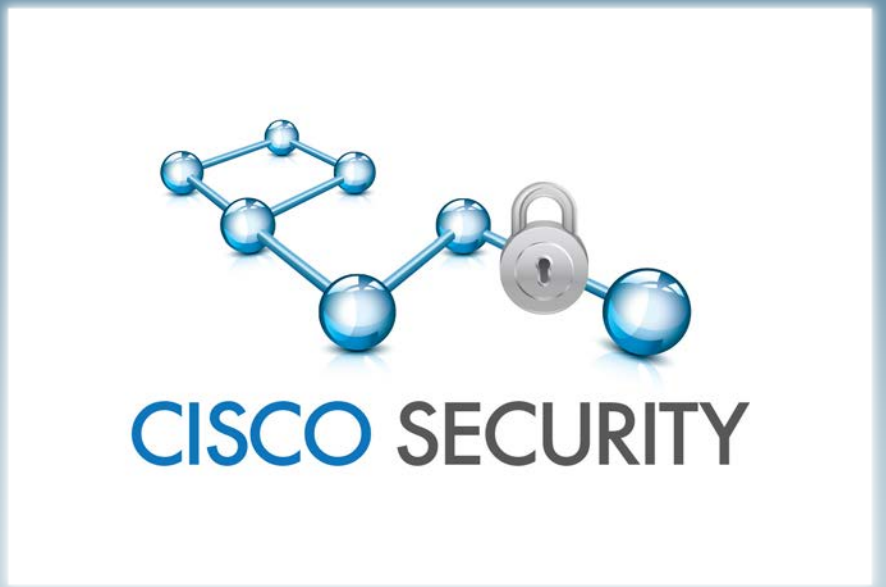
Cisco Security in Practice

Presenter: Socratis Tsiamezis
DC Manager Carta Worldwide Cyprus



Agenda

- What is security?
- Do these issues influence your business?
- Security best practices
- Deploy security as an integrated system
- Most common network security threats
- Pain caused by downtime
- When Cisco ISE comes to play
- Issues with personal devices @ work
- Cisco ISE 2.0

What is security?

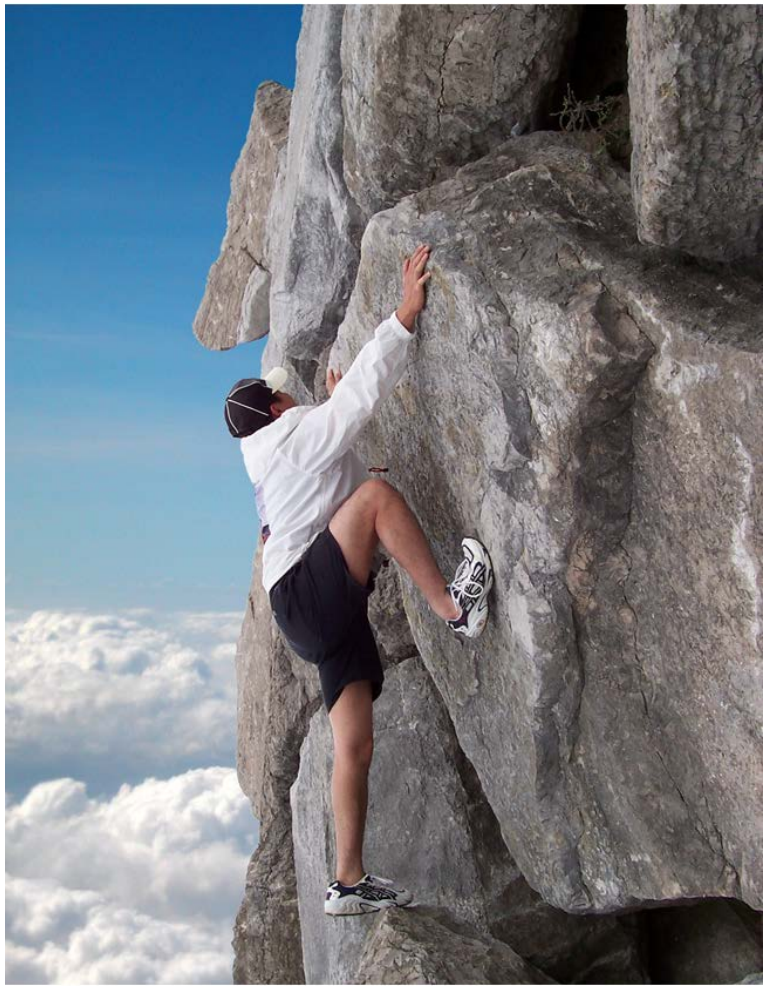
’ Security is a not a product, but a process.’
— Bruce Schneier

- You can’t just add it to a system after the fact. It’s vital to understand the real threats to a system, design a security policy appropriate to those threats, and build the necessary countermeasures.

