



Datenblatt

Outpost Firewall Pro 2009

Ihre unerlässliche Verteidigung gegen Internetbedrohungen

Was macht eine Verteidigung unerlässlich?



Neue Arten von Bedrohungen erfordern auch neue Arten des Schutzes. In Massen versandte Viren und Würmer werden immer mehr durch profitorientierte Angriffe ersetzt, die durch Spyware und Botnets Identitäten, Geld und anderes wertvolles elektronisches Eigentum stehlen sollen.

Angeichts der Komplexität und Vielfalt der heutigen Bedrohungen brauchen die

Anwender einen Schutz, der den Hauptverbreitungsweg kontrolliert - ihre Internetverbindung. Zero-Day-Angriffe, eine der neuesten und am schwierigsten zu erkennenden Angriffe, nehmen immer mehr zu. Eine entsprechende Reaktionsmöglichkeit darauf muss vorhanden sein, damit Anwender ein angemessenes Maß an Sicherheit haben, wenn sie online gehen. Selbst das einfache Surfen im Internet ist heutzutage voller Risiken, von der Gefahr durch Drive-By-Infektionen bis zur unbeabsichtigten Preisgabe persönlicher Informationen.

Es gibt zwar zahlreiche Paket-Sicherheitslösungen, die angeblich vollständigen Schutz bieten, in der Praxis hängen sie jedoch alle von einer Firewall ab, die die erste Schutzstufe gegen die Verbreitung von Malware und gegen Datendiebstahl bietet. Die hoch entwickelten und schwierig zu erkennenden Schadprogramme von heute können mit Antiviren-Programmen allein nicht aufgehalten werden; um das Programmverhalten zu überwachen und um den Anwender bei verdächtigen, unbefugten oder ausdrücklich schädlichen Aktivitäten zu benachrichtigen, noch bevor sie Schaden anrichten können, sind proaktive Sicherheitstools erforderlich. Da Angriffe aus dem Internet mittlerweile den größten Teil der Malware-Angriffe ausmachen, ist eine Lösung, die speziell zur Abwehr von Online-Bedrohungen entwickelt wurde, unerlässlich.

Genau so ein Tool ist Outpost Firewall Pro. Das Programm hält Malware und Hacker-Angriffe auf, bevor sie aktiv werden können, indem es den Internetzugriff jederzeit überwacht und kontrolliert. Darüber hinaus arbeitet es größtenteils automatisch, so dass die Anwender bei der Arbeit oder beim Spielen im Internet nicht unterbrochen werden. Outpost Firewall Pro ist ein preisgekrönter Schutz, der leicht, anpassbar, zuverlässig und einfach zu verwenden ist. Da das jeder Computer verdient, lesen Sie weiter und erfahren Sie mehr darüber, wie Outpost den Anwendern den widerstandsfähigsten Schutz bietet, der in der heutigen Welt der Cyber-Bedrohungen möglich ist.

Haupt-Technologien

- **Zweiwege-Firewall** zur Überwachung des Netzwerkzugriffs
- **Intrusion Detection System (IDS) und Ethernet-Schutz** für eine automatische Verteidigung gegen Schwachstellen-Sondierungen und interne Sicherheitsverletzungen
- **Anti-Spyware-Funktion**, um Ihren PC frei von Spyware zu halten
- **Hostschutz** zur proaktiven Blockierung unbekannter Bedrohungen
- **Web- & Transaktions-Sicherheit** zum Schutz vor Internet-Gefahren
- **Selbstschutz** zur Gewährleistung eines kontinuierlichen Schutzes
- **Automatisierte, aktualisierbare Konfigurationen** zur Arbeitserleichterung

