Panda
SecurityforBusiness

Technische Systemvoraussetzungen

AdminSecure Administration Server:
Pentium III 800 MHz (or faster); 256 MB RAM; Hard disk: 25 MB + 120 MB (Database).
Operating systems: Windows NT4 SP6, and Terminal Server, Windows 2000 and 2000 Server SBS, Windows XP/XP 64 bits, Windows Server 2003 Enterprise Edition / SBS / R2, Windows Server 64 bits, Windows Vista 32 bits/64 bits, Windows Server 2008.

AdminSecure Repository Server:
Pentium III 800 MHz (or faster); 128 MB RAM; Hard disk: 250 MB.
Operating systems: Windows NT4 SP6, and Terminal Server, Windows 2000 and 2000 Server SBS, Windows XP/XP 64 bits, Windows Server 2003 Enterprise Edition / SBS / R2, Windows Server 64 bits, Windows Vista 32 bits/64 bits, Windows Server 2008.

AdminSecure Console:
Pentium II 266 MHz; 64 MB RAM; Hard disk: 140 MB.
Operating systems: Windows 2000 / XP / XP 64 bits, Windows NT4 SP6 and Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Vista 32 bits/64 bits, Windows Server 2008.

Panda Security for Desktops:
Pentium III 300 MHz (or faster). 64 MB RAM (128 MB if TruPrevent Technologies are enabled); Hard disk: 200 MB.
Operating systems: Windows / 2000 / ME / XP SP3 / XP SP3 64 bits, Windows NT4 (SP6) Windows Vista 32 bits/64 bits, Windows Vista (SP1). TruPrevent not supported in Windows 95 and 64 bits.

Panda Security for File Servers:
Windows Servers:
Pentium 300 MHz (or higher); 256 MB RAM. Hard disk: 85 MB
Operating systems: Windows NT 4.0 SP6 Domain Controller, Small Business Server, Terminal Server and Cluster. Windows Server 2000 Domain Controller, Stand Alone, Terminal Server, Small Business Server and Cluster. Windows Server 2003 SP1 and SP2 (32bits and 64 bits) Enterprise Edition, Small Business Server and Cluster. Windows Server 2003 R2 (32 bits and 64 bits). Windows Server 2008, Server Core 2008, Small Business Server 2008. TruPrevent not supported in 64 bits.

Novell Netware Servers: 486 Processor or later.; 32 MB RAM; Hard disk: 12 MB.
Operating systems: Novell Netware 4.11, 5.0, 5.1, 6.0 ó 6.5.
Panda Security for Linux Servers:
Pentium II or AMD 400 MHz (or later); RAM: 128 MB; Hard Disk: 150 MB.
Supported Distributions: Red Hat Enterprise Linux: 5.0 Server and Workstation, 4.0 Advanced Server, Enterprise Server and Workstation. SuSE Linux Enterprise: 10 Server and Desktop, 9 Server and desktop. Ubuntu: 7.04 (Feisty), 6.06 LTS. Desktop/Server (Dapper). Debian GNU/Linux 4.0.

Panda Security for Exchange:
For Exchange Server 5.5: Pentium II 500 MHz (or later); 256 MB RAM; Hard Disk: 250 MB.
Operating systems: Windows NT Server 4.0 (or later) with Service Pack 5 (or later) and Windows 2000.
Applications: Microsoft Exchange Server 5.5 with Service Pack 3. Exchange cluster.

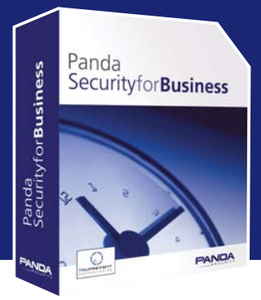
For Exchange Server 2000/2003:
For Exchange Server 5.5: Pentium II 500 MHz (or later); 256 MB RAM; Hard Disk: 250 MB.
Operating systems: Microsoft Windows 2000 Advanced Server SP3 or later, Windows Server 2003/R2.
Applications: Microsoft Exchange Server 2000 with SP 1 (or later) or Exchange 2003, including cluster.