- Imagine that your network is a living organism, then security is your immune system

Do these issues influence your business?

- Damage to the company image after a security breach
- Legal liabilities resulting from a breach
- Gaining back your customer's confidence
- Lost revenues resulting from a breach
- Loss of employee morale
- Fear of Theft or Fraud



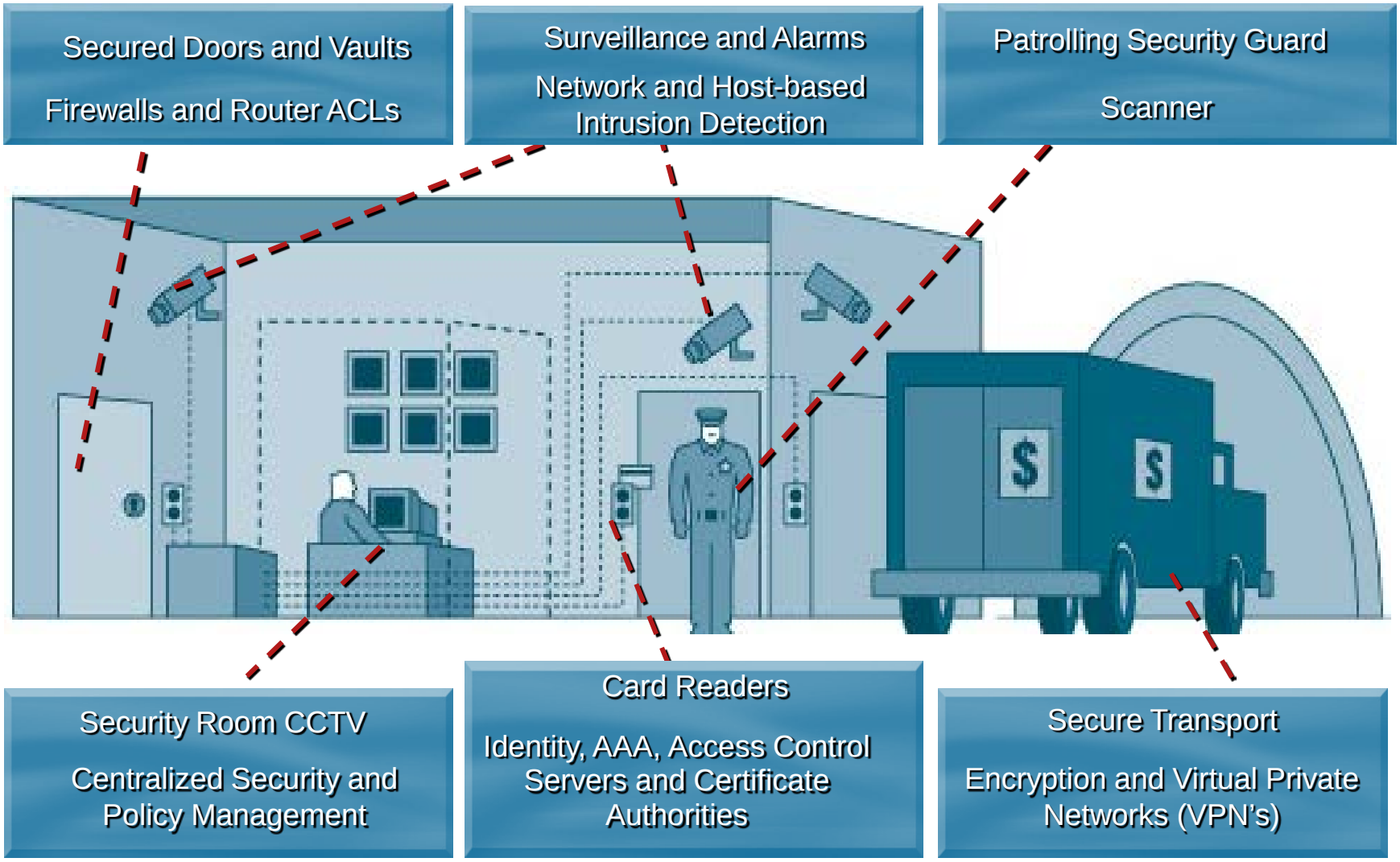
Security Best Practices

- A network administrator should have the following in his/her arsenal
  - ACLs – Allow or deny incoming and outgoing traffic based on predefined rules
  - IDS/IPS – Monitor network or system activities for any malicious activity
  - Centralized security and policy management – develop a structured approach to log analysis and incident tracking

Security Best Practices (cont.)