Hauptvorteile

- Die preisgekrönte Firewall wehrt Hacker und Malware ab, so dass die Benutzer sich sicher fühlen können, wenn sie online sind. Die Zweiwege-Kontrolle bedeutet, dass keine unautorisierte Netzwerkaktivität möglich ist; der spezielle Ethernet-Schutz schützt lokale Netzwerke gegen sogenannte Man-in-the-Middle-Angriffe und WiFi-Angriffe. Die Komponente IP-Blockierliste blockiert Verbindungen zu vorab festgelegten Internet-Hosts und hält Ihre Familienmitglieder so von den Websites fern, die Sie als unangemessen betrachten.
- Der Hostschütz überwacht Verhalten und Interaktionen von Programmen, um proaktiv vor unbefugter Aktivität zu schützen. So werden Trojaner und Rootkits von Anfang an aufgehalten, ohne dass dazu jedes verdächtige Objekt auf bekannte Malware überprüft werden muss. Der Hostschutz von Outpost hat bei allen aktuellen Leaktests eine Erfolgsquote von 100 % erreicht und bietet zuverlässigen Schutz gegen unbekannte und/oder hoch entwickelte Hacker-Angriffe.
- Das integrierte Anti-Spyware-Modul bietet umfassenden Schutz gegen alle Arten von Spyware und schützt die Anwender automatisch vor den Risiken durch gefährdete private Informationen, vor unbefugten Systemänderungen, aufdringlichen Popup-Fenstern und anderen Online-Ärgernissen.
- Das vielseitige Modul Web-Kontrolle schützt die Anwender bei ihren Surf-Aktivitäten vor den dunkleren Seiten des Internets, indem es sie von Webseiten fernhält, die mit Drive-By-Downloads infiziert sind. Es verhindert die unbeabsichtigte Preisgabe persönlicher Informationen, verringert die Gefährdung durch potenziell unsichere Internet-Eigenschaften und schützt die Identität.
- Die Selbstschutz-Funktion von Outpost stellt sicher, dass es nicht durch gezielte Angriffe deaktiviert werden kann, so dass ein ununterbrochener Schutz gewährleistet ist.
- Dank des erweiterten Protokollierungsmechanismus und der neuen Prozessaktivitäts-Ansicht, die ausführliche Informationen zu allen momentan aktiven Programmen anzeigt, werden die Anwender mit ultimativer Transparenz und Bedienungsfreundlichkeit geschützt.

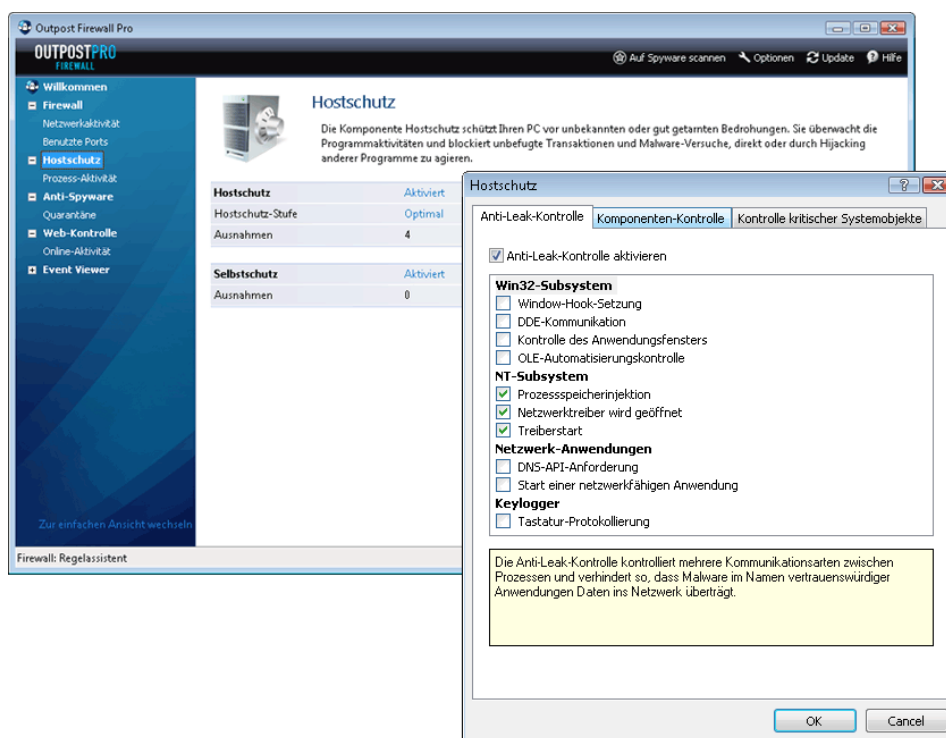
Outpost Firewall Pro wurde dazu entwickelt, die Bedürfnisse von Anwendern zu erfüllen, die sich der Notwendigkeit einer widerstandsfähigen, leistungsstarken Sicherheitslösung bewusst sind. Während das Programm Anwendern jeder Erfahrungsstufe mit den Standardeinstellungen bereits direkt nach der Installation einen hervorragenden Schutz bietet, umfasst Outpost Firewall Pro außerdem eine umfassende Auswahl an anpassbaren Einstellungen und Optionen, mit denen erfahrenere Anwender ihren Schutz genau abstimmen und individuell gestalten können. Auch Anwender mit weniger Erfahrung genießen den herausragenden Schutz, da sie mit Outpost die meisten Einstellungen automatisch festlegen und anwenden lassen können, so dass mögliche Konfigurationsfehler ausgeschlossen sind. Durch die intuitive Benutzeroberfläche und die leicht zugänglichen Steuerungsmöglichkeiten ist das Programm für jeden leicht zu verwenden.

