

## Outpost Network Security Datenblatt

### Die Sicherheitsherausforderung für kleine Unternehmen

*"Im Laufe des letzten Jahres verringerte sich die durchschnittliche Überlebensdauer eines ungeschützten Netzwerkcomputers von 40 auf 20 Minuten."*

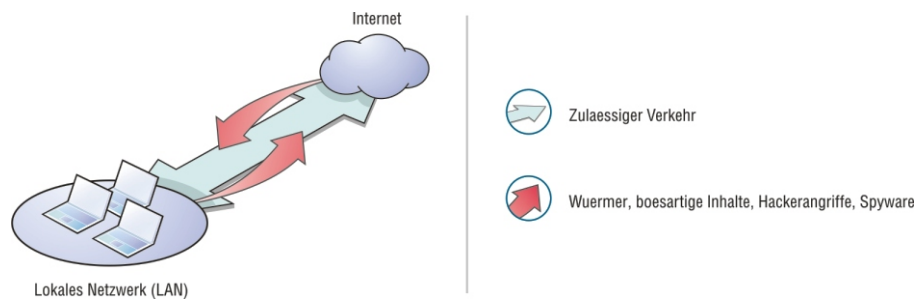
*SANS Institute, Bethesda*

Kleine Unternehmen können sich den Luxus einer eigenen IT-Sicherheitsabteilung meist nicht erlauben, sind jedoch ebenso wie größere Unternehmen auf einen umfassenden und wirksamen Schutz vor der stets wachsenden Bedrohung durch Hacker-Angriffe aus dem Internet, Spyware u. a. angewiesen. Bereits ein einziger Angriff auf eine Windows-Sicherheitslücke – bevor diese im System behoben werden konnte – kann ganze Desktops zerstören und damit schwere finanzielle Einbußen und eine dramatisch verminderte Produktivität nach sich ziehen. Bedrohungen wie Spyware, Würmer, trojanische Pferde, Hacker-Angriffe und andere bösartige Software können ganz unterschiedliche Auswirkungen auf Unternehmen haben – von schlechter PR bis hin zum Verlust kritischer Daten.

Möglicherweise unterschätzen kleine Unternehmen das Erfordernis eines umfassenden Schutzes, in dem Glauben, ihr Unternehmen sei zu klein und unbedeutend, um Ziel solcher Angriffe zu werden. Unglücklicherweise ist durch die von Hackern verwendeten automatischen Tools und Methoden zum Ausfindigmachen anfälliger Computer kein Unternehmen, egal wie groß oder klein, vor diesen Angriffen gefeit.

Bei Endpunkt-PCs, die auf das Internet zugreifen oder über das lokale Netzwerk kommunizieren, erfolgt eine wechselseitige Datenübertragung – Daten werden entweder vom Computer gesendet oder gehen auf diesem ein. Stehen keine geeigneten Datensicherheitsverwaltungstools zur Verfügung, kann nicht kontrolliert werden, welche Daten von wem und wohin übertragen werden.

Und dann gibt es da noch die auf Dienstreisen unverzichtbaren mobilen PCs. Durch Remotverbindungen wird der Computer (wie auch das Netzwerk, wenn der mobile PC nach Ende der Dienstreise wieder an dieses angeschlossen wird) zum Ziel für alle möglichen unerwünschten "Cyber-Besucher".



### Die Lösung

#### Kontrolle:

In einem Unternehmen, in dem die Mitarbeiter über ein unterschiedliches Maß an Computererfahrung verfügen und verschiedene Abteilungen und Benutzergruppen entsprechend den jeweiligen Risikostufen unterschiedlichen Sicherheitsrichtlinien unterliegen, ist ein zentrales Verwaltungstool zur effektiven Kontrolle der Sicherheit von Client-Systemen unabdingbar. So wird gewährleistet, dass die Aufgabe der Endpunktsicherung von dem diesbezüglich qualifiziertesten Mitarbeiter übernommen wird – jemandem, der den Schutz der Clients über eine Art globale „Kommandozentrale“ bereitstellen, verwalten und aktualisieren kann.

#### Schutz:

Herkömmliche Lösungen wie Antiviren- und eigenständige Anti-Spyware-Produkte bieten zwar eine solide Grundlage. Allerdings entstehen heutzutage täglich neue Bedrohungen, sodass sich Unternehmen keinesfalls ausschließlich auf signaturbasierte Erkennungsmethoden verlassen sollten. Diese Art des reaktiven Schutzes muss noch durch proaktive Schutzmechanismen erweitert werden, mit denen potenzielle Probleme isoliert werden können, während der Anbieter neue Signaturen vorbereitet.

