Staying out of the Front Page Headlines Using NEPS Lecture

ZEN04 **Novell Training Services** www.novell.com

ATT LIVE 2012 LAS VEGAS

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

U.S.A.

www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Staying Out of the Front Page Headlines Using Novell Endpoint Protection Suite (NEPS)

Product Positioning & Important Features

Novell®

Agenda

- Introducing NEPS
  - Why NEPS?
  - Product Positioning
  - Product Components
  - Upgrade Path
- Full-Disk Encryption Features of NEPS
  - Purpose of Full-Disk Encryption (FDE) & Problems Addressed with FDE
  - Types of FDE
  - Authenticating to Windows when FDE is enforced
- Endpoint Security Management Features of NEPS
  - Purpose of Endpoint Security Management (ESM)
  - Overview of ESM Policies
- Patch Management Features of NEPS
  - Benefits of Patch Management (ZPM)
  - Understanding ZPM Terminology & Concepts
  - Understanding the Patch Management Process

Novell.

Introducing NEPS

Why NEPS? - Your Organization Doesn't Need This Kind of Brand Awareness!

- BP Global
  - An employee lost a laptop in March 2011 containing the personal data of over 13,000 claimants seeking damages due to the 2010 oil spill
  - Information lost included: name, addresses, phone numbers, and social security numbers
  - Laptop was password protected but data was unencrypted
  - Reported by CBS News and just about everyone else
- Department of Veteran Affairs
  - An employee takes a laptop and external drive containing the names, birth dates, and social security numbers of 26.5 Million US Veterans
    - Information was not encrypted and laptop was not password protected
    - The laptop and drive was stolen in a robbery from the employee's house
  - Costs:
    - $14 Million to notify all the Veterans
    - Three years of litigation in which the plaintiffs in the class action suit are awarded $20 Million

Novell.

Why NEPS? - Your Organization Doesn't Need This Kind of Brand Awareness!

- Sutter Physicians Services & Sutter Medical Foundation
  - Unencrypted laptop stolen from their administrative offices in November 2011
  - Approximately 3.3 million patients whose health care provider is supported by SPS had their names, addresses, dates of birth, phone numbers, email addresses, medical record numbers and health insurance plan name exposed
  - Costs:
    - Two class action lawsuits have been filed. One suit seeks $1,000 for each member of the class
- California Department of Public Health
  - An employee copied the records of 9,000 employees to a private unencrypted hard drive in April 2011
  - Names , Social Security Numbers, address, birthdays, next of kin, and other workers' compensation information was exposed
- **Sources:**
  - **http://www.privacyrights.org/data-breach**
  - **http://www.datanymity.com/breaches/db_index.php**
  - **http://www.databreaches.net**

Novell.

Product Positioning

- Targeted at organizations -
  - Whose main concern is security as opposed to configuration management
  - Who already own ZCM but are missing the security products
  - Organizations that are in highly-regulated businesses
    - especially those concerning customer or patient records

- What does NEPS Provide?
  - An “out-of-the-box” endpoint protection and security solution that:
    - Protects data from malicious attacks or from unintended but risky user behaviour
    - Provides protection regardless of the endpoint’s location or connectivity to the corporate network
    - Is managed with a central web-based console
  - Adaptability - NEPS can set different levels of security based on the endpoint’s location.
    - Without needing to remove the endpoint from its user in order to make changes
  - Security that can’t be circumvented by the user or a hacker’s independent boot media

Novell.

