LES ENJEUX DE LA SÉCURITÉ INFORMATIQUE: MYTHES, RÉALITÉS ET POINTS D'INTERROGATIONS

GRIFES – 30 Novembre 2004

Vincent Bieri

Marketing Manager, Security

EMEA Technology Marketing Organisation

The need for information security

- We are operating in an increasingly hostile marketplace
- We have become totally reliant on IT
- We are extending our enterprises outside our trusted environments and increasing our range of services
- There is an increasingly demanding framework of regulation and law
- Our organisation’s good name is paramount, and our reputation is priceless. We have to protect these from harm

The challenges we all face

- There is widespread complacency about information security
- There exists a false sense of security
- Historically, we have not focussed on the “selling” of information security
- Traditionally, technical solutions have been adopted as solutions for what are essentially “people” problems
- We have tended to be our own worst enemies - the business manager versus the “techie”

What the Experts Say....

- Bill Gates: **'Security Off Top-Five List in Two Years‘**

  "I think within the next two years [security] will get off the top five list [of concerns] ... it's probably two years until all the issues around easy quarantine, and everybody being educated and having all the really great auditing tools out there ...“

- Professor Hannu H. Kari of the Helsinki University of Technology : **‘Internet will crash in 2006’**

  “The explosive growth of computer viruses and unsolicited email has contributed to the coming crash. The next phases are the deterioration of computer grid reliability and an increase in the manipulation of internet content”

Agenda

Cisco.com

- What are the Risks and Threats ?
- The Time for Information Security is now, but how ?
- The Technology to the Rescue ?
- What is the Cisco Security Strategy ?
- Summary

WHAT ARE THE RISKS AND THREATS ?

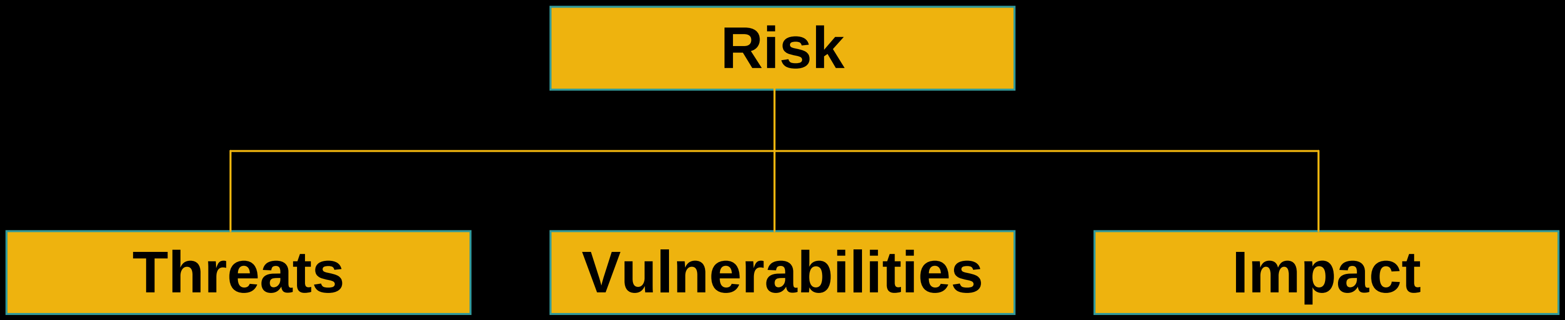
How to you usually get in Trouble ?

- Information security is not only about being killed by an alligator….

- ...It is usually about being eaten to death by a thousand chickens…

The Risk Model

- Risk is not the same as threat
- There are many “formula” to evaluate risk but overall they always relay on three events and their probability to happen
- Risk is a question of view point



What is at Risk ?

- **Your Assets are...**

  Information and systems

  Reputation

  Potential

  People

  Property

What are the Impacts ?

- **Direct**

  Financial loss (revenue and capital)

  Damage to the credit rating

  Breach of regulation or law

- **Indirect**

  Damage to reputation

  Loss of customer confidence

  Loss of shareholder confidence

  Loss of management control

There are Many Threats

- Threats are many and varied, with both internal and external sources and known and unknown ones…

  Web site defacement, denial-of-service attacks, infection by worm or virus, theft of intellectual property, etc.

  BotNets ‘owned’ by organised crime syndicates for sending spam and DDos extortion attacks

  Phishing scams

Evolution of Security Threats

- Vulnerability-to-exploit window is now just **5.8** days
- The average number of monitored 'bots rose from under 2,000 to more than **30,000** ***per day***
- Increase in Severe, Easy-to-Exploit Vulnerabilities – more than 1,237 new vulnerabilities

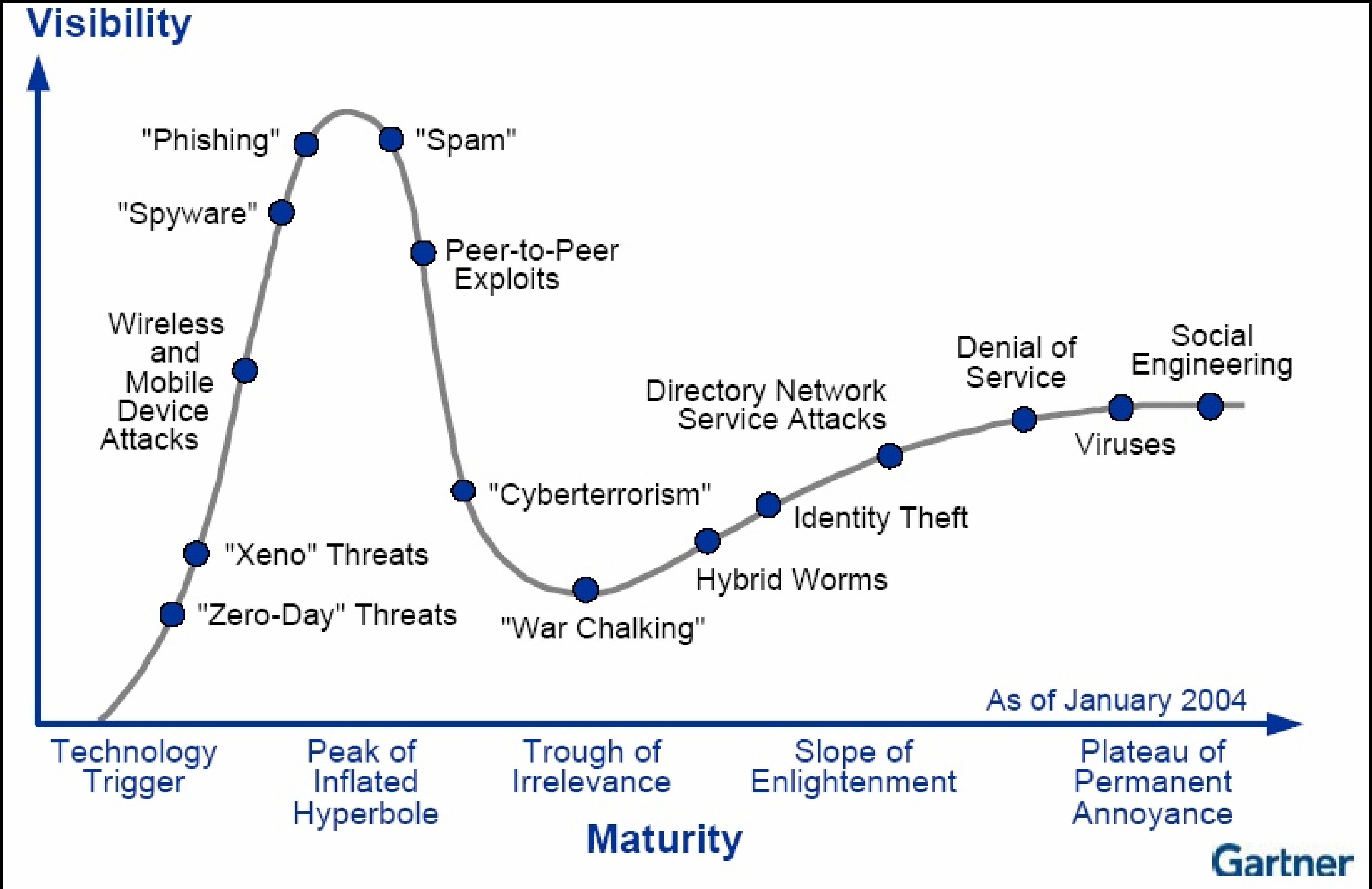
  an average of **48 new vulnerabilities per week**
- More than **4,496 new Windows viruses and worms** documented