Hauptmerkmale

Proaktive Sicherheit

Vorbeugender Schutz vor Bedrohungen

Outpost Firewall Pro bietet die erste Verteidigungslinie ("first line of defense") gegen schädliche Software, indem proaktiv kontrolliert wird, wie Programme sich auf einem PC verhalten und interagieren, so dass Sicherheitsverletzungen verhindert werden. Das Hostschutz-Modul überwacht proaktiv und blockiert hoch entwickelte Hacker-Techniken, die dazu eingesetzt werden, Daten zu gefährden oder zu stehlen. Durch die Analyse von Bedrohungen und die Anzeige umsetzbarer Warnhinweise blockiert es Zero-Day-Angriffe und andere unbefugte Aktivitäten und bietet so Schutz vor Botnets, Rootkits und unbeabsichtigter Datenpreisgabe. In dieser neuesten Version wurde die Bandbreite überwachter Ereignisse und Abläufe für einen noch besseren und noch anpassbareren Schutz erweitert. Outpost schneidet in sämtlichen derzeit bekannten Leaktests hervorragend ab, mit zusätzlichem Schwerpunkt auf Keylogger-ähnlichen Aktivitäten.



Selbstschutz

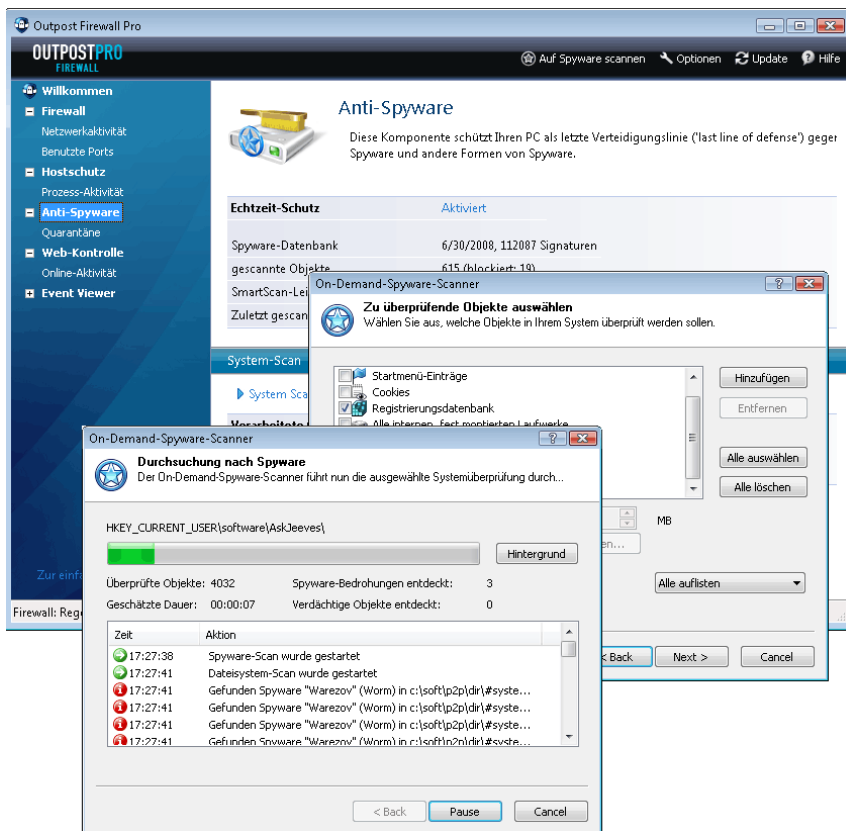
