



5 Steps to Advanced Threat Protection



Agenda

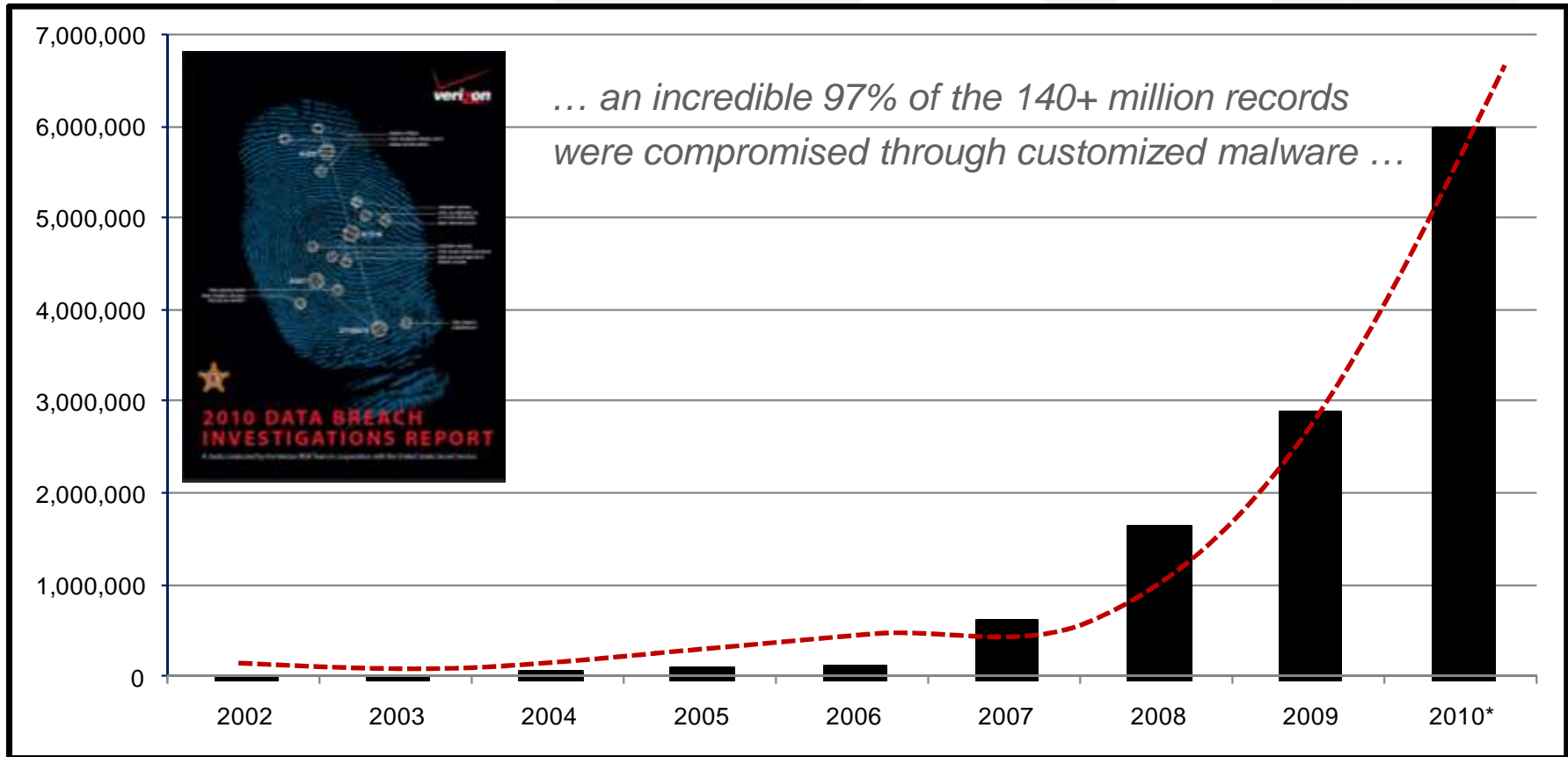
- Endpoint Protection Gap
- Profile of Advanced Threats
- Consensus Audit Guidelines
- 5 Steps to Advanced Threat Protection
- Resources

20 Years of Chasing Malicious Software

- Tries to keep a list of all bad software
- Tries to identify bad behavior
- Lets unrecognized executables run
- The moles have gotten faster and smarter



