

Patch and Remediation v7

IN THIS PRODUCTSHEET:

- » The Challenge
- » The Solution
- » Key benefits
- » Norman Patch and Remediation provides
- » Key features

The Challenge

As IT environments have become increasingly complex, supporting virtual, distributed, and disparate platforms, companies must ensure that they maintain control of their endpoints. Ensuring secure and standard endpoint configurations and patch management for third party applications and operating systems is paramount to reducing IT risk and improving endpoint operations. With an average of more than 15 new vulnerabilities reported daily¹, staying on top of vulnerability management should be on top of the IT departments work list.

The Solution

Norman Patch and Remediation provides rapid, accurate and secure patch management for applications and operating systems, allowing you to proactively manage threats and IT risk even in the most complex of IT environments. This optimization is achieved by automating the patching process from vulnerability identification to patch collection, distribution, remediation and verification reporting. Norman Patch and Remediation significantly reduces the exposure to cybercriminal and malware risk while decreasing the cost of endpoint operations and compliance reporting requirements.

Key benefits

Single Solution for Heterogeneous Environments: Vulnerability audits and remediation with wide support across major OS platforms (Microsoft Windows, Linux, MacOS, Sun Solaris, HP, etc.) – all from a single console.

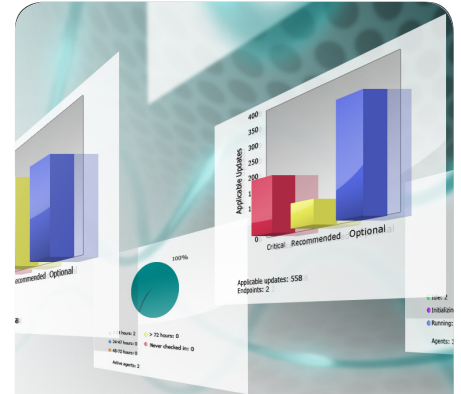
Provides a Consolidated, Single Tool To Meet All Your Patching Needs: Enforces corporate patch policies regardless of the endpoint platform or applications. Optimizes IT operations and provides an improved security posture and reduced TCO via a broad vulnerability assessment and remediation database.

Automated Discovery and Assessment of IT Assets: Provides inventory and management of both physical and virtual environments via in-depth assessment of vulnerabilities, patch status, security configurations, installed software and managed and unmanaged hardware inventory.

Continuous Policy Enforcement: Automatically enforces patches, configurations, remediations and other custom and repetitive tasks.

Diverse, Flexible Reporting: Provides detailed information across the patch and remediation management process, including agent policy status, vulnerability deployments, asset inventory and more.

Virtual Environment Support: Ensures visibility and control of both physical and virtual environments with effective management.



HOW NORMAN PATCH AND REMEDIATION WORKS:



1. DISCOVER - application, operating system and configuration vulnerabilities on managed endpoints through comprehensive agent-based scan.
2. PROFILE - for every patch is created including software, hardware, drivers and existing and missing patches for each machine.
3. REMEDIATE - vulnerabilities and rapidly deploy patches based on defined policies.
4. REPORT - on operational, management and compliance initiatives.

1) Average of reported vulnerabilities, 2006 through 2010. Source: National Vulnerability Database (<http://nvd.nist.gov>)

Norman Patch and Remediation provides

- » An intuitive management console for easy patch and remediation administration across multiple platforms - Windows, Unix, Linux and Mac OS - as well as many third party applications, including the largest repository of Adobe vulnerability content.
- » Integrated asset discovery for full network visibility and continuous control across both physical and virtual environments.
- » Automated policy baselines to ensure that patches, configurations, remediations, and other tasks are continuously enforced.
- » Extensibility and customization via Norman Content Wizard including power policy management, software deployment and removal, desktop configuration templates and custom task scripting.

Key features

Improved Management console: Features web-, role- and workflow-based navigation to simplify and optimize endpoint operations.

Automated Discovery and Assessment of IT Assets: Full visibility into both physical and virtual environments via schedulable discovery, in-depth vulnerability assessment, patch status, security configurations, installed software and managed and unmanaged hardware inventory.

Actionable Reporting: Provides detailed information across the patch and remediation management process, including agent policy status, vulnerability deployments, asset inventory, and supports many compliance reporting requirements.

Single Solution for Diverse Environments: Broad support across major OS platforms and third party applications all from one console (Windows, Linux, MacOS, Sun Solaris, HP, POSIX and infrastructure devices, Adobe® and QuickTime®, etc.)

Comprehensive Patch, Remediation, and Configuration Capabilities: Assessments include security configurations, OS, application and patch-level related vulnerabilities, null passwords, known hacking tools, malware, common worms, and P2P software check.

Continuous Monitoring and Enforcement: Automatically enforces patches, configurations, remediations and other custom and repetitive tasks. Baseline policies can be easily exported and applied across multiple groups and servers for consistency.

SYSTEM REQUIREMENTS

Server: Windows Server 2003, 2008 or 2008 R2 with Microsoft SQL Server 2005 or 2008 and .NET Framework

Agent coverage: Apple Mac OS X, CentOS, HP-UX, IBM AIX, Novell SUSE Linux, Oracle Enterprise Linux, Red Hat Enterprise Linux, Sun Solaris, Microsoft Windows (Windows 2000 and newer)

LANGUAGE COVERAGE

Chinese (Simplified)
Chinese (Traditional)
Danish
Dutch
English
Finnish
French
German
Italian
Japanese
Korean
Norwegian
Portuguese
Spanish
Swedish

Related products:

NORMAN CONTENT WIZARD

Norman Patch and Remediation Advanced includes Norman Content Wizard (NCW), a powerful tool to create custom patches, enforce security policies and power management.

NCW automates time-consuming system and desktop management tasks. It lets you optimize your IT environment and take advantage of cost and resource saving options via power management capabilities.

Extending vulnerability management capabilities without requiring additional solutions, NCW works in conjunction with Norman Patch and Remediation to provide user friendly development, centralized management and enforcement of capabilities throughout an organization.



Norman ASA is a world leading company within the field of data security, internet protection and analysis tools. Through its SandBox technology Norman offers a unique and proactive protection unlike any other competitor. While focusing on its proactive antivirus technology, the company has formed alliances which enable Norman to offer a complete range of data security services.

Norman was established in 1984 and is headquartered in Norway with continental Europe, UK and US as its main markets.

NORMAN®



www.norman.com

Norman SandBox® US Patent Number 7,356,736