Product Components

- NEPS Components target Windows managed devices
  - All components use the same centralized management console
  - Security solution that doesn't just work at the security perimeter, but rather is part of the endpoint device regardless of where its located
- ZENworks Full-Disk Encryption (ZFDE):
  - Encrypts the endpoint's entire drive: boot record, OS, registry, applications, the whole "nine yards"!
    - Can add an additional authentication dialog from a hardened Linux partition
- ZENworks Endpoint Security Management (ZESM):
  - Secures & controls the following on a Windows managed device:
    - Applications, access to removable devices and hardware ports,
    - data encryption on removable devices, protects the ZESM Agent components from attack
- ZENworks Patch Management (ZPM):
  - Automate & control patching of devices by defining policies
    - Automatically scan for vulnerabilities
    - Force compliance on all endpoints and report

Full-disk Encryption Features of NEPS

NEPS: Full-disk Encryption

- Understanding the Problems FDE Addresses:
  - Windows login can be easily beaten
  - Simply buy a $19 piece of software:
    - Boot the computer from CD
    - View all User Accounts and data
    - Delete and set passwords
  - Even BitLocker can be compromised
    - Well publicized Firewire-based physical attack
    - Uses direct memory access to get at the key for encryption / decryption that's loaded into memory prior to the user logging in


Security Research

Firewire-based Physical Security Attacks on Windows 7, EFS and BitLocker

Benjamin Böck
Security Research Lab
Secure Business Austria
bboeck@securityresearch.at

With kind support from David Huemer

V 1.0, 2009-08-13

Latest version at
http://www.securityresearch.at/publications/windows7_firewire_physical_attacks.pdf

1 Overview

This paper discusses Firewire-based physical security attacks on Microsoft Windows 7. In the course of my research, I was successfully able to bypass the Windows 7 RTM[1] authentication check and logon with any password.

Novell.

NEPS: Full-disk Encryption

- Understanding the Purpose of FDE:
  - Protects “data-at-rest”
  - Data can not be accessed if:
    - Machine has been turned off
    - Machine is in hibernate or stand-by mode.
  - So if a machine is lost or stolen and is turned off or in stand-by, the data is *completely protected*.
  - Attacks that would compromise Windows user names and passwords will not succeed
  - Literally everything on the machine's drive(s) is encrypted

Novell.

NEPS: Full-disk Encryption

- Types of Full-Disk Encryption: *Hardware-based*
  - Provides support for hard drives that use an on-board hardware encryption chip
    - All data written to the drive or read from drive passes through the hardware encryption chip first
    - This approach does not have a performance impact on operating system or applications
    - All encryption / decryption is done on a dedicated processor on the drive itself
    - Encryption Key is supplied on the drive by manufacturer
  - First release of FDE (with ZCM 11.2) will support :
    - Seagate Momentus FDE.x Drives
    - Future releases will support drives adhering to the TCG's OPAL Standard

Novell.

NEPS: Full-disk Encryption

- Types of Full-Disk Encryption: *Software-based*
  - Used for machines with “standard” drives in them
    - IDE, EIDE, SATA (essentially any type of “laptop” type drive)
    - Of any drive size
    - But must be formatted with NTFS
  - Drive must go through an initial encryption process
    - Time required varies with whether or not
      - the entire drive is encrypted
      - or just used sectors are encrypted
    - Encryption happens at sector level – not the file level
    - As a rough estimate, figure 30 minutes per 10GB of data

Novell.

NEPS: Full-disk Encryption

- Authenticating to Windows Managed Devices that have an FDE Policy Enforced
  - Pre-boot Authentication (PBA)
    - When FDE Policy is enforced a special partition is created at the end of the System Volume
    - This partition contains a hardened version of Linux and is referred to as the *PBA Partition*
  - The PBA Environment can be set up to interact with the user or not
    - **Transparent PBA:** FDE Policy is configured so that the only authentication dialog seen by the user is the Windows Login Dialog
    - **PBA Authentication:** The FDE Policy is configured so that prior to Windows boot a special PBA Authentication Dialog is displayed
      - User must pass the PBA Authentication before Windows boots
      - User may also see the Windows Login Dialog if configured in the FDE Policy

Novell.

NEPS: Full-disk Encryption

- Authenticating when the enforced FDE Policy Enforced uses PBA Authentication:
  - Credentials entered into PBA Authentication Dialog can be passed on to Windows Login
    - Called **Single Sign-on and is configured in the FDE Policy**

NEPS: Full-disk Encryption

- So now **FDE** is protecting your organization's confidential business data and intellectual property if an employee losses their laptop...

