Securing OS Legacy Systems

Alexander Rau
National Information Security Strategist
Sample Agenda

1. Today’s IT Challenges
2. Popular OS End of Support & Challenges for IT
3. How to protect Legacy OS systems
4. Q&A
Today’s IT Challenges
What poses the greatest security risk to servers?
Servers are the Target: “Endpoints simply provide an initial foothold”

Variety of compromised assets across 47,000+ security incidents

Verizon 2013 Data Breach Investigations Report: “When you consider the methods used by attackers to gain a foothold in organizations – Brute Force, stolen creds, phishing, tampering – It’s really not all that surprising that none receive the high difficulty rating...”
Compromising Servers

Most breaches are caused by:

- Unpatched systems
  - Operating systems
  - Applications
- Careless mistakes
- System configuration
- Zero day vulnerabilities
- Targeted malware
- Malicious employees
- Stolen credentials
- Untrusted applications
Popular OS End of Support & Challenges for IT
Legacy Operating Systems

– Microsoft Windows 2000 Server
  – Mainstream support ended on June 30, 2005
  – Extended support ended on July 13, 2010

– Microsoft Windows XP
  – Mainstream support ended on April 14, 2009
  – Extended support ended on April 8, 2014

– Microsoft Windows Server 2003
  – Mainstream support ended on July 13, 2010
  – Extended support until July 14, 2015
Challenges

• Time (too many servers) and cost (licenses, time & resources) to upgrade

• Business Critical Legacy Applications that run on EOL OS and are too costly to port over or are no longer supported themselves
End of Support does not equal unsecure

• The EOL OS might no longer be in compliance with Security Policies or Compliance Frameworks (ie. PCI, ISO 27002, COBIT, ...)
  – Usually servers should be patched in accordance with a patch policy ie. critical/ASAP, High/30 days, Medium/60 days and low/90 days

• PCI is throwing a life line of compensating controls which could also be applied to other frameworks
  – Compensating control definition:
    "Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:
    1) Meet the intent and rigor of the original stated PCI DSS requirement;
    2) Provide a similar level of defense as the original PCI DSS requirement;
    3) Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
    4) Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement."
How to protect Legacy OS systems
What do Hackers Target on Systems?

Legacy OS protection

- Enforce Registry Integrity
- Enforce File Integrity
- Enforce device controls
- Enforce application activity
- Enforce Memory Protection
- Enforce network controls
Legacy OS protection

Behavior Control
- Monitor, consolidate, and forward logs for storing and reporting
- Monitor file integrity in real-time
- Alert/notify for early response
- Lockdown config. settings
- Enforce security policy
- De-escalate privileges
- Restrict device access
- Restrict traffic flow
- Whitelisting
- Prevent zero-day attacks
- Restrict OS behavior
- Buffer overflow protection
- Exploit Prevention

System Controls
- Close back doors
- Limit connectivity by application
- Restrict traffic flow
- vSphere Protection
- Lockdown config. settings
- Enforce security policy
- De-escalate privileges
- Restrict device access

Network Protection
- vSphere Protection
- Close back doors
- Limit connectivity by application
- Restrict traffic flow

Auditing & Alerting
- Monitor, consolidate, and forward logs for storing and reporting
- Monitor file integrity in real-time
- Alert/notify for early response
- Whitelisting
- Prevent zero-day attacks
- Restrict OS behavior
- Buffer overflow protection
- Exploit Prevention

Intrusion Detection (IDS)
- Lockdown config. settings
- Enforce security policy
- De-escalate privileges
- Restrict device access
- Whitelisting
- Prevent zero-day attacks
- Restrict OS behavior
- Buffer overflow protection
- Exploit Prevention

(Agent-less) Antimalware (AV)
Legacy OS protection

**FEATURES**
- Policy based protection
- System lock down
- Application Whitelisting
- Privilege de-escalation
- Exploit/malware prevention
- Remediation automation
- Compliance enforcement
- Real-time file integrity monitoring
- User Monitoring
- Broad OS and platform coverage
- Agentless AV Protection*

**VALUE**
- Complete protection across physical and virtual servers
- High performance and reduced downtime
- Lower cost management and administration

Detection + Prevention + (Agentless) Antimalware Protection
new Protection Strategy Workflow

- **Application-centric Security Model** - Simplify server hardening by introducing an intuitive policy wizard and protection strategy, transitioning from a policy-by-technology approach.

- **Protected Application White Listing** - Enhance traditional white listing or strict default-deny controls by providing pre-built application profiles and additional OS level protections.

- **Sandboxing and Process Access Control** - Apply additional controls over running processes to protect against new classes of threats. Out-of-box policies are available for Web, Email, Database, and Domain Controller servers.
Granular Approach vs. holistic approach

Detection
- Behavior Control
- System Controls
- Network Protection

Prevention
- Auditing & Alerting

White Listing / Application Control
- (Agent)less Antimalware (AV)
- File Integrity Monitoring

Agentless

VALUE
- Complete protection across physical and virtual servers
- High performance and reduced downtime
- Lower cost management and administration
Q&A
Thank you!

Alexander Rau
Alexander_Rau@symantec.com