Die Malware von heute versucht häufig, Sicherheitssoftware zu beenden und so den Infektionsprozess zu vereinfachen. Durch die Umsetzung eines robusten, manipulationssicheren Schutzes für alle Komponenten verhindert Outpost Firewall Pro, dass mit Ausnahme des autorisierten Programmbenutzers jemand den aktiven Schutz deaktivieren oder beenden kann.

Anti-spyware-funktion

Grundlegender Spyware-Schutz

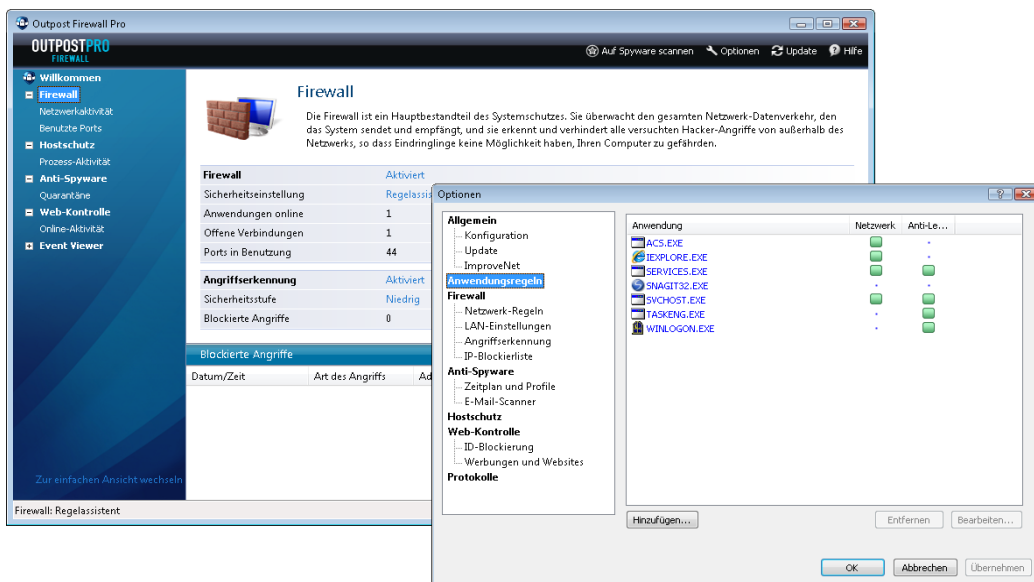
Das Anti-Spyware-Modul von Outpost schützt PCs gegen die Bedrohung durch Spyware - von der Anzeige störender Werbung über Hijacking der Browser-Startseite bis hin zum Diebstahl der Benutzer-Identität und vertraulicher Daten. Spyware wird in jedem möglichen Stadium blockiert - Installation, Aktivierung, Übertragung von Informationen und Neu-Installation. Der On-Demand-Scanner durchsucht das System nach Spuren deaktivierter Spyware und löscht sie vollständig. Selbst wenn der aktive Spyware-Schutz während speicherintensiver Aufgaben, z. B. während eines Online-PC-Spiels, deaktiviert wird, werden

