Changing face of endpoint security

SANTHOSH SRINIVASAN
CISSP, CISM, CRISC, CEH, CISA, GSLC, CGEIT

DIRECTOR – SHARED SERVICES, HCL TECHNOLOGIES

Changing face of end point security

- End points are now the perimeter of the network
- Pressure from business to support a wide variety of end points (smart phones, tablets, personal laptops)

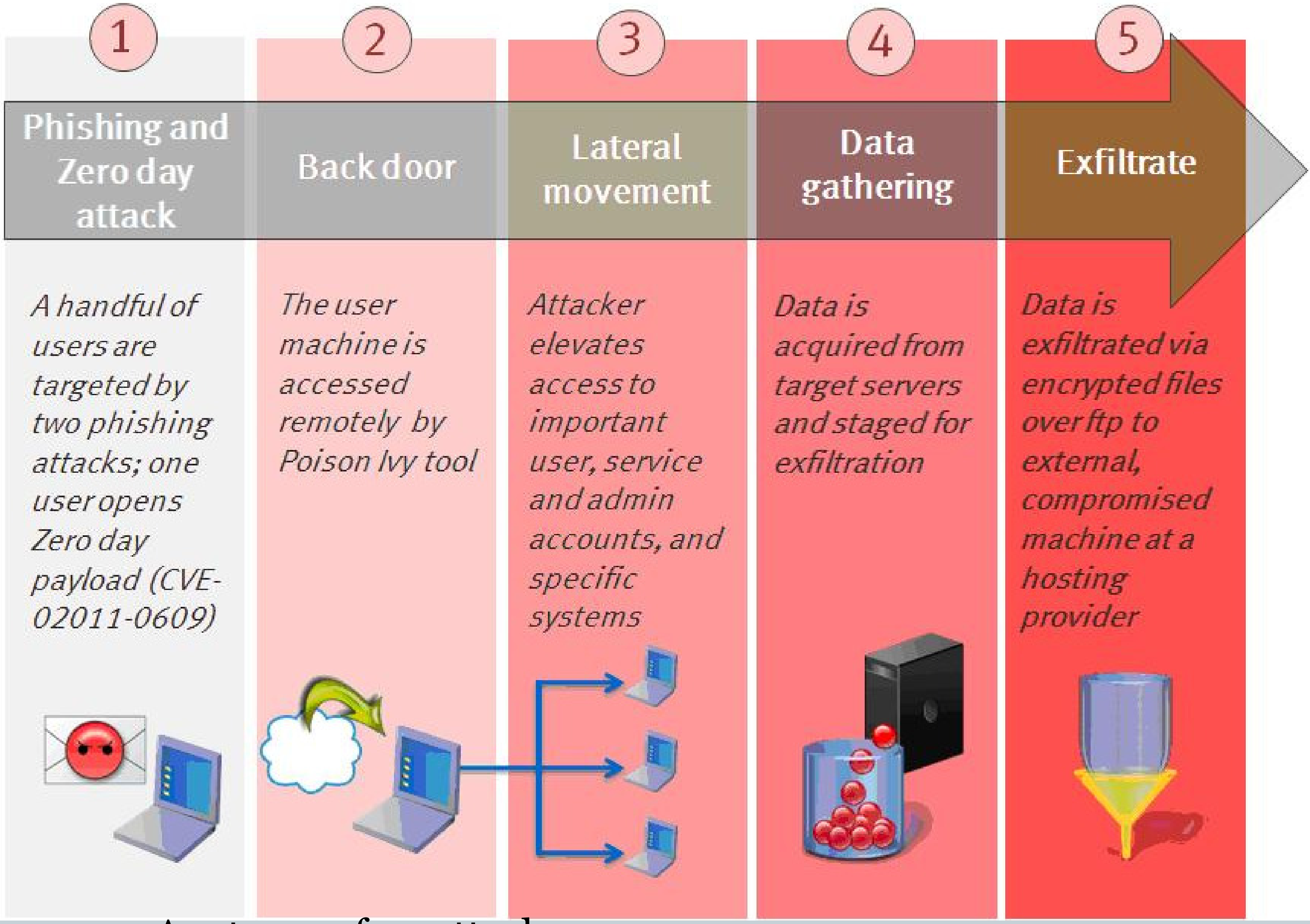
Current and emerging threats

- **The threat landscape.** What do the three biggest security incidents of 2010 – Aurora, Stuxnet, and WikiLeaks – have in common? All involved attacks on the endpoint (respectively: exploitation of a zero-day IE vulnerability, worm infiltration of a closed network through a USB, and data exfiltration via a USB).

