

Patch and Remediation

¹ National Vulnerability Database,
1. März, 2009

WICHTIGE FUNKTIONEN

detaillierte Erfassung und Beurteilung aller IT-Ressourcen

offene Architektur zur Unterstützung komplexer Umgebungen

Unterstützung heterogener Netzwerkumgebungen

schnelle, automatische Patch-Bereitstellung

NAC-Unterstützung

automatische Beseitigung von Schwachstellen und Konfigurationsproblemen

hochgradig skalierbar

Multi-Patch-Bereitstellungen

umfassendes Reporting

rollen- und richtlinienbasierte Verwaltung

Software-Sicherheitslücken identifizieren und schließen – Konfigurationsabweichungen vermeiden

Die Flut an Software-Sicherheits-Patches, die ständig von den Herstellern herausgegeben werden und die Verwendung der Produkte in heterogenen Umgebungen machen es IT-Administratoren schwer, auf dem aktuellen Stand zu bleiben und diese Patches zu implementieren. Der Produktlebenszyklus von Software und Betriebssystemen wird immer weiter verkürzt und Software vorzeitig auf den Markt gebracht. Das lässt die Zahl von Bugs und Entwicklungsfehlern exponentiell ansteigen: Pro Tag werden im Durchschnitt 19 neue Sicherheitslücken bekanntgegeben.¹

Spielen Sie Ihre Karten richtig aus – den Bedrohungen stets einen Schritt voraus



Schnelle, genaue und sichere Patch-Verwaltung

IT-Abteilungen sind heute vornehmlich damit beschäftigt, virusinfizierte Benutzerdesktops zu bereinigen. Malware-Angriffe werden immer bloß abgewehrt, anstatt das Unternehmensnetzwerk proaktiv abzusichern und das Ausnutzen von Sicherheitslücken zu vermeiden.

Einem vor Kurzem gestarteten Virusangriff folgten in einer einzigen Nacht 6.000 verschiedene Modifikationen; ein Patch für die zugrundeliegende Sicherheitslücke war jedoch bereits seit einem Monat verfügbar. Hinzu kommt die zunehmende Verbreitung von Web 2.0, sozialen Netzwerken und virtuellen Umgebungen, die Malware am Arbeitsplatz neue Wege eröffnet.

Patch and Remediation von Norman rationalisiert und automatisiert den Patch-Verwaltungsprozess auch in hochkomplexen heterogenen Netzwerkumgebungen. Durch proaktive Warnungen können Sie Probleme unmittelbar beheben.

Norman Patch and Remediation bietet

- schnelle, genaue und sichere Patch-Verwaltung
- automatische Erfassung, Analyse und Bereitstellung von Patches
- Schutz Ihres Unternehmens vor Würmern, Trojanern, Viren und anderen Bedrohungen
- effektive Verwaltung mit deutlich geringeren Betriebskosten durch eine einzelne konsolidierte Lösung für heterogene Netzwerke

Hauptvorteile

- ermöglicht Ihnen, künftigen Bedrohungen einen Schritt voraus zu sein
- rationalisiert die Patch-Verwaltung in heterogenen Umgebungen
- bietet Echtzeit-Einblick in den Patch-Status und die Netzwerksicherheit insgesamt
- senkt die Betriebskosten durch Zeit- und Aufwandsersparnis im IT-Bereich

NORMAN ContentWizard

Norman Content Wizard (NCW) ist ein leistungsstarkes Tool, das zeitraubende System- und Desktopverwaltungsaufgaben automatisiert. Es hilft Ihnen dabei, die IT-Umgebung zu optimieren und mit Hilfe effektiver Energieverwaltungsfunktionen Kosten und Ressourcen zu sparen.

NCW bietet erweitertes Schwachstellen-Management in Verbindung, eine Erweiterung des nutzerfreundlichen, zentral verwalteten und richtlinienbasierten Norman Patch and Remediation.

Weitere Informationen erhalten Sie unter www.norman.de.