- But –
  - What happens if a valid user authenticates to FDE's PBA
  - And tries to insert an unapproved USB device into their laptop
  - Or tries to copy data to a USB device that shouldn't be copied from their laptop?

- This is where ZENworks Endpoint Security Management of the NEPS Suite comes into play!

Novell.

Endpoint Security Management Features of NEPS

NEPS: Endpoint Security Management

- Purpose of ESM:
  - Manage applications available on the endpoint
    - No Restrictions, No Execution, No Network Access
  - Control how the hardware ports and removable devices on the endpoint are used
  - Behaviour of how ESM Policies are enforced can change based on the current *Security Location* of the endpoint.
- Location Awareness
  - Managed endpoint can determine “where it is” based on how administrator defines:
    - Network Environments
    - Security Locations
  - Means the that ESM Policies enforced at any given time:
    - Depend on the endpoint’s *calculated* Security Location
    - And that the endpoint’s capabilities and level of security can automatically change from Security Location to Security Location.

Novell.

NEPS: Endpoint Security Management

- 11 ESM Security Policies in all
  - 9 control OS and hardware functionality
  - 2 control and protect the ESM components of the ZENworks Adaptive Agent (ZAA) and how it operates
- Application Control Policy
  - Is used to prevent applications from:
    - running on the managed device
    - accessing the Internet
- Communications Hardware Policy
  - Disable or enable the endpoints of hardware ports
- Data Encryption Policy
  - Two types of encryption:
    - File & Folder also called "***Safe Harbor***"
    - and Device Based

Novell.

NEPS: Endpoint Security Management

- Firewall Policy
  - Hooks into all network drivers on the endpoint
    - Highly configurable
    - Uses less CPU cycles as compared to an Application-level Firewall
- Storage Device Control Policy
  - Control access to device that enumerates to OS as a Drive ID
- USB Connectivity Policy
  - Controls access to the USB Bus itself
    - Enable / Disable access to USB Thumb Drives, External Drives, USB Printers, Human Interface Drives
    - Can *black-list* or *white-list* USB Thumb Drives or External Drives
- VPN Enforcement Policy
  - Enforce VPN Usage for remote users
    - Automatically launch VPN Client software for the user

Novell.

NEPS: Endpoint Security Management

- Wi-Fi Policy
  - Used to manage the endpoint's wireless capabilities and environment
- Scripting Policy
  - Allows for the running of scripts based on the occurrence of a given event
    - Scripts can be written in JScript or VBScript
- Security Settings Policy
  - Designed to protect the ESM components of the ZAA from being tampered with or uninstalled
- Location Assignment Policy
  - Used by ESM Components of ZAA to decide which assigned ESM policies to enforce based on the endpoint’s current security location

Novell.

NEPS: Endpoint Security Management

- Now –
  - **FDE** is protecting your organization from data breaches due to lost equipment and
  - **ESM** can
    - prevent data breaches due to copying confidential data to external devices
    - And prevent unwanted software from being copied to the endpoint
- But –
  - What happens if the Windows Operating System has a vulnerability that allows surreptitious access to the endpoint
  - Or a well-known application has a security hole that can be exploited
- This is where ZENworks Patch Management comes into play!

Novell.

Patch Management Features of NEPS

NEPS: Patch Management

- The problem:
  - Testing and applying patches to combat viruses and malware is never ending
  - IT may not know if all endpoints have been properly patched and are in compliance
  - IT may not be able to prove their supported endpoints are in compliance
    - Even if they can, doing so is time consuming and expensive – the so-called *Audit Tax*
  - IT needs to be able to identify threats and quickly address them

Novell.

