



Datenblatt

Outpost Security Suite Pro 2009

Proaktiver Schutz für intelligente Internetnutzer

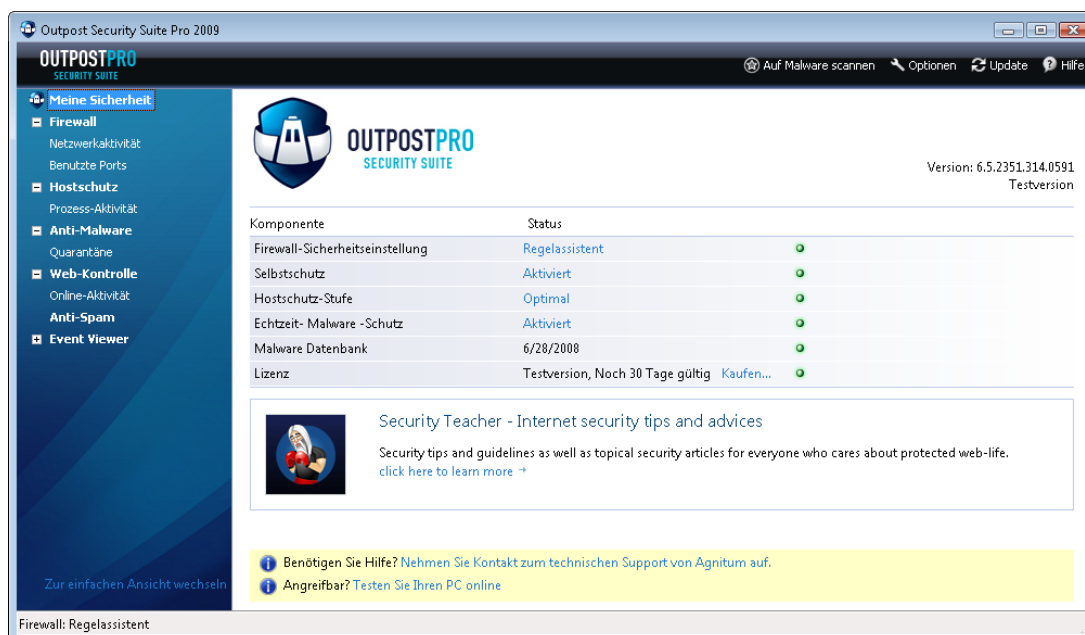
Warum proaktiver Schutz?

Das heutige Internet erfordert einen völlig neuen Ansatz beim Thema Sicherheit. Beinahe alles ist miteinander verbunden und läuft in Echtzeit ab. Und das trifft auch auf drohende Gefahren zu. Wirkungsvolle Sicherheitssoftware muss jederzeit auf der Hut vor neuer, immer raffinierterer Malware sein.

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 Phishing und Social Engineering Identitäten, Geld und anderes wertvolles elektronisches Eigentum stehlen sollen.

Für einen vollständigen Schutz gegen diese neuen Risiken muss eine wirksame Sicherheitslösung einen vielschichtigen Ansatz verwenden, der ein proaktives, verhaltensbasiertes Blockieren ebenso verwendet wie die traditionellere, auf Signaturdatenbanken beruhende Erkennung. Sie muss außerdem leicht zu benutzen sein – andernfalls *wird* sie nicht benutzt.

Auf dem hoch gelobten Schutz der Outpost Pro Firewall aufbauend, kombiniert die Outpost Security Suite Pro von Agnitum die größten Vorteile beider Ansätze in einem einzigen, integrierten Produkt, das individuell anpassbaren Schutz und absolute Zuverlässigkeit bietet. Outpost Security Suite Pro ist 24 Stunden am Tag, sieben Tage die Woche wachsam und schützt Daten - egal, welche Aktivitäten gerade am PC ausgeführt werden.



The screenshot shows the main interface of the Outpost Security Suite Pro 2009. On the left is a navigation menu with categories like 'Meine Sicherheit', 'Firewall', 'Hostschutz', 'Anti-Malware', 'Web-Kontrolle', and 'Event Viewer'. The main area displays the 'OUTPOSTPRO SECURITY SUITE' logo and a table of system components and their status.

