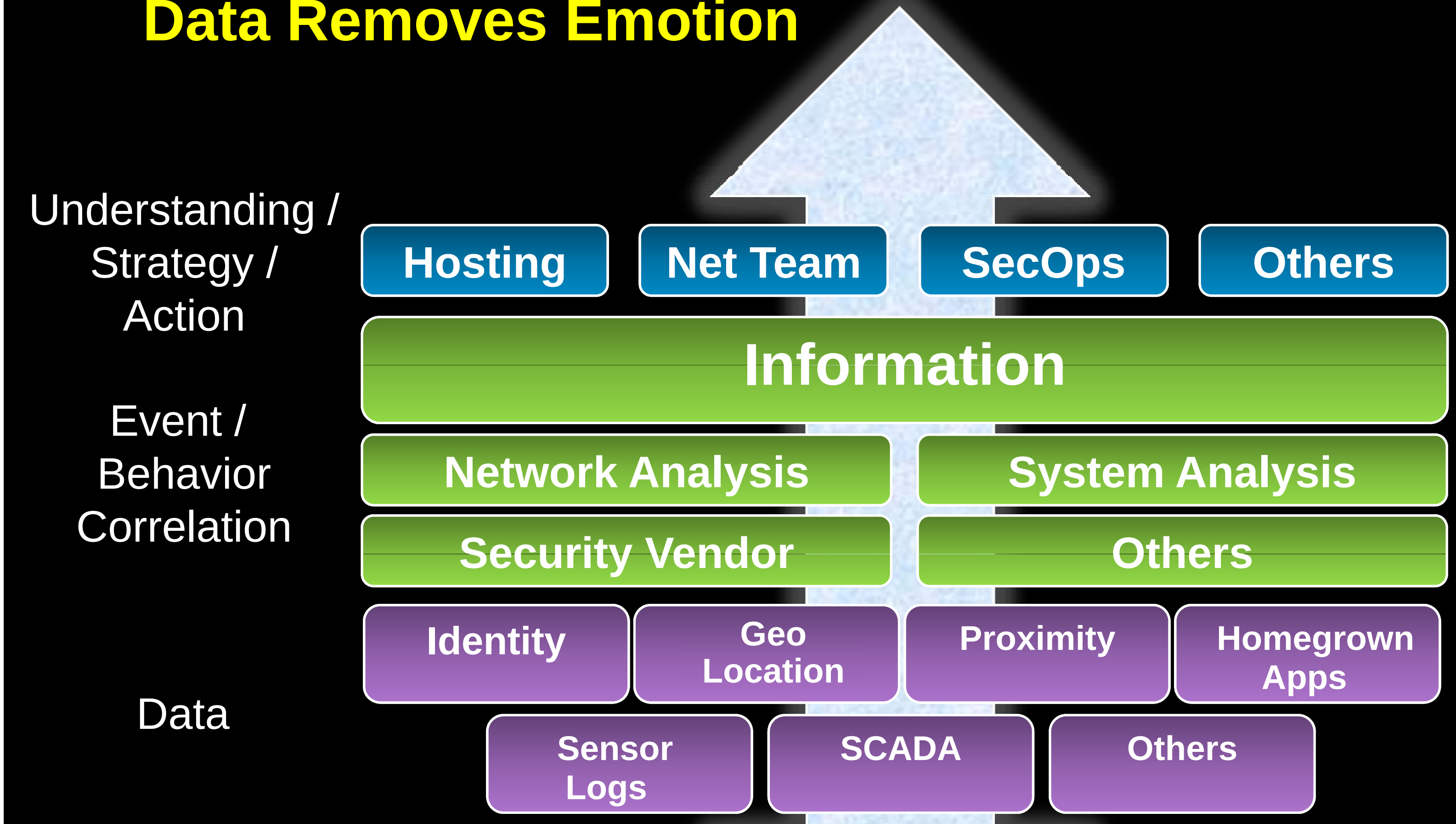
- Stop asking for best practices –
  start asking "what's effective and how effective is it?"

- What can I see, what don't I know,
  how will I know it when I need to?

- What can I shamelessly copy from someone else?