NEPS: Patch Management

- The solution:
  - Automate the entire patching process based on administrator created policies
  - Have a proactive solution that:
    - lets IT know automatically what devices are in or out of compliance
    - will automatically download OS and Application patches and create bundles for assignments to devices
    - Allows you to create a baseline of patches that devices must have
    - automatically includes new endpoints as they come on-line so that they are automatically included in the patching and compliance reporting process
    - Provides patching for the widest range of operating system platforms:
      - Windows 2003, 2008, XP, Vista, and 7; SLES, SLED, and Red Hat Linux, MAC OS-X, and more!

Novell.

NEPS: Patch Management

- Components and Terms:
  - Patch Management Subscription Service
    - Runs on a designated Primary Server in the zone
    - Contacts Lumention's and Microsoft's patch sites for content
    - Turns that content into ***DAU Bundles*** and ***Remediation Bundles***
  - DAU Bundles
    - Bundles automatically built by the Subscription Service
    - Contains "*fingerprints*" and ZAA executables
    - Are automatically assigned to registered devices in the ZCM zone
  - Remediation Bundles
    - Bundles containing the actual patch content that addresses a given vulnerability
    - Usually contains multiple MSI or exe files that must be installed on the managed device to address the given vulnerability
    - Administrator must deploy the Remediation Bundle or add it to a "***baseline***" in order for the patches to be applied to the managed device

Novell.