  More than **4½ times** the number in the same period in 2003

Source: Symantec Internet Security Threat Report, September 2004, for H1CY04

Evaluating Threats

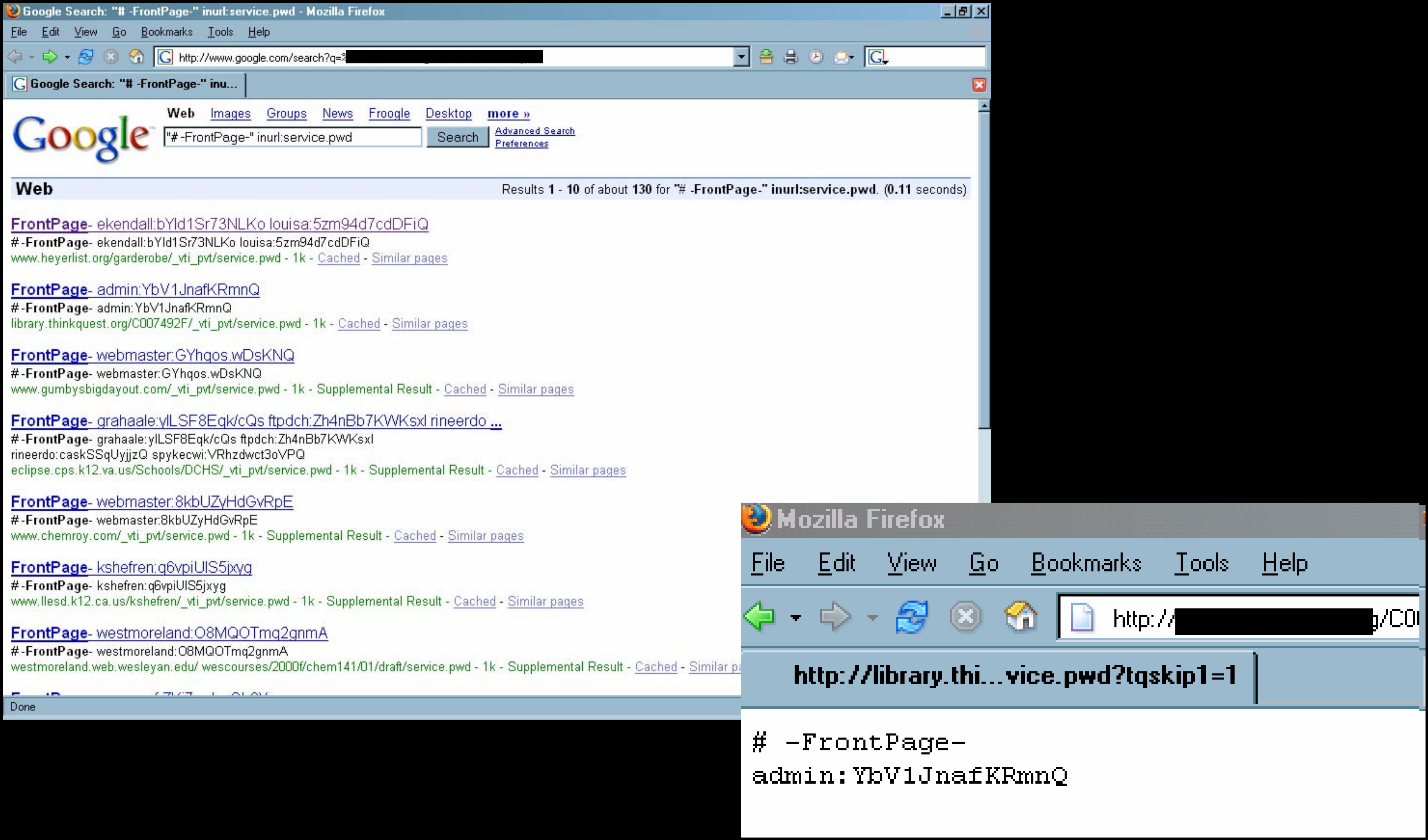
Gartner Security Threat Hype Cycle



But don’t Forget These Threats...

- Human error or ignorance
- Systems malfunction
- Loss of services, facilities or equipment
- Poor patch management
- Natural hazards

Even Google is a Threat !


Google Search: "# -FrontPage-" inurl:service.pwd - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.google.com/search?q=%[redacted]
Google Search: "# -FrontPage-" inu...
Google
Web Images Groups News Froogle Desktop more »
Search
Advanced Search
Preferences

"# -FrontPage-" inurl:service.pwd

Web Results **1** - **10** of about **130** for "# **-FrontPage-" inurl:service.pwd**. (**0.11** seconds)

FrontPage- ekendall:bYld1Sr73NLKo louisa:5zm94d7cdDFiQ
#-**FrontPage**- ekendall:bYld1Sr73NLKo louisa:5zm94d7cdDFiQ
www.heyerlist.org/garderobe/_vti_pvt/service.pwd - 1k - Cached - Similar pages

FrontPage- admin:YbV1JnafKRmnQ
#-**FrontPage**- admin:YbV1JnafKRmnQ
library.thinkquest.org/C007492F/_vti_pvt/service.pwd - 1k - Cached - Similar pages

FrontPage- webmaster:GYhqos.wDsKNQ
#-**FrontPage**- webmaster:GYhqos.wDsKNQ
www.gumbysbigdayout.com/_vti_pvt/service.pwd - 1k - Supplemental Result - Cached - Similar pages

FrontPage- grahaale:ylLSF8Eqk/cQs ftpdch:Zh4nBb7KWKsxl rineerdo ...
#-**FrontPage**- grahaale:ylLSF8Eqk/cQs ftpdch:Zh4nBb7KWKsxl
rineerdo:caskSSqUyjjzQ spykecwi:VRhzdwct3oVPQ
eclipse.cps.k12.va.us/Schools/DCHS/_vti_pvt/service.pwd - 1k - Supplemental Result - Cached - Similar pages

FrontPage- webmaster:8kbUZyHdGvRpE
#-**FrontPage**- webmaster:8kbUZyHdGvRpE
www.chemroy.com/_vti_pvt/service.pwd - 1k - Supplemental Result - Cached - Similar pages

FrontPage- kshefren:q6vpiUIS5jxyg
#-**FrontPage**- kshefren:q6vpiUIS5jxyg
www.llesd.k12.ca.us/kshefren/_vti_pvt/service.pwd - 1k - Supplemental Result - Cached - Similar pages

FrontPage- westmoreland:O8MQOTmq2gnmA
#-**FrontPage**- westmoreland:O8MQOTmq2gnmA
westmoreland.web.wesleyan.edu/ wescourses/2000f/chem141/01/draft/service.pwd - 1k - Supplemental Result - Cached - Similar pa