Komponente	Status
Firewall-Sicherheitseinstellung	Regelassistent ●
Selbstschutz	Aktiviert ●
Hostschutz-Stufe	Optimal ●
Echtzeit- Malware -Schutz	Aktiviert ●
Malware Datenbank	6/28/2008 ●
Lizenz	Testversion, Noch 30 Tage gültig Kaufen... ●

Below the table, there is a section for 'Security Teacher - Internet security tips and advices' with a small icon and a link to learn more. At the bottom, there are two yellow informational banners: 'Benötigen Sie Hilfe? Nehmen Sie Kontakt zum technischen Support von Agnitum auf.' and 'Angreifbar? Testen Sie Ihren PC online'.

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
- **Kombinierter Virenschutz und Spyware-Scanner** für Rundum-Verteidigung gegen Malware
- **Hostschutz** zur proaktiven Blockierung unbekannter Bedrohungen
- **Spamschutz**, um den Posteingang von Junk-E-Mails freizuhalten
- **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 Hostschutz überwacht Verhalten und Interaktionen von Programmen, um proaktiv vor unbefugter Aktivität zu schützen. So werden Trojaner, Rootkits und Keyloggers 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.
- Die leichte, hocheffiziente Scan-Engine kombiniert das preisgekrönte Antiviren-Modul mit dem Anti-Spyware-Modul, um schädliche Programme automatisch zu erkennen und zu desinfizieren oder zu entfernen. Die Zugriffsüberwachung ist ständig auf der Hut vor Malware-Versuchen, auf den PC zu gelangen oder sich dort zu aktivieren; die flexible Architektur gewährleistet Scans mit hoher Geschwindigkeit und niedrigem Ressourcenverbrauch.
- 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.
- Das lernfähige Anti-Spam-Modul hält den Posteingang frei von Junk-E-Mails - und mit der Zeit wird es dabei noch besser, da es lernt zu erkennen, welche E-Mails die Anwender als unerwünscht betrachten.
- 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 Security Suite 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 Security Suite Pro außerdem eine umfassende Auswahl an anpassbaren Einstellungen und Optionen, mit denen erfahrener 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

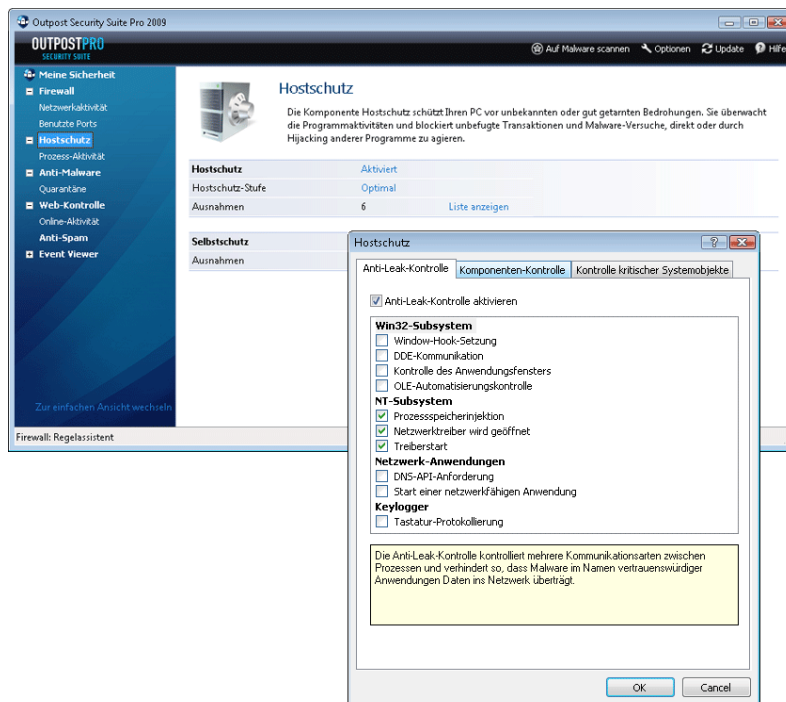
Konfigurationsfehler ausgeschlossen sind. Durch die intuitive Benutzeroberfläche und die leicht zugänglichen Steuerungsmöglichkeiten ist das Programm für jeden leicht zu verwenden.

