



Datenblatt

Outpost Network Security 3.2

Überblick

In diesen Zeiten der wirtschaftlichen Herausforderungen stehen Zuverlässigkeit, Leistungsfähigkeit und Kosteneffizienz für Unternehmen beim Kauf von Sicherheits-Softwarelösungen ganz oben auf der Prioritätenliste. Outpost Network Security 3.2 (ONS 3.2) ist eine kluge Wahl, wenn es darum geht, Kosten zu senken und gleichzeitig eine solide Netzwerksicherheit sicherzustellen. Niedrige Kosten pro Arbeitsplatz, einfache Installation, Verwaltung und Konfiguration, eine solide Leistung mit minimaler Ressourcenbelastung, hohe Flexibilität und zahlreiche Anpassungsoptionen vereint mit preisgekrönten Technologien machen ONS 3.2 zur perfekten Software-Lösung für den Schutz des digitalen Eigentums Ihres Unternehmens.

Mit Outpost Network Security 3.2 ist Ihre Organisation umfassend gegen alle möglichen Arten von Sicherheitsbedrohungen geschützt: gegen Hacker, Betriebsunterbrechungen und Stillstandszeiten, Viren und Malware, Angriffe per E-Mail und aus dem Internet, Datenverluste und unzulässige Internet-Nutzung. Die zentralen Verwaltungsfunktionen sorgen für einen benutzerfreundlichen, reibungslosen Endpunkt-Schutz für jede Organisation mit begrenzten firmeneigenen IT-Mitteln.

Die Sicherheitsherausforderung für kleine und mittlere Unternehmen

Wirtschaftlich turbulente Zeiten haben einen exponentiellen Anstieg der Angriffe auf elektronische Kommunikationswege und andere wertvolle Daten mit sich gebracht, so dass Unternehmen gezwungen sind, den Schutz ihrer unternehmenskritischen Datenbestände zu überdenken. Sicherheitslücken in Software bereiten den Weg für Zero-Day-Angriffe durch Malware sowie für Datendiebstahl, also müssen Unternehmen diese Bedrohungen minimieren, bevor ein Angreifer sie ausnutzen kann. Gleichzeitig steigt die Zahl von mutierenden und polymorphen Viren, die mit herkömmlichen, signaturbasierten Methoden nicht entdeckt werden, sprunghaft an, und auch hoch entwickelte Rootkits und Trojaner erfordern den Einsatz neuer und intelligenterer Reaktionsmechanismen. Und natürlich ist der Mensch selbst nach wie vor der größte Einzelschwachpunkt jeder Sicherheits-Infrastruktur, wenn etwa Nutzer unpassende Websites besuchen, vertrauliche Daten auf USB-Speichermedien aus dem Unternehmen bringen und die Inhalte dann verkaufen oder verlieren. Die verbreitete und unzulässige Nutzung von sozialen Netzwerken, Online-Videos und Chat-Websites verschlimmert die Situation noch zusätzlich.

Während die Anwender die Sicherheitskontrollen auf Endpunkt-Ebene auf die Probe stellen, stehen diejenigen, die als IT- oder Sicherheits-Administratoren agieren müssen, vor der nahezu unmöglichen Aufgabe, deren Schutz jeweils richtig zu konfigurieren und auf dem neuesten Stand zu halten, um auch die aktuellsten Bedrohungen abwehren zu können. Selbst Firmen mit ein paar Dutzend PCs benötigen eine zentralisierte Möglichkeit, die Schutz-Lösung zu installieren, zu konfigurieren und per Fern-Verwaltung zu steuern, ohne jeden einzelnen Arbeitsplatz täglich aufsuchen zu müssen - oder Informatik studiert haben zu müssen.

Die Software-Lösung ONS 3.2

Auf einen Blick

Outpost Network Security schafft eine sichere Umgebung im gesamten Netzwerk, vom Endpunkt bis hin zum Server. Seine automatisierten Schutz-Tools laufen auf den Client-Rechnern im Hintergrund-Betrieb, schützen die Endpunkte vor den neuesten Bedrohungen und gewährleisten, dass sich Malware nicht innerhalb des Netzwerks und darüber hinaus verbreiten kann. Der Client-Schutz wird von einer einzigen Verwaltungskonsole aus installiert, auf die von jedem Computer aus zugegriffen werden kann, so dass der Administrator den Schutz des Arbeitsplatzrechners per Fern-Verwaltung steuern kann. Die Konfiguration, das Ausführen von Sicherheitsaufgaben und die Aktualisierung der Client-Software können alle von einem einzigen Ort aus durchgeführt werden.