neue Netzwerkverbindungen im Hintergrund proaktiv auf Spyware überprüft, bevor sie zugelassen werden.



Netzwerksicherheit und kontinuierät Verbindungssicherheit

Die Zweiwege-Firewall überwacht die ein- und ausgehenden Verbindungen des Computers und verhindert einen unbefugten lokalen und Remote-Netzwerkzugriff. Sie verbirgt Zugangsports und macht so die Anwesenheit des Anwenders im Internet unsichtbar. Das Modul Ethernet-Schutz bewacht die Netzwerkverbindungen und verhindert Angriffe von innen, indem es die Datenübertragung über das Netzwerk kontrolliert. Das beseitigt das Risiko, dass Daten wie z.B. Chat-Fenster oder legitime Browser-Sitzungen an einen falschen Bestimmungsort geschickt oder während der Übertragung abgefangen werden.



Programm-zugriffskontrolle

Die Firewall kontrolliert, welche Programme auf das Internet zugreifen dürfen und schützt den PC proaktiv sowohl vor Zero-Day-Bedrohungen als auch vor "Phone Home"-Versuchen von Malware-Programmen.

Umfassende abdeckung

Outpost Firewall Pro schützt sämtliche Verbindungsarten (Ethernet, WiFi, DSL, Kabel, Mobilfunk und Einwahlverbindung) und wendet automatisch die erforderlichen Sicherheitseinstellungen an, wenn der Computer mit einem neuen Anbieter verbunden wird.

Schutz vor eindringlingen

Das Modul Angriffserkennung blockiert automatisch bekannte Arten von Hacker-Angriffen und verhindert, dass sie Zugriff auf den Computer bekommen.

Datenschutz und internetsicherheit

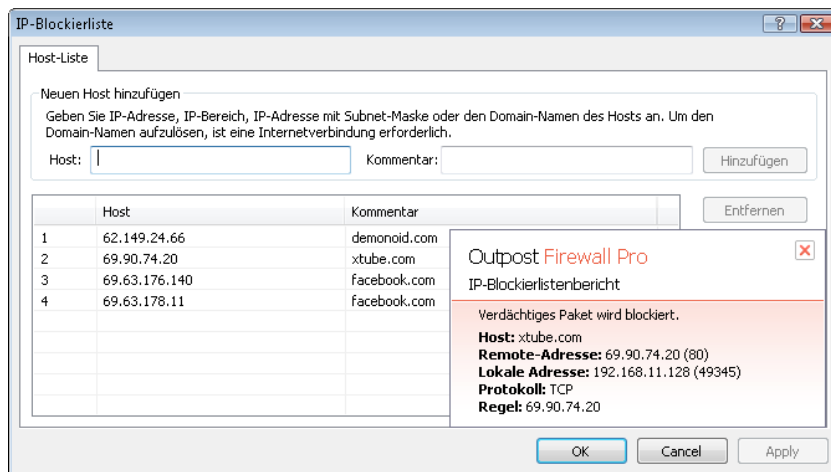
Eingeschränkter zugriff auf unsichere websites

Outpost kann den Zugriff auf potenziell gefährliche oder unerwünschte Websites auf der Grundlage einer vordefinierten Liste von URLs optional melden und blockieren. Diese Filterung verhindert, dass Anwender das Opfer einer unbeabsichtigten Drive-By-Malware-Infektion oder eines Phishing-Angriffs werden, bei dem versucht wird, Passwörter, Login-Informationen und andere empfindliche Daten zu stehlen. Die Liste der blockierten Seiten wird über die automatischen Anti-Malware-Updates aktualisiert und kann bearbeitet werden, um sie an individuelle Vorlieben anzupassen.

