



# Umfassende Endpoint Security über eine einzige Konsole

Sicherung sämtlicher Endgeräte ohne Verlust der zentralen IT-Kontrolle.

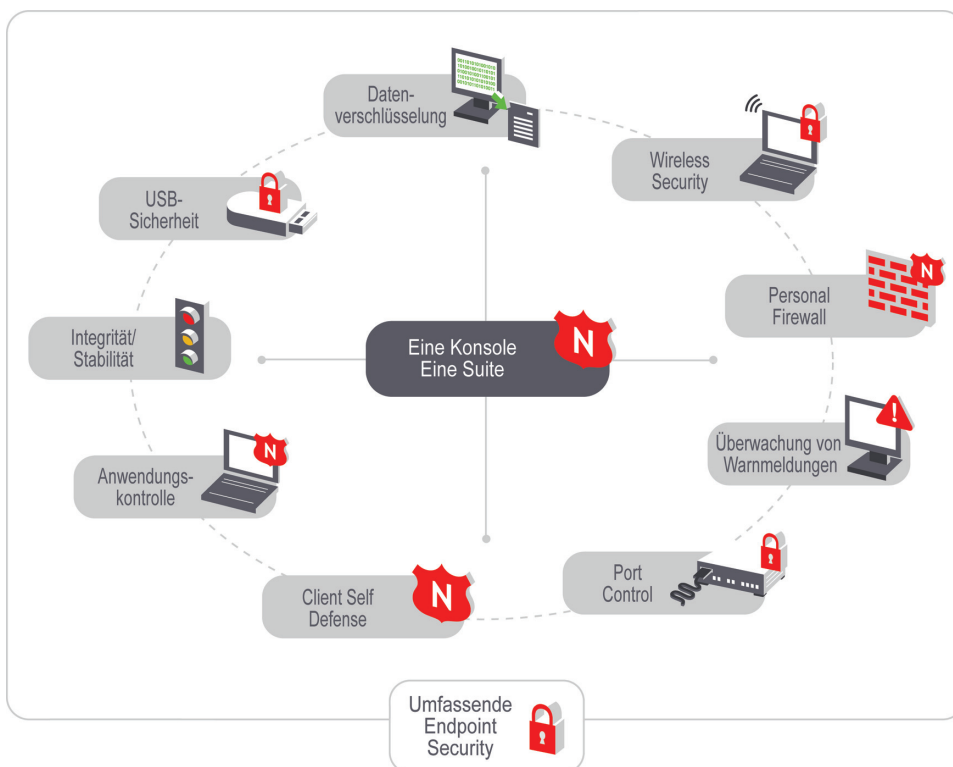


Abbildung 1: Sichern Sie von einer einzigen Konsole aus mit Novell ZENworks Endpoint Security Management den Sicherheitsbereich jedes Netzwerkendpunktes.

## Einfache, zentrale, umfassende Sicherheit für Ihre drahtgebundenen und drahtlosen Netzwerkendpunkte

Gehen Sie beim Thema Endpoint Security auf Nummer sicher und übertragen Sie diese Verantwortung nicht auf Ihre Anwender. Zu viele Unternehmen verlassen sich darauf, dass ihre Mitarbeiter die eigene Firewall konfigurieren, für den eigenen Virenschutz sorgen und den eigenen VPN-Client

verwenden, wenn sie sich außerhalb des Büros befinden. Aber Anwender sind weder qualifiziert noch zuverlässig genug, um derartige Sicherheitsentscheidungen treffen zu können. Sie mögen zwar die Programme, mit denen sie tagtäglich arbeiten, in- und auswendig kennen, haben aber nicht die geringste Ahnung, was passiert, wenn sie in einer Sicherheitsanwendung auf OK klicken.

### ■ Lösungen:

Endpoint Security Management

### ■ Produkte:

Novell ZENworks Endpoint Security Management



„Der Versuch, verwaltungsfreundliche Endpoint Security-Lösungen für heterogene IT-Umgebungen – einschließlich mobiler und Wireless-Clients – anzubieten, endet bei den meisten Anbietern in einem regelrechten Flickwerk aus verschiedensten Technologien. Novell dagegen bringt jetzt eine innovative Architektur auf den Markt, die umfassende und automatisierte Verwaltung und Durchsetzung von Sicherheitsrichtlinien auf allen Clients ermöglicht.“

**Charles Kolodgy**

Research Director  
IDC, Juni 2007



Lassen Sie Ihre Benutzer sorgenfrei arbeiten.  
Übertragen Sie die Verantwortung für  
Endpoint Security auf Ihre IT-Administratoren.  
Novell bietet richtlinienbasierte Lösungen für  
jeden Aspekt der Desktop- und mobilen  
Sicherheit, von den Außenbereichen des  
Netzwerkperimeters bis hin zum Kern.  
Und das Ganze mit nur einer einzigen  
benutzerfreundlichen Managementkonsole.

