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

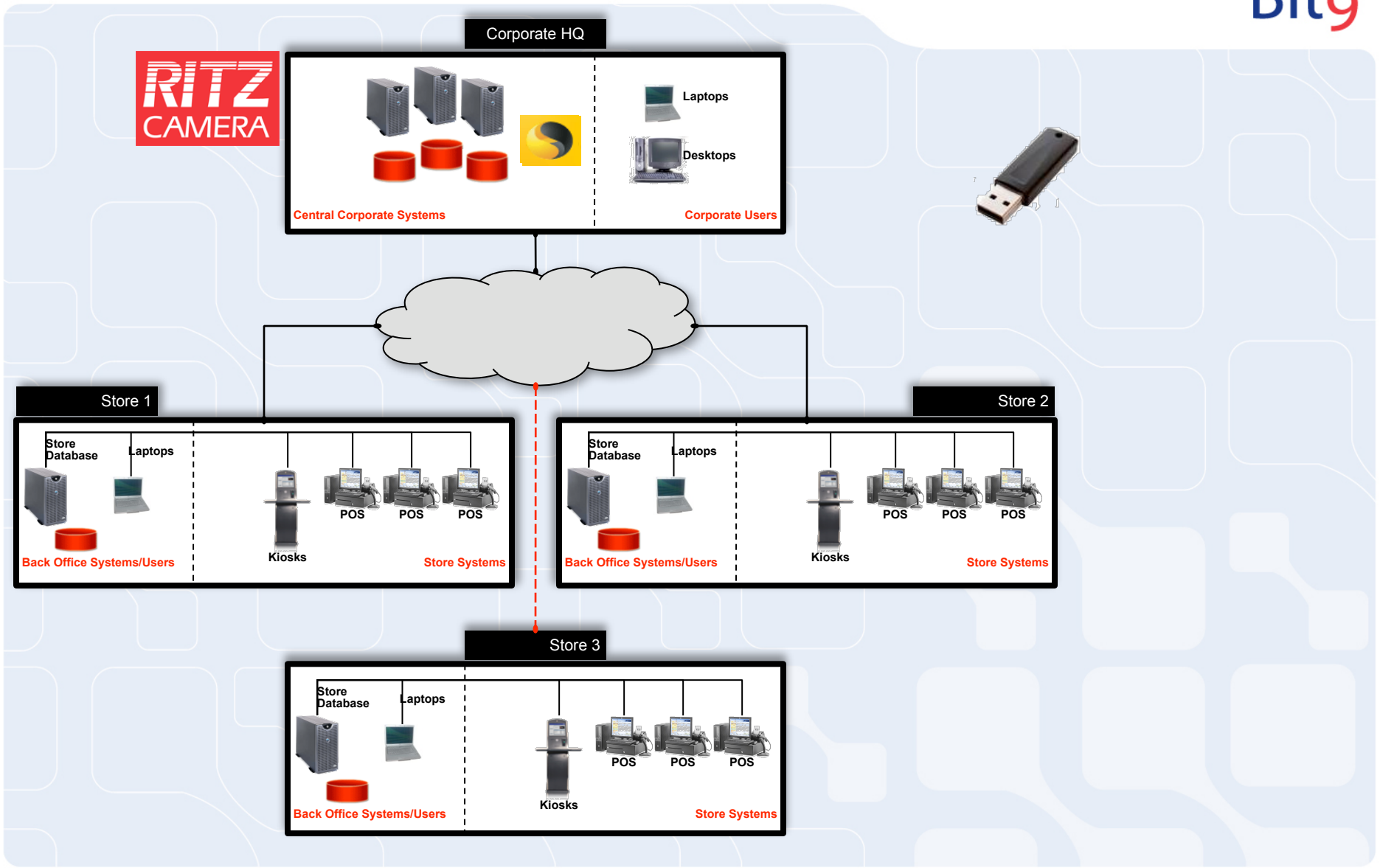
Regularly Monitor and Test Networks

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

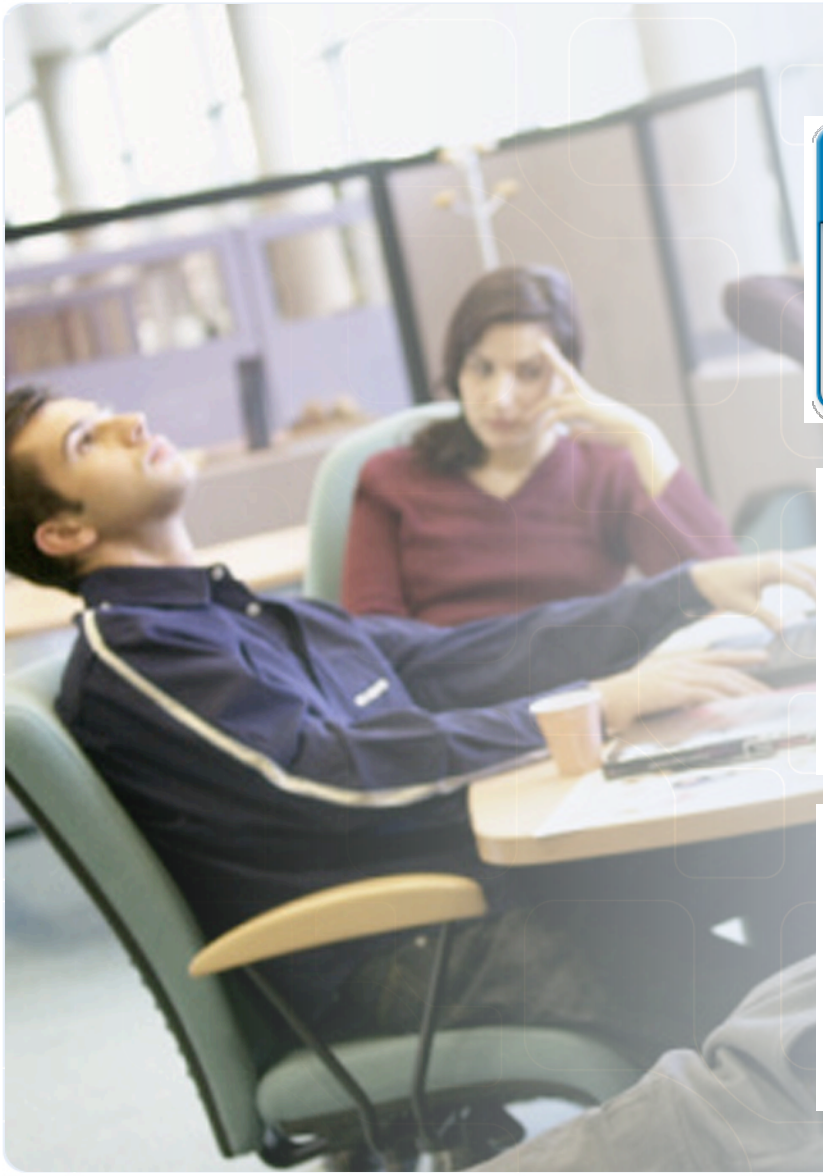
Store Systems Architecture



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

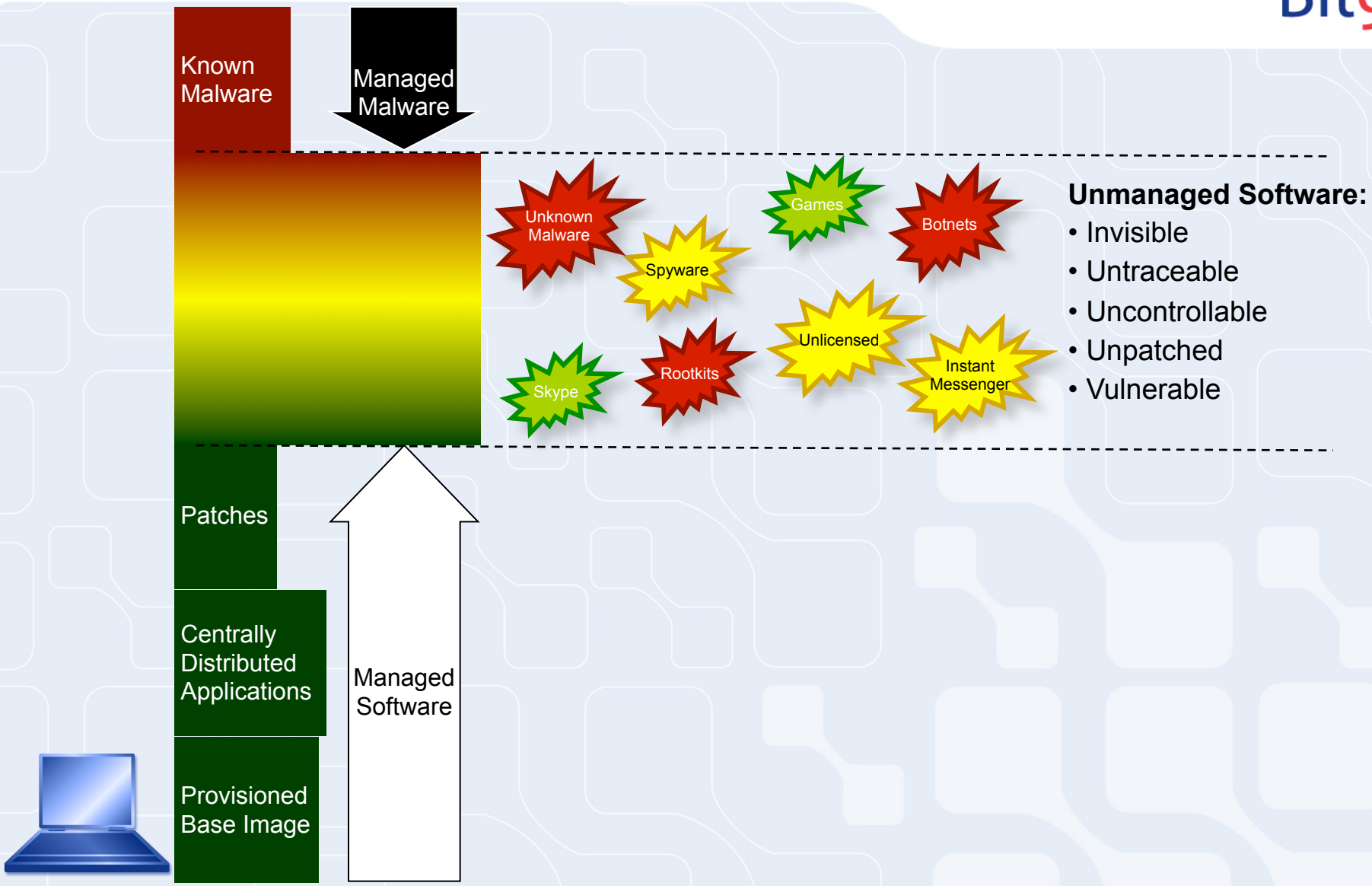
Polluted Systems

Computers polluted with illegal and unauthorized software

Excessive Support Calls

Disruptive software causing down time and performance degradation

The Gap in Control

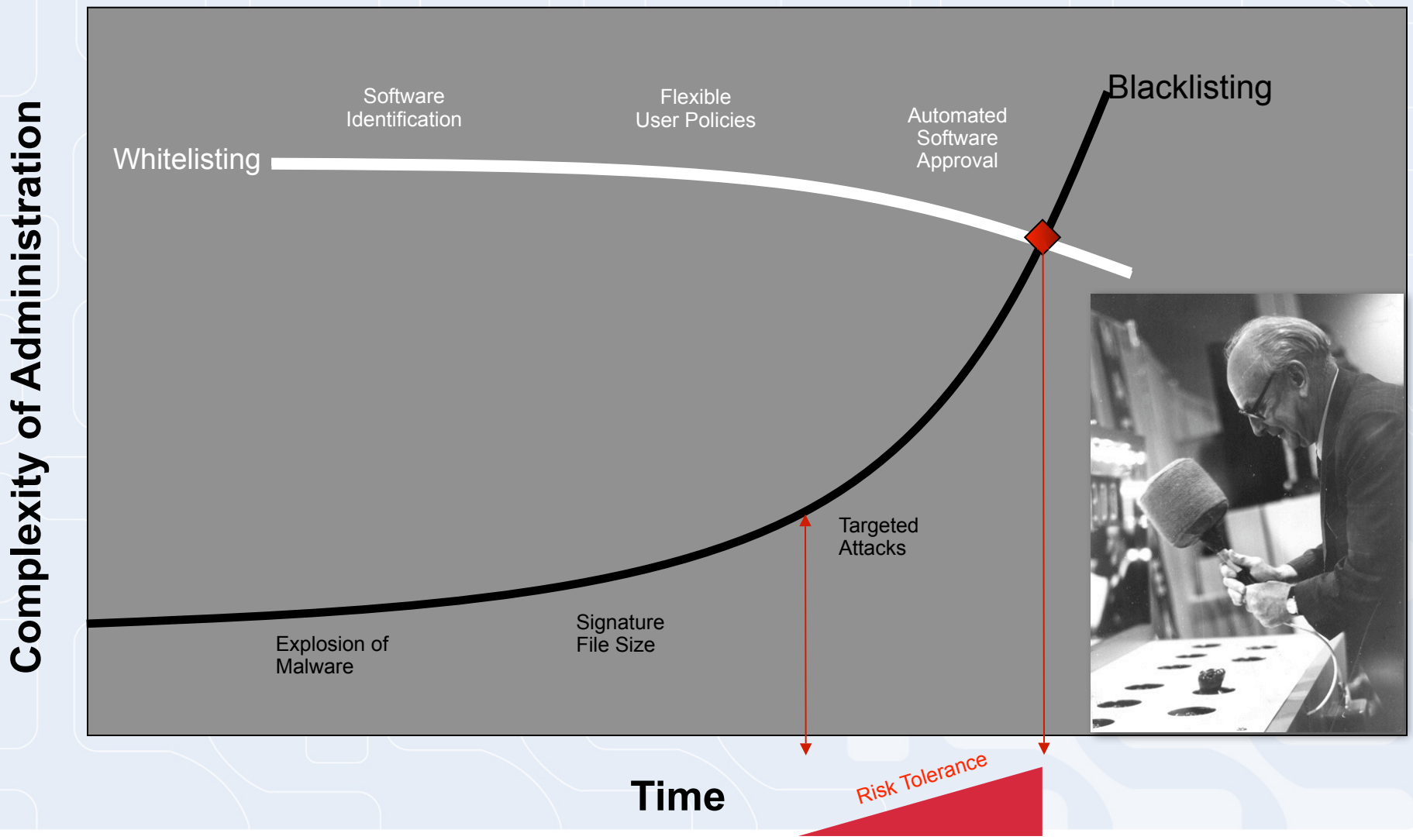


Trying to Close The Gap

Mainstream approaches unsuccessful …

- Ineffective against new threats; bloating signature files
- IT always has to get involved; app requires admin rights
- Very difficult to manage; static controls

Security at an Inflection Point



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

Replacing Antivirus at Ritz Camera

Gartner

Gartner's Most Innovative Software Solution at the Gartner IT Security Summit …
June 4, 2008

PCI Security Standards Council™

VeriSign

"Bit9 would not be considered a compensating control;
it would be the control."

APPLICATION CONTROL AND DEVICE CONTROL FOR WINDOWS DESKTOPS