Exponential Growth In Malware



Trying to Keeping Pace

2,895,802 signatures / year

7,933 signatures / day

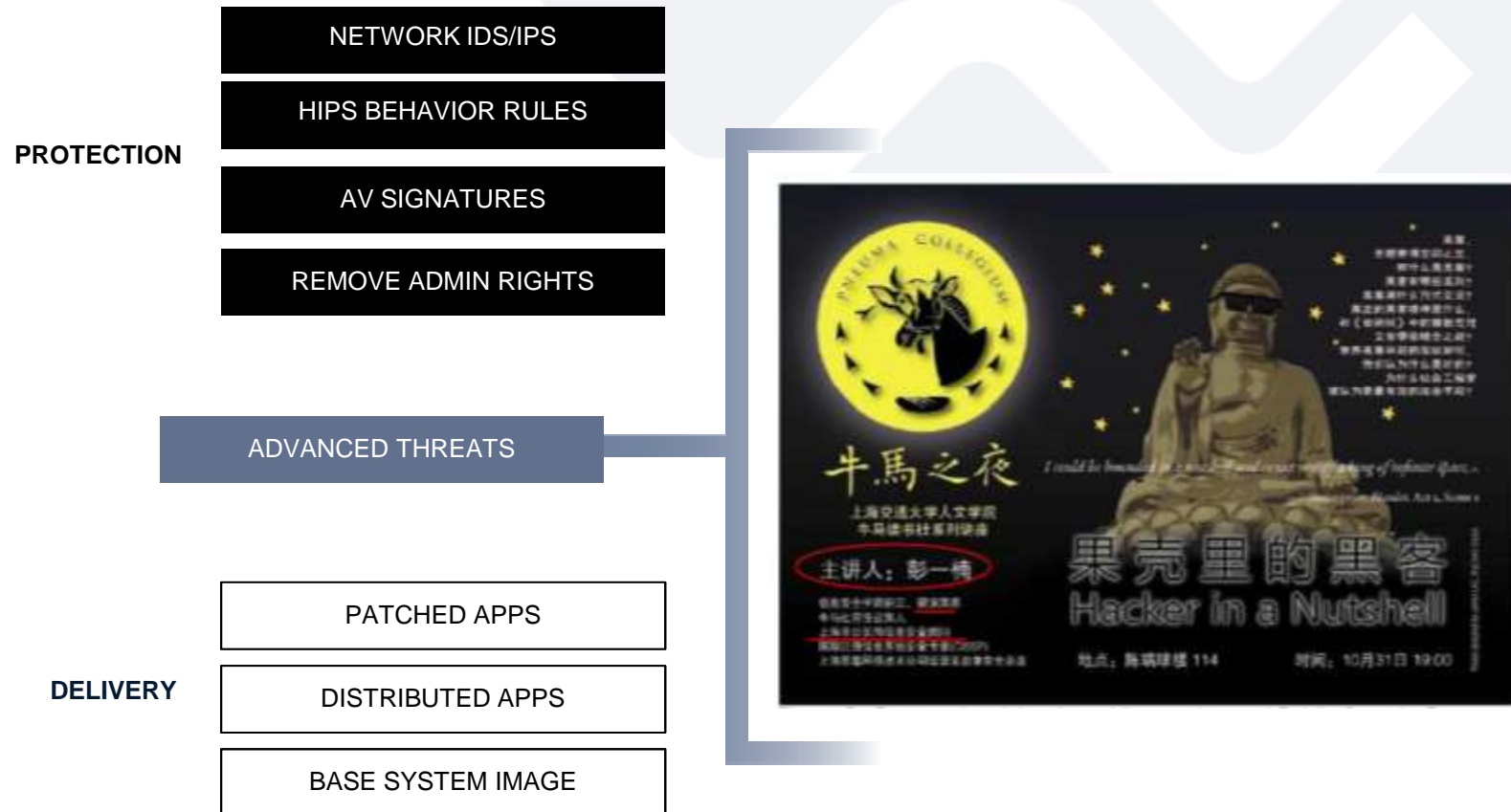
330 signatures / hour

5 signatures / minute

1 signature / 12 seconds



Endpoint Protection Gap



Socially Engineered Threats



The screenshot shows a USA Today news article. The main headline is "How cybercriminals invade social networks, companies". The article is dated 3/4/2010 and is by Byron Acohido. It features a graphic of a laptop with a skull and crossbones on the screen, surrounded by a red starburst. The article text describes a social engineering attack where a hacker hijacked a Facebook account to send a message to Alice, who then clicked on a link, leading to a keylogger being dropped on her company laptop. The article also includes a "USER SAFETY TIPS" section and a sidebar with social media sharing options.

USA TODAY Home News Travel Money Sports Life Tech

Technology Technology Live Science Fair Science & Space Products Gaming Wi-Fi Center

How cybercriminals invade social networks, companies

Updated 3/4/2010 1:53 PM | Comments 122 | Recommend 88 | E-mail | Save | Print | Reprints & Permissions | RSS

By **Byron Acohido, USA TODAY**

SAN FRANCISCO — "Hey Alice, look at the pics I took of us last weekend at the picnic. Bob"

That Facebook message, sent last fall between co-workers at a large U.S. financial firm, rang true enough. Alice had, in fact, attended a picnic with Bob, who mentioned the outing on his Facebook profile page.