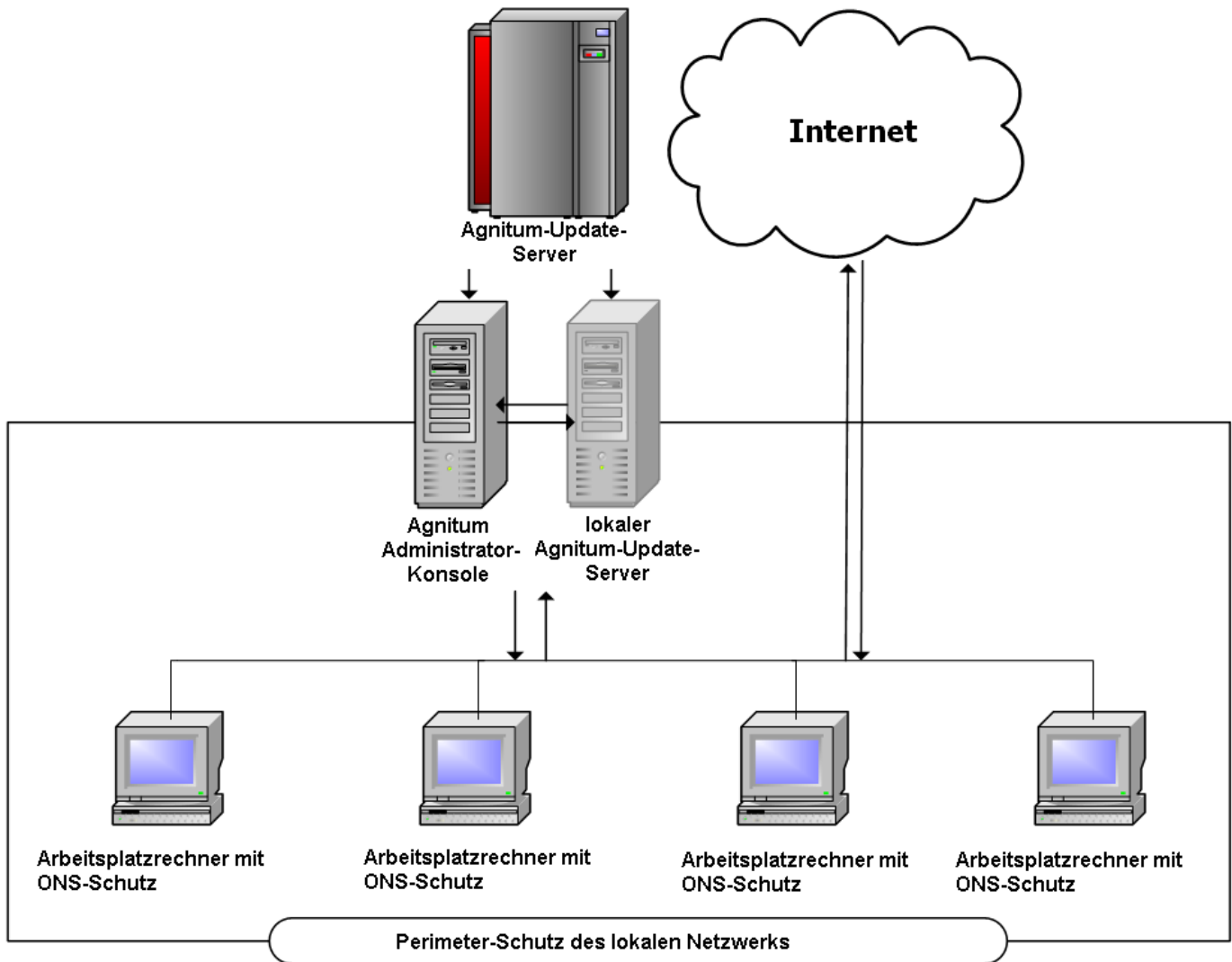
Outpost Network Security ist die ideale Wahl für Organisationen mit:

- Netzwerken mit 5 bis 500 PCs
- Mitarbeitern, die mobil, per Telearbeit oder auf Reisen tätig sind
- mehreren Niederlassungen
- begrenztem Budget.