#### Flexibilität:

Hardwareanwendungen können zwar effektive Schutzvorrichtungen bieten, lassen sich jedoch schwerer für individuelle Anforderungen konfigurieren und verfügen zudem nicht über die Flexibilitäts-, Kontroll- und Aktualisierungsfunktionen von Softwareanwendungen.

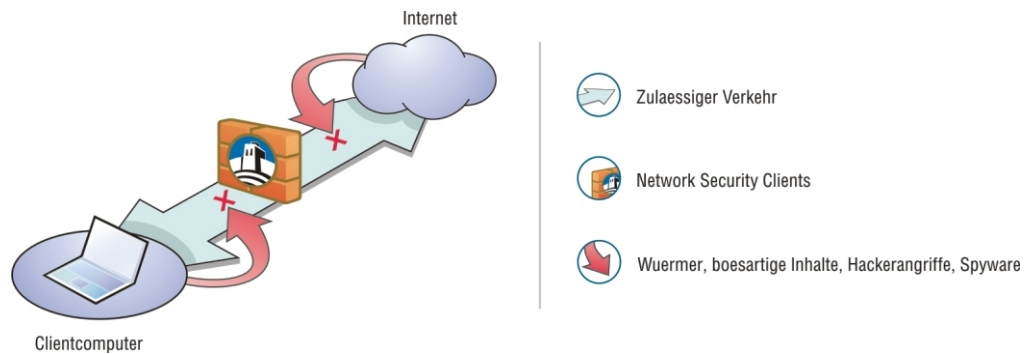
#### Benutzerfreundlichkeit:

Auch die besten Schutzvorrichtungen sind wirkungslos, wenn sie nicht ordnungsgemäß angewendet werden. Lässt sich die Lösung nur schwer konfigurieren, verwalten und warten, führt dies unweigerlich zu Problemen. Eine jährlich vom Computer Security Institute in Zusammenarbeit mit dem FBI durchgeführte Studie zeigt jedes Jahr aufs Neue, dass Unternehmen trotz aller Vorsicht und selbst nach der Einführung scheinbar angemessener Sicherheitsmaßnahmen immer wieder mit Problemen durch Spyware und Viren zu kämpfen haben, weil diese Maßnahmen nicht ordnungsgemäß implementiert wurden.

### Outpost Network Security

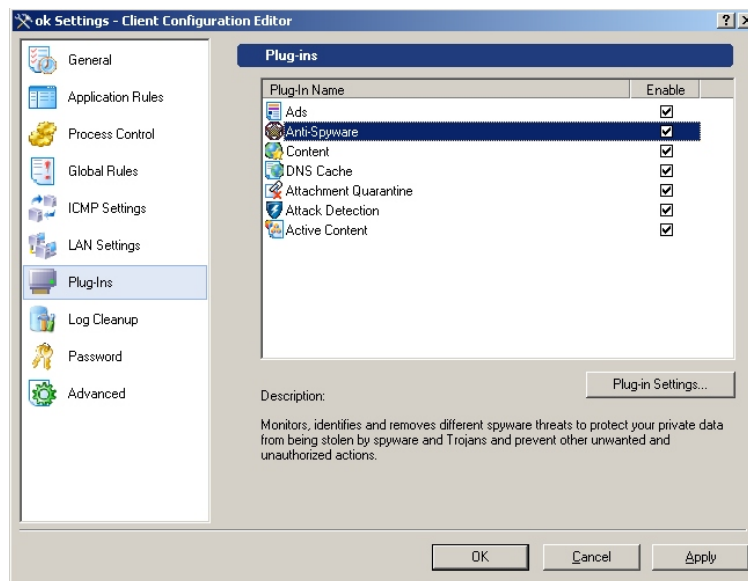
Hier setzt Outpost Network Security (ONS) an und bietet eine Lösung für einen umfassenden Schutz vor den heutigen Sicherheitsbedrohungen, die sich einfach implementieren, verwalten und warten lässt. Outpost Network Security zeichnet sich durch Folgendes aus:

- Bewährter Firewall-Schutz
- Proaktive und reaktive Maßnahmen zum Schutz vor Spyware
- E-Mail-Sicherheit
- Inhaltsfilter



Basierend auf der preisgekrönten Outpost Firewall Pro- und Anti-Spyware-Technologie, dem Ergebnis jahrelanger Erfahrung und umfangreichen Feedbacks von Millionen Benutzern bietet Outpost Network Security eine breite Palette leistungsfähiger Schutzmechanismen für kleine und mittelständische Unternehmen:

- Durch die Ermöglichung einer zentralen Bereitstellung, Verwaltung und Aktualisierung des Client-Schutzes über eine Remoteverbindung von einer einzigen Konsole aus kann mit ONS ein zuverlässiger Endpunktschutz gewährleistet werden, und die Kosten sowie der Ressourcenaufwand können niedrig gehalten werden.
- Mit dem mehrschichtigen Firewall-Schutz von ONS, der leistungsstarke paket- und anwendungs-basierte Filter, Stealth-Technologie, Angriffsschutz, Isolierung von E-Mail-Anhängen und Datenschutz in einer benutzerfreundlichen Aufmachung vereint, werden Clients vor bekannten und unbekanntem Bedrohungen proaktiv geschützt.
- Der integrierte Spyware-Schutz bekämpft Infektionen in jeder möglichen Phase – erster Kontakt, Verseuchung und mögliche ungewollte Datenpreisgabe. Mit Tools wie der stets aktiven Spyware-Überwachung und dem On-Demand-Scanner sowie der Möglichkeit, vertrauliche Daten zu sichern, wird die Bedrohung durch Spyware für Ihr Netzwerk praktisch eliminiert.
- Durch die Gruppenunterstützung können Administratoren die Schutzmaßnahmen individuell auf das Sicherheitsprofil einer jeden Abteilung oder Benutzergruppe abstimmen, unabhängig davon, welches Risikoprofil diese aufweist.
- Mit dem automatischen Agnitum Update Service können Administratoren ein Sicherheitsaktualisierungspaket für einen einzelnen Client herunterladen und es auf allen Workstations installieren. Auf diese Weise wird eine geringere Bandbreite benötigt und Zeit gespart. Durch tägliche Aktualisierungen von Spyware-Signaturen wird sichergestellt, dass die Clientcomputer immer über den neuesten Schutz verfügen.



## Eliminierung von Sicherheitsrisiken

Outpost Network Security bietet umfassenden Schutz für alle Endpunkt-PCs, indem für ausgewählte Workstations im Netzwerk automatisch Client-Firewalls bereitgestellt und konfiguriert werden. Sofort nach der Installation der Firewall werden die Clients durch die Überwachung sämtlicher Datenübertragungen und die Anwendung kommunikationsspezifischer Regeln vor Angriffen geschützt.

### Umfassender Schutz vor Spyware

Der sich stets auf dem neuesten Stand befindliche, automatisch Spyware-Schutz beugt Systeminfektionen vor, ohne die Clients dabei zu beeinträchtigen. Das Anti-Spyware-Modul stellt eine aktive Spyware-Überwachung sowie einen On-Demand-Scanner bereit. Zudem können vertrauliche Daten gesichert werden, um einen versehentlichen oder willentlichen Export von einem Clientcomputer zu verhindern.

### Sichere Verbindungen

Über eine mehrstufige Filterung des Datenverkehrs wird Ihr Netzwerk vor unnötigen oder böartigen Verbindungen geschützt. Dadurch, dass Endbenutzer-PCs im Internet für Hacker unsichtbar gemacht werden, können diese empfindliche Desktops nicht lokalisieren. Das Angriffserkennungsmodul verhindert bekannte und unbekanntem Angriffe auf geschützte Workstations und gibt optional eine Warnmeldung an den Client aus. Von Administratoren zugewiesenen Anwendungsregeln steuern die Internetzugriffsrichtlinie für Clients und können bei Bedarf schnell und problemlos geändert werden.

"86 % aller  
Computerstraftaten haben  
ihren Ursprung innerhalb  
des Unternehmensnetzwerks"

Intranet Security

### Anwendungsintegrität

Durch integrierte Mechanismen zur Codekontrolle wird verhindert, dass als vertrauenswürdige Programme getarnte bösartige Anwendungen und Komponenten unbemerkt aktiviert werden. Die Clients werden damit vor einem heimlichen Einschleusen von Code und vor Spoofing geschützt. Das Modul für aktive Webinhalte verhindert Drive-by-Infektionen, indem es die Installation und/oder Aktivierung bösartiger, selbstaktivierender Objekte unterbindet. Durch die Isolierung von Anhängen wird die Aktivierung verdächtiger E-Mail-Anhänge verhindert und das Netzwerk somit vor eventuell darin enthaltenen Viren und Würmern geschützt.