The screenshot shows the Outpost Firewall Pro interface. The left sidebar contains navigation options: Willkommen, Firewall, Hostschutz, Anti-Spyware, Web-Kontrolle (highlighted), and Event Viewer. The main area displays the 'Web-Kontrolle' settings, which are activated. Below this, there are sections for 'Internet- und E-Mail-Sicherheit' and 'ID-Blocker'. A pop-up window titled 'Outpost Firewall Pro Website-Blacklist-Meldung' is overlaid on the bottom right, showing a blocked website: 'www.adwarebutcher.com' with the address 'www.adwarebutcher.com' and a link to 'Zugriff auf Website zulassen'. The pop-up also includes a checkbox for 'Diese Meldung nicht mehr anzeigen'.

IP-Blockierliste sorgt für sauberes Surfen

Neu! Auf der Grundlage des Plug-Ins BlockPost in früheren Outpost-Versionen ermöglicht die IP-Blockierliste es den Anwendern, den Zugriff auf festgelegte Internet-Domains einzuschränken. Als wertvolles Werkzeug sowohl für empfindlichere Personen als auch besorgte Eltern wird die IP-Blockierliste ein- und ausgehende Verbindungen zu und von Internet-Zonen mit schlechten Absichten, wie z.B. zu solchen, die Spyware verbreiten oder aufdringliche Werbung und abstoßenden Spam liefern. Die blockierten Einträge können entweder manuell festgelegt oder als von öffentlich geführten Quellen zusammengestellte Liste importiert werden.



Sicherer Speicherort für persönliche Daten

Alle mit dem ID-Blocker vom Anwender festgelegten vertraulichen Informationen - z.B. Bankkontonummern und Passwörter - werden beim Verlassen des PCs über Kommunikationskanäle wie Instant Messaging, Internet oder E-Mail blockiert. Der ID-Blocker schützt vor Identitätsdiebstahl und Phishing-Angriffen, die auf persönliche, vertrauliche Informationen abzielen. Darüber hinaus stellt er sicher, dass niemand sonst - auch kein anderes Mitglied des Haushalts - diese Informationen versehentlich oder vorsätzlich im Internet preisgeben kann.

Werbefreies, anonymes surfen

Durch die Verwaltung von Cookies und externen Verweis-URLs ermöglicht Outpost den Anwendern ein hohes Maß an Privatsphäre, wenn sie Shopping-, Unterhaltungs- oder Nachrichtenseiten besuchen und erlaubt es dabei gleichzeitig vertrauenswürdigen Websites, nur die Informationen zu sammeln, die zum Personalisieren der Webseiten nötig sind. Darüber hinaus können die Anwender mit Outpost Firewall Pro die Elemente einschränken, die auf Websites angezeigt werden, so dass das Surfen sauberer und schneller wird. Die Anwender können ebenfalls festlegen, welche Websites Bilder anzeigen, Werbebanner rotieren, externen Code wie ActiveX oder Java-Scripte ausführen oder Popup-Fenster einblenden dürfen (oder nicht dürfen). Die neueste Version von Outpost gewährleistet Kompatibilität selbst mit den komplexesten und technisch ausgeklügeltsten Websites und bietet so reibungslose Leistung und verbesserte Online-Sicherheit.

Überwachung & Kontrolle

Überwachung der Netzwerkaktivität

Die Überwachung der Netzwerkaktivität in Outpost zeigt jede Verbindung an, die der PC des Anwenders mit anderen Computern im Internet oder im lokalen Netzwerk herstellt, so dass Anwender jederzeit sehen können, was gerade auf ihrem PC geschieht und nicht autorisierte Verbindungen schnell beenden können. In der neuen Version können Verbindungen nach Anwendung gruppiert/die Gruppierung aufgelöst werden, und Sie können alle vorhandenen Regeln schnell und einfach direkt von der Programmoberfläche aus bearbeiten.