Schwerpunkte des ONS-Schutzes

- Automatisierter Viren- und Spyware-Filter kontrolliert die Endpunkt-Sicherheit in Echtzeit
- On-Demand-Sicherheitsscanner überprüft Remote-Rechner auf Malware
- Bidirektionale Firewall überwacht Verbindungen und schützt vor internen und externen Netzwerk-Angriffen
- USB-Sperre hält die Firmendaten unter Ihrer Kontrolle und verhindert Datenlecks
- Der System-Wächter ermöglicht es dem Administrator, eine Liste der zu schützenden Programme auf dem System sowie umfassender Windows-Einstellungen und Konfigurationsdateien zu erstellen.
- Web-Kontrolle gewährleistet, dass Anwender nicht auf gefährliche oder eingeschränkte Websites zugreifen können
- Verhinderung von Identitätsdiebstahl schränkt die Übertragung vordefinierter Textblöcke wie z. B. von Passwörtern und Kreditkartennummern ein
- Selbstschutz verhindert, dass Malware den Endpunkt-Schutz unbefugt beendet
- Überwachung der Prozess- und Netzwerk-Aktivitäten verfolgt Fern-Ereignisse in Echtzeit nach
- Fern-Protokolle ermöglichen Überprüfung der Aufzeichnungen vergangener Aktivitäten

Outpost Network Security 3.2 schützt die digitalen Perimeter Ihrer Organisation



Vorteile von Outpost Network Security 3.2

Keine Sicherheits-Zwischenfälle

Informationen zählen zu den wertvollsten Aktiva innerhalb eines Unternehmens. Outpost gewährleistet die Integrität Ihrer Daten durch eine Reihe solider Sicherheitsmechanismen:

- **Virenschutz zur Gewährleistung einer malwarefreien Umgebung**

Die VB100-zertifizierte Engine, bestehend aus Virenschutz und Spyware-Schutz, schützt dauerhaft vor schädlicher Software, die intern auftritt (etwa durch den Empfang als E-Mail-Anlage) oder extern erhalten wird (z.B. durch Ausbreitung durch einen infizierten USB-Flash-Speicher). Die Bedrohung wird umgehend neutralisiert, bevor sie anderen Rechnern im Netzwerk schaden kann. Remote-Virenskans und zentralisierte On-Demand-Virenskans können jederzeit an gewählten Endpunkten gestartet werden.

- **Zweiwege-Firewall zum Schutz der LAN-Verbindung**

Die preisgekrönte Firewall-Technologie gewährleistet die Sicherheit und den störungsfreien Betrieb Ihres Unternehmensnetzwerks. Outpost Network Security umfasst ein einzigartiges Angriffserkennungs-System, um den Datenverkehr vor Lauschangriffen zu schützen, eine Filterung auf Paket- und Anwendungsebene, um unerwünschte oder schädliche Verbindungen zu blockieren und einen eingebetteten Code-Schutz, um angreifbare Web-Elemente zu stärken und ist damit die ultimative Abwehr gegen alle Datensicherheits-Risiken und Hackerangriffe.

- **System-Wächter**

Der System-Wächter ermöglicht es dem Administrator, eine Liste der zu schützenden Programme auf dem System sowie umfassender Windows-Einstellungen und Konfigurationsdateien zu erstellen. Alle Programme, die als geschützt gekennzeichnet wurden, werden vom System-Wächter vor unbefugter Manipulation oder Gefährdung geschützt.

- **Web-Kontrolle**

Jetzt können Administratoren Endpunkte so konfigurieren, dass der Zugriff auf nicht autorisierte Websites nach bestimmten Schlüsselwörtern in der URL oder im Text der Seite blockiert wird.

