

Betriebsausfälle und die Folgen einer Malware-Infizierung auf Workstations verhindern

Die Anzahl der IT-Bedrohungen steigt und variiert dramatisch. Neue Bedrohungen zu erkennen und die Folgen einer Infektion zu beseitigen, ist grundlegend, um Produktivitäts- und Datenverlusten entgegenzuwirken.

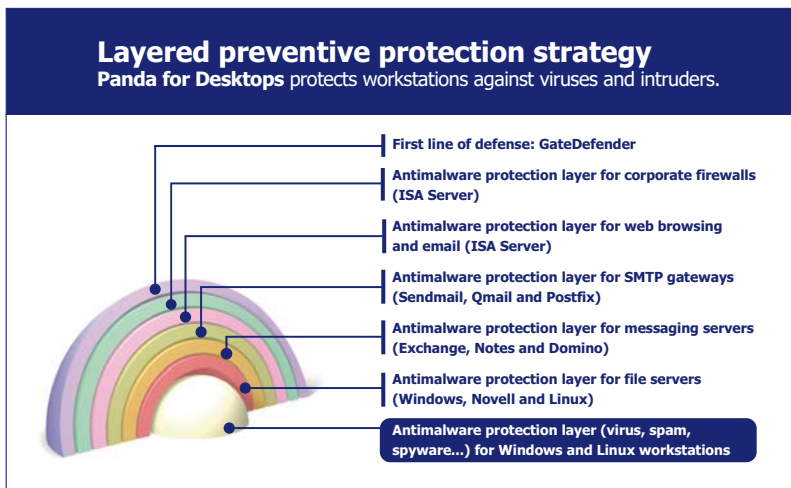
Die meisten Attacken richten sich gegen unerfahrene Anwender, die alle möglichen Dateien herunterladen und öffnen. Immer häufiger beinhalten Downloads Malware in Form von Spyware oder Adware. Ebenso verbreiten auch Spam-Mails immer mehr Schädlinge wie z.B. Netzwerkwürmer.

Diese Nutzer kann ein Administrator nur mit einem automatischem, proaktivem System schützen.

Vollständiger Schutz ohne Performanceverlust auf den Workstations

Panda Security for Desktops ist der ideale Schutz für Workstations, um den stetig steigenden Bedrohungen durch Hacker, Viren, Würmern, Spyware, Rootkits, Spam und anderen, unternehmensschädlichen Inhalten, entgegen zu wirken.

Neben herausragenden Erkennungs- und Desinfektions-Technologien ist **Panda Security for Desktops** extrem leistungsfähig. Minimaler Ressourcenverbrauch und ein geringer Administrationsaufwand entlasten das Netzwerk und den Administrator. Panda AdminSecure, das integrierte Management-Tool, stellt eine einfache Verteilung auf allen Workstations und Laptops sicher und minimiert somit das Infektionsrisiko auf allen angeschlossenen Systemen. AdminSecure bietet des Weiteren jederzeit einen umfassenden Echtzeit-Überblick über den aktuellen Sicherheitslevel des Netzwerks.



Main Benefits

- **Zentrale Verteilung und Verwaltung** sowie Umsetzung netzwerkinterner Sicherheitsrichtlinien.
- **Echtzeit-Monitoring** und Reporting.
- **Workstation-Schutz** auf allen Ebenen.
- **Einschränkung der Nutzer-Rechte**, um potentiell gefährliche Aktionen zu unterbinden.
- **Steigerung der Administrator- und Netzwerk-Performance.**

Key-Features

- Maximaler Schutz** vor Viren, Eindringlingen, Rootkits, und anderen Bedrohungen dank der effektiven Erkennung interner Schwachstellen.
- **Unmittelbare Reaktion** auf neue Bedrohungen innerhalb des kompletten Netzwerks durch **automatische, stündliche Updates, proaktive Technologien** und zentrale Quarantäne.
 - **Host based Intrusion Prevention System (TruPrevent)** schützt durch verhaltensbasierte Erkennung vor unbekannter Malware und DoS- sowie Buffer-Overflow Angriffen.
 - **Content-Filter und Anti-Spam-Modul** schützen vor gefährlichen und zeitraubenden, ungewollten Inhalten.
 - **Panda MalwareRadar**, das erste integrierte Security Audit Tool, bietet maximalen Schutz gegen zielgerichtete Attacken und Sicherheitslücken. Tiefgreifende Online-Scans nutzen Technologien, die auf normalen Workstations nicht ausgeführt werden können.
 - **Vollständige Kontrolle** über alle internen und externen Systeme, sobald diese sich mit dem Netzwerk verbinden.



Maximaler Schutz und minimales Infektionsrisiko

Panda for Desktops schützt gegen Schädlinge, die neue Schwachstellen ausnutzen, ebenso zuverlässig, wie gegen Würmer, die über „Social-Networking-Technologien“ ins System eindringen. Auch der Zugriff auf vertrauliche Daten durch Spyware oder untreue Mitarbeiter wird verhindert. Die Überwachung nahezu aller Protokolle sichert sämtliche Kommunikationsplattformen (z.B. MSN-, AOL- und Yahoo Messenger) sowie die komplette E-Mail Kommunikation. Ebenso überwacht es die Angestellten indem es die Ausführung potentiell schädlicher Software verhindert.