HOMELAND SECURITY: Seeks citizen cybercrime fighters
SLIPPERY WORM: Koobface changes its tricks

So Alice clicked on the accompanying Web link, expecting to see Bob's photos. But the message had come from thieves who had hijacked Bob's Facebook account. And the link carried an infection. With a click of her mouse, Alice let the attackers usurp control of her Facebook account and company laptop. Later, they used Alice's company logon to slip deep inside the financial firm's network, where they roamed for weeks. They had managed to grab control of two servers, and were probing deeper, when they were detected.

USER SAFETY TIPS

Twitter and Facebook offer similar advice for dealing with bad links and compromised social-networking accounts. Twitter warns: if you

Share
Yahoo! Buzz
Add to Mix
Facebook
Twitter
More
Subscribe
myYahoo
Google
More

- Hijack a Facebook Account
- Send Facebook Message
- Relationship Leveraged
- Recipient Click on Message
- Keylogger Dropped
- Login Extracted

Profile of an Advanced Threat



Remote Control



Linked in facebook Google



1 Trusted Relationships

Uses Malware to Persist

Poses as Legitimate

Moves Laterally

Uses Control

Operation Aurora

A highly sophisticated malware penetration by Chinese hackers against high profile companies.

Consisted of:

- 0-day browser exploit
- Flexible payload
- Custom encrypted C&C traffic

The Initial Exploit

Exploits MS10-002

.jpg file on a remote server is accessed

Drops encrypted a.exe file to C:\%appdata%\



The Backdoor

- A.exe decrypts to B.exe
- B.exe drops a DLL into \system32 and changes the name to match existing services
- File times are modified to evade forensics
- This DLL is loaded into a **svchost.exe** process

Registry key added:

SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SvcHost\
Value: SysIns
Data: Ups***

Registry key added:

SYSTEM\CurrentControlSet\Services\
RaS***\Parameters\
Value: ServiceDLL
Data: <path to backdoor>





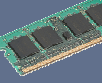

What Can It Do?

Trojan Backdoor Capabilities:







- Adjust process privileges & terminate processes
- Control services
- Remote file execution
- Registry manipulation
- File system manipulation (search, remove, copy)
- System manipulation (turn system off, reboot, clean events)
- Call other components, inter process communication

Advanced Threats Target ...

Critical Resources

-  Registry
-  Config Files
-  Portable Storage Devices
-  Applications
-  Memory
-  Operating System

Visibility and Control

-  Registry Protection
-  File Integrity Monitoring
-  Device Control
-  Application Whitelisting
-  Memory Injection Protection
-  OS Tamper Protection

Consensus Audit Guidelines (CAG)

- Nov 2009, Version 2.3
- 20 Prioritized Controls
- Derived from Attack Knowledge
- Prescriptive
 - How attackers exploit the lack of this control
 - How the control is implemented, automated, and measured
 - Procedures and tools for implementing and automating this control
- Technology and Process Controls

Automatable Critical Controls

1. Inventory of Authorized and Unauthorized Devices
- 2. Inventory of Authorized and Unauthorized Software**
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know
10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention

CAG Control #2

How can this control be implemented, automated, and its effectiveness measured?

Quick Win:

Devise a list of authorized software

Improve Visibility & Attribution:

Deploy software inventory tools throughout the organization The tool should also monitor for unauthorized software installed on each machine.