- **Sperrung des USB-Zugriffs zur Sicherung des digitalen Eigentums von Unternehmen**

Es besteht immer die Gefahr, dass Ihre internen Daten kopiert werden und aus dem Unternehmen gelangen. Outpost Network Security blockiert den Zugriff auf USB-Massenspeicher auf den Ziel-Hosts, so dass ein unbefugtes Durchsickern von Unternehmensdaten und die Verbreitung von Malware durch das Anschließen von Flash-Speichern verhindert werden.

Müheleose Einführung und Installation und automatische Updates

- **Zentralisierte Einrichtung zur Minimierung des IT-Arbeitsaufwands**

Mit intuitiven Tools, die die Domänenstruktur des Unternehmensnetzwerks darstellen, kann eine Sammel-Installation und -Einrichtung innerhalb kürzester Zeit durchgeführt werden.

- **Online- und Offline-Updates zur Aktualisierung des Schutzes**

Sicherheits-Updates für mit dem Intranet verbundene Rechner werden täglich von einem einzigen Netzwerk-Speicherort aus durchgeführt, z.B. vom Agnitum-Server, einem lokalen Update-Server oder einem lokalen Ordner mit aktualisierten Datenbanken.

Zentralisierte Verwaltung und Einrichtung

- **Gruppensegmentierung für einen gezielteren Schutz**

Verbundene Computer können in mehrere Gruppen aufgeteilt werden, von denen jede ihre eigenen Sicherheitsrichtlinien hat. Das trägt dazu bei, die zu schützenden Teilnehmer einfacher zu verwalten und gezielter zu schützen und darüber hinaus gefährdeteren Gruppen (z.B. einer Gruppe mobiler Anwender, die sich unterwegs mit Dritt-Netzwerken verbinden) strengere Richtlinien zuzuweisen.

- **Fern-Konfiguration für eine einfache, praktische Verwaltung**

In der neuen Version von Outpost Network Security können miteinander verbundene Computer von jedem verbundenen Arbeitsplatz-Rechner aus durch eine universelle Management-Konsole verwaltet werden. Administratoren können benutzerdefinierte Internetzugriffs-Richtlinien zuweisen und Blacklists mit URL-Adressen festlegen, auf die im Netzwerk nicht zugegriffen werden darf.

Verbesserte Einsicht in Remote-Ereignisse

- **Echtzeit-Kontrolle der Endpunkt-Aktivitäten für vollständige Transparenz**

Wenn Ihr Netzwerk einmal eingerichtet ist, ist es schwierig, die Ereignisse auf den einzelnen Rechnern zu kontrollieren. Outpost umgeht diese Einschränkung, indem es eine Echtzeit-Überwachung der System- und Netzwerk-Aktivitäten für jeden Remote-Hostrechner bietet. Mit diesem nützlichen Tool können Administratoren sehen, auf welche Websites zugegriffen wird oder welche Programme aktuell auf jedem Computer im Netzwerk aktiv sind. So sind sie in der Lage, vorhandene Zugriffs-Richtlinien für die Ziel-Hostrechner schnell zu bearbeiten.

- **Remote-Protokollierungssystem für einen besseren Einblick in frühere Aktivitäten**

Die Remote-Protokollierung von Outpost zeigt den Verlauf aller vergangenen Ereignisse auf den Remote-Rechnern an und ermöglicht es den IT-Verantwortlichen so, ein Problem schnell zu finden und zu beheben, ohne ihren Arbeitsplatz zu verlassen.

Leichtgewichtiger Schutz im Dauerbetrieb

- **Schnellerer, ressourcenfreundlicher Betrieb für einen reibungsloseren Schutz mit SmartScan 3**

Dank zahlreicher Optimierungen und einzigartiger, leistungssteigernder Technologien wird der Client-Schutz von Outpost im Hintergrund ausgeführt, ohne grundlegende System-Ressourcen zu beanspruchen. Die Sicherheitsüberprüfungen werden bis zu zehnmal schneller durchgeführt als die einiger Konkurrenzprodukte.

- **Verhinderung eines unbefugten Beendens, um die Schutzkontinuität zu gewährleisten**

Der Outpost-Schutz der Arbeitsplatz-Rechner kann nicht durch gezielte Angriffe zur Beendigung deaktiviert werden, d.h. Ihre vernetzten Clients sind rund um die Uhr geschützt.