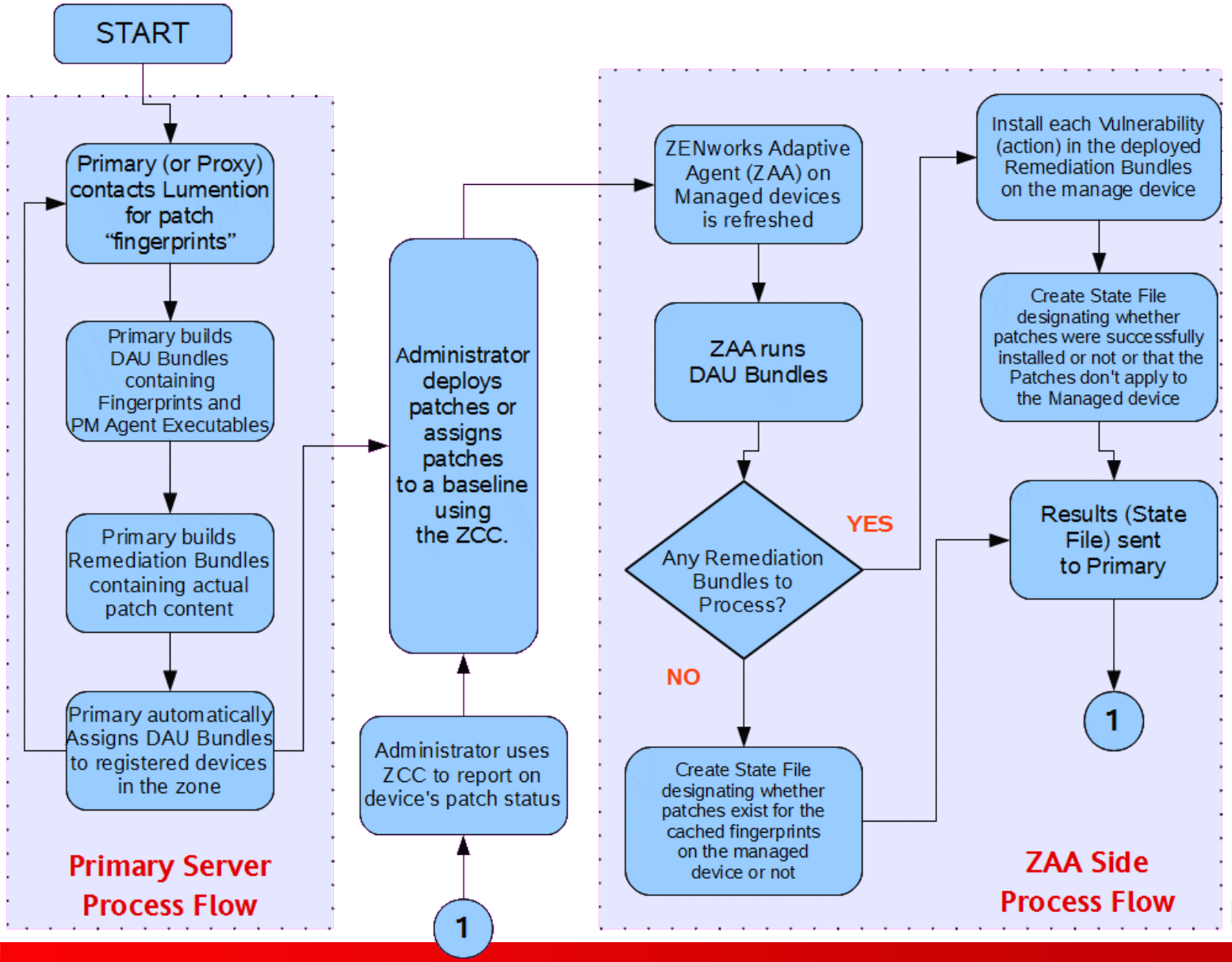
NEPS: Patch Management

- Components and Terms:
  - Baseline
    - Is a set of Administrator selected patches that are assigned to either a static or dynamic device group
    - Ensures that the patches in the Baseline remain on the managed device
  - Workstation Analysis Application
    - Is a program named analyze.exe
    - Distributed to managed device via any assigned DAU Bundle
    - Reads the cached fingerprints to determine whether or not the patch identified by any given fingerprint has been installed on the managed device
  - Patch Remediation Tool
    - Is a program named remediate.exe
    - Distributed to managed device via any assigned DAU Bundle
    - Applies the patch content in a Remediation Bundle to the managed device

Novell.

NEPS: Patch Management

- Patch Management Process Flow:



NEPS: Patch Management

- Patch Management Reporting via the ZCC:

Patches | Dashboard | Status

Status

Name	Status
Signature Download	Complete
Last Signature Download Time	Apr/02/2009 09:45:24
Bundle Download	In Progress
Last Patch Download	Apr/02/2009 09:45:29
Number of Failed Download(s)	9
Number of Patches Queued for Caching	103
Number of Active Patches	1268
Number of New Patches(less than 30 days)	77
Latest Patch Released On	Apr/01/2009 00:00:00