Done

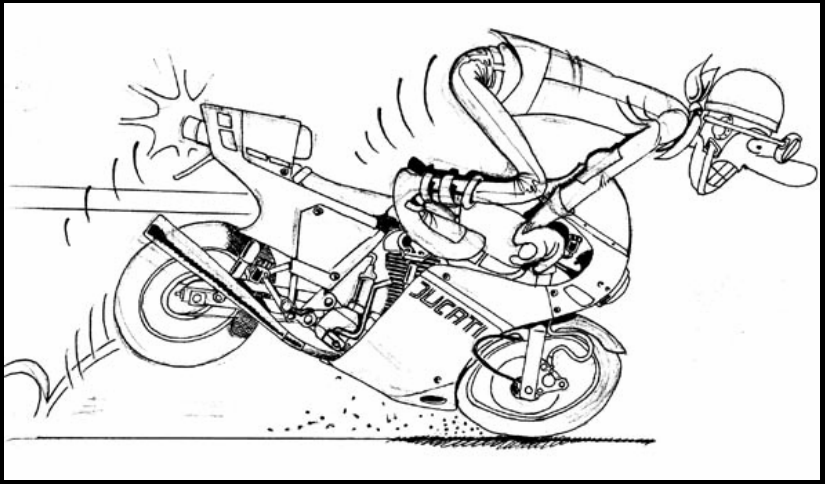
Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://[redacted]
http://library.thi...vice.pwd?tqskip1=1

```
# -FrontPage-
admin:YbV1JnafKRmnQ
```

THE TIME FOR INFORMATION SECURITY IS NOW, BUT HOW ?

Why do you have Brakes ?

To slow down ? .....



....No, to go faster!!!

Security = Top Business Issue

Gartner: Top Ten Business Trends In 2004

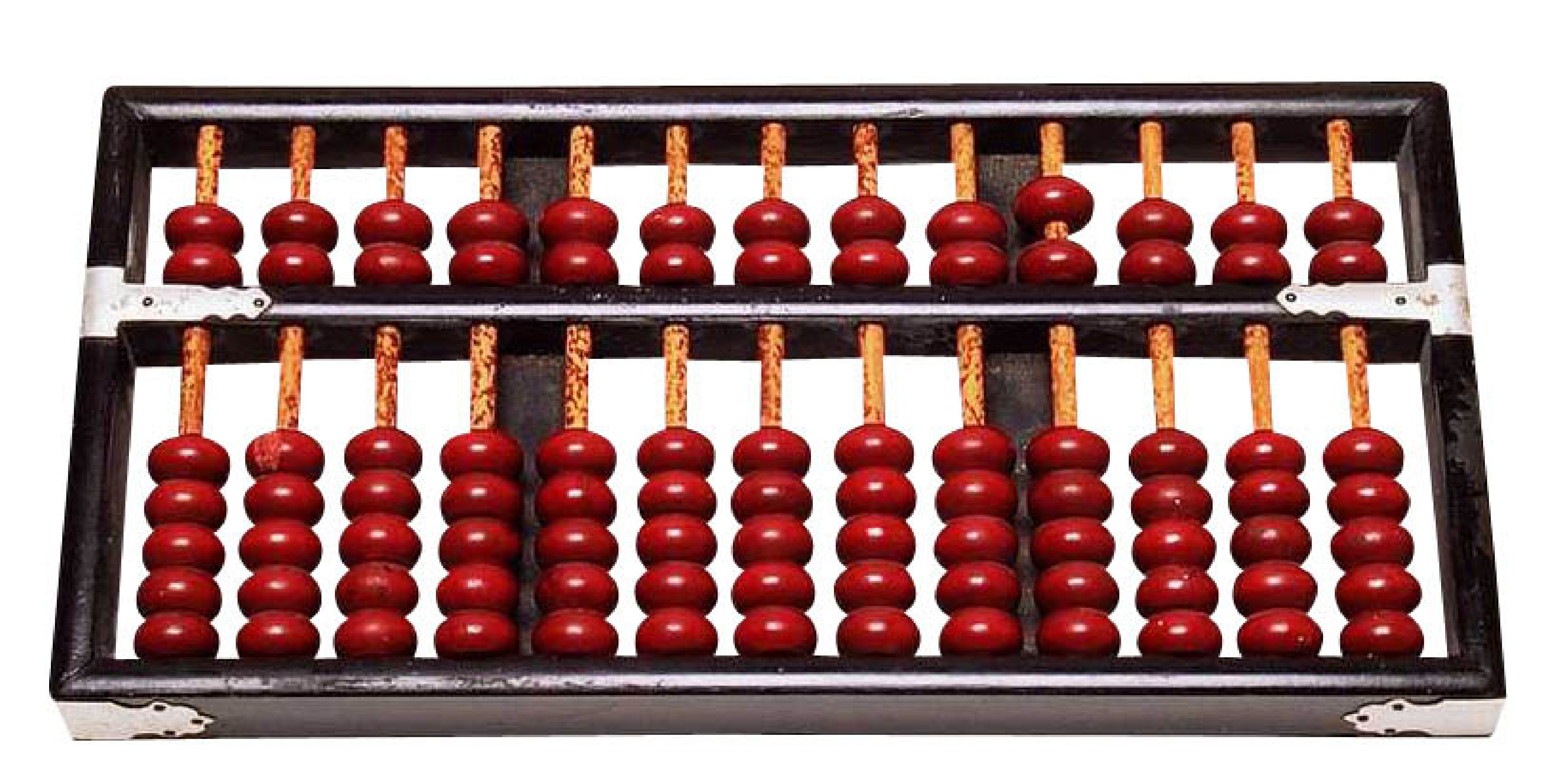
	Ranking			
	2002	2003		2004
Security breaches/business disruptions	-	12	↑	1
Operating costs/budgets	1	1	↓	2
Data protection and privacy	4	2	↓	3
* Need for revenue growth	-	-	↑	4
* Use of information in products/services	-	-	↑	5
* Economic recovery	-	-		6
Single view of customer	3	5		7
Faster innovation	5	3		8
Greater transparency in reporting	-	7		9
Enterprise risk management	-	4		10

↑ ↓ Selected change in ranking compared with 2003

* New question for 2004

The Truly Secure Computer Paradigm is not an Option

Cisco.com



Complex Infrastructures with New Technologies that must be Secured

- Mobility
- Wireless
- Storage
- Voice and Messaging
- ATM (Bank)
- Manufacturing Plants
- Web Services
- Outsourcing
- Grid Computing

And all is interconnected within and outside the organization

Principles of a Strategic Approach to IT Security

- Business focused
- Progressive
- Involves everyone
- Becomes part of the organisation’s culture
- Monitors and measures its own improvements
- Contributes to profit

Benefits of a Strategic Approach to IT Security

- **Improving:**

  availability and timeliness of business information

  integrity and reliability of business information

  confidentiality of business information

  accountability for actions taken using information

  authenticity of information

- **Reducing:**

  the number of, and losses from, security incidents and breaches

  the fraudulent use of business information

  insurance premiums

Rethinking Security

Business objectives should drive security decisions

Three Fundamental Security Questions:

1. What are you trying to do?

- What are your business objectives?
- What technologies or services are needed to support these objectives?
- Do they leverage your existing resources?
- Are they compatible with your current infrastructure and security solutions?

2. What risks are associated with this?

- Will you introduce new risks not covered by your current security solutions or policy?

3. How do you reduce that risk?

- How valuable are the assets at risk? What is your tolerance for risk?