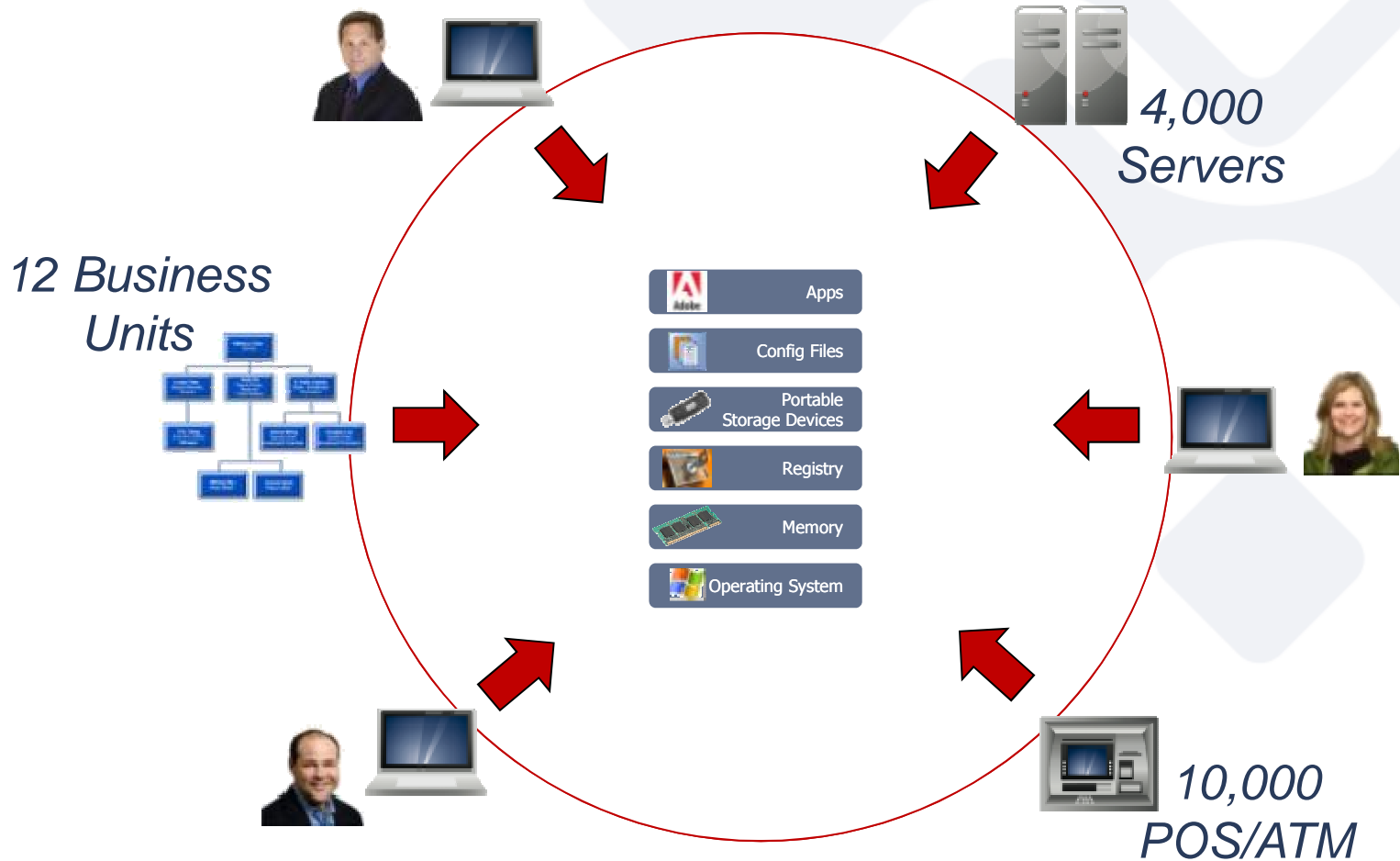
Harden Configurations:

Prevent configuration drift and unauthorized changes that Introduce risk.

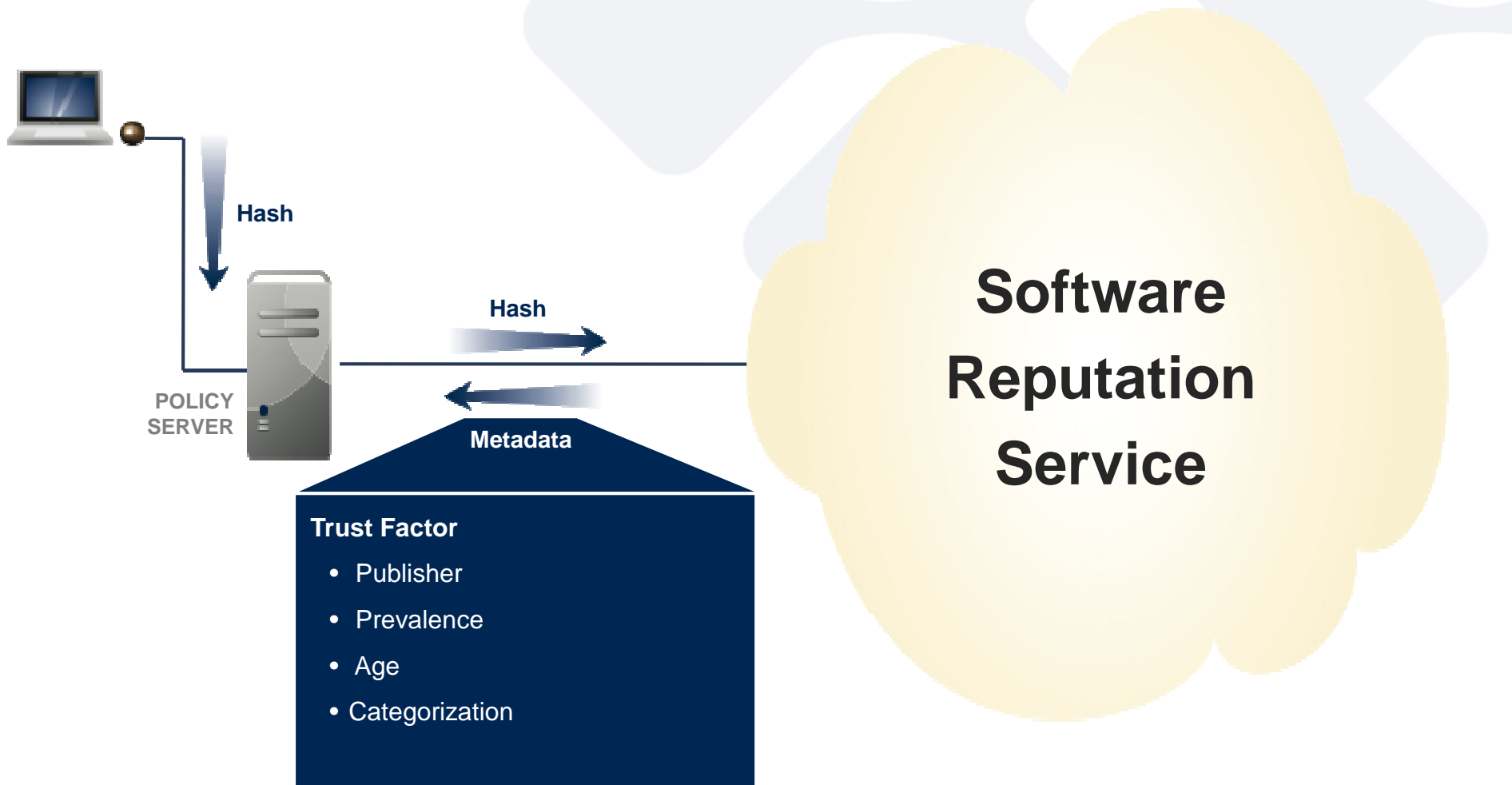
Advanced:

Deploy software white-listing technology that allows systems to run only approved applications and prevents execution of all other software on the system.

Step 1: Continuous Monitoring



Step 2: Assign Reputation to Software

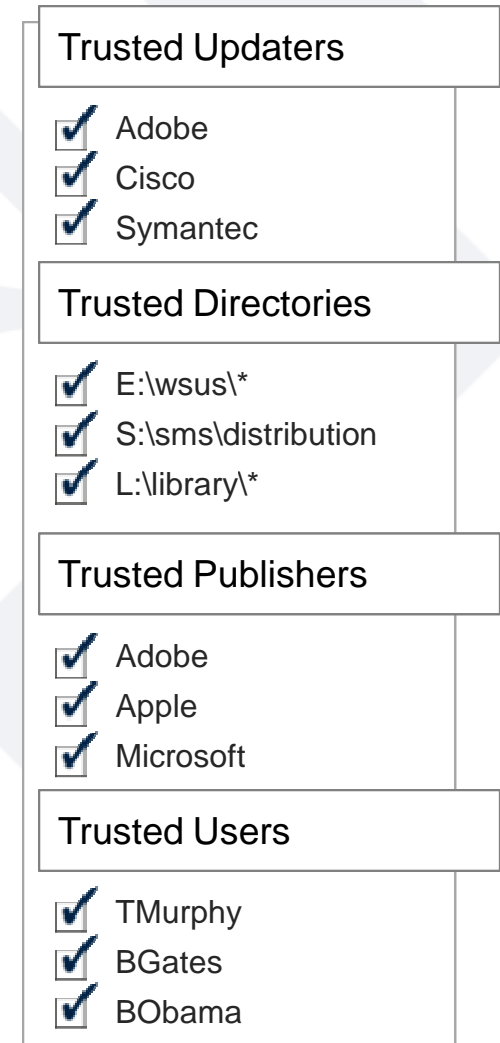
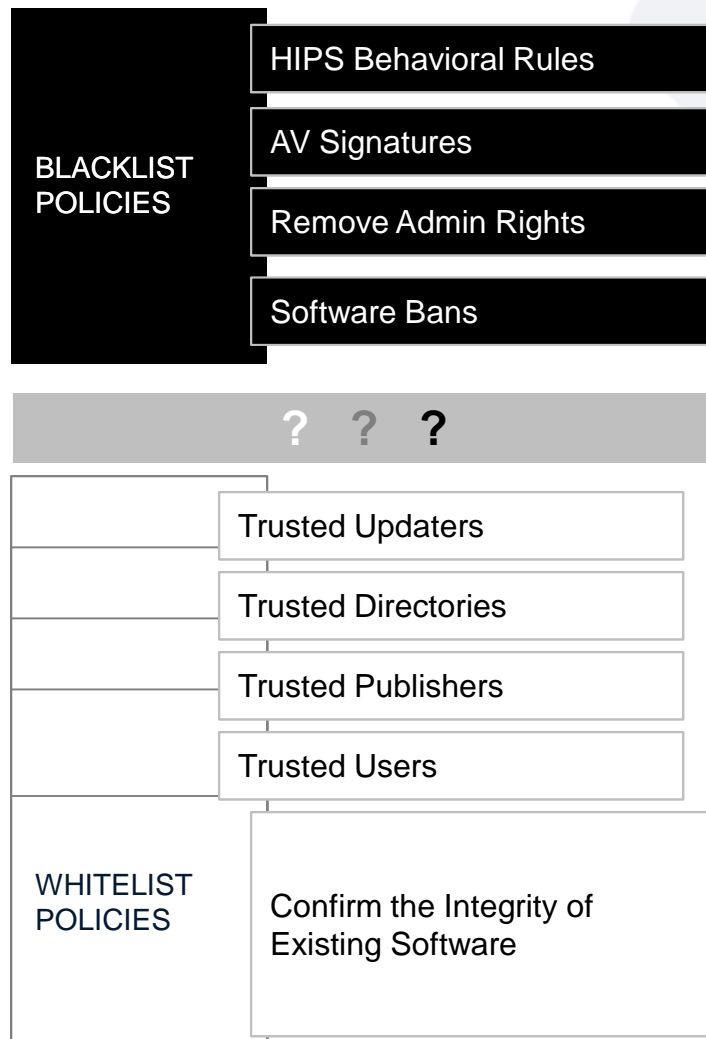