For Exchange Server 2007:
Intel EM64T or AMD64 platforms at least 2 GB of RAM, at least 250 MB hard disk space apart from Exchange 2007.
Operating systems: MS Windows Server 2003 x64 or Windows Server 2003 R2 x64, Windows Server 2008 (only for Exchange 2007 SP1).
Applications: Microsoft Exchange Server 2007 and Exchange 2007 SP1.

Panda
SecurityforBusiness

Panda SecurityforBusiness

Der beste Schutz für Ihr Unternehmensnetzwerk



95% aller KMU's haben eine Antivirenlösung in ihrem Netzwerk installiert. Trotzdem sind 72% dieser Netzwerke mit Malware infiziert!

Nahezu alle KMU's haben eine Sicherheitslösung zum Schutz Ihrer sensiblen Daten installiert. Die meisten dieser Unternehmen beschränken sich dabei auf den Einsatz einer reinen Antivirenlösung und fühlen sich dadurch ausreichend geschützt. Tatsächlich ist es jedoch so, dass ein hoher Anteil dieser Unternehmensnetzwerke mit Malware infiziert ist.

Auf der einen Seite sind die meisten dieser Infektionen für die Unternehmen nicht zwangsläufig lebensbedrohend. Auf der anderen Seite belegt eine Gartner-Studie eindeutig, dass etwa die Hälfte aller KMU's mindestens einmal die Internetverbindung trennen, und somit Umsatz- und Produktivitätsverluste hinnehmen mussten.

Dies bedeutet, dass traditionelle Antivirenlösungen nicht mehr den heutigen Anforderungen gewachsen sind. Aktuelle Malware ist derart programmiert, unbemerkt ihre destruktiven Aufgaben zu erledigen. Moderne Bedrohungen sind extrem komplex, variabel und maßgeschneidert auf das Angriffsziel.

"Annähernd 50% aller SMBs mussten bereits aufgrund einer Malware-Infektion, die Internetverbindung trennen. Die damit verbundenen Umsatz- und Produktivitätsverluste treffen diese Unternehmen in der Regel merklich."
Gartner: User Survey Analysis: IT Security Opportunities in the SMB Market, North America, 2007.

Die Lösung: Panda Security for Business

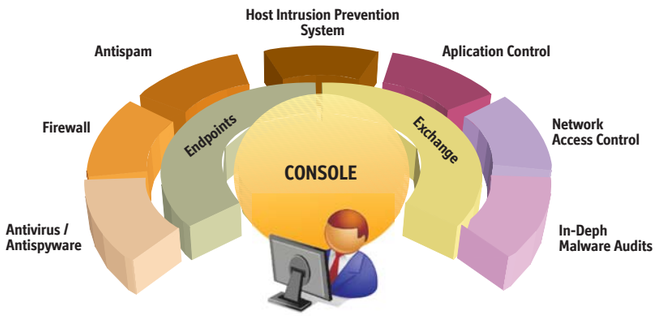
Panda Security for Business bietet maximalen Schutz vor allen aktuellen und zukünftigen Bedrohungen.

Panda Security kombiniert leistungsstarke proaktive Technologien (TruPrevent) und tiefgreifende periodische Security Audits (Malware Radar) zu einer leistungsstarken Sicherheitslösung gegen bekannte und unbekannte Angriffen.

Die „All-in-One-Konsole" (AdminSecure) versetzt Administratoren in die Lage, alle sicherheitsrelevanten Security Layer einfach und zentral zu verwalten. Eine intuitive Bedienung garantiert einfache und zeitnahe Verteilung innerhalb des Netzwerks und die volle Kontrolle aller angeschlossenen Systeme.