Rethinking Security

Risk reduction requires integrated solutions and services

- **Security is NOT just about products**

  Security solutions must be chosen with business objectives in mind

  They must also:

  - Leverage existing infrastructure and intelligence

  - Contribute to correlative analysis and response

  - Provide automated, collaborative defense

  - Be INTEGRATED parts of a security SYSTEM

- **Security IS about RISK REDUCTION in a rapidly evolving environment**

  Maximum risk reduction is ALWAYS achieved with an integrated solution built on a flexible and intelligent infrastructure

Rethinking Security
Improving your Security

- Security is a Continuous Process
    - Review your network
    - Use configuration and architecture changes, additional controls and additional products
    - Test your defences by simulating attacks
        - External, internal, wireless and dial-in (modem)
        - Identify accessible systems; platforms; vulnerabilities; and then proving attack vectors that exploit those vulnerabilities

THE TECHNOLOGY TO THE RESCUE ?

Are you trying ?

- to **filter** heavily
- to **hardened** well
- to run regular system **inventories**
- to **patch**
- to keep **signatures** up-to-date
- to only load/run well **known files**

Security Technologies Are Changing

PAST	NOW
Firewall	App Based Virtualized Firewall
IDS / IPS	Universal AD (IDS+IPS+DDOS)
VPN Transport	Stateful & Dynamic VPNs
Secure Load balancing	Content/Application Security (SSL, Compression)

WHAT IS THE CISCO SECURITY STRATEGY ?

Cisco Security Strategy

- Create Integrated and Secure Intelligent Networks with Auto-Response Capabilities (AKA, Self-Defending Network) to improve reaction times and reduce windows of vulnerability
- This requires:

  Security features into the network infra-structure

  A presence on the Endpoint as well as the Network Edge

  Complimentary Anomaly-based (coarse-grained) and Signature-based (fine-grained) detection methods

  A proper Trust and Identity Infrastructure

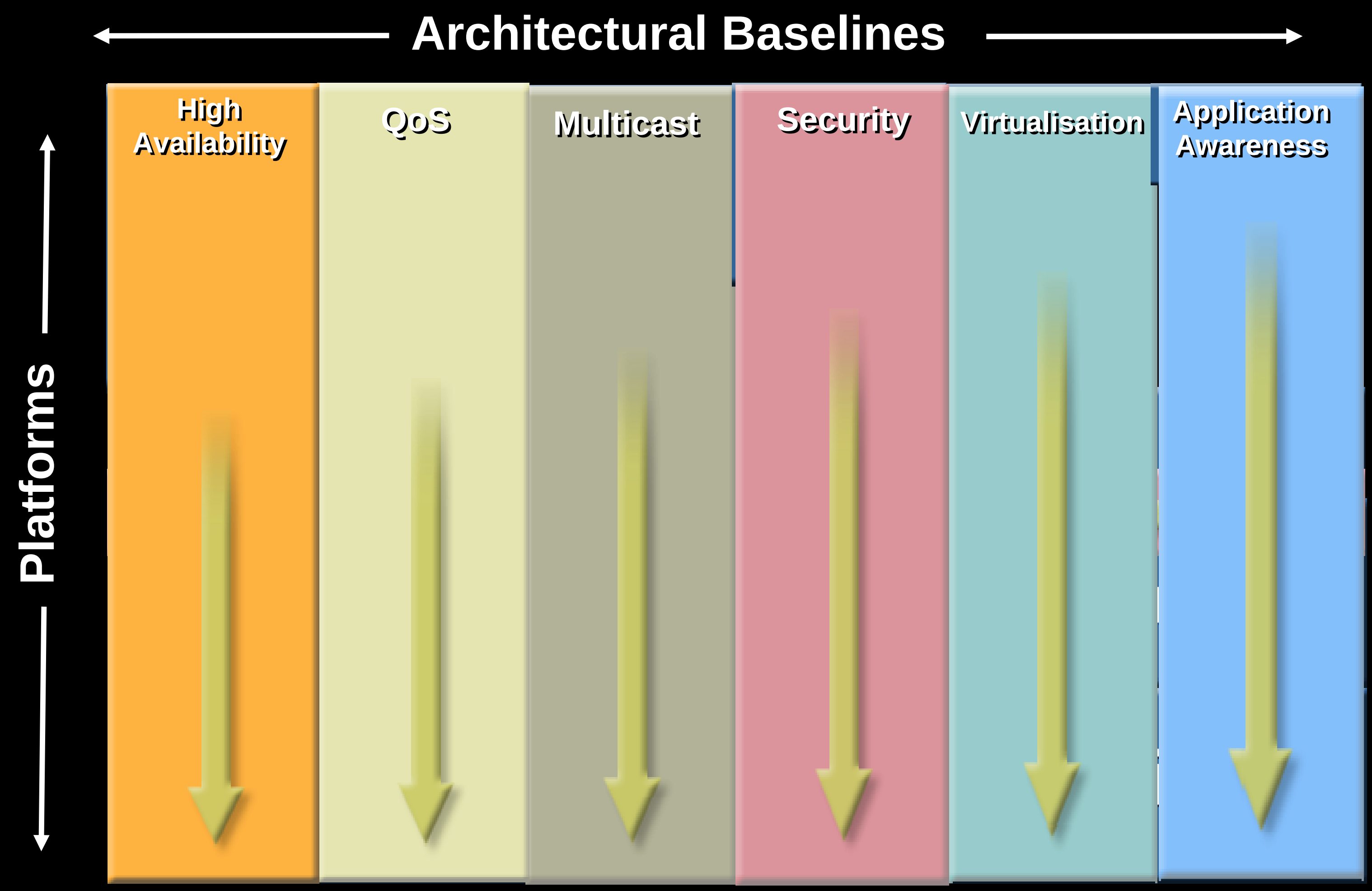
  Services

The Network as a System to Enable Business

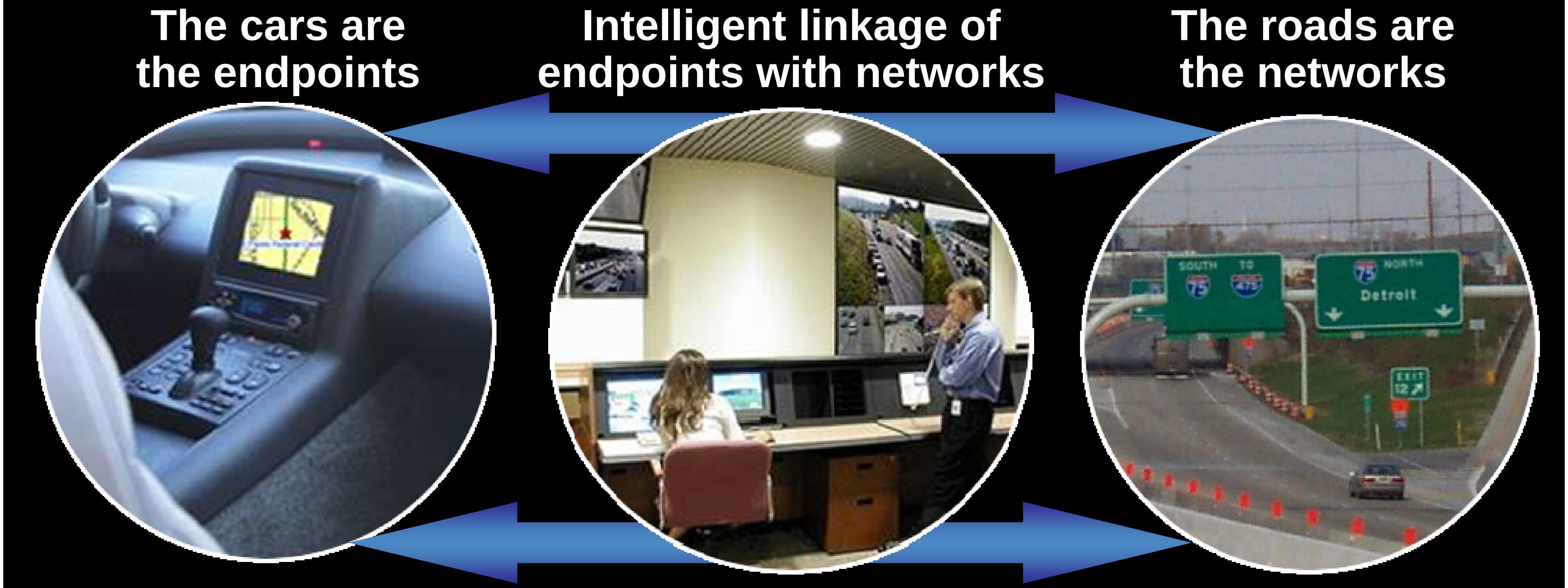
- The network used to be a transport that enabled application-layer traffic to move between end-points
- Today’s networks add value in many areas
  - Content management, QoS, rich media, etc.
- Next-generation networks takes this further…
  - Enable and support applications via technology, using services embedded in the very fabric of the network
  - Performance, quality, security, scalability and more…
- Your network = competitive advantage

