Ritz Camera Leverages Whitelisting for Picture Perfect Security
About Ritz Camera ...

- Nation’s Largest Retail Camera and Photo Chain
- +3,000 Stores with Kiosks, POS and Servers
- PCI Data Security Standard - Level 1 Merchant
PCI Data Security Standard Requirements

**Build and Maintain a Secure Network**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

**Regularly Monitor and Test Networks**
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

**Maintain an Information Security Policy**
Requirement 12: Maintain a policy that addresses information security
Challenges

• Antivirus Signature Deployment
  – Signature File Size
  – Disconnected and Low Bandwidth Stores

• Applications that require administrative rights
  – Store Clerks with Admin Rights
  – No control over USB ports

• PCI compliance
  – Unable to Demonstrate Consistent Protection
The Bottom Line at Ritz

Brand At Risk
New threats continually outsmart existing defenses

Polluted Systems
Computers polluted with illegal and unauthorized software

Excessive Support Calls
Disruptive software causing downtime and performance degradation
The Gap in Control

Managed Software

- Known Malware
- Patches
- Centrally Distributed Applications
- Provisioned Base Image

Managed Malware

Unmanaged Software:
- Invisible
- Untraceable
- Uncontrollable
- Unpatched
- Vulnerable

Unknown Malware
- Spyware
- Rootkits
- Unlicensed
- Games
- Instant Messenger
- Botnets
- Skype
Trying to Close The Gap

Mainstream approaches unsuccessful...

- Antivirus: Ineffective against new threats; bloating signature files
- Remove Admin Rights: IT always has to get involved; app requires admin rights
- Restriction Policies: Very difficult to manage; static controls
Security at an Inflection Point

- Time
- Complexity of Administration
- Whitelisting
- Software Identification
- Flexible User Policies
- Automated Software Approval
- Blacklisting
- Targeted Attacks
- Risk Tolerance
- Explosion of Malware
- Signature File Size
What is Whitelisting?

**Application Whitelisting**

Define trusted software and allow it to run;
Block all other software

**Device Whitelisting**

Define trusted devices and allow usage;
Block all other devices
How Do You Define Trust?

• Application Attributes
  – Cryptographic Hash
  – Source
  – Publisher

• Device Attributes
  – Vendor
  – Model
So What Approach Did Ritz Take?

- **Base Image**
  - Define a Whitelist of Trusted Software
  - Define “Ritz” as a Trusted Publisher
  - Remove Antivirus

- **Updates**
  - Digitally Sign Custom Code
  - Store Staff Maintain Admin Rights
  - Authorize Specific USB Drives
"Bit9 would not be considered a compensating control; it would be the control."
The Final Result …

Security
- No more malware
- Eliminate problems caused by antivirus bloating

Compliance
- No more unauthorized applications
- Audit every file copied to/from portable storage

Maintainability
- More reliable systems
- Extend the life of systems with limited capacity
Ritz Camera:  
Application Whitelisting to achieve PCI Compliance

Harvard Business Review:  
Boss, I Think Someone Stole Our Customer Data

Microsoft MVP:  
Running a Fully Controlled Windows Desktop Environment