Panda Security for Business ist die einzige Lösung, die alle notwendigen Schutzmodule ohne zusätzliche Kosten in einer kompletten Suite vereint: Anti-Malware, IPS-System, Security-Audit-Tool, Application-Management und Netzwerks-Zugangskontrolle.

Besonders profitiert die Panda Security-Lösung von der **„Collective Intelligence"**. Diese „Scanning in the Cloud"-Technologie erhöht die Erkennungsrate bekannter und unbekannter Malware, minimiert Reaktionszeiten und bietet maximalen Netzwerkschutz.



"Das beste Beispiel eines Herstellers, der den revolutionären Ansatz gewagt hat, ein vollständiges Intrusion Prevention System in eine Workstation-Lösung zu integrieren, ist Panda Security. Mit der Lösung „ClientShield" bietet Panda, ohne Zusatzkosten, eine Endpoint-Security-Lösung die acht von neun mögliche Schutzmodule eines Host based Intrusion Prevention Systems beinhaltet."
Gartner: How to Get Free Anti-spyware (or Antivirus) Protection.

Main Benefits

- **Schützt vertrauliche und kritische Informationen** vor zielgerichteten Attacken und unbekannter Malware. Fortschrittliche Verhaltensanalysen und proaktive Technologien gewährleisten einen maximalen Schutzlevel.
- **Reduziert die Betriebskosten** durch eine zentrale, einfach zu bedienende Management Konsole.
- **Maximaler „Return of Investment"** durch die Integration der Security Module Antimalware, Security-Audit, Netzwerk- und Applikations-Zugriffskontrolle in einer Lösung.
- **Steigert die Mitarbeiter-Produktivität** durch das herausfiltern von Spam-Mails und der Sperrung von unerwünschten Applikationen.
- **Verbessertes Risiko-Management** durch Echtzeit-Analyse der aktuellen Bedrohungssituation und tiefgreifender Security Audits.

Key-Features

- **Zentrale „All-in-one-Konsole"** zur Adminstration des kompletten Netzwerks inklusive Real-Time-Monitoring.
- **Integriertes Intrusion Prevention System** und verhaltensbasierte Erkennungstechnolgien bieten maximalen Schutz vor unbekannten Bedrohungen.
- **Ausführliche Security-Audits (Malware-Radar)** und Erkennungs-Tools spüren fortschrittliche Bedrohungen zuverlässig auf.
- **Netzwerk-Zugriffskontrolle** verhindert den Zugriff infizierter oder nicht geschützter Systeme auf das Netzwerk.
- **Applikation-Kontrolle** gibt Administratoren die volle Kontrolle über alle Endpoint- und Netzwerk-Ressourcen.
- **Anti-Spam-Modul** eliminiert unerwünschte Mails auf den Desktops und Exchange Servern.
- **Detaillierte, konfigurierbare Reports** können automatisiert versendet werden und gewährleisten Real-Time Informationen über den Netzwerkstatus.
- **Zentrale Quarantäne** verhindert den Zugriff und die Ausführung von verdächtigen Dateien. Automatisiertes Versenden an die PandaLabs möglich.
- **Echtzeit** Informations- und Alarmsystem.

Weitere Informationen und eine Testversion erhalten Sie unter: **www.pandasecurity.com**

PANDA SECURITY

PANDA SECURITY | *One step ahead.*

www.pandasecurity.com

Zentrale „All-in-One“-Management-Konsole

Panda AdminSecure, das zentrale Administrations-Tool von Panda Security for Business, bietet Echtzeit-Informationen über den aktuellen Schutzlevel des kompletten Netzwerks. Das Nutzer-Interface stellt detaillierte Informationen über alle angeschlossenen Systeme, Workstations, Laptops, File- und Exchange-Server, zur Verfügung.

AdminSecure passt sich jeder Unternehmensnetzwerktopologie an und ermöglicht es, unabhängig von Betriebssystemen, die Anzahl oder Sprachversionen der zu schützenden Systeme festzulegen.