Universal-Kompatibilität

- **Moderne Software- und Hardware-Unterstützung für erweiterte Einsatzmöglichkeiten**

ONS 3.2 bietet eine optimierte Unterstützung für die 32- und 64-Bit-Versionen aller aktuellen Windows-Plattformen, einschließlich Windows 7, Windows Vista SP2, Windows Server 2008 und Windows Server 2008 R2.

Outpost Network Security 3.02 – Merkmale

Datensicherheit und Geheimhaltung

- **Leistungsstarker Malware-Schutz**

Outpost Network Security bietet umfassenden Schutz gegen alle Arten von Malware-Bedrohungen, einschließlich Viren, Spyware, Trojanern und Internetwürmern. Es schützt die Arbeitsplatzrechner Ihres Unternehmens rund um die Uhr, unabhängig vom Erfahrungsgrad der Anwender. Neu! Der automatisierte Hintergrund-Scanner verhindert einen Malware-Befall in Echtzeit, während der zentralisierte On-Demand-Dateiscanner die einzigartige Technologie SmartScan 3 von Agnitum verwendet, um eine schnelle und effiziente Erkennung und Bereinigung aller Datenspeicherbereiche – lokal, Remote und gemeinsam genutzt – zu erreichen. Ein IT-Administrator kann einen beliebigen Remote-Scan auf jedem ausgewählten Arbeitsplatzrechner ausführen (vorausgesetzt, die Verwaltungskonsole ist dort installiert). Darüber hinaus werden durch die Funktion ‚Geplante Scans‘ die Unternehmens-Computer in regelmäßigen Abständen auf neue Infektionen hin überprüft. Aktualisierte Bedrohungs-Signaturen werden täglich über einen zugewiesenen Punkt in Ihrem Netzwerk verteilt – über den Agnitum-Server, einen lokalen Update-Server oder einen lokalen Ordner mit aktualisierten Datenbanken.

- **Kontinuität des Netzwerk-Betriebs**

Die Client-basierte ONS-Firewall schützt ein- und ausgehende Netzwerk-Verbindungen, filtert den gesamten Datenverkehr nach den vom Administrator festgelegten Zugriffsrichtlinien und blockiert unerwünschte oder schädliche Datenübertragungen. Der einzigartige Ethernet-Schutz schützt vor Man-in-the-Middle-Angriffen, die Netzwerk-Daten abfangen sollen, und gewährleistet so, dass die übertragenen Daten immer den gewünschten Empfänger erreichen.

- **System-Wächter**

Der neue System-Wächter, Nachfolger der vorherigen Komponente Kritische Objekte, schützt kritische System-Speicherorte und die Registrierungsdatenbank und gewährleistet so, dass an diesen entscheidenden Bereichen keine unbefugten Änderungen vorgenommen werden. Der System-Wächter ermöglicht es dem Administrator, eine Liste der zu schützenden Programme auf dem System sowie umfassender Windows-Einstellungen und Konfigurationsdateien zu erstellen. Dabei kann es sich um Registry-Einstellungen, Netzwerk-Eigenschaften, Zugänglichkeit von Host-Dateien, Interaktionen von Adobe Flash- und Reader-Plug-Ins und andere angriffsanfällige Objekte handeln. Alle Programme, die als geschützt gekennzeichnet wurden, werden vom System-Wächter vor unbefugter Manipulation oder Gefährdung geschützt.

- **Sperrung von USB-Geräten**

Um eine Verbreitung von Malware aus externen Quellen sowie das unzulässige Kopieren von internen Unternehmensdaten zu verhindern, können Firmen die Verwendung von USB-Speichergeräten für bestimmte Mitarbeiter einschränken.

- **Internet-Sicherheit**

Das Internet ist heute die Hauptquelle für Bedrohungen der Unternehmenssicherheit. Outpost Network Security sorgt für eine hohe Produktivität und ein niedriges Risiko, indem es die Anzahl von Web-Inhalten, die auf einzelnen Arbeitsplatz-Rechnern ausgeführt oder angezeigt werden dürfen, eingeschränkt. Durch das Blockieren unsicherer Skripte bis hin zur Unterdrückung von unnötigen Internet-Grafiken, Animationen und Werbe-Bannern verhindert ONS Drive-By-Downloads und andere verborgene Angriffe aus dem Internet. Darüber hinaus können Vorgesetzte den Zugriff auf bestimmte unsichere Internet-Domänen auf Anwender-Basis blockieren.