Building a Systems-Based Infrastructure

Cisco.com



The Value of a Systems-Based Infrastructure



The cars are the endpoints

Intelligent linkage of endpoints with networks

The roads are the networks

SYSTEM-BASED TRAFFIC NAVIGATION AND MANAGEMENT

- Traffic monitoring
- Detours/reroutes pushed to auto navigation system
- Automated toll booths

Security Relevance to the Systems-Based Infrastructure

Infrastructure Resilience

- A secure network in which to conduct business

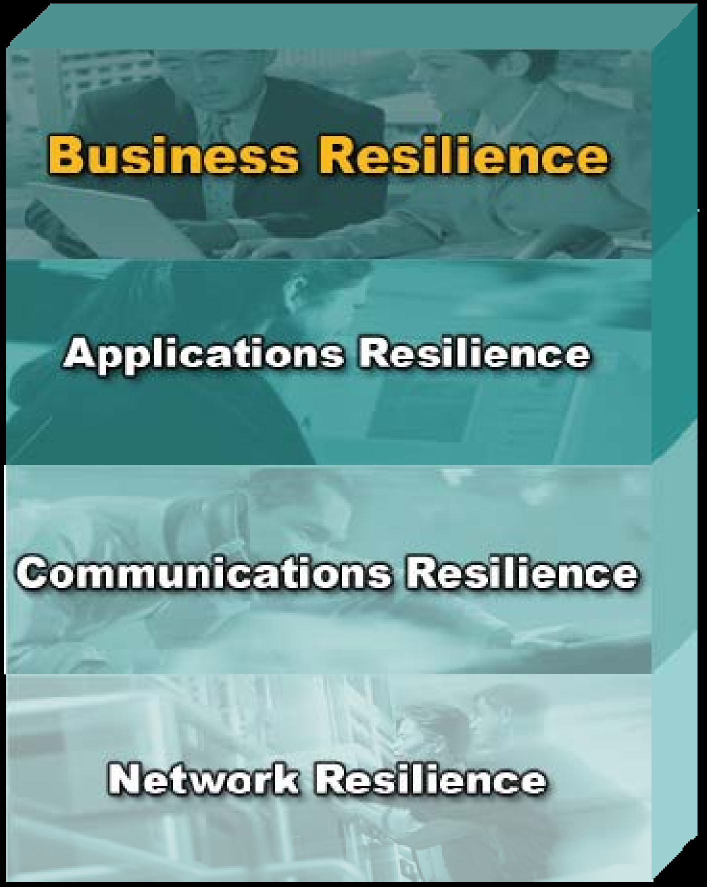
  Minimize risk

  Minimize exposure

  Maximize flexibility

- A companies business architecture mandates a solid secure infrastructure

  Can’t implicitly trust people, networks, computers, applications and processes



The Age of the ‘Soft Inside’ is Past

- You may trust your employees and local networks, but malicious code doesn’t care…

  Sasser, Blaster, Slammer, MyDoom, Bagel, Netsky…

  To date in 2004 the cost of major virus attacks is estimated at $16.7B globally Source: Computer Economics

- Where is your data?

  Mobile workers, partner extranets, flexible workforce, etc.

- How close to your data are your security controls?

The Age of the ‘Soft Inside’ is Past (cont.)

- Key strategies:
    - Identity management
    - End-point security
    - Flexible yet secure ‘internal’ networks
    - Data centre consolidation and security
    - Secure and resilient external connectivity
    - Defence-in-depth
- These strategies enable higher security **and** a lower overall cost of ownership

Admission Control is Key

- Too easy for an unsecured individual to gain physical and logical access to a network

  Username and password simply isn't sufficient

- A network port is either enabled or disabled

  More choices needed!

- 802.1x is part of the solution…

- …with Network Admission Control

  Focused on reducing damage from emerging security threats such as viruses and worms

The Internet Revolution Changed the Trust Context for Security

- In the Beginning.... Trust Was Implicit
- In 2004 the Internet reaches 2B people...Who can you trust?
- No one knows if...

  you are a hacker

  you are a spammer

  you are sending a virus

  your machine is infected

  if you are you!

The Real World Identity Trust Model

- It is about who you are...
- But also about validation of a security compliance

  from where you arrive

  where you go

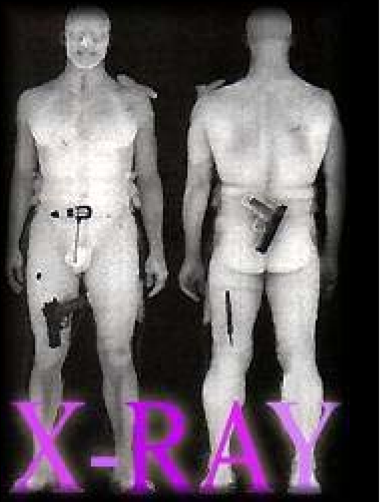
  what you do and want to do

  what are you carrying

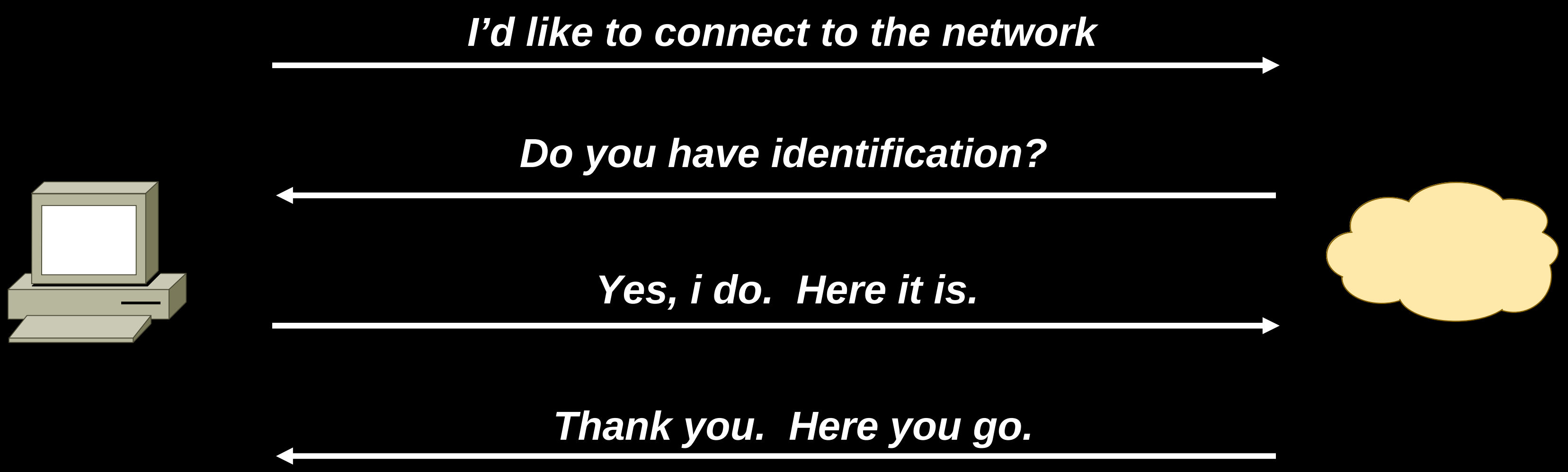
  your track records

  your health situation

- The context is as important as to prove who you are



Typical Identity Trust Model on the Network



I'd like to connect to the network

Do you have identification?