See, Don’t Feel – Analyze

Data Removes Emotion



Understanding / Strategy / Action

Hosting | Net Team | SecOps | Others

Information

Event / Behavior Correlation

Network Analysis | System Analysis

Security Vendor | Others

Data

Identity | Geo Location | Proximity | Homegrown Apps

Sensor Logs | SCADA | Others

“I have a series of questions, and the data gives the answers”

~ or ~

“I don’t know the questions yet; let’s look at the data”

A Trend is Emerging…

Trusted System or Service

Trusted Platform

- Authentication
- Trojan Prevention
- Strong Identity
- Secure Storage
- Monitoring
- Hardware Assurance

Software Assurance

- Threat Modeling
- Identity Assurance
- Safe Libraries
- Run-Time Defenses
- Static Analysis
- Security Defect Triage and Resolution
- Compliance and Vulnerability Testing

Supply Chain Security

- Preferred Suppliers
- Secure Logistics

Independent Product Certification

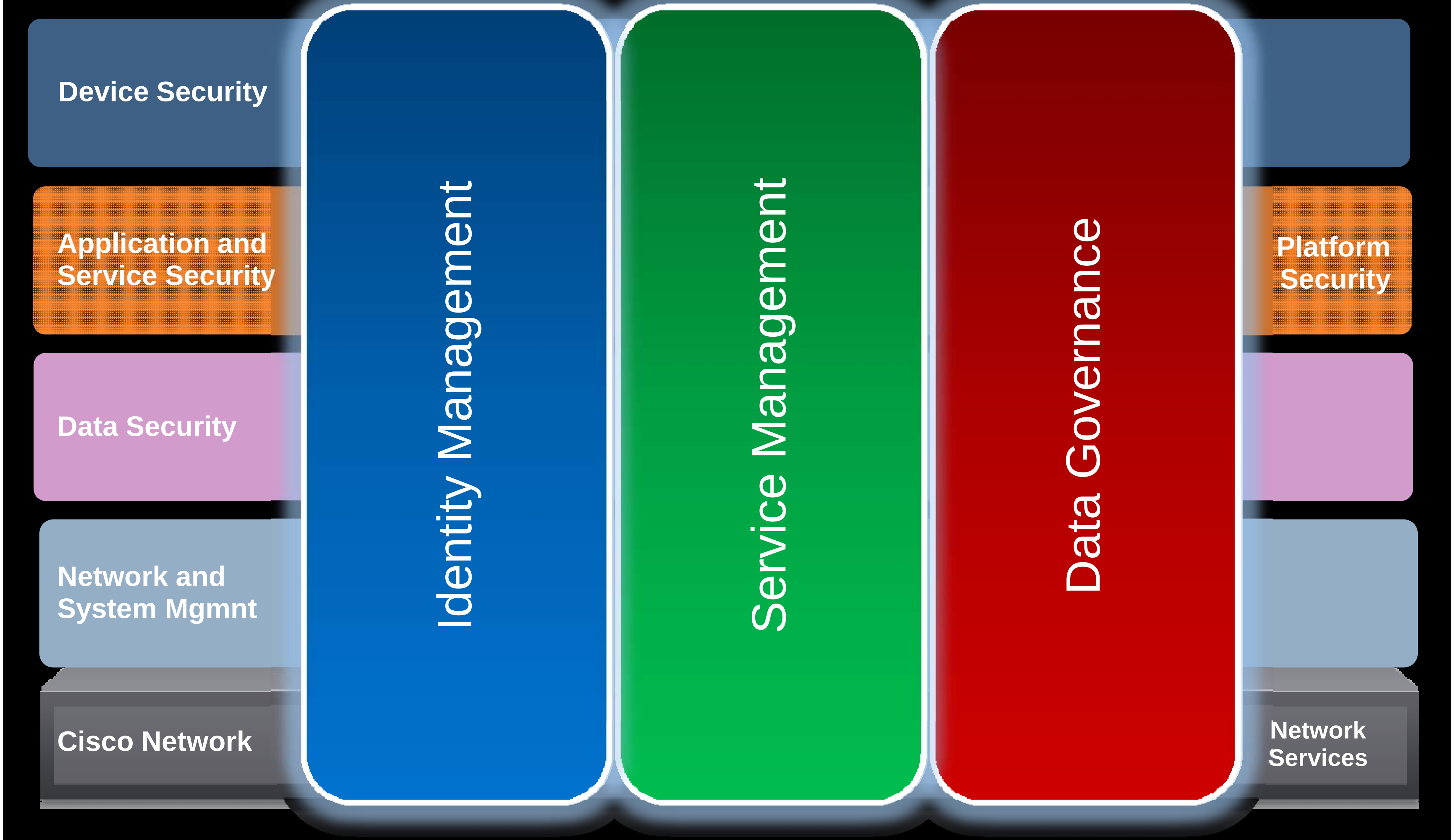
- Standards-Based
- Mutually Recognized

My Responses

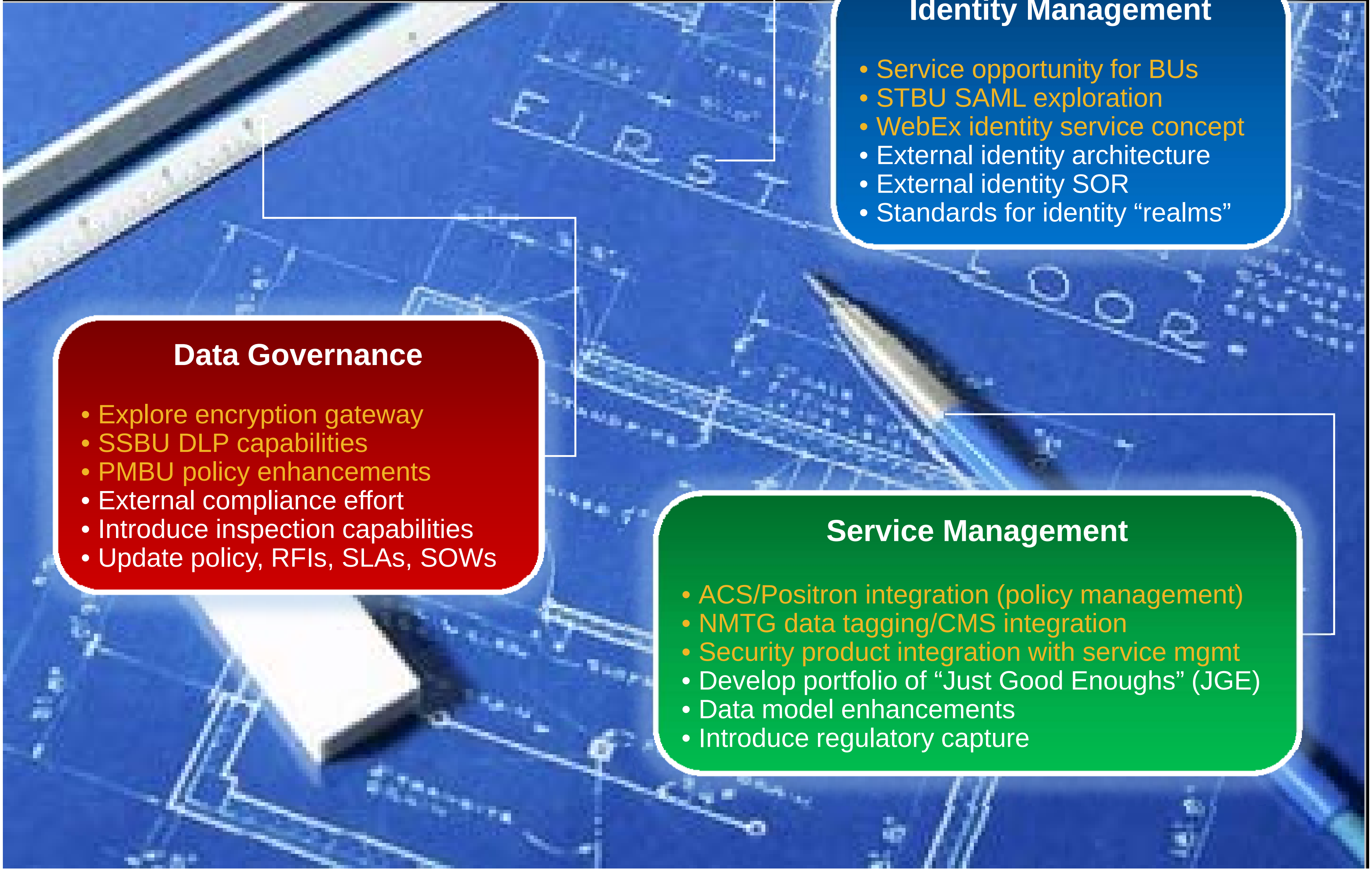
The Hard Work… Has Just Begun

- Manual → Automated
- Borders → Everywhere
- Unknown → Known/Assured

Enterprise Security Architecture Framework



High-Level Targets



Identity Management

- Service opportunity for BUs
- STBU SAML exploration
- WebEx identity service concept
- External identity architecture
- External identity SOR
- Standards for identity “realms”