Fortschrittliche proaktive Erkennung

Panda Security for Business beinhaltet die fortschrittlichsten, automatischen proaktiven Technologien, die keine Interaktion des Administrators erfordern. Sowohl eine genetische heuristische Erkennung als auch eine Verhaltensanalyse bieten maximalen Schutz vor bekannten und unbekannten Bedrohungen.

Detaillierte Security Audits

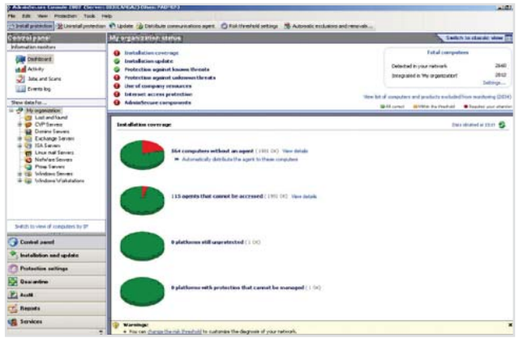
Panda MalwareRadar ist das automatische Audit-Tool zur Erkennung von möglichen Infektionspunkten, die traditionelle Lösungen nicht erkennen.

Basierend auf der **„Collective Intelligence“**-Technologie bietet Malware Radar maximalen Schutz vor versteckten Bedrohungen ohne Aufwand oder zusätzlicher Infrastruktur.

MalwareRadar bietet automatische Security Audits des kompletten Netzwerks und fasst die Ergebnisse in umfassenden Reports zusammen. Des Weiteren liefert es Desinfektions-Routinen und Vorschläge zur Problemlösung.

Network Access Control

Panda ist der einzige Hersteller, der eine Netzwerk-Zugangs-Kontrolle standardmäßig integriert hat. Dieses Feature stellt sicher, dass infizierte oder ungeschützte Systeme keinen Zugriff auf das Netzwerk erhalten.



Application Control

Der Einsatz einiger Applikationen kann die Netzwerksicherheit gefährden oder die Produktivität der Mitarbeiter beeinträchtigen. Dank Panda Security´s Application Control sind Administratoren in der Lage festzulegen welche Programme ausgeführt werden dürfen.

Detaillierte Reports

Konfigurierbare und exportierbare Reports bieten den Administratoren jederzeit einen dataillierten Überblick über den Sicherheits-Status des Netzwerks.

Die Reports können auf Wunsch an mehrere E-Mail-Adressen versendet werden.

Anti-Spam Schutz für Workstations und Exchange Server

Panda Security for Business ist die einzige Lösung, die ein Anti-Spam-Modul für Workstations und Exchange Server beinhaltet und somit die Produktivität erhöht und den Netzwerk-Traffic entlastet.

Die Anti-Spam-Engine erreicht Erkennungsraten von über 95%.

Zentrale Quarantäne

Um eine mögliche Infektion zu verhindern, wird eine unbekannte Bedrohung oder ein potentiell schadhaftes Programm automatisch in die zentrale Quarantäne verschoben bevor Schaden entstehen kann. Um Zeit und Arbeitsaufwand zu sparen, ist ein automatisierter Versand an die PandaLabs möglich.

Alarm- und Informationssystem in Echtzeit

Panda Security überwacht permanent den Sicherheitsstatus des Netzwerkes sowie die Performance der Administrations- und Distributions-Server. Das integrierte Warnsystem informiert den Administrator selbstständig in Echtzeit bei sicherheitsrelevanten Vorfällen.

Panda Collective Intelligence:

“Für Antivirenhersteller ist es überlebensnotwendig, nach immer neuen Wegen zu suchen, um den wachsenden Bedrohungen entgegen zu wirken. Cloud-based Collective Intelligence Services sind der nächste große Schritt. Ich erwarte, dass jeder Antiviren-Hersteller den Schritt zu dieser oder ähnlichen Technologie wagen muss, sofern dieser überleben will.”
Yankee Group: Andrew Jaquith.