Current and emerging threats

- Attack vectors are varied
  - Zero day attacks
  - Third party application vulnerabilities
  - Browser based attacks
- Malware and Advanced persistent threats
  - Highly targeted, constantly evolving, custom developed malware

Anatomy of an attack



1 Phishing and Zero day attack

A handful of users are targeted by two phishing attacks; one user opens Zero day payload (CVE-02011-0609)

2 Back door

The user machine is accessed remotely by Poison Ivy tool

3 Lateral movement

Attacker elevates access to important user, service and admin accounts, and specific systems

4 Data gathering

Data is acquired from target servers and staged for exfiltration

5 Exfiltrate

Data is exfiltrated via encrypted files over ftp to external, compromised machine at a hosting provider

Anatomy of an attack
http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Challenges

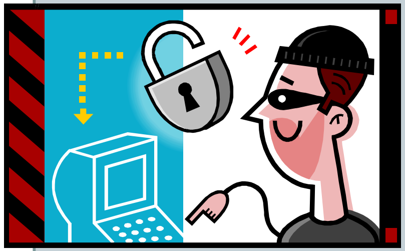
Corporate data on personal assets

Data protection on laptops and removable media

Remote wipe

Centralized policy management for diverse end points

Authentication & authorization strategy



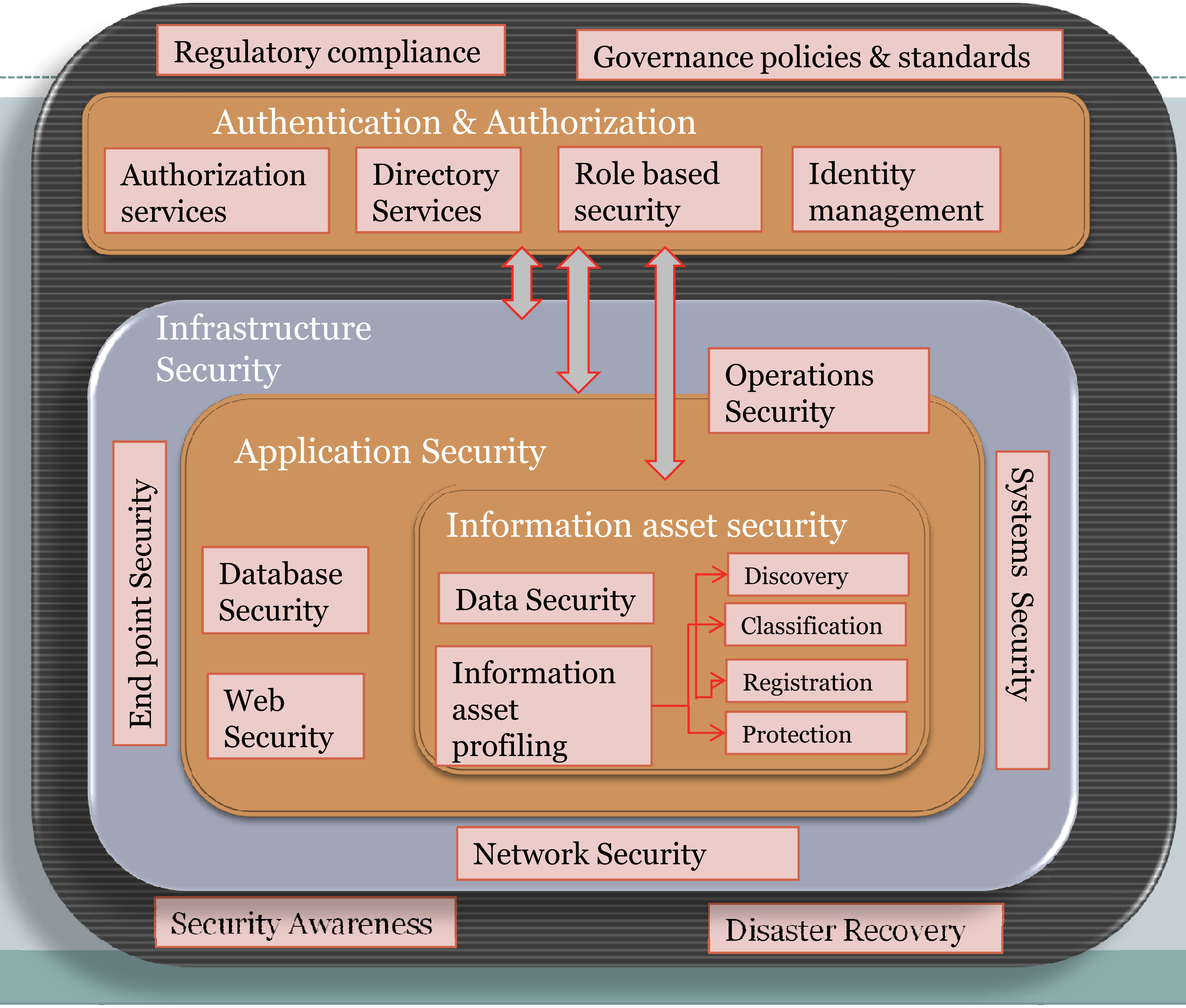
Intrusion prevention

Encryption in transit and at rest

Data leakage

Patch management for O/S and apps

Security framework



Regulatory compliance

Governance policies & standards