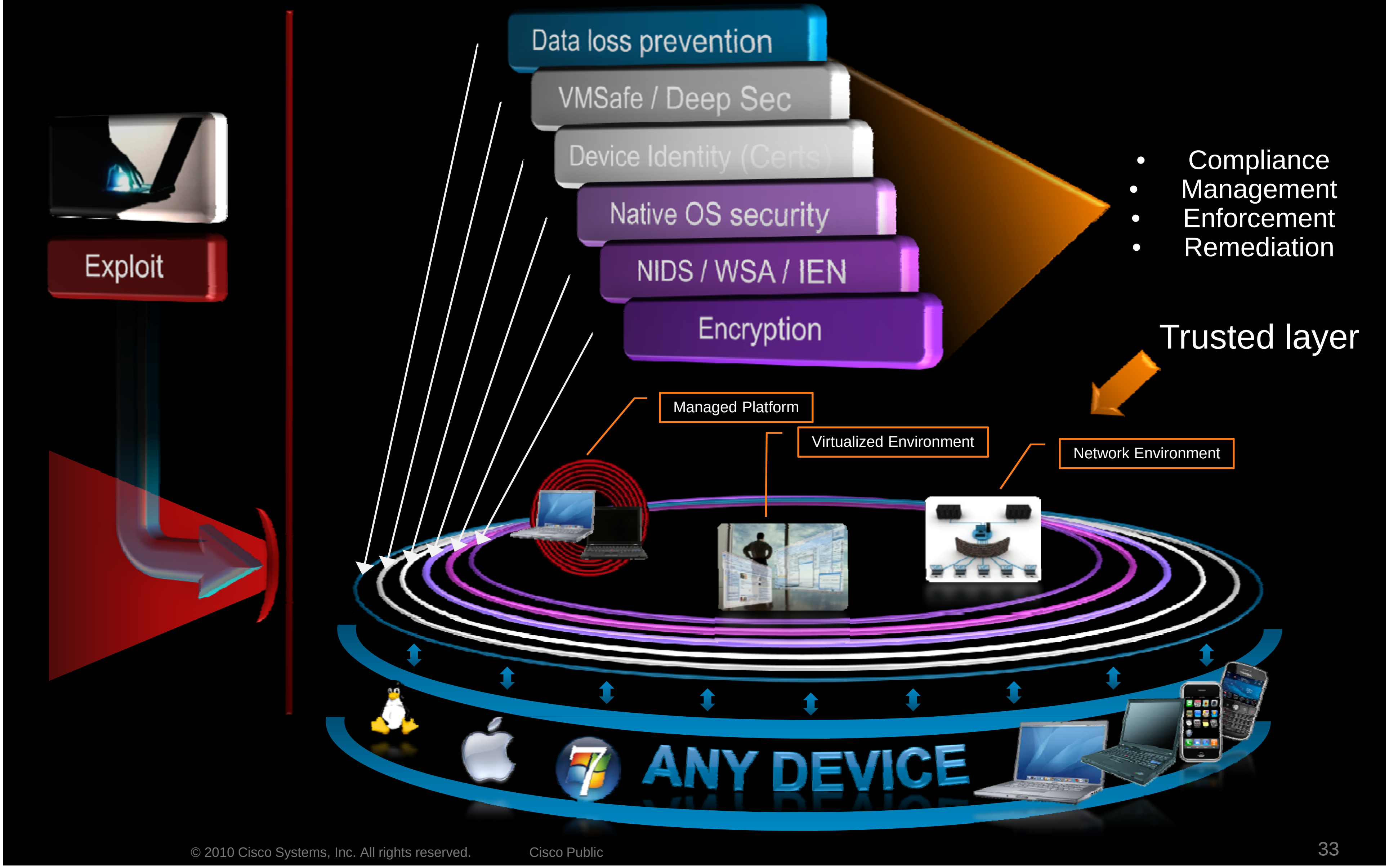
Data Governance

- Explore encryption gateway
- SSBU DLP capabilities
- PMBU policy enhancements
- External compliance effort
- Introduce inspection capabilities
- Update policy, RFIs, SLAs, SOWs

Service Management

- ACS/Positron integration (policy management)
- NMTG data tagging/CMS integration
- Security product integration with service mgmt
- Develop portfolio of “Just Good Enoughs” (JGE)
- Data model enhancements
- Introduce regulatory capture

Future Client Platform Environment



Exploit

Data loss prevention

VMSafe / Deep Sec

Device Identity (Certs)

Native OS security

NIDS / WSA / IEN

Encryption

- Compliance
- Management
- Enforcement
- Remediation

Trusted layer

Managed Platform

Virtualized Environment

Network Environment

ANY DEVICE

Key Takeaways

- Conclusions

  This Phase is Different

  Big changes are having a profound affect on security

  “Know thyself” - attain a high degree of situational awareness

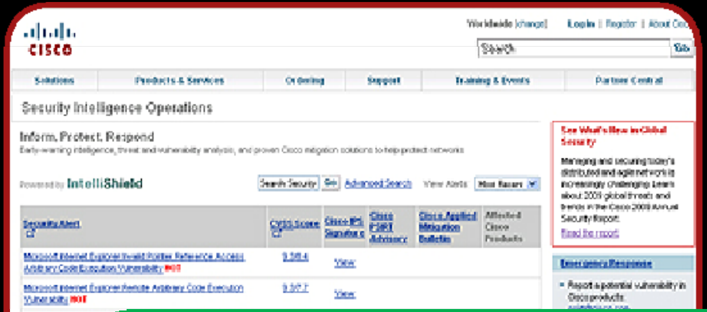
  Ask the right questions to get the right answers