Laut einer Studie des Ponemon Institute im Jahr 2006 zum Thema „Kosten von Sicherheitsverstößen“ gaben Unternehmen im Durchschnitt 5 Millionen US-Dollar aus, um verlorene Daten oder gestohlene Daten wiederherzustellen, wobei für jeden betroffenen Kundendatensatz im Durchschnitt Kosten in Höhe von 182 US-Dollar anfielen. In 49 Prozent der Fälle war der Grund für den Datenverlust der Diebstahl eines Notebooks, Desktops, PDAs oder USB-Laufwerks.

Nur der Sicherheitsadministrator verfügt über die Expertise und weiß beispielsweise, welche Konsequenzen es hat, wenn eine bestimmte Anwendung Zugriff auf das Netzwerk erhält oder wenn ein bestimmter Port für eingehenden Datenverkehr geöffnet wird. Wenn Sie Anwendern erlauben, diese Entscheidungen zu treffen, ist das Chaos in Ihrem Unternehmensnetzwerk sozusagen vorprogrammiert.

Novell ZENworks Endpoint Security Management bietet IT-Sicherheitsexperten vollständige Kontrolle über die Desktopsicherheit. Die umfassenden, richtliniengestützten Lösungen werden von einer einzigen Konsole aus verwaltet und decken alle Aspekte von Endpoint Security ab.

Die Lösungen können den Anforderungen entsprechend individuell implementiert werden oder als vollständig integrierte Suite komplette Endpoint Security ermöglichen – von den Außenbereichen des Netzwerkperimeters bis hin zum Kern.

#### **Personal Firewall**

Novell bietet eine der weltweit sichersten und zugleich benutzerfreundlichsten Firewalls zum Schutz vor Hackern, Malware, protokollspezifischen Angriffen u. v. m. Schützen Sie Ihre Anwender, ohne dass diese etwas davon bemerken oder etwas dafür tun müssten. Die Lösung von Novell unterscheidet sich von den typischen Personal Firewalls dahingehend, dass sie nicht nur auf der Anwendungsebene oder als Firewall-Hook-Treiber agiert, sondern

in den NDIS-Treiber (Network Driver Interface Specification) jeder Netzwerkschnittstellenkarte integriert ist. Dies sorgt für optimale Leistung und gleichzeitig wird unerwünschter Datenverkehr bereits im Ansatz blockiert. Unsere Adaptive Port Blocking-Technologie bietet Ihnen unübertroffenen Schutz vor protokollbasierten Angriffen, darunter beispielsweise unbefugte Port-Scans sowie SYN Flood-, NetBIOS- und DDOS-Attacken. Entscheiden Sie standortabhängig anhand von IP- oder MAC-Adressen, ob ein bestimmter Host vertrauenswürdig ist. Zudem können Sie Netzwerkstrukturen einbeziehen, die bestimmte Übertragungstypen nutzen, wie beispielsweise IP-Multicast, ARP, ICMP und 802.1x.

#### **Wireless Security**

Kontrollieren Sie zentral, wann, wie und wo Benutzer Verbindungen herstellen dürfen. Unbefugte Zugriffe werden nicht nur entdeckt, sondern rund um die Uhr an allen Standorten vollständig verhindert. Wi-Fi-Verbindungen lassen sich auf autorisierte und bekannte Zugriffspunkte oder eine bestimmte festgelegte Verschlüsselungsstärke beschränken und können bei Bedarf standortabhängig sogar ganz unterbunden werden. Kontrollieren Sie ohne Probleme Schlüssel, MESH- und WiMAX-Umgebungen. Setzen Sie je nach Richtlinie die Verwendung eines VPN durch u. v. m.

Mit all diesen Funktionen haben Sie die vollständige Kontrolle über sämtliche Wi-Fi-Verbindungen – und brauchen sich über Hacker keine Gedanken mehr zu machen. Benutzer können überall und zu jeder Zeit ihrer Arbeit nachgehen, ohne dass sie dabei eigene Sicherheitsentscheidungen treffen oder Sicherheitsschlüssel eingeben müssten.