Panda Security Zertifikate

TruPrevent: Intelligenter, verhaltensbasierter Schutz

Als Teil des fortschrittlichsten, proaktiven Schutzes integriert Panda Security das Intrusion Prevention System „TruPrevent“ in alle Lösungen.

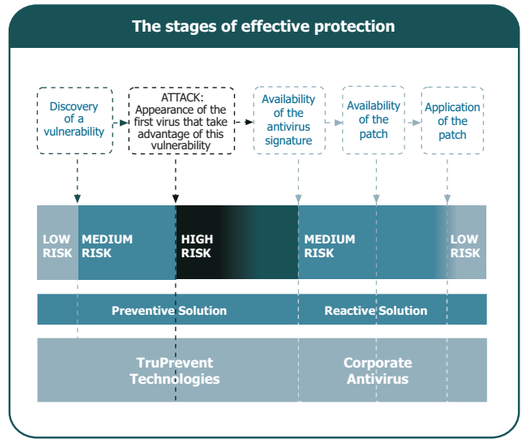
Dank der Erkennungsleistung unbekannter Malware anhand einer umfassenden Verhaltensanalyse, ist Panda´s TruPrevent Technologie das erste System seiner Art, das in der Lage ist, Ausfallzeiten sowie Infektionen und die damit verbundenen Kosten zu minimieren.

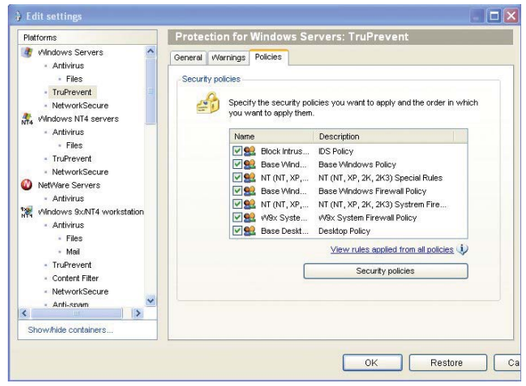
Die Truprevent Technologien sind die Lösung für Workstations und Server, um nicht erkannte Malware automatisch und zuverlässig zu blocken. Würmer, Netzwerk-Viren, Spyware und andere Malware, die von traditionellen Lösungen nicht erkannt werden konnte, wird an der Ausführung gehindert und der Administrator umgehend informiert.

Der Einsatz der TruPrevent Technologien hat viele Vorteile:

- Reduzierung des kritischen Zeitfensters bei neuen Bedrohungen, die Sicherheitslücken ausnutzen, bevor diese geschlossen werden können.
- Gewährleistung des Netzwerk-Sicherheits-Standards durch das Blocken von Hacker-Angriffen, Diebstahl vertraulicher Daten sowie Infektionen durch externe Systeme. Dies gilt ebenfalls für WiFi-Verbindungen und externe Mitarbeiter/Dienstleister.
- Flexibles Security Policy Management garantiert eine vollständige Umsetzung der netzwerkinternen Sicherheitsrichtlinien und schützt so vor Fremdzugriff und Datenmissbrauch durch unzufriedene Mitarbeiter.

Die Truprevent Technologien sind die perfekte Ergänzung zu klassischen Antivirenlösungen und bieten intelligenten Schutz vor neuen Bedrohungen auf allen Netzwerkebenen.





	Panda Security For Business	Panda Security For Business with Exchange	Panda Security For Enterprise
AdminSecure	✓	✓	✓
Panda Security for Desktop	✓	✓	✓
Panda Security for File Server	✓	✓	✓
Panda Security for Exchange		✓	✓
Panda Security for ISAServers			✓
Panda Security for Domino Servers			✓
Panda Security for Sendmail, Qmail und Postfix			✓
Panda Security for Commandline			✓
Panda Security for Management SDK			✓