Yes, i do. Here it is.

Thank you. Here you go.

Open Questions for the Endpoint

How secure Is this network ?

How secure are the other ones connected ?

Will this network prevent me to receive a virus?

Open Questions for the Network

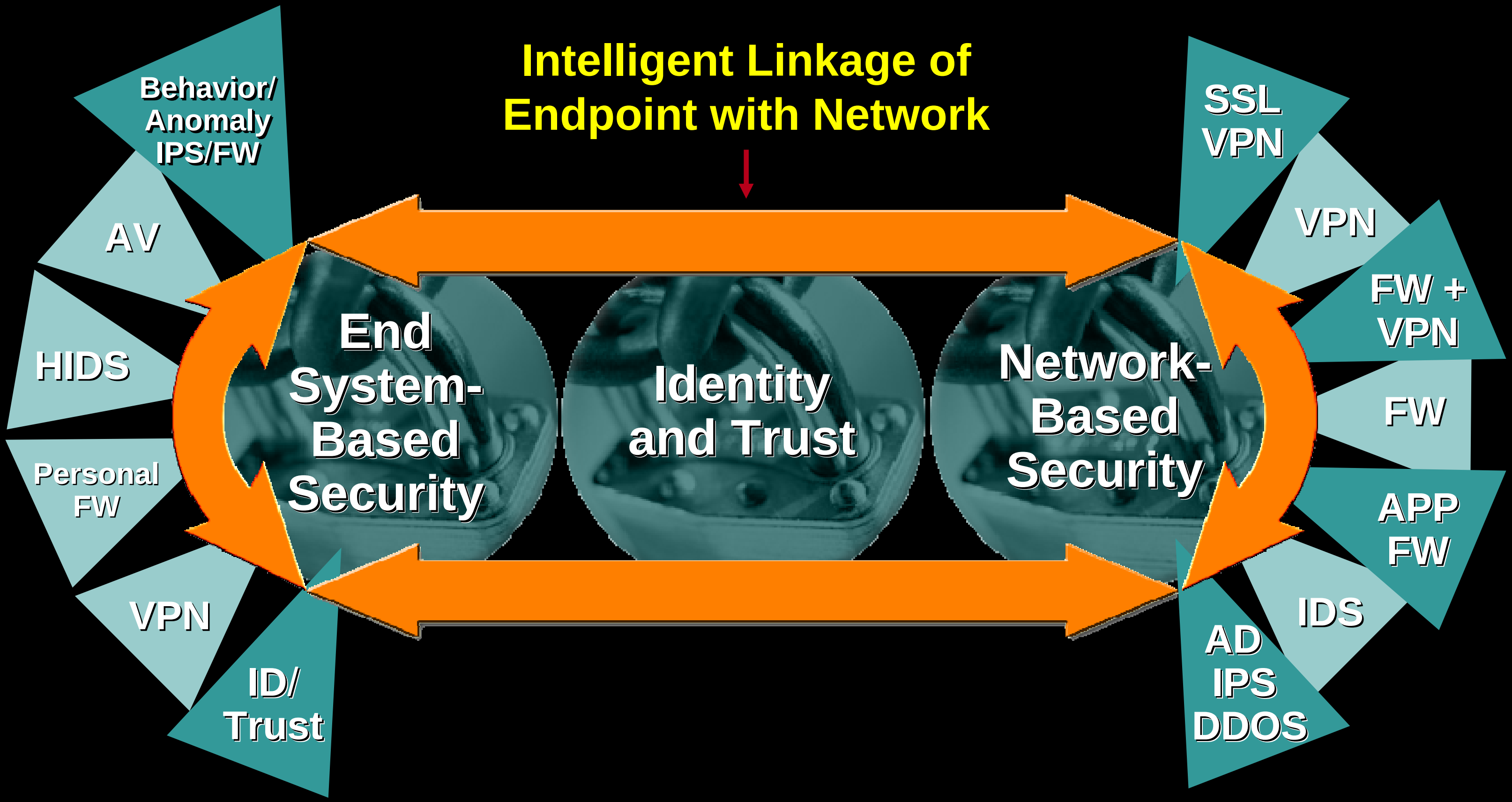
How secure Is this endpoint ?

Is it safe for the other to have accepted this endpoint ?

What if this endpoint starts to send a virus ?

Integrating the Endpoints with the Network

Intelligence requires trust



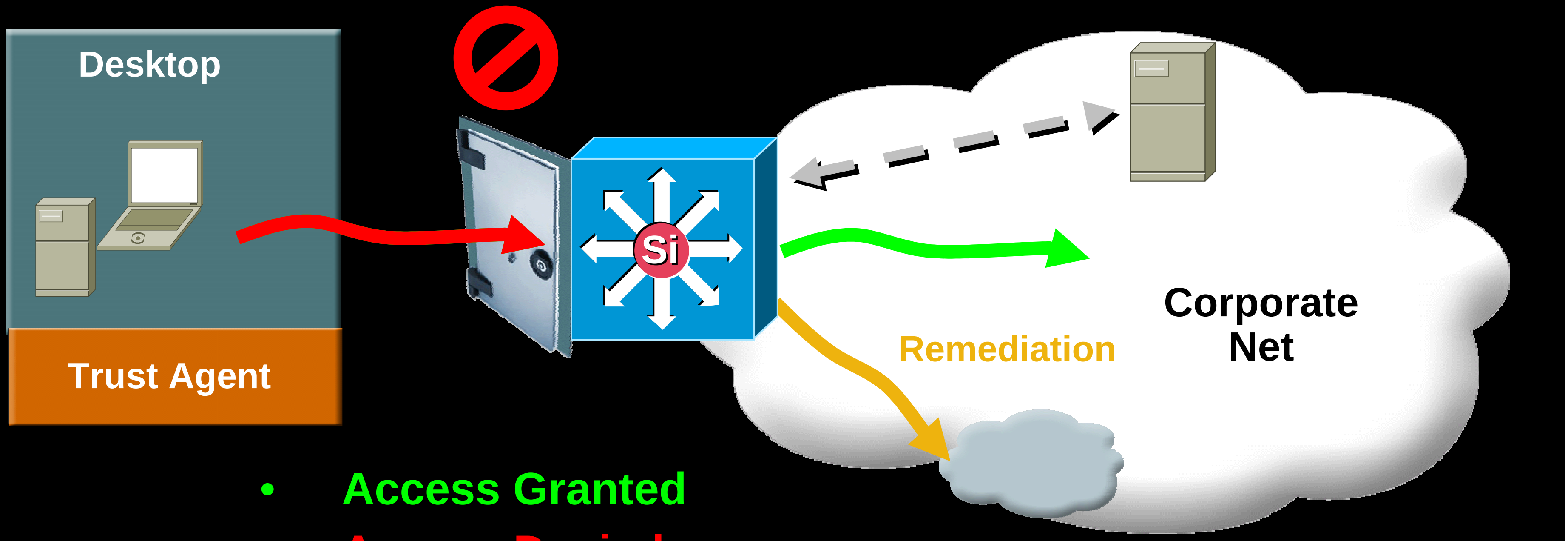
- Endpoint security solutions know security context and posture
- Policy servers know compliance and access rules
- Network infrastructure provides enforcement mechanisms