Authentication & Authorization

Authorization services

Directory Services

Role based security

Identity management

Infrastructure Security

Operations Security

Application Security

End point Security

Systems Security

Information asset security

Database Security

Web Security

Data Security

Information asset profiling

Discovery

Classification

Registration

Protection

Network Security

Security Awareness

Disaster Recovery

Good practices

- Have a well thought out information security strategy
  - Identify business risks
  - Map business risks to IT risks
  - Perform a risk assessment
  - Modify security policies to address IT & business risks
  - Develop short term and long term security strategies to address security policies
  - Define requirements for solutions to execute the strategy

Good practices

- Have a good corporate acceptable use policy
- Revise security policies related to
  - Social media
  - Usage of personal computing devices
    - Usage of removable drives (USB drives)
    - Smartphones & tablets
    - Bluetooth devices

End point security strategy

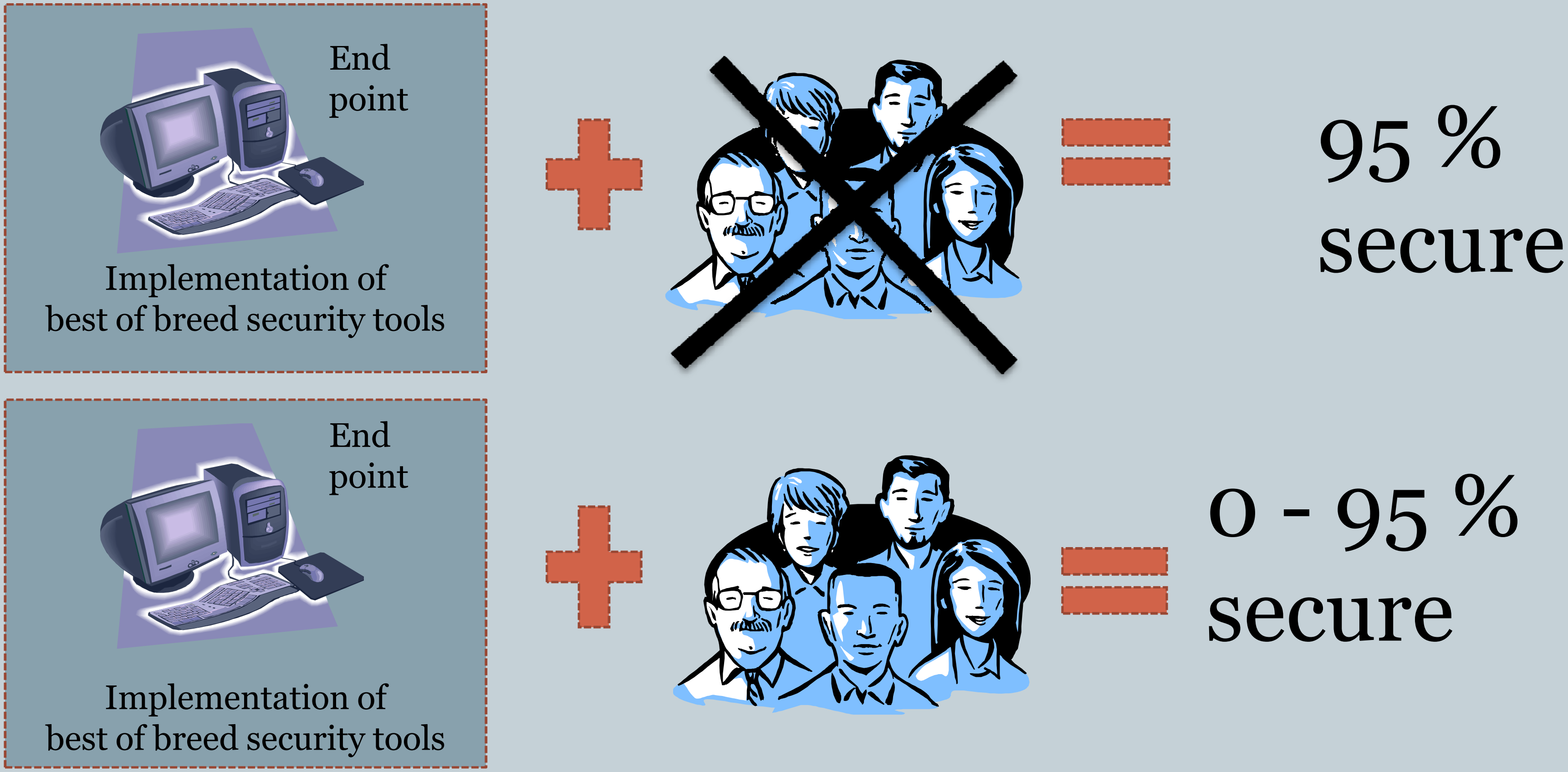
- Key aspects to a good strategy
  - Know your information
  - Create a baseline strategy for all end points
  - Have additional layers of security for end points having sensitive information