Zeitnahe Updates und globale Quarantäne

Panda for Desktops ist eine stabile und effektive Lösung, die neben den periodischen, inkrementellen Updates, eine zentrale Quarantäne gegen neue Bedrohungen bietet.

TruPrevent Technologien gegen unbekannte Bedrohungen und Angreifer

Das Host based Intrusion Prevention System „TruPrevent“ überwacht alle laufenden Prozesse auf potentiell schadhafte Verhalten. Die erkannten neuen Bedrohungen werden geblockt und deren Verbreitung gestoppt. Dank der SmartClean2 Technologie können sie sogar größtenteils vollautomatisch desinfiziert werden.

Die Genetic Heuristic Engine, die eine Ausführung schadhafte Prozesse vor der Ausführung unterbindet, macht **Panda for Desktops** zur intelligenten Lösung. Die automatische Deep Packet Inspection Firewall analysiert permanent den Datenstrom und ein spezielles Buffer-Overflow Detection Modul überwacht den Speicher.

Anti-Spam und Content-Filter

Panda Security for Desktops beinhaltet neben dem Schutz von MAPI, POP3, SMTP und IMAP-Mail eine effektive Anti-Spam-Lösung. Regelbasierte Erkennungstechnologien kommen ebenso zum Einsatz wie bayesische Verhaltensmuster. Die lernfähige Anti-Spam-Lösung integriert sich perfekt in Microsoft Outlook oder Outlook Express.

Des Weiteren blockt das Anti-Spam-Modul, sofern gewünscht, alle potentiell schadhafte Dateien. Panda for Desktops schützt ebenso vor Phishing Angriffen und bietet die Möglichkeit, spezielle Dateien anhand der Dateieindung oder des MIME-Typen zu filtern.

Steigerung des Schutz-Levels

NetworkSecure, das integrierte Modul zur Steigerung des Security-Levels innerhalb des Netzwerkes, reglementiert, ähnlich wie CISCO NAC, den Netzwerk-Zugriff. Anhand von MAC-Adressen kann der Zugriff limitiert und somit die Gefahr von unberechtigtem Netzwerkzugriff minimiert werden.

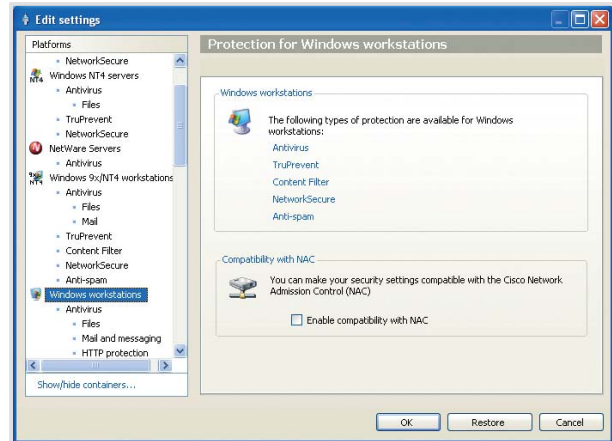
Das integrierte Roaming-System ermöglicht auch die Administration und Aktualisierung externer Systeme, unabhängig von ihrem Standort. Eine sichere Verbindung wird hierbei durch ein spezielles Extranet gewährleistet.

Panda for Desktops kann als eigenständiges Produkt oder als integriertes Modul in den Suiten „Panda Security for Business“ und „Panda Security for Enterprises“ erworben werden.

Zentrale Verteilung und Administration

Dank des integrierten Administrations-Tools „AdminSecure“ könnte die Verteilung und Administration des kompletten Netzwerkes nicht einfacher sein. Die Verteilung kann direkt aus der Konsole anhand der IP-Adresse oder der Workstation-Bezeichnung heraus erfolgen. Sie ist auch mit Hilfe externer Tools, wie SMS oder Tivoli, problemlos möglich.

Einmal aufgesetzt hat der Administrator einen zentralen Netzwerküberblick in Echtzeit über den Sicherheitsstatus des kompletten Netzwerkes. On-Demand Scans sowie detaillierte Reportings über den Status der Workstations und Distributions-Server sind problemlos zentral abrufbar.



Technische Systemvoraussetzungen

Panda Security for Desktops: Pentium 300 MHz oder schneller, Festplatte: 90 MB, RAM: 64 MB (512 MB wenn TruPrevent Technologies aktiviert sind). Betriebssystem: Windows XP 32/64 bit, 2000, Me, NT Workstation 4.0 SP6 und Windows 9x, Vista 32/64 bit, compatible WEPOS 1.1 und Tablet PC.

"Alle unsere 1.000 Workstations sind mit Panda Security bestmöglich geschützt."
Luis Valmiki. Systems Manager. Portucel. PORTUGAL.

Panda Security Zertifikate