Hauptmerkmale

Proaktive sicherheit

Vorbeugender schutz vor bedrohungen

Outpost Security Suite 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

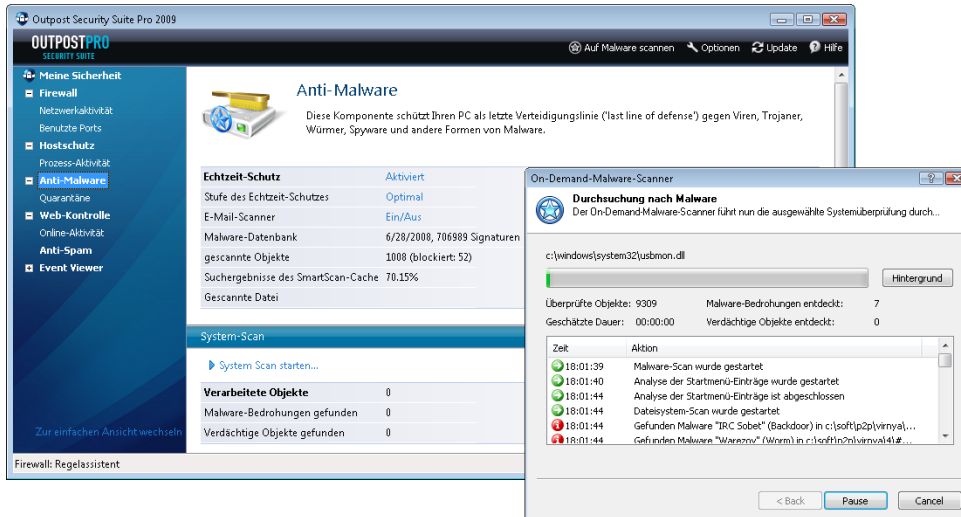
Die Malware von heute versucht häufig, Sicherheitssoftware zu beenden und so den Infektionsprozess zu vereinfachen. Durch die Umsetzung eines robusten, manipulationssicheren Schutzes für alle Komponenten verhindert Outpost Security Suite Pro, dass mit Ausnahme des autorisierten Programmbenutzers jemand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

Leistungsfähige anti-malware-funktion

Rundum-schutz vor malware

Das universelle Anti-Malware-Modul bietet sowohl Antiviren- als auch Anti-Spyware-Funktionen und gewährleistet so, dass Computer vor allen Schadprogrammen geschützt sind, die sie beim Surfen im Internet befallen könnten. Die Zugriffsüberwachung hält Ausschau nach Malware-Objekten in den

Schlüsselbereichen des PCs und desinfiziert, isoliert oder entfernt gefundene Objekte sofort, während der On-Demand-Scanner den Anwendern die Möglichkeit bietet, Bedrohungen auf Festplatten, in Netzwerkordnern, auf DVDs oder externen Speichergeräten zu suchen und zu entfernen. E-Mail-Anhänge werden bei der Ankunft oder beim Versand in Echtzeit überprüft, und Anwender können jede verdächtige Datei zur späteren Überprüfung in den Quarantäne-Bereich verschieben. Ein zusätzlicher Schutz verhindert nun, dass Rootkits und andere hoch entwickelte Malware-Programme auf den PC geladen werden und sich dort einbetten.



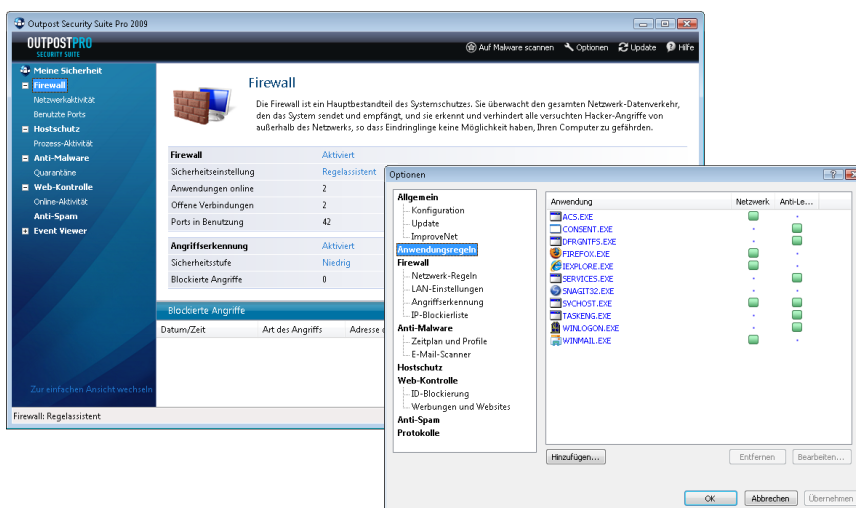
Geplante Scans und Ausnahmen

Die Anwender können einen flexiblen Zeitplan für regelmäßige Malware-Scans festlegen und darüber hinaus benutzerspezifische Scan-Kriterien wie etwa die Überprüfung kritischer Systembereiche nach jedem Update der Malware-Definitionen angeben.