Network Admission Control

Validate security compliance and build trust

Client attempts connection

Authentication and policy check of client



Quarantine VLAN

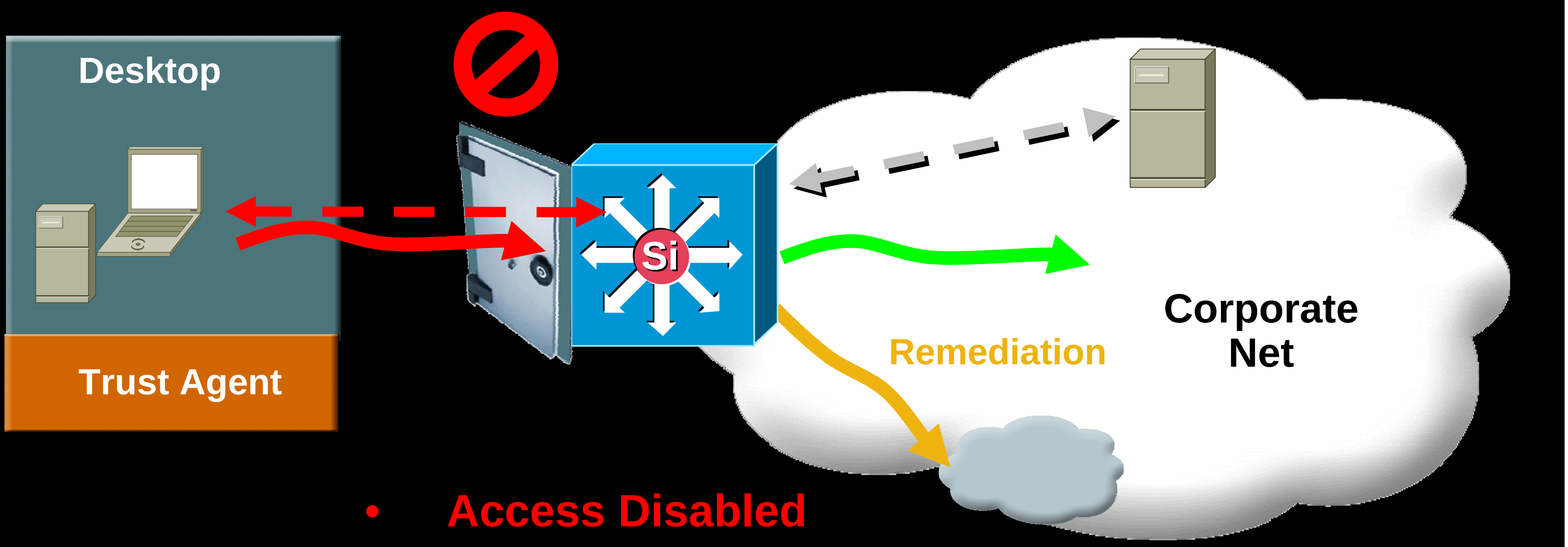
- Access Granted
- Access Denied
- Quarantine Remediation

Network Infection Containment

Maintain trust and respond to improper activity

Client actively Connected

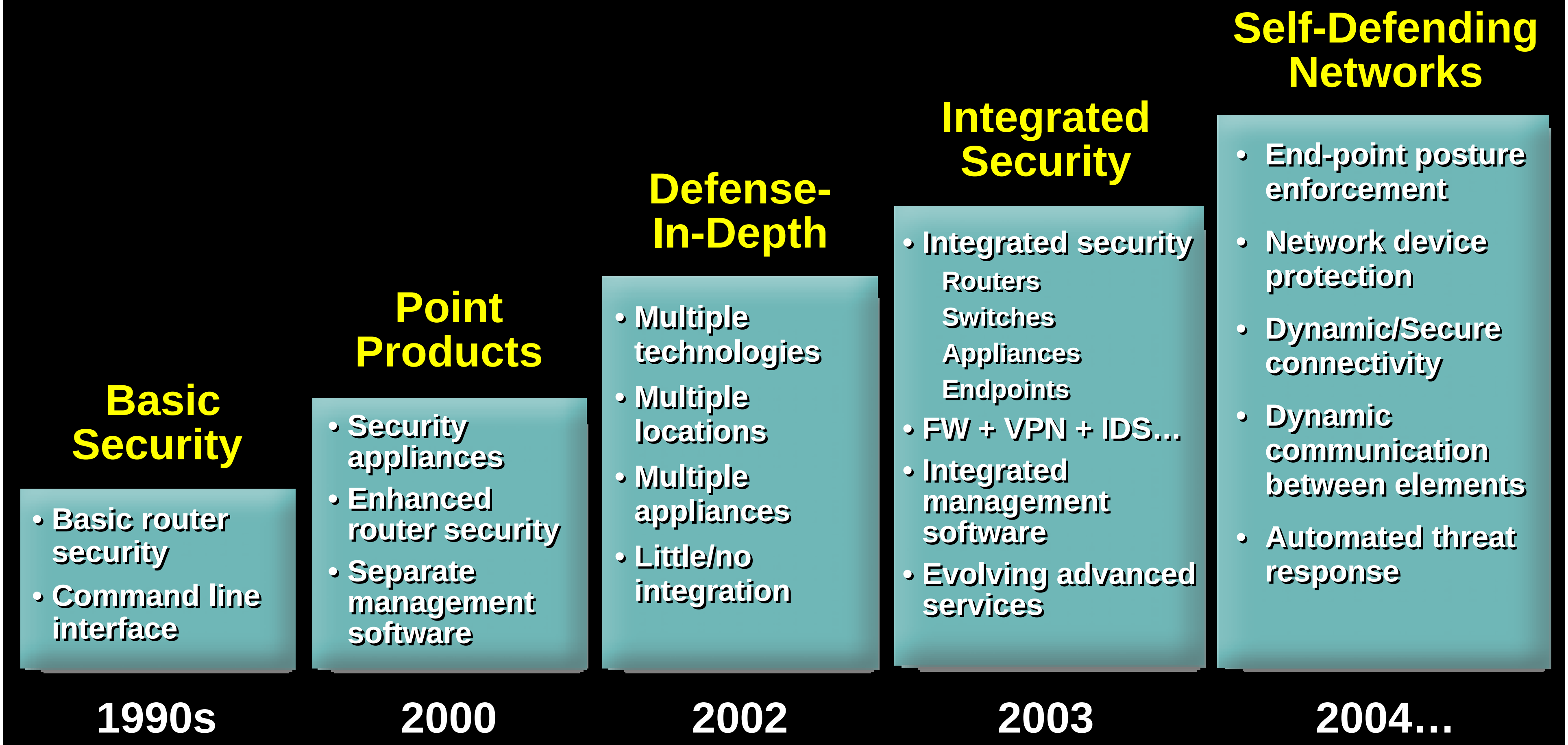
Client Indicates improper activity



- Access Disabled
- Quarantine Remediation

Evolution of the Cisco Security Strategy

Cisco.com



Basic Security

- Basic router security
- Command line interface

1990s

Point Products

- Security appliances
- Enhanced router security
- Separate management software

2000

Defense-In-Depth

- Multiple technologies
- Multiple locations
- Multiple appliances
- Little/no integration

2002

Integrated Security

- Integrated security
  - Routers
  - Switches
  - Appliances
  - Endpoints
- FW + VPN + IDS…
- Integrated management software
- Evolving advanced services