SYSTEM VORAUSSETZUNGEN

Server: Windows Server 2003 mit Microsoft SQL Server 2005 und .NET Framework, 2008 nur englische Betriebssysteme

Agentenschutz:

Apple Mac OS X,
Hewlett Packard HP-UX,
IBM AIX, Novell SUSE Linux,
RHEL, Sun Solaris
Windows: 98, NT, 2000, XP, Vista
Windows Server:
2003, 2003 R2, 2008, 2008 R2

UNTERSTÜTZTE SPRACHEN

Chinesisch (traditionell)
Chinesisch (vereinfacht)
Dänisch
Deutsch
Englisch
Finnisch
Französisch
Italienisch
Japanisch
Koreanisch
Niederländisch
Norwegisch
Portugiesisch
Schwedisch
Spanisch



So funktioniert Norman Patch and Remediation:

1. **Erkennung** von Sicherheitslücken in Anwendungen, Betriebssystemen und Konfigurationen auf verwalteten Endgeräten durch umfassende agentenbasierte Überprüfung.
2. **Erstellung eines Profils** über jeden Patch einschließlich Software, Hardware, Treiber sowie vorhandener und fehlender Patches für jedes Gerät.
3. **Beseitigung** von Sicherheitslücken und zeitnahe Nutzung verfügbarer Patches, die auf definierten Richtlinien basieren.
4. **Reporting** zu betrieblichen, verwaltungstechnischen und Compliance-Aktivitäten.

Kundenmeinung:

„Seit wir dieses Produkt eingeführt haben und die zentrale Verwaltungsfunktion nutzen, waren wir keinen größeren Virenangriffen mehr ausgesetzt. Wichtige Patches können schnell auf alle Geräte in unserem dezentralisierten Netzwerk angewendet werden.“

Wichtige Funktionen

- ▶ **Detaillierte Erfassung und Beurteilung aller IT-Ressourcen:** liefert umfassende Einblicke in die Netzwerksicherheit zur Bestandsaufnahme und Verwaltung von physikalischen und virtuellen Umgebungen; detaillierte Begutachtung von Sicherheitslücken, Patch-Status, Sicherheitskonfigurationen, installierte Software- und Hardware-Bestände
- ▶ **Offene Architektur:** Norman Patch and Remediation unterstützt offene Standards und verschiedene Inhaltsquellen und bietet eine benutzerdefinierte, vielseitige Verwaltungs-Plattform
- ▶ **Unterstützung heterogener Netzwerkeumgebungen:** Überprüfung und Schließung von Sicherheitslücken mit umfassender Unterstützung aller gängigen Betriebssysteme (Windows, Linux, MacOS, Sun Solaris, HP usw.), OSIX und Infrastrukturgeräte – all das von einer einzigen Konsole aus
- ▶ **Multi-Patch-Bereitstellungen:** Bereitstellung mehrerer Patches für mehrere Computer in einer Verteilung
- ▶ **Automatisches Reporting:** Email-Benachrichtigungen können an Administratoren gesendet werden, um diese auf Probleme aufmerksam zu machen (einschließlich Abonnementfehler, Probleme bei der Fehlerbehebung oder bald ablaufende Lizenzen)
- ▶ **Umfassende Aktionen zur Fehlerbehebung:** im Rahmen der Kontrolle auf Sicherheitslücken wird Folgendes überprüft: Sicherheitskonfigurationen, Sicherheitslücken im Betriebssystem und Anwendungen, ungültige Passwörter, Sicherheitslücken in der Patch-Ebene, bekannte Hacker-Tools, Malware, verbreitete Würmer und P2P-Software
- ▶ **Umfassendes Reporting:** über 20 Standard-Berichte mit detaillierten Informationen zur Verwaltung von Patch and Remediation, einschließlich Richtlinienstatus, Sicherheitslücken, Ressourcenbestand und mehr
- ▶ **Hochgradig skalierbar:** komplette Absicherung weltweiter Netzwerke mit Hochverfügbarkeits-Strukturen und Verteilungspunktarchitektur; Pakete werden lokal zwischengespeichert, so dass der Netzwerkverkehr minimiert und die Bandbreitennutzung optimiert wird
- ▶ **Rollen- und richtlinienbasierte Verwaltung:** stellt sicher, dass all Ihre Systeme eine obligatorische Baseline-Richtlinie erfüllen – einen Schlüsselaspekt der Unternehmenssicherheit
- ▶ **NAC-Unterstützung:** Bewertet automatisch Endgeräte, die versuchen, auf das Netzwerk zuzugreifen; nimmt entsprechende Korrekturen vor, bevor der Zugriff gewährt wird



Norman zählt zu den führenden Unternehmen und Pionieren für die Entwicklung proaktiver Lösungen zur Absicherung von Unternehmensdaten und für die Entwicklung von Forensik-Tools zur Malware-Erkennung. Die Produkte von Norman schützen Endanwender und Netzwerke in Unternehmen jeder Größenordnung vor Malware und ermöglichen die Analyse von Schadcode. Norman wurde im Jahr 1984 in Oslo gegründet und vertreibt die Produkte weltweit über eigene Niederlassungen und ein ausgedehntes Partnernetz.

www.norman.de

Norman SandBox® US Patent Number 7,356,736

NORMAN®