Know your information

Less than 5% of a company's information are the crown jewels for the company

- Identify Information assets across the corporation
- Classify the information based on business criticality, IP, business impact etc.
- Prioritize the information assets based on business classification and business impact.
- Have a layered strategy to protect this information

Security awareness



End point

Implementation of best of breed security tools

95 % secure

End point

Implementation of best of breed security tools

0 - 95 % secure

Desktop application vulnerabilities

- Reduce the application foot print on the desktops
- Develop process to patch these applications on a regular basis.

Develop a End Point security baseline

Policy enforcement will vary based on ownership of asset

Document security policies and baselines for different ownership scenarios

End Point Security strategy is going to vary based on ownership

Standard security baselines

Standard application delivery mechanisms

Standard patching processes

Standard OS platform (Windows 7)

Standard mobile platform (iOS, Android, RIM)

Centralized management and policy deployment

End point security baseline

- Automated patch management
- Enterprise managed firewall and HIPS
- Enterprise anti-malware
- Network Access control (health check, compliance check)
- Program control
- Device connection control and lockdown
- 802.1x authentication for wired and wireless
- Anti-spam
- SIEM solution

Other scenarios

- Usage of virtual desktops for third party contractors, external vendors
- Usage of a network firewall to segment partners
- Setting up sensitive users in a DMZ with restricted access control at the network layer

Assess current status vs. requirement

- Based on threat assessment and policy requirement identify components of end point security that are relevant to your environment

Functionality	Current status	Existing Products	Requirement
Client Antivirus	☑	McAfee	☑
Personal firewall	☑	Zonelabs	☑
Host IDS/IPS	□		☑
Anti-spyware	□		☑
Patch management (assessment/remediation)	☑	WSUS	☑
Endpoint vulnerability assessment	□		☑
Data Encryption (emails, desktop, servers)	□		☑
Device Control	□		☑
Program Control	□		☑
Endpoint policy management and policy enforcement	☑	Zonelabs console, EPO	☑
Compliance assessment and host checking	□		☑
802.1x authentication	□		☑
Data leakage prevention (end points)	□		□

What are your core principles for product selection

- Single console to manage all these products
- Ease of deployment of agents
- Reduced agent foot print on end points
- Centralized policy management and enforcement
- Centralized compliance reporting

Next steps

- Map vendors against your requirements
- Analyze vendors against your core principles
- Develop test plans for POC
- Conduct a POC with the vendors who have met your requirements
- Talk to existing customers of the selected vendors
- Review POC outcomes
- Review pricing
- Select the product

Summary

- Having the best of breed products does not solve the problem
- The overall security architecture needs to be looked in totality
- Soft measures (policy, user awareness) need to be implemented in addition to technical solutions
- Understanding business needs will help in gaining more acceptance

Questions