Passwort-schutz, mehrere Konfigurationsprofile

Die Anwender können Passwörter einrichten, um ihre Konfigurationen vor unbeabsichtigter oder vorsätzlicher Änderung zu schützen und darüber hinaus mehrere Konfigurationsprofile erstellen und verwenden, die dem jeweils aktuellen Gefährdungsgrad entsprechen. Für erfahrenere Anwender ist die Möglichkeit, durch den Befehl zum Speichern/Laden von Konfigurationen mehrere Wiederherstellungspunkte zu setzen, ein großer Vorteil.

Einfachere Verwaltung von Ereignisprotokollen

Der frühere Log Viewer von Outpost zeigte den Verlauf vergangener Ereignisse auf einem Computer. Die neue Version bietet eine verbesserte Durchschaubarkeit und Handhabung im Log Viewer, mit zusätzlicher Unterstützung für eine Auflistung nach Kategorien, die nach verschiedenen benutzerdefinierten Kriterien sortiert und gefiltert werden kann.

Kompatibilität

Treiber-Zertifizierung und Kompatibilität mit neuesten Windows-Plattformen

Outpost hat die Zertifizierung WHQL (Windows Hardware Quality Labs) erhalten, das bedeutet, dass der Schutz den strengen Qualitäts-, Kompatibilitäts- und Stabilitätsanforderungen von Microsoft entspricht.

Anpassungsfähige firewall-regeln

Beim Reisen mit einem Laptop oder beim Wechsel des Internet-Anbieters müssen die Anwender ihr Sicherheitsprogramm nicht manuell an die neuen Verbindungseinstellungen anpassen - Outpost erledigt das automatisch durch die Zuweisung verbindungsspezifischer Parameter wie der DNS oder Gateway-Server-Adressen als Umgebungsvariablen.

Entertainment-modus für unterbrechungsfreien spiel- und filmgenuss

Wenn die Anwender im Vollbild-Modus Computerspiele spielen oder sich auf ihren PCs Filme anschauen, sorgt der Entertainment-Modus von Outpost dafür, dass das Programm sie nicht mit Warnmeldungen unterbricht, wenn es eine neue Aktivität entdeckt. Benachrichtigungen über neue Aktivitäten werden mit den Standard-Sicherheitseinstellungen im Hintergrund bearbeitet, ohne das aktuelle Schutzlevel zu beeinträchtigen. Die Benutzer können die Anwendungen, die automatisch den Wechsel in den Entertainment-Modus auslösen sollen, individuell auswählen.

Benutzerfreundlichkeit und einfache bedienung

Selbstlern-modus

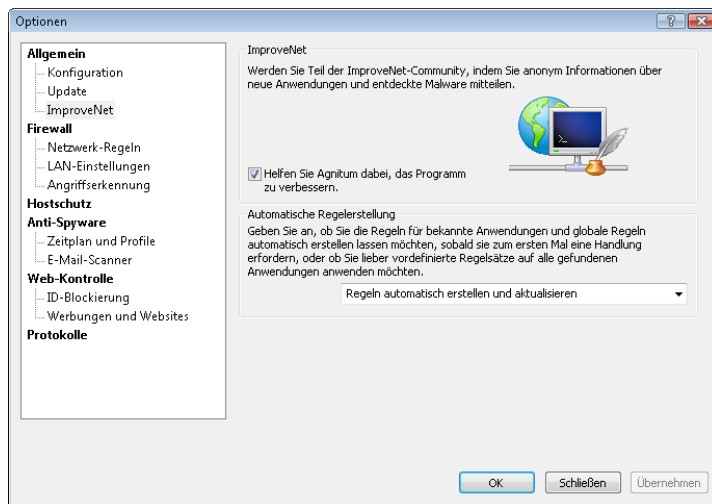
Beim ersten Start von Outpost wird ein spezieller "Lern-Modus" ausgeführt, in dem alle Warnmeldungen unterdrückt werden. In diesem Zeitraum lernt das Programm im Stillen die typischen Programmaktivitäten und Firewall-überwachten Verbindungen des Anwenders kennen. Nach Ablauf dieser Lernphase kehrt das Programm in den normalen Modus zurück und wird nur dann zu einer Eingabe auffordern, wenn eine neue Aktivität erkannt wird. So wird die Anzahl von Warnmeldungen, die eine Reaktion des Anwenders erfordern, erheblich verringert.