NIST NSRL vs. Bit9 GSR

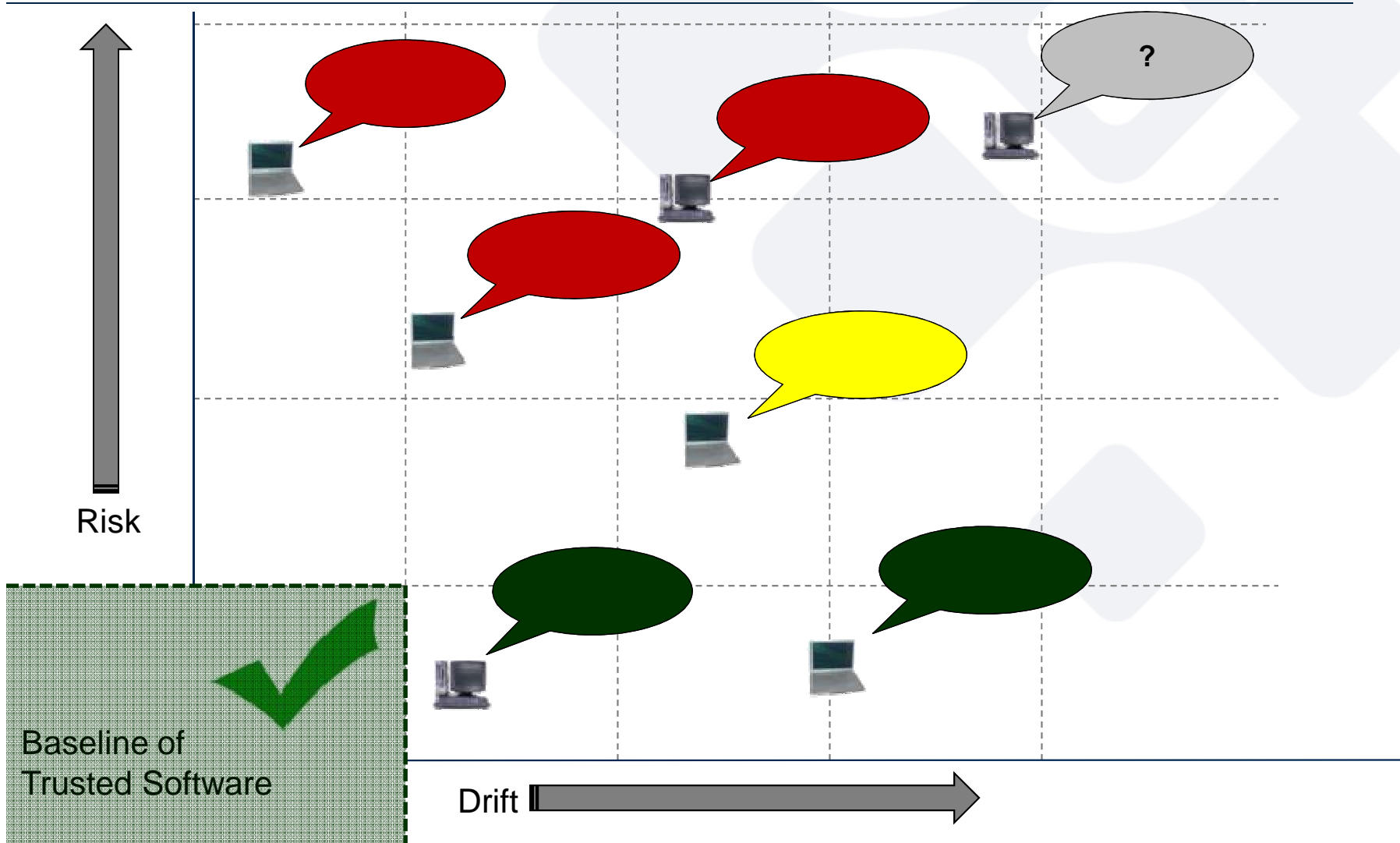
The New Standard

Attribute	NIST NSRL	Bit9 GSR	Bit9 Difference
Number Files Indexed	53,300,000	7,100,000,000	13,321%
Number of Unique Files	16,700,000	481,000,000	2,880%
Number of Unique Packages	24,000	15,300,000	63,750%
Non-English Files	2,700,000	50,000,000	1,852%
Updates	Quarterly	Realtime	Coverage
Meta-data	*Partial	Complete	Comprehensive
Certificates	No	Yes	Software Integrity
Categorization	Yes	Yes	Manageability
Threat Level	**Partial	Yes	Threat Coverage
Vulnerability Info	No	Yes	Risk Assessment