  Look to the data to point the way

More Information

Security Intelligence Operations

www.cisco.com/security



Worldwide [change] | Log In | Register | About Cisco

Search | Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

Security Intelligence Operations

Inform. Protect. Respond

Early-warning intelligence, threat and vulnerability analysis, and proven Cisco mitigation solutions to help protect networks

Powered by IntelliShield | Search Security | Go | Advanced Search | View Alerts: Most Recent

Security Alert	CVSS Score	Cisco IPS Signature	Cisco PSIRT Advisory	Cisco Applied Mitigation Bulletin	Affected Cisco Products
Microsoft Internet Explorer Invalid Pointer Reference Access Arbitrary Code Execution Vulnerability HOT	9.3/8.4	View			
Microsoft Internet Explorer Remote Arbitrary Code Execution Vulnerability HOT	9.3/7.7	View			
Threat Outbreak Alert: Messages on Mar...					
Threat Outbreak A... Purchase Confirm...					
Network Time Pro... Service Vulnera...					

» More

See What's New in Global Security

Managing and securing today's distributed and agile networks is increasingly challenging. Learn about 2009 global threats and trends in the Cisco 2009 Annual Security Report.

Read the report

Emergency Response

- Report a potential vulnerability in Cisco products

Security

Insights from the Cisco Security Community

Join the Conversation

- The Platform
- Channels
- Collaboration
- Data Center Networks
- Digital Consumer
- Digital Media
- Economy
- Emerging Countries
- High Tech Policy
- Innovation
- Inside Cisco
- Mobility
- Security
- SP360: Service Provider
- Virtual Environments

March 15, 2010

Medicine, Taxation, and Identity in Cyberspace

There are innumerable benefits to digitized record-keeping. I can't say enough about the benefits of correlation and collation of information that could be gained from taking information off of paper and moving it into computers. For health information, the potential benefits are incredible and could markedly advance individual well-being. The portability and accessibility of electronic records alone, not to mention the visualization and mining of trends, association between care and outcomes, and the effectiveness of diagnosis, treatment, and costs, all stand to benefit patients and their health.

But as health records move to digitization, some individuals are taking an opportunity to commit fraud, due to weaknesses in the system. There are risks that exist with paper records that could be mitigated by digitized records, but once healthcare organizations digitize, new risks can arise.

Read More.

Search

○ Posts ○ Author

Go

Cisco Around the Web

- Follow us on Twitter
- Join us on Facebook
- Subscribe on iTunes
- Watch our Videos
- [illegible] on Flickr

Security Blog

blogs.cisco.com/security

Security Education

www.cisco.com/go/securityeducation

Information Security Programs

Cisco is committed to empowering employee, customer, and partner security by sharing best practices and executive thought leadership.

See Cisco's internal campaign in action.

» Learn More

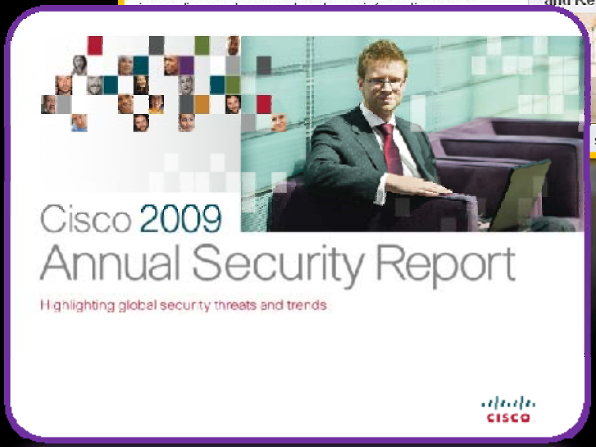
Watch Video

Data Loss Prevention | Enterprise Security | Government Security | Security Education | Security Process

Protecting intellectual property is one of the most important steps a business can take to safeguard its assets. Lost data can cost an organization millions of dollars, and

Safeguard Business Data and Resources

Stewart talks about how



Cisco 2009

Annual Security Report

Highlighting global security threats and trends

2009 Security Annual Report

www.cisco.com/go/securityreport

cisco