Cache Status

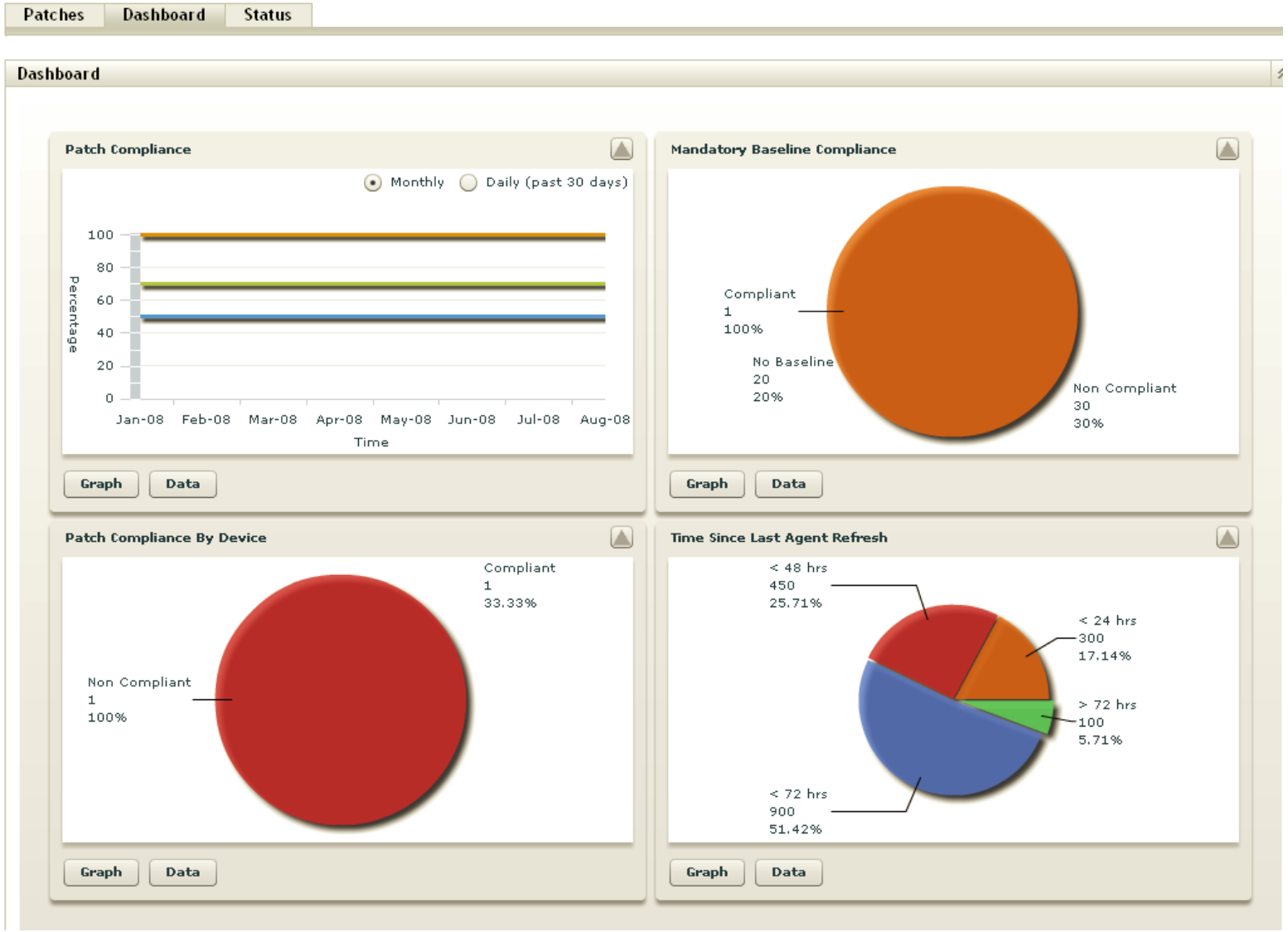
Name	Status	Error Detail (if any)
Adobe APSB09-03 APSB09-04 Reader (English) 9.1 Security Update for Windows (Rev 2)	Queued	
F-Secure Anti-Virus DEF File (March 25, 2009)	Queued	
MS09-007 Security Update for Windows 2000 (KB960225)	Queued	
MS09-008 Security Update for Windows 2000 (KB961063)	Queued	
Symantec Norton AntiVirus Def files x86 version (March 30, 2009)	Queued	
MS09-008 Security Update for Windows Server 2008 (KB961063)	Queued	
MS09-008 Security Update for Windows Server 2003 (KB961064)	Queued	
MS08-052 Security Update for Windows Server 2003 (KB938464)	Queued	
MS09-008 Security Update for Windows Server 2003 (KB961063)	Queued	
Adobe APSB09-03 APSB09-04 Reader 7.1.1 Security Update for Windows (All Languages)	Queued	

1 - 10 of 112 show 10 items

Novell.

NEPS: Patch Management

- Patch Management Reporting via the ZCC:



Novell.

Summary

Summary – Why Invest in NEPS?

- The costs per endpoint for NEPS can be far less than the costs of a single instance of a:
  - Compromise of mission critical data or
  - Data Breach
- Endpoint Protection that is:
  - Adaptable via enforcement of security policies
  - Protects vital data on the endpoint and enforces patch compliance
  - Follows the endpoint where ever it may roam
  - Configurable with a central browser-based management console

Novell.

Corporate Headquarters
1800 South, Novell Place
Provo, Utah 84606

801.861.7000 (Worldwide)
800.452.1267 (Toll-free)

Join us on:
www.novell.com