Step 3: Define Trusted Software



Step 4: Isolate Unauthorized Software



Step 5: Deny Questionable Software

BLACKLIST

? Deny Execution

WHITELIST

Default Open
Monitor Policy



User Asked For Permission
Block and Ask Policy



Default Deny
Flexible Lockdown Policy



Advanced Threat Protection In Action



POLICY SERVER



Default Deny
Flexible Lockdown Policy

Execution Allowed

- Trusted Publisher
- Trusted User
- Trusted Directory
- Trusted Updater

Execution Blocked

- ✗ No Trust Established
- ✗ Botnets
- ✗ Rootkits
- ✗ Infected USB Drive
- ✗ Spoof AV
- ✗ Targeted Attacks



Case Study: “Red Team” Exercise

“Austere Challenge”

- Friendly exercise to test security
- “RED TEAM” attempts to penetrate defenses
- Fishing e-mails have been traditionally successful
- Detailed in “After Action Report” (AC08)

Implemented Application Whitelisting

- Identify Who Clicked on Link
- Blocked Targeted/Custom Malware
- 100% deterrent of “RED TEAM” Fishing Attempts



Case Study:

Leveraging Software Intelligence

Challenge

- Identify, categorize, neutralize vulnerable and/or malicious software
- Typical PC has 15,000 executable files
- Labor intensive and error prone task

Solution

- Software Reputation Service
- Identify known good software to isolate bad
- Reduces forensics from weeks to days



Case Study:

Device Whitelisting

Challenge

- Malware continually bypasses network/web/email defenses
- Unauthorized use of Portable Storage Devices
- Lost devices jeopardizing security
- Unsanctioned devices introducing malware

Solution

- Whitelist approved portable storage devices by model/type
- Only allow Kingston Data Traveler
- Ensures all information is encrypted
- Log device usage and files copied to/from the device



Resources

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation

Prepared for
The US-China Economic and Security Review Commission



Project Manager
Steve DeWessa 703.596.1066 stevew@esrsc.gov

Principal Author
Bryan Kohler

Subject Matter Experts
George Bakis
Christopher Barrett

Northrop Grumman Corporation
Information System Sector
7575 Collins Drive
McLean, VA 22102
October 9, 2009

NORTHROP GRUMMAN

Risk Score Advisor

The following grading scale is provided by Information Assurance and may be revised periodically.

Site Risk Score	9,640.9
Hosts	194
Average Risk Score	49.7
Risk Level Grade	A
Rank in Enterprise	81
Rank in Region	7

Average Risk Score	
At Least	Grade
0.0	
40.0	
75.0	
110.0	
160.0	
260.0	
400.0	

The [redacted] Site Risk Score was calculated as follows:

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
Vulnerability	1,450.6	7.5	15.0 %	From 1 for the lowest risk vulnerability
Patch	645.0	3.3	6.7 %	From 3 for each missing "Low" patch to
Security Compliance	2,580.3	13.3	26.6 %	From 9 for each failed Application Log Membership check
Anti-Virus	2,364.0	12.2	24.5 %	6 per day for each signature the older the
SCIE Compliance	35.0	0.2	0.4 %	5 for each missing or incorrect version s
AD Computers	112.0	0.6	1.2 %	1 per day for each day the AD comput
AD Users	250.0	1.3	2.6 %	1 per day for each account that does no
				age > 60, plus 5 additional if the passw
SMD Reporting	2,110.0	10.9	21.9 %	100 + 10 per day for each host not repo
Vulnerability Reporting	56.0	0.3	0.6 %	After a host has no scans for 15 consec
Security Compliance Reporting	36.0	0.2	0.4 %	After a host has no scans for 30 consec
Total Risk Score	9,640.9	49.7	100.0 %	



FileAdvisor™

The Best Search Engine for Identifying Software on Files

Enter File Name or Hash:

Search Faster for Free!

Install the FileAdvisor Desktop Utility and simply right-click to identify any executable file on your computer.

[Download Now](#) | [Learn More](#)

What is FileAdvisor?

Bit9 FileAdvisor is a comprehensive catalog of executables, drivers, and patches found in commercial (Windows®) applications and software packages. Malware and other unauthorized software that affects Windows computers is also indexed. As the largest and the most accurate database of its kind, FileAdvisor enables you to submit a file name or hash and get the following information:

- Original name and size of the file
- Publisher that created the file
- Products in which the file appears
- Sources of distribution
- Likelihood that the file poses a threat
- And more!