- AAA– Allow to verify identity of, grant access to, and track actions of users
- Internal and External Scanners – Run vulnerability scans on a monthly basis to identify issues
- Encryption / VPNs – Secure transfer of data in and out of the network
- Physical security – Monitor the physical premises via cameras, sensors, and access controls

Deploy security as an integrated system



Most common network security threats

- Everything is a target – including your printer
- Viruses, worms, and Trojan horses – a bit 90s but they still exist
- Spyware, adware, ransomware – for a quick profit
- Hacker attacks – like in the movies
- Denial of service attacks – its pretty bad
- Data theft – usually the admin's fault
- Identity theft – usually the user's fault
- Zero-day attacks – never see it coming

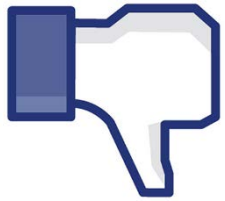
Pain caused by downtime

- The average cost of a data center downtime across industries was approximately $5,600 per minute. According to a study by the Ponemon Institute

$5600
downtime per minute
Ponemon INSTITUTE

Top 2 downtimes in 2015

Facebook - experienced 3 outages in 1 month. Aside from those who enjoy social media and the outages affected companies that depend on Facebook for their operation and products



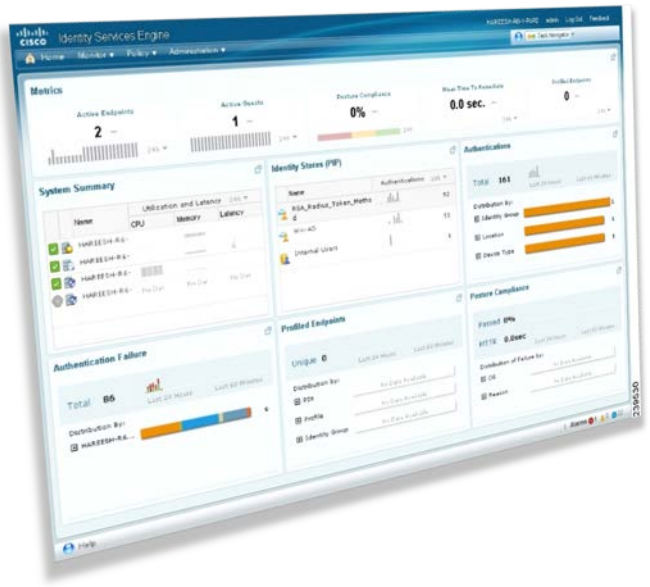
PayPal - one of PayPal's data centers shut down the payment service for just about two hours. (PayPal processes around 645 million dollars per day)

Cisco ISE Identity Service Engine 2.0

When Cisco ISE comes to play

- The enterprise network no longer sits within four secure walls. It extends to wherever employees and data travel
- Employees today demand access to work resources from more devices and through more non-enterprise networks than ever before.
- As your network expands, the complexity of arranging resources, managing different security solutions, and controlling risk grows as well.
- You need to identify mitigate and remediate security threats on devices accessing your network

Issues with personal devices @ work



- More than 1/2 of all Wi-Fi networks can be hacked
- Administrators cannot protect what they cant see
- 90% of organizations do not know who is accessing their network
- Usually personal devices do not have the latest patches and AV Signatures
- 60% of users will download sensitive data on a personal device

Cisco ISE 2.0

Features and Benefits

Cisco ISE 2.0 Manages and protects the mobile enterprise

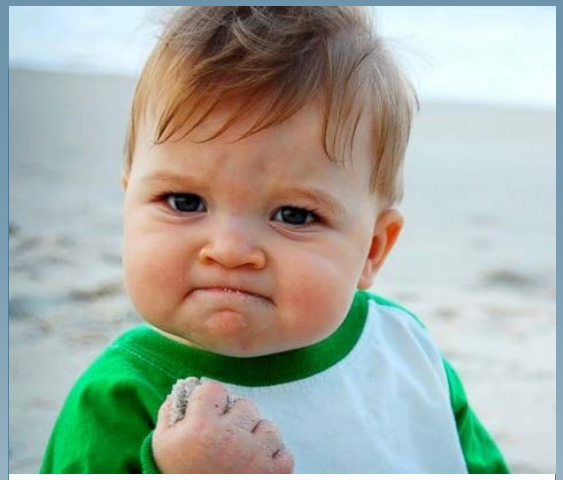
- Accurate identification of every user and device - Device profiling and posture with predefined templates
- Easy provisioning of all devices – Automatic supplicant provisioning and certificate enrollment for devices
- Centralized, context-aware policy management to control user access: whoever, wherever, and from whatever device – Highly secured wire, wireless or VPN
- Rich contextual data about connected users and devices to rapidly detect, mitigate, and remediate threats

Cisco ISE 2.0

All in one enterprise policy control

Cisco ISE 2.0

Release Goals and Objectives



Achievements

- Comprehensive secure access
- More productive workers and end users
- Lower operating costs

Integration

- AAA
- TACACS+
- AD Support
- Available as a physical or virtual appliance

Operation Efficiency

- Centralized management
- Works across Wired, Wireless and VPN
- Simplified Troubleshooting

cisco.com/go/ise