- **Selbstverteidigung gewährleistet Schutz rund um die Uhr**

ONS 3.0 enthält Selbstverteidigungs-Technologien, die jeden Versuch von unbefugten Dritter blockieren, seinen Schutz zu beenden – so wird ein unterbrechungsfreier Schutz sichergestellt.

Kontroll- und Verwaltungsmöglichkeiten

- **Zentralisierte Installation und Administration**

Der Client-Schutz wird von einer zentralen Verwaltungs-Konsole aus ganz einfach durch Auswahl der Ziel-Empfänger installiert. Innerhalb weniger Minuten sind alle zugewiesenen Endpunkte geschützt. Alle nachfolgenden Verwaltungsprozesse können von jedem Arbeitsplatzrechner im Netzwerk aus durchgeführt werden.

- **Segmentierung nach Benutzer-Gruppen**

Durch die Unterstützung von Benutzergruppen können verschiedene Konfigurationen und Zugriffsrichtlinien auf verschiedene Benutzer angewandt werden, je nach dem Grad ihrer Risikoanfälligkeit.

- **Detaillierter Einblick in Remote-Ereignisse**

ONS 3.0 bietet Administratoren einzigartige Möglichkeiten zur Ereigniskontrolle auf Remote-Rechnern in Echtzeit. Die Aktivitäts-Berichte umfassen Informationen wie z.B. aktive Programme und Prozesse, Netzwerk-Adressen, auf die zugegriffen wird und andere aktuelle Statistiken.

- **Umfassende Ereignis-Protokollierung**

Durch die umfassende Protokollierung der vergangenen Aktivitäten an den Endpunkten können Administratoren Verbindungsprobleme schnell und einfach finden und beheben, den Status der Malware-Entfernung anzeigen lassen und auf andere Wartungsinformationen zugreifen.

Systemanforderungen von Outpost Network Security 3.2:

Unterstützte Plattformen:

ONS 3.2 bietet eine optimierte Unterstützung für die 32- und 64-Bit-Versionen aller aktuellen Windows-Plattformen, einschließlich Windows 7, Windows Vista SP2, Windows Server 2008 und Windows Server 2008 R2.

Hardware:

CPU mit 500 MHz oder schneller (X86-/x64-/Multicore), 256 MB RAM, 100 MB freier Festplattenspeicher.

Versionsfortschritte bei Outpost Network Security 3.2

Produkt-Version	Outpost Office Firewall	Outpost Network Security 2.0	Outpost Network Security 3.0	Outpost Network Security 3.2
Firewall für den Schutz von Endpunkt-Verbindungen	ja	ja	ja	ja
Anti-Spyware-Funktion für Malware-Grundschutz	ja	ja	ja	ja
Anti-Virus-Funktion für umfassenden Malware-Schutz	nein	nein	ja	ja
System-Wächter(schützt kritische System-Speicherorte)	nein	nein	nein	ja
Vereinfachter Einsatz durch Cloud-Installation	nein	nein	ja	ja
Fern-ausführbare On-Demand-Malwarescans	nein	nein	ja	ja
Zugriffssperre für USB-Speichergeräte	nein	nein	ja	ja
Web-Kontrolle	nein	nein	nein	ja
Zentral verwaltete URL-Blacklist	nein	nein	ja	ja
Segmentierung in Benutzergruppen für einen gezielteren Schutz	nein	ja	ja	ja
Fernanzeige der Protokolle vergangener Ereignisse	nein	nein	ja	ja
Echtzeit-Überwachung von Endpunkt-Aktivitäten	nein	nein	ja	ja
Unterstützung der Administratoren-Konsole/des Client-Programms für aktuellste Windows-Versionen (Vista und Server 2008)	nein	nein	nein	ja

Probieren Sie es aus!

Um sich selbst davon zu überzeugen, wie einfach Sie Ihr Kleinunternehmen gegen die Bedrohungen von heute und morgen schützen können, gehen Sie auf <http://www.agnitum.de/produkte/netzwerk-sicherheit/> und laden Sie sich eine voll funktionsfähige 30-Tage-Testversion von ONS 3.0 herunter.