#### **Gerätesteuerung**

Für optimale Sicherheit und Leistung wird die Gerätesteuerung auf den untersten Ebenen verwaltet, wobei über LAN, Modem, Bluetooth, Infrarot-Anschluss, 1394 (Firewire) sowie serielle und parallele Anschlüsse hergestellte Verbindungen sicher kontrolliert werden.

## Umfassende Endpoint Security über eine einzige Konsole

[www.novell.com](http://www.novell.com)

### Datenverschlüsselung

Die Verschlüsselungslösung sichert auf Endgeräten und Wechselmedien gespeicherte Daten, sodass diese nur von autorisierten Benutzern gelesen werden können. Auf diese Weise werden vertrauliche Daten auf verloren-gegangenen oder gestohlenen Notebooks geschützt. Die Verwaltung der Schlüssel wird unternehmensweit transparent gehandhabt und erfordert keinerlei Eingreifen seitens der Anwender.

### USB-Sicherheit

USB-Sicherheit sorgt dafür, dass Daten nicht vorsätzlich oder unbeabsichtigt auf Wechselspeichermedien übertragen werden. Speichergeräte wie USB-Sticks, iPods, Kameras, Drucker, CD- und DVD-Laufwerke können mit Schreibschutz versehen oder ganz deaktiviert werden, während die Festplatte des Endgerätes und alle Netzlaufwerke zugänglich und betriebsbereit bleiben. Sie haben die Möglichkeit, White Lists für genehmigte USB-Sticks zu verwenden und diese mit Datenverschlüsselung zu kombinieren. Es gibt keinen besseren Schutz vor internen und externen Datenverlusten – sei es nun vorsätzlich oder unbeabsichtigt dazu gekommen.

Zur Einhaltung von Unternehmensrichtlinien und staatlichen Verordnungen können Sie den Zugriff auf lokale Speichergeräte, die ohne Erstellung eines Audit-Protokolls Daten kopieren, erlauben, blockieren oder einschränken. Erstellen Sie Genehmigungen, die flexibel durchgesetzt werden und auf automatisierten Richtlinien basieren, die den Standort des Benutzers oder sogar die Seriennummer des Gerätes berücksichtigen. Falls Sie beispielsweise Schreibzugriff auf ein Wechselspeichergerät erlauben, haben Sie die Möglichkeit, automatisch detaillierte Warnmeldungen und Berichte zu jeder Datei, die auf dieses Gerät übertragen wurde, zu erstellen.

Im Gegensatz zu anderen Lösungen ermöglicht Novell die Kontrolle auf Speichergerät- und Dateisystemebene. Somit werden Geräte, die keine

Sicherheitsbedrohung darstellen (wie eine USB-Maus oder eine USB-Tastatur), nicht blockiert und können störungsfrei verwendet werden. Sie können sogar mehrere Funktionen, die sich einen einzigen USB-Anschluss teilen, unabhängig voneinander verwalten.

### Anwendungskontrolle

Die Anwendungskontrolle gewährleistet, dass nur zulässige Anwendungen auf den IT-Ressourcen des Unternehmens ausgeführt werden. Erstellen Sie White oder Black Lists oder erzwingen Sie vor dem Herstellen einer Netzwerkverbindung die Ausführung bestimmter Anwendungen wie beispielsweise VPNs.

### Stabilität und Integrität

Stellen Sie sicher, dass auf den Desktops Ihrer Mitarbeiter rund um die Uhr, sowohl mit als auch ohne Netzwerkverbindung, Virenschutz-, Spyware-Software oder andere Programme gemäß den Richtlinien ausgeführt werden. Sorgen Sie dafür, dass Sicherheitspatches für das Betriebssystem sowie Virenschutzdateien und andere kritische Sicherheitselemente stets vorhanden und aktuell sind. Basierend auf von Ihnen definierten Auslösern können Sie Services warnen, abschalten oder Maßnahmen gegen sie ergreifen oder auch ein benutzerdefiniertes Skript ausführen lassen.

