Panda
Securityfor**Enterprise**

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 / 98 / 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.

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 Security for Domino Servers:
Pentium 133 MHz (or later); 128 MB RAM; Hard Disk: 55 MB Domino cluster.
Operating systems: Windows NT Server 4.0 SP6a (or higher), Windows 2000, Windows 2000 Advanced Server and Windows Server 2003.
Applications: Lotus Domino 4.5.x (or later). Domino Server 8.5 (32 bits).

Panda Security for ISA Servers:
For Microsoft ISA Server 2000:
Pentium II 300 Mhz o higher; RAM: 256 MB; Hard disk: 90 MB.
Operating systems: Windows 2000 Server, Advanced Server SP 1 (o higher) or Windows Server 2003/R2.
Microsoft ISA Server 2004 (Standard and Enterprise Edition) and Microsoft ISA Server 2006 (Standard and Enterprise Edition): Pentium III a 550 MHz o higher (up to 4 CPUs on one server). RAM: 256 MB; Hard Disk: 180 Mb with NTFS.
Operating systems: Windows 2000 Server, Advanced Server SP 4 (or higher) or Windows Server 2003/R2.

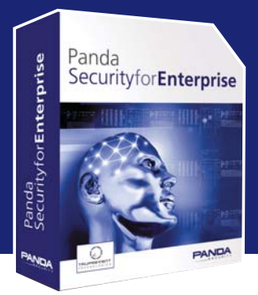
Panda Security for Qmail, Panda Security for SendMail and Panda Security for PostFix:
Pentium II 200 MHz (or higher); 64 MB RAM; Hard Disk: 80 MB, 90MB for PostFix.

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

PANDA SECURITY

Panda Securityfor**Enterprise**

Proaktiver Schutz und Einhaltung der Sicherheitsrichtlinien



Malware-Attacken kosten große Unternehmen 2,2% ihres jährlichen Umsatzes obwohl traditionelle Sicherheitslösungen installiert sind.

Alle großen Unternehmensnetzwerke haben traditionelle Antivirenlösungen zum Schutz Ihres Netzwerkes installiert. Dank dieser Lösungen sind diese Netzwerke grundlegend vor massiven Malware-Ausbrüchen geschützt. Leider sind diese Produkte jedoch anfällig für zielgerichtete Angriffe oder Zero-Day-Attacks.

Tatsache ist, dass die Schäden, die diese Unternehmen beispielsweise 2008 hinnehmen mussten, durchnschnittlich 2,2% des Jahresumsatzes ausmachten. In vielen Fällen attackierte Malware die Netzwerk-Ressourcen oder legte diverse Systeme lahm. Diese Art der Angriffe führt zu einem massiven Produktivitätsverlust. Häufig sind diese Firmen auch zielgerichteten Angriffen ausgesetzt. Diese Attacken sind in der Regel „lautlos" und werden von traditionellen, verhaltensbasierten Sicherheitslösungen nicht erkannt. IT-Sicherheitsherseller, die weiterhin auf die signaturbasierte Erkennung setzen, sind aufgrund der massiv gestiegenen Bedrohungssituation nicht in der Lage, vollständigen Schutz zu bieten.

Große Unternehmen benötigen eine komplette Lösung. Das Management des vollständigen Netzwerks sowie proaktive und präventive Abwehrtechnologien sind unbedingt erforderlich. Die aktuelle Bedrohungssituation erfordert umfassende Sicherheitsrichtlinien und eine Lösung, die diese Bedürfnisse aufnimmt und professionell umsetzt.

Netzwerk-Sicherheitsrichtlinien schützen vor Umsatz- und Produktivitätsverlusten und sind somit fester Bestandteil der täglichen Arbeitsabläufe.

"Große Netzwerke haben die Standard-Client-Sicherheit größtenteils im Griff. DOS- und serverbasierten, zielgerichteten Attacken gegenüber ist man jedoch in der Regel wehrlos ausgeliefert. Große Unternehmen sind ganz besonders und in immer größerem Maße, Ziele dieser zielgerichteten Angriffe…"
Infonetics: The Cost of Network Security Attacks: Infonetics Research.

Die Lösung: Panda Security for Enterprises

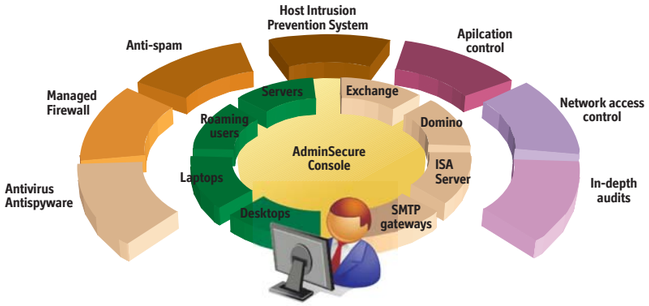
Panda Security for Enterprises bietet die fortschrittlichsten **proaktiven Technologien.** Die **flexible Architektur** ermöglicht kompletten Netzwerkschutz auf allen Ebenen. Applikations- und Netzwerk-Zugangskontrolltechnologien runden die Lösung ab.

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

Die Panda Security Lösung für große Unternehmensnetzwerke bietet maßgeschneiderten Schutz für alle potentiellen Angriffsziele: Workstations, File-, E-Mail (Exchange & Domino) und ISA Server sind ebenso geschützt wie MTAs.