Automatische konfiguration

Für die meisten Programme, die auf das Internet zugreifen, werden die Regeln automatisch angewandt, so dass die Anwender nicht jedes Mal manuell Regeln eingeben müssen, wenn eine neue Anwendung auf das Internet zugreift oder mit einem anderen Programm kommuniziert. Das bedeutet, dass sich die Anwender die meiste Zeit über nicht mit Fragen hinsichtlich des Internetzugriffs auseinandersetzen müssen. Das verringert die Anzahl der Unterbrechungen sowie die Risiken durch unsichere Konfigurationen. Outpost enthält eine Vielzahl an vordefinierten Zugriffs-Sicherheitseinstellungen; diese Einstellungen können jederzeit an individuelle Anforderungen angepasst werden.

Improvenet bietet mehr gebrauchsfertige konfigurationen

ImproveNet ist ein System zur Sammlung und Verteilung von Programmkonfigurationen auf freiwilliger Basis. Nach der Überprüfung und Genehmigung durch die Techniker von Agnitum werden Regelsätze, die von Outpost-Anwendern eingesandt wurden, an den gesamten Benutzerstamm verteilt. So erhalten alle Anwender immer die sichersten und aktuellsten Regeln für eine Vielzahl von Aktivitäten und Anwendungen.



Smartadvisor - kontextabhängige sofort-hilfe

Falls ImproveNet keine Antwort bieten kann, ist der SmartAdvisor immer zur Hand und hilft den Anwendern, bei der Konfiguration der Zugriffsinformationen für ein Programm die richtige Entscheidung zu treffen.

Automatische aktualisierungen

Jedes Mal, wenn während der Lizenzdauer ein Update für Outpost Firewall Pro herausgegeben wird, lädt das Update-Modul automatisch die neueste Version vom Agnitum-Server herunter und wendet sie an, sobald es die Zustimmung des Anwenders erhalten hat.

Leistung und optimierung

Schnellere, Intelligenter Scans

SmartScan, die intelligente Dateierkennungs-Überwachung, überprüft nur die geänderten Teile des Dateisystems und vermeidet so eine wiederholte Überprüfung von Dateien, die sich seit dem letzten Scan nicht geändert haben. Die schnelle und intelligente Anti-Spyware-Engine beeinträchtigt die Gesamt-Systemleistung überhaupt nicht und kann im Hintergrund ablaufen, während Sie arbeiten. SmartScan wurde weiter optimiert, um eine bis zu zehnmal so schnelle Leistung bei einigen Scans und einigen Datenstrom-Überprüfungsvorgängen zu bieten.

Spezifikationen

Unterstützte Plattformen: Windows 32-Bit und 64-Bit (Vista, XP, Server 2003, 2008), Windows 2000 (SP3 und höher).

Hardware-Anforderungen: 450 MHz oder schnellere CPU (x-86/x-64/Multicore), 256 MB RAM, 100 MB freier Speicherplatz.

© 2008 Agnitum Ltd. All rights reserved. Agnitum®, Outpost Firewall Pro™, Outpost Security Suite Pro™ and Outpost Antivirus Pro™ are trademarks or registered trademarks of Agnitum Ltd.