### Schutz persönlicher Daten

Mit den optionalen Funktionen zur Erhöhung des Datenschutzes kann der Internetverlauf von Endbenutzern unkenntlich gemacht werden, was deren Computer vor bestimmten Risiken bewahren kann. Wenn Sie jedoch die Online-Aktivitäten Ihrer Mitarbeiter verfolgen möchten, kann diese Option auch deaktiviert werden.

### Produktivitäts- und Leistungssteigerung

Mit dem Werbungsmodul werden Werbebanner auf Websites und in HTML-E-Mails blockiert, wodurch sich die Geschwindigkeit, mit der Webinhalte angezeigt werden können, beträchtlich erhöht (und die Benutzer gleichzeitig nicht mehr in Versuchung geraten, diese Banner anzuklicken). Zusätzlich ermöglicht das Inhaltsmodul Administratoren, die Blockierung von Webseiten mit unerwünschten Inhalten individuell anzupassen.

## Geringer Verwaltungsaufwand

Die zentrale Bereitstellung, Verwaltung und Aktualisierung von Outpost Network Security bietet störungsfreien, voll automatisierten Schutz.

### Einfache Bereitstellung

Der Client-Schutz kann augenblicklich von einer einzelnen Administratorenkonsole für alle oder ausgewählte Workstations bereitgestellt werden. Eine Installation von ONS auf einem Server oder Domänencontroller ist nicht erforderlich – das Command Center-Modul kann prinzipiell auf jeder beliebigen dedizierten Workstation gehostet werden, die die Systemanforderungen erfüllt. Für die Firewallinstallation in einer Windows 2000-Domäne (oder höher) können Windows-Gruppenrichtlinien verwendet werden.

### Zentrale Verwaltung

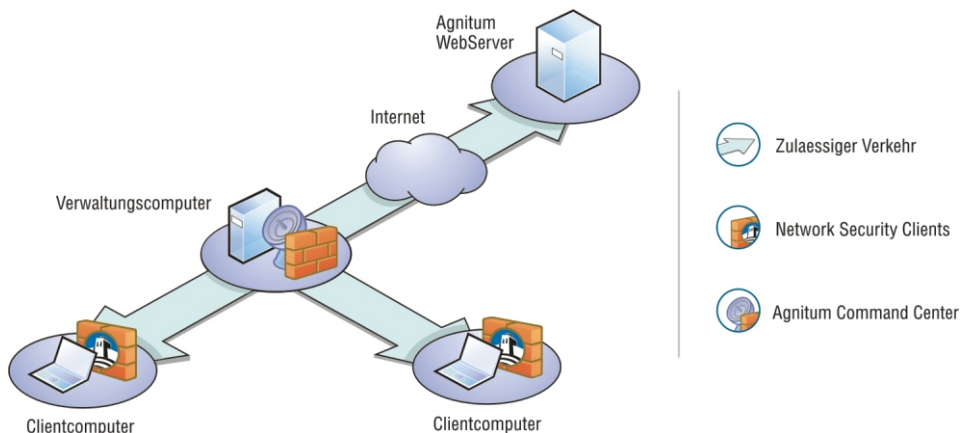
Mit Agnitum Command Center kann der Schutz einzelner Workstations von einem zentralen Standort aus gesteuert werden. Die Verwaltung, Überwachung und Fehlerbehebung erfolgt für jede einzelne Firewallinstallation von diesem zentralen Standort aus. Dadurch wird der Zeit- und Personalaufwand für Administrationsaufgaben in beträchtlichem Maße verringert.

### Schnelle Updates

Der Agnitum Update Service ermöglicht den zeitplangesteuerten zentralen Download von Updates. Da die Updates nur einmal gedownloadet werden müssen und dann auf mehreren Clients gleichzeitig installiert werden können, bleiben die Auswirkungen dieses Vorgangs auf die Netzwerkleistung minimal.

### Benutzerfreundlichkeit

Outpost Network Security verfügt über eine vertraute Benutzeroberfläche, und das Command Center ist als MMC-Snap-In implementiert. Da die Firewall-Einstellungen vorheriger Outpost Firewall Pro-Installationen übernommen werden können, gestaltet sich der Konfigurationsvorgang einfach und schnell.



## Systemanforderungen

### Minimale Hardwareanforderungen:

Hauptprozessor: x-86-kompatibler Prozessor, 450 MHz oder höher  
Speicher: serverseitig: 256 MB; clientseitig: 128 MB  
Freier Festplattenspeicher: 50 MB

### Betriebssystem:

Serverseitig: Windows 2003 Server, Windows 2000, Windows NT  
Clientseitig: Windows XP, Windows 2000, Windows Me, Windows 98