### Client Self Defense

Die Client Self Defense-Lösung schützt den Endpunkt, indem sichergestellt wird, dass der Sicherheits-Client nicht modifiziert, von Hackern geknackt oder deinstalliert werden kann. Selbst mit Administratorrechten kann ein Benutzer nicht die Durchsetzung der Richtlinien deaktivieren. Je nach Netzwerkstandort des Endpunkts zu einem bestimmten Zeitpunkt werden vom Security Client:

- richtlinienbasierte Filter für ein- und ausgehenden Datenverkehr implementiert.
- richtlinienbasierte Kontrollen der verwendeten Hardware, wie z. B. Wireless Access Points, Wechselmedien und Netzwerkadapter, implementiert.

**Aufrechterhaltung der Integrität von Sicherheitseinrichtungen**  
Sicherheitsadministratoren definieren Integritätsstandards und können mithilfe der Softwarelösung jeden Endpunkt in Echtzeit auf die Einhaltung dieser Standards überprüfen. Dadurch wird beispielsweise gewährleistet, dass Virenschutz-, Backup-, Audit- und andere Prozesse richtliniengemäß funktionieren. Tritt an einem Endpunkt ein Sicherheitsverstoß auf, können Sie eine Reihe von Gegenmaßnahmen ergreifen, die von Quarantäne über Sperrung bis hin zu erweiterter Berichterstattung und Überprüfungsmechanismen reichen, selbst wenn der Endpunkt zu diesem Zeitpunkt nicht mit einem Netzwerk verbunden war.

Kontrollieren Sie alle Ihre Endpunkte mithilfe zentraler Richtlinien –  
zu Hause, im Büro oder unterwegs.

[www.novell.com](http://www.novell.com)

- *Berichtsdaten erfasst.*
- *Sicherheitsanwendungen gemäß Richtlinien, die für bestimmte Situationen festgelegt wurden, ausgeführt.*

Damit diese Funktionen nicht deinstalliert, modifiziert oder deaktiviert werden und sensible Daten somit in falsche Hände geraten könnten, verfügt die Client Defense-Lösung über folgende Sicherheitsmechanismen:

- *Zur Deinstallation des Clients ist entweder ein Passwort oder ein von einem IT-Administrator erstelltes Installationspaket erforderlich.*
- *Zum Anhalten/Beenden eines Service ist gemäß der definierten Richtlinie ein Passwort erforderlich.*
- *Windows Task Manager-Anfragen zur Terminierung von Sicherheitsprozessen sind nicht zulässig.*

- *Überwachung und Schutz kritischer Dateien, Schlüssel und Registry-Werte gegen ungültige Änderungen.*
- *Es wird gewährleistet, dass der NDIS-Filtertreiber an die Netzwerkkarte gebunden ist.*

### **Alerts/Monitoring/Reporting**

Alerts/Monitoring/Reporting bietet ein skalierbares, einfaches Verfahren zur Erstellung, Verteilung, Durchsetzung und Überwachung von Sicherheitsrichtlinien auf Endgeräten, ohne dass Benutzer gezwungen werden, Sicherheitsentscheidungen zu fällen oder Einstellungen anzupassen.

Die Berichterstellung über die Einhaltung von Richtlinien wird dabei wirkungsvoll von den robusten und anpassbaren Berichterstellungsfunktionen von Senforce unterstützt.



### **Novell Services**

Informationen zu den Novell Services wie Consulting, Training und Support erhalten Sie im Internet unter:

[www.novell.com/consulting](http://www.novell.com/consulting)  
[www.novell.com/training](http://www.novell.com/training)  
[www.novell.com/support](http://www.novell.com/support)

### **Weitere Informationen**

Informationen zu Novell Produkten erhalten Sie beim Novell Fachhandelspartner oder besuchen Sie uns im Internet unter: [www.novell.com/products](http://www.novell.com/products)

### **Novell GmbH**

Nördlicher Zubringer 9-11  
40470 Düsseldorf  
Tel: +49-(0)211-56 31-0  
Fax: +49-(0)211-56 31-250  
[www.novell.de](http://www.novell.de)

### **Novell GmbH**

Heiligenstädter Lände 27c  
A - 1190 Wien  
Tel: +43-(0)1-367 74 44  
Fax: +43-(0)1-367 74 44 20  
[www.novell.at](http://www.novell.at)

### **Novell (Schweiz) AG**

Leutschenbachstrasse 41  
CH - 8050 Zürich  
Tel: +41-(0)43-299 78 00  
Fax: +41-(0)43-299 75 01  
[www.novell.ch](http://www.novell.ch)