Discover what the unknown files on your computer actually are.

© 2009 Bit9, Inc. All rights reserved. | [Terms of Use](#) | [Privacy Policy](#) | [Tell a Friend](#)

Application Whitelisting Review

Test Center Scorecard						InfoWorld
	Accuracy/ Effectiveness	Coverage	Administration	Reporting	Value	Overall Score
	30%	15%	25%	10%	20%	
Bit9 Parity Suite 5.01	10	8	9	9	10	9.4 EXCELLENT
	30%	15%	25%	10%	20%	
CoreTrace Bouncer 5	9	9	9	8	9	8.9 VERY GOOD
	30%	15%	25%	10%	20%	
Lumension Application Control	8	9	8	9	9	8.5 VERY GOOD
	30%	15%	25%	10%	20%	
McAfee Application Control 5.0	9	9	9	8	8	8.7 VERY GOOD
	30%	15%	25%	10%	20%	
SignaCert Enterprise Trust Services 3.0	8	9	8	8	8	8.2 VERY GOOD

InfoWorld
November 4, 2009
GET TECHNOLOGY RIGHT

APPLICATION WHITELISTING REVIEW
Bit9 Parity Suite **EXCELLENT**
InfoWorld

Bit9 Parity 5.0 shines brightest among whitelisting competitors with strong protection and useful risk metrics

BY ROGER A. GRIMES | INFOWORLD

As many product vendors can readily tell you, this review is the ultimate computer security critic and a tough writer to please. I'm notoriously critical of overhyped products. Although I've evaluated a number of whitelisting products over the years, I've never given a product 10 in any scorecard category — not even Bit9 Parity in one of the few computer security products that, if deployed in your Windows environment, will radically and immediately reduce your enterprise's level of security risk. It's not perfect, and it did not score perfect 10 in every field — but it earned the highest score this reviewer has ever given.

Started in 2002 from a SOFT grant, Bit9 Parity was the most mature whitelisting product in this review. It provides broad coverage of Windows filetypes and filetypes, and its functionality and features assist users with making the right trust decisions needed to secure their environment. Bit9 Parity's server console, called Parity Center (shown image), runs on Windows Server 2003, with Bit9 installed and a Microsoft SQL Server database. The Parity client supports Windows 2000 and later, including embedded versions. Bit9 Parity comes linked, like SignaCert, to a cloud service with more than 7.2 billion legitimate and malicious files pre-defined and hashed.

Malware can be scanned to create baseline catalogs and individual files and folders can be whitelisted or blacklisted. When Bit9 takes application control to a new level in its rating identified files as to their trust and risk, based upon hash, digital signature (if included), software category (if known), and location. All reported client features are compared against known malware and legitimate resident files. For example, if a managed, trusted user downloads Apple iTunes, it may violate corporate policy, but not necessarily be a real security risk to the enterprise. However, a known malware program or unidentified file would be marked as higher risk. Bit9 Parity's risk and trust ratings (shown image) allow you to discriminate between the merely noncompliant, such as iTunes and Photos, and a security threat, such as the Fluoride virus. It's important to note that Bit9 doesn't automatically decide what is the appropriate treatment for a particular risk level; it just reports the result and lets the administrator define the policy.

Bit9 Parity has three main policies and an emergency mode. In Monitor mode, users are allowed to execute anything, but all operations are monitored. In Block & Ask mode, users are asked to approve execution of unknown programs. And in Lockdown mode, execution of all unknown and unapproved programs is blocked. Emergency Lockdown mode returns to a previously known secure state, blocking all execution of originally unapproved programs across all managed machines, regardless of whether trusted users later whitelisted them.

Each policy can be tied to a computer, user, group, organizational unit, or other Active Directory component. Parity can be integrated into Bit9's ePolicy Orchestrator administrative console, and it works with multiple whitelisting products.

Software can be pre-approved in the same way as shown by most competitors: Trusted Applications, Paths, Trusted Users,

Copyright © 2009 by InfoWorld Media Group, Inc., a subsidiary of ZDNet Company. All rights reserved. Bit9 Parity Suite, the Parity Suite, ePolicy Orchestrator, and the Bit9 logo are trademarks of Bit9 Parity Suite, Inc. All other trademarks are the property of their respective owners.

Recommendations

Continuous Monitoring

- Audit Critical Resources
- Establish Real-time Forensics

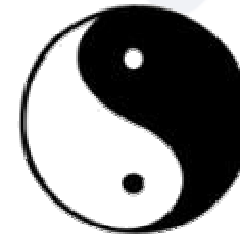


Baseline Configurations

- Define Policies and Trust
- Share and Communicate End User Risk

Blacklist and Whitelist

- Continue to Run Existing Defenses
- Whitelist Trusted Sources of Change



Questions/Slides

Tom Murphy
Chief Strategy Officer
Bit9, Inc.

+1 617.393.7441
tmurphy@bit9.com