





INFORMATION SECURITY DECISIONS

Hosted by  

# Essentials of Endpoint Security



## Review and Best Practices

---

---

---

---

---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

# The road we travel:

1. The Problem
2. Client and Clientless Technologies
3. Policies that can / should be enforced
4. Remediate Non-compliant endpoints
5. Current and Emerging Technologies
6. Selection Criteria
7. Deployment Priorities

---

---

---

---

---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  

# What's at stake?



# BILLIONS

---

---

---

---

---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

## The "WHY"



**Infection in Chicago**

**Spreads to your office in Dublin**




---

---

---

---


---

---

---



---

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

## Client and clientless technologies

- **Client based**
  - Most common
  - Software must be loaded on the endpoint
  - With and without integrated personal firewalls
  - Multiple endpoint operating systems supported
- **Clientless**
  - Newer technology
  - No software required on the endpoint
  - Currently only one vendor
  - Windows support only currently – more on the way
  - "Guest" feature


---

---

---

---


---

---

---



---

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

## Policies

- Personal firewalls with correct configurations
- Anti-Virus with current DATs
- Security patches
- Correct browser settings
- Custom software configurations
- Policies can check:
  - Registry settings
  - Executable version, date/time and MD5 hash
  - File interdependencies


---

---

---

---



---

---

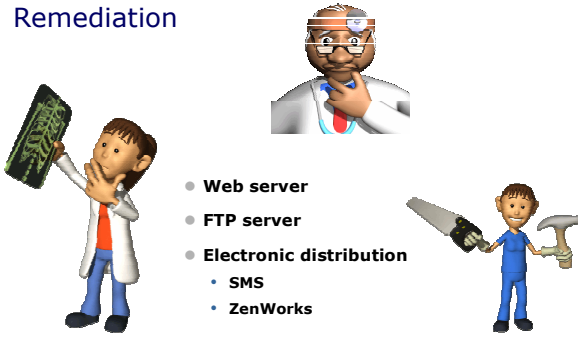
---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Remediation



- Web server
- FTP server
- Electronic distribution
  - SMS
  - ZenWorks

---

---

---

---



---

---


---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Current and emerging technologies



- DHCP server integration
- Switch and router integration
- Clientless technology improvements

---

---

---

---



---

---

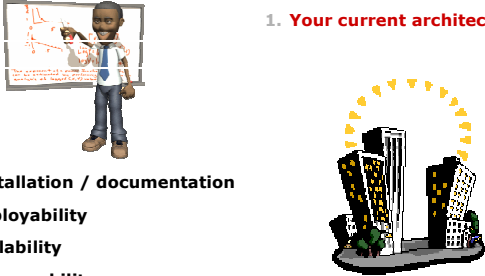
---

---

INFORMATION SECURITY DECISIONS

Hosted by  

## Selection criteria



1. **Your current architecture**
1. Installation / documentation
2. Deployability
3. Scalability
4. Manageability
5. Reporting

---

---

---

---


---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

### Feature sets:

Agent/firewall			X	X		X
Agent-less	X					
Host OS						
Windows			X	X	X	X
Linux	X	X				
Client OS(es)						
Windows	X	X	X	X	X	X
Linux		X				
MAC		X	X			
Unix		X				
PocketPC		X				
Other		X				
Failover	X	X	X	X		
LDAP	X	X	X	X		X
802.1x	X	X	X	X	X	X

---

---

---

---

---

---


---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

### How they stacked up:

	Installation	Deployability	Manageability	Reporting	Compliance	Security	Summary
Stillsecure	A	C+	B	D+	B	C	B- Most promising architecture
Zone Labs	B+	C+	B+	A-	B+	A	B+ Solid, mature performance
Sygate	A-	C+	B	A	B+	C	B- Most mature product
Endforce	C	C	C-	D+	B	D+	C- Least mature, but flexible
Senforce	C+	C+	C	C+	B	C	C+ Average when compared to others
Infoexpress	B-	B+	C+	C	A-	A	B- Most impressive operationally

---

---

---

---

---

---


---

---

---

---

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

### Deployment priorities

- Remote access
  - Discreet component of your network
  - Easily defined
- Central (Data) location
- Enterprise

---

---

---

---

---

---

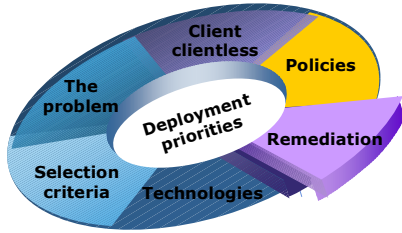
---

---

---

---

## Summary



---

---

---

---

---

---

---

---