Netzwerksicherheit und Kontinuität

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 Security Suite 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.

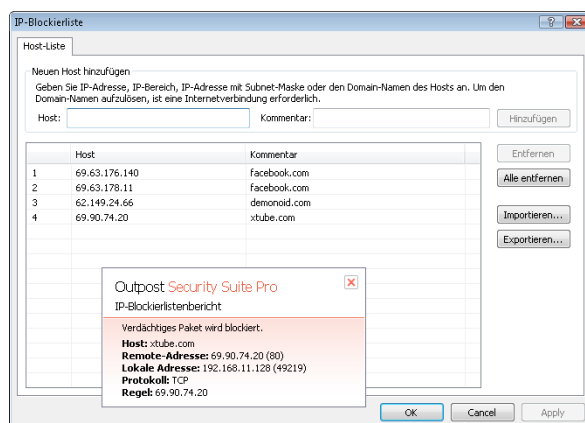
Datenschutz und internetsicherheit

Schutz vor spam

Die Bayesische Anti-Spam-Engine von Outpost Security Suite Pro hält Postfächer frei von Junk-E-Mails. Anwender können das Modul so trainieren, dass es ihre persönliche Definition von Spam erkennt und anwendet und so mit zunehmender Verwendungsdauer immer leistungsfähiger wird und ihnen mehr Zeit spart. Der Spamschutz von Outpost bietet jetzt vollständige Unterstützung für das beliebte E-Mail-Programm The Bat!.

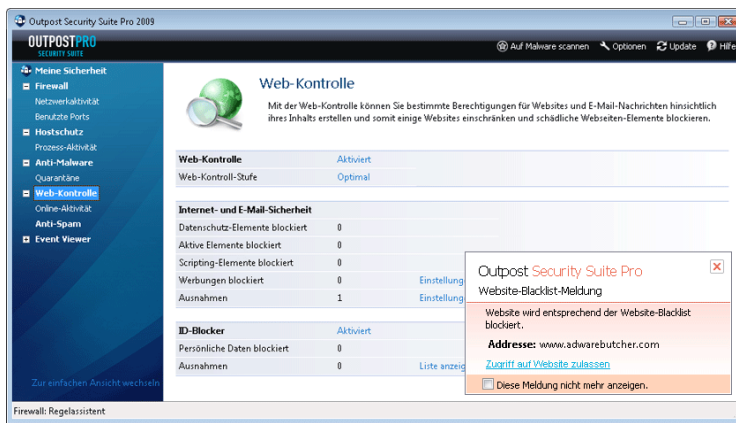
IP-Blockierliste sorgt für sauberes Surfen

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.



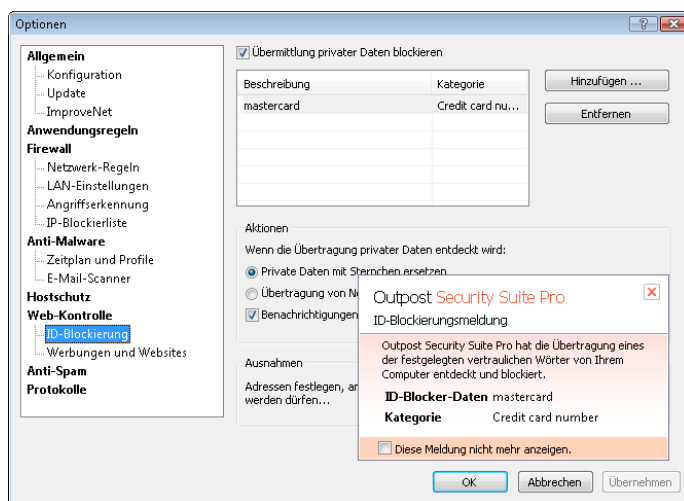
Eingeschränkter zugriff auf unsichere websites

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.



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 Security Suite 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 die Suite 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 große Bandbreite vordefinierter 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 Security Suite 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, intelligentere 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-Malware-Engine beeinträchtigt die Gesamt-Systemleistung nicht und kann im Hintergrund ablaufen, während am PC gearbeitet wird. 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).

Unterstützte E-Mail-Programme für die Anti-Spam-Funktion: The Bat!, Windows Mail, Outlook Express, Outlook (alle Versionen).

Unterstützte E-Mail-Protokolle und Dienste: POP3, SMTP, IMAP.

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 Security Suite Pro™, Outpost Firewall Pro™ and Outpost Antivirus Pro™ are trademarks or registered trademarks of Agnitum Ltd.