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



"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 Technologiengewährleisten einen maximalen Schutzlevel.
- **Unterstützung bei der Implementierung** und Durchführung von Netzwerk-Sicherheitsrichtlinien durch Netzwerkzugangs- und Applikationskontrollen.
- **Reduzierung der 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.
- **Steigerung der Mitarbeiter-Produktivität** durch das Herausfiltern von Spam-Mails und der Sperrung von unerwünschten Applikationen.
- **Verbessertes Risiko-Management** durch Echtzeit-Analyse der aktuellen Bedrohungssituation und ausführliche Security-Audits.

Key-Features

- **Zentrale „All-in-one-Konsole"** zur Adminstration des kompletten Netzwerks inklusive Real-Time-Monitoring.
- **Integriertes Intrusion Prevention System** und verhaltensbasierte Erkennungs-Technolgien bieten maximalen Schutz vor unbekannten Bedrohungen.
- **Tiefgreifende 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.
- **Applikations-Kontrolle** gibt Administratoren die volle Kontrolle über alle Endpoint und Netzwerk-Ressourcen.
- **Systemübergreifender Schutz** und flexible Architektur gewährleisten einen gleichmäßig hohen Sicherheitsstandard in heterogenen Netzwerken auf allen Servern, Gateways und Exchange-Plattformen.
- **Detaillierte, konfigurierbare Reports** können automatisiert versendet werden und gewährleisten **Echtzeit-Informationen** über den Netzwerkstatus.

PANDA SECURITY | *One step ahead.*

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 Netzwerktopologie an und ermöglicht, unabhängig von Betriebssystemen, die Anzahl oder Sprachversionen der zu schützenden Systeme festzulegen.

Fortschrittliche proaktive Erkennung

Panda Security for Enterprise 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

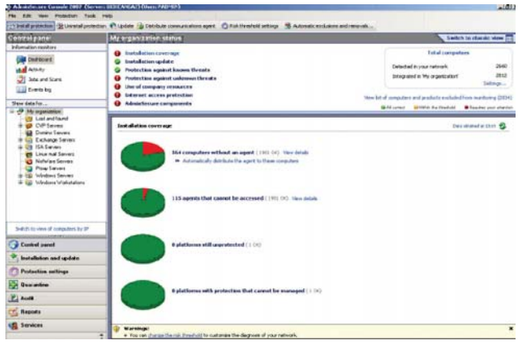
Panda MalwareRadar ist das automatische Audit-Tool zur Erkennung von möglichen Infektionspunkten, die traditionelle Lösungen nicht erkennen.

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



Anti-Spam-Schutz für Workstations und Exchange Server

Panda Security for Enterprise 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%.

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.

Mehrschichtige und flexible Architektur

Panda Security for Enterprise bietet maßgeschneiderten Schutz für heterogene Netzwerkumgebungen auf nahezu allen Servern, Gateways und Exchange Plattformen. Das integrierte Software Development Kit ermöglicht die Integration von Management- oder Verteil-Tools externer Anbieter.

Commandlinesecure, die ideale Lösung für alle Administratoren, die ein heterogenes Netzwerk ohne Windows-Interface verwalten, ist ebenfalls Bestandteil von Panda Security for Enterprise.

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.

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 das jeder Antivirus 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.

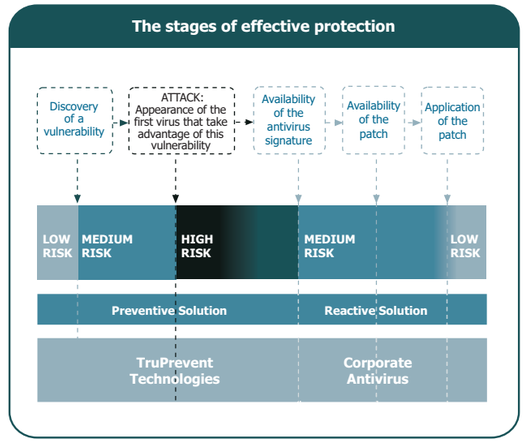
Dank der Erkennungsleistung unbekannter Malware anhand einer umfassenden Verhaltensanalyse, ist Panda´s TruPrevent Technologie das erste System seiner Art, das in der Lage ist, Ausfallzeiten sowie Infektionen und die damit verbundenen Kosten zu minimieren.

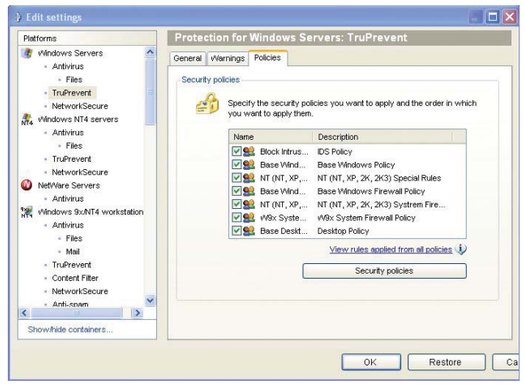
Die Truprevent Technologien sind die Lösung für Workstations und Server, um nicht erkannte Malware automatisch und zuverlässig zu blocken. Würmer, Netzwerk-Viren, Spyware und andere Malware, die von traditionellen Lösungen nicht erkannt werden konnte, wird an der Ausführung gehindert und der Administrator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