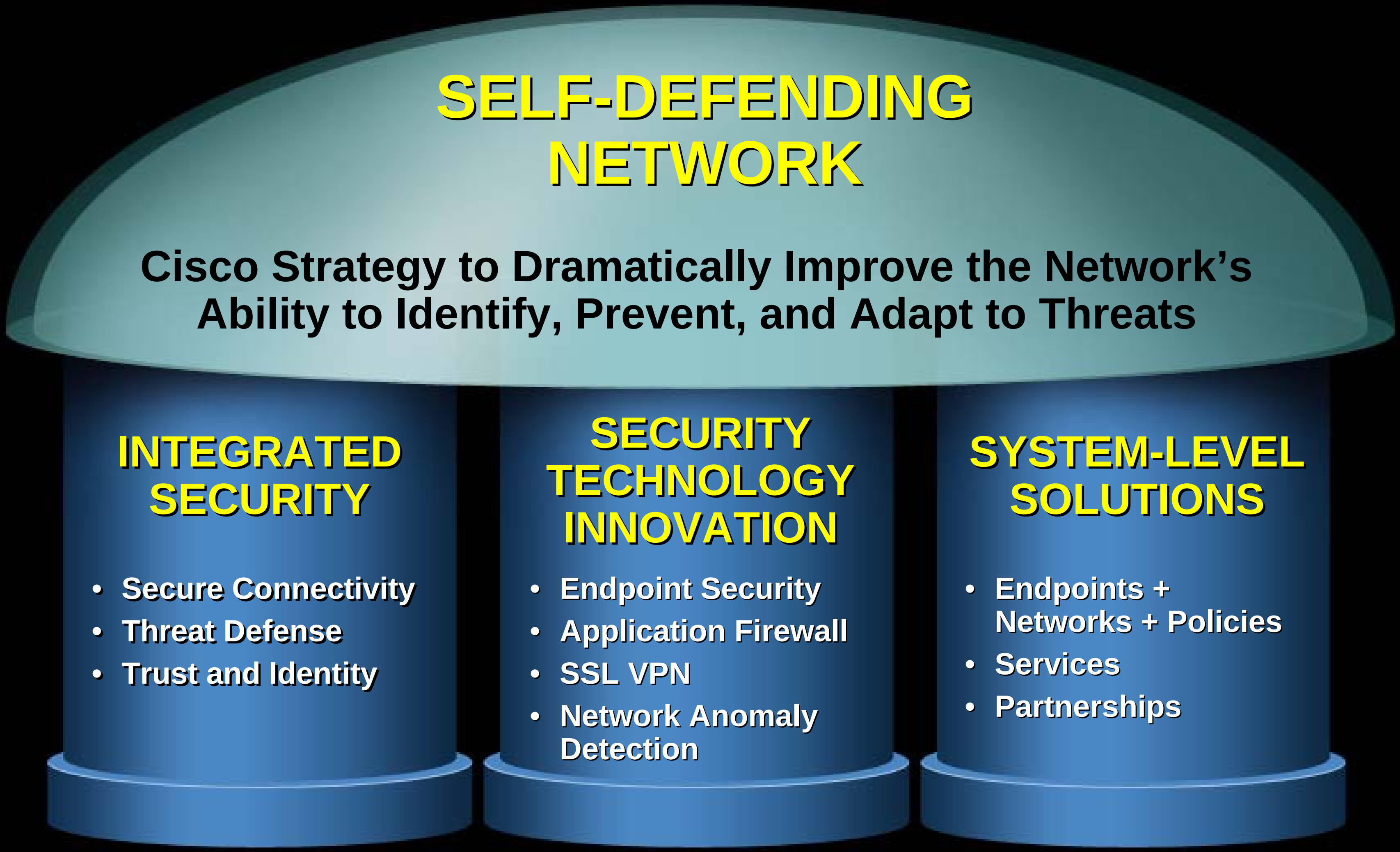
2003

Self-Defending Networks

- End-point posture enforcement
- Network device protection
- Dynamic/Secure connectivity
- Dynamic communication between elements
- Automated threat response

2004…

Self-Defending Network Strategy



SELF-DEFENDING NETWORK

Cisco Strategy to Dramatically Improve the Network's Ability to Identify, Prevent, and Adapt to Threats

INTEGRATED SECURITY

- Secure Connectivity
- Threat Defense
- Trust and Identity

SECURITY TECHNOLOGY INNOVATION

- Endpoint Security
- Application Firewall
- SSL VPN
- Network Anomaly Detection

SYSTEM-LEVEL SOLUTIONS

- Endpoints + Networks + Policies
- Services
- Partnerships

Three Essential Elements of Risk Reduction

Confidentiality

Ensuring that unauthorized parties cannot access critical corporate or customer information, data, or communications

Secure Connectivity

Integrity

Guaranteeing the identity of users, ensuring the integrity of their devices, and controlling access to user-appropriate data and resources

Trust and Identity

Availability

Protecting network resources to ensure maximum resiliency and availability to users, even during severe security events

Threat Defense

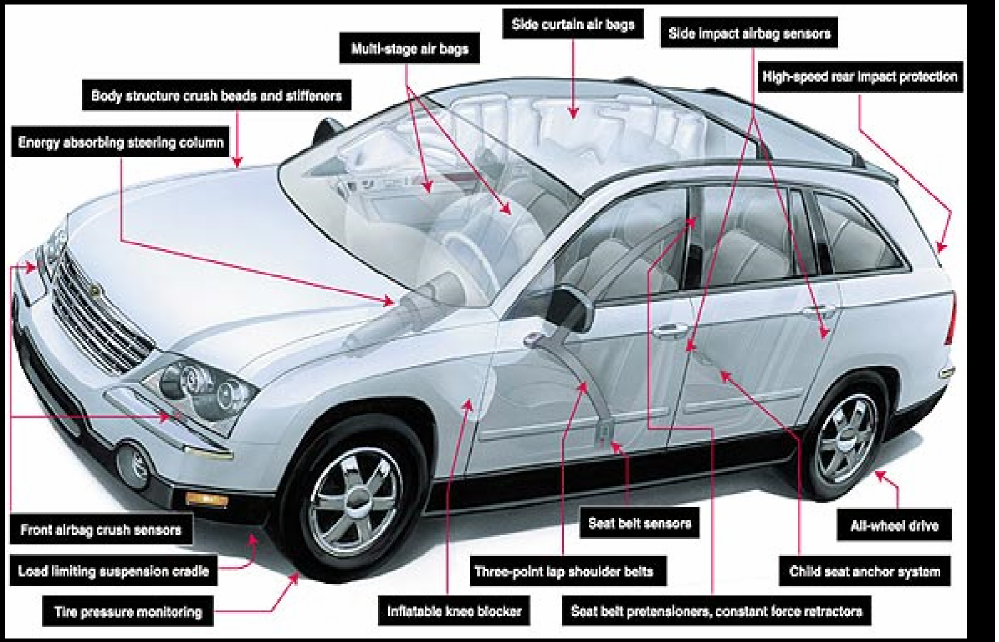
Three Essential Elements of the Self-Defending Network

SUMMARY

Summary

- The threats are evolving …and here to stay!
- Businesses and business practices are evolving… and taking security as a top priority!
- The network is part of the problem and the solution
- An integrated and holistic approach to information security, based on proven conceptual frameworks, and providing defense-in-depth is absolutely the best way to protect your organization
- Cisco can help you achieve this goal

Last Word: Security Is Not An Option !


Side curtain air bags
Side impact airbag sensors
Multi-stage air bags
High-speed rear impact protection
Body structure crush beads and stiffeners
Energy absorbing steering column
Front airbag crush sensors
Seat belt sensors
All-wheel drive
Load limiting suspension cradle
Three-point lap shoulder belts
Child seat anchor system
Tire pressure monitoring
Inflatable knee blocker
Seat belt pretensioners, constant force retractors

Security as a Option

- Security is an add-on
- Challenging integration
- Not cost effective
- Cannot focus on core priority

Security as part of a System

- Security is built-in
- Intelligent collaboration
- Appropriate security
- Direct focus on core priority

Q & A

CISCO SYSTEMS ®