CASESTUDY

Bit9

Ritz Camera Centers Sees Picture-Perfect Security with Bit9 Application Control and Device Control Solutions

RITZ CAMERA

Configuration Control of Retail Machines

Before installing Bit9, 100% of Ritz Camera Centers' 5,159 retail store systems required local administrative privileges because of their digital imaging applications. This created a continuous challenge for Ritz to maintain control and compliance of software installations on these machines, which were exposed to unauthorized/malicious software installation and data leakage —as well as user-installed software.

The Internet, public Wi-Fi and USB storage devices give users easy access to popular applications for communication, analysis, searching, and more. However, unlike business software packages that are centrally deployed and managed, user-installed applications remain largely invisible to the IT organization. Frequently, they are the culprit behind a variety of desktop support, security, and compliance problems.

"The software being installed included everything from free utilities and toolbars to personally purchased software such as Adobe Photoshop and games," said Bob O'Hern, Vice President, Information Systems, Ritz Camera Centers, Inc. "Along with this software came frequent instances of spyware and malware that were equally disruptive.

All of this led to a significant number of machines degrading in performance or becoming unstable, requiring hours of the helpdesk's time to resolve. Many machines actually had to be re-imaged in order to return them back to a stable, productive state.

Key Benefits to Ritz

- Establish "lockdown" controls on store systems
- Preserve Ritz Camera Centers' brand name
- Enforce software license and PCI compliance
- Remove anti-virus software on store systems
- Eliminate security vulnerabilities
- Dramatically reduce IT support costs

"By locking down kiosks and servers with Bit9 Parity, Ritz is able to protect its brand name while enforcing compliance and eliminating risk of security vulnerabilities."

—Bob O'Hern, Vice President, Information Systems, Ritz Camera Centers, Inc.

Locking Down Store Systems

Faced with these problems, organizations like Ritz seek to eliminate the problem altogether by locking down their employees' desktops through Windows User Account controls. Unfortunately, this solution is only a partial one. Plagued by complex administration and customer satisfaction issues, IT organizations are looking beyond Windows User Account policies for a more powerful way to manage their desktops.

Ritz sought a better way to control the configuration and security of their in-store systems while maintaining PCI compliance and reducing risks.

Thus Ritz turned to Bit9's application and device control solution to lock down each and every one of its retail store systems to protect them from malware and data leakage. Retailers who control the configuration of their in-store systems, such as Ritz, can vastly improve their information security and more easily adhere to compliance regulations.

"Ritz is committed to securing its in-store systems and Bit9 is enabling us to achieve our goals," O'Hern continued. "By locking down kiosks and servers with Bit9 Parity, Ritz is able to protect its brand name while enforcing compliance and eliminating risk of security vulnerabilities."

Continued

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

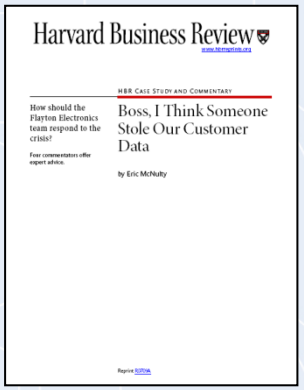
Maintainability

- More reliable systems
- Extend the life of systems with limited capacity

bit9.com/resources

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