

# Panda GateDefender Performa

Maximaler Perimeter-Schutz



## Jede Internetverbindung stellt für Unternehmens-Netzwerke eine potentielle Gefahr dar

99% aller Infektionen, die Unternehmensnetzwerke angreifen, werden via Internet übertragen. 70% des gesamten Internet Traffics besteht aus unproduktivem, nicht unternehmensrelevanten Inhalten.

Der Verlust sensibler Daten ist eine der schwerwiegendsten Folgen, die Internet-Bedrohungen für Unternehmen bedeuten können.

Die erste Verteidigungslinie gegen Content basierte Gefahren ist eine Perimeterschutzlösung, die proaktiv gefährliche und unerwünschte Inhalte blockiert und vor dem Verlust kritischer Informationen schützt.

**"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."**  
*Andrew Jaquith, Yankee Group*

## Die Lösung: Panda GateDefender Performa

Panda GateDefender Performa ist eine leistungsstarke Appliance für Perimeter-Schutz. Die Lösung schützt Unternehmensnetzwerke proaktiv vor allen Internetbedrohungen. Dabei lässt sie sich mühelos in jede Infrastruktur implementieren ohne wertvolle Ressourcen zu belasten.

Die Appliance erweitert ihre proaktiven Schutztechnologien um die „Collective Intelligence“ um alle Netzwerkrisiken effektiv zu bekämpfen. Panda GateDefender Performa besteht aus fünf Schutz-Modulen:

- **Malware-Schutz:** Automatischer Schutz gegen alle Malware-Exemplare.
- **Content-Filter:** Ermöglicht die Definition verschiedener Sicherheits-Richtlinien.
- **Spam-Filter:** Befreit Posteingänge zuverlässig vom Spam.
- **IM/P2P-Blocking:** Unterbindet den Missbrauch der Netzwerk-Ressourcen.
- **Web Filtering:** Blockt den Zugriff auf unproduktiven Web-Seiten.



Die GateDefender Serie ist in drei Hardware-Modellen erhältlich, die individuell an Größe und Datenvolumen einzelner Unternehmen angepasst werden können:

	Traffic flow	GD SB	GD 9100	GD 9500 Lite	GD 9500 Large
HTTP	Mbps	40	400	500	700
	Transactions/sec	98	2950	4726	4726
SMTP	Messages/sec	80	220	400	550
TCP	Connections/sec	84	1008	3028	3028
	Concurrent connections	550	9800	18000	18000

### One step ahead...

**"Im Jahr 2010 werden brauchbare Lösungen schädliche Inhalte von ein- und ausgehenden Daten über Protokolle filtern."**

*Gartner*

**Panda GateDefender Performa funktioniert nach diesem Prinzip bereits seit seiner Markteinführung im Jahr 2004. Dies bestätigt die führende Position Panda Security's für technologische Innovationen.**

### Vorteile

- **Proaktive Erkennung und Entfernung** unbekannter Bedrohungen.
- **"Plug and Protect"**. Keine Konfiguration oder Aufrüstung der Netzwerkarchitektur notwendig.
- **Gewährleistet die permanente Verfügbarkeit** von Internet und E-Mail selbst im Falle einer Störung oder eines Ausfalls.
- **Erhöht die Mitarbeiterproduktivität** dank:
  - Entfernung vom Spam aus den ankommenden E-Mails
  - Einschränkungen in der Nutzung von P2P- und Instant Messaging-Anwendungen
  - Kontrolle des Zugangs zu Web-Inhalten
- **Annähernd 100% Spam-Erkennung** dank neuer, verbesserter Anti-Spam-Techniken.
- **Niedriger Ressourcenverbrauch** verbessert die Performance und steigert die Produktivität.
- **Sichert den Ruf des Unternehmens**, indem der unwissentliche Missbrauch der internen Rechner zum Versand vom Spam verhindert und infizierte Rechner aufgespürt werden.

### Key Features

- **Proaktiver Schutz** durch innovative Technologien. In der Appliance wirken heuristische Analysen, 'Collective Intelligence' sowie Quarantäne und optimieren die Erkennungsraten.
- **Umfassende Sicherheit.** Perimeter-Schutz gegen alle Bedrohungen: Dies beinhaltet „Best-of-breed“-Technologien gegen alle Malware-Arten und potentiell gefährliche Inhalte (Panda), Spam (Cloudmark) oder unerwünschte Web-Inhalte (IBM/Cobion). Zusätzlich wird der Gebrauch gefährlicher Programme wie P2P oder IM beschränkt.
- **Flexibles Risiko-Management.** Die Definition verschiedener User-Gruppen ermöglicht es, individuelle und flexible Sicherheitsrichtlinien für jeden Netzwerk-User zu erstellen. Alle ein- und ausgehenden Inhalte werden dem jeweiligen User-Profil entsprechend analysiert.
- **Erkennung von Zombies** auf individuellen Computern und Mail-Servern durch die Erkennung von ausgehenden SMTP-Mails.
- **Garantierter Datenfluss.** Die Bypass-Option hält auch bei Systemfehlern den Datenfluss aufrecht.
- **Spammer-Blacklist.** Steigert die Spam-Erkennungsrate bis annähernd 100%.
- **Automatischer Schutz.** Automatische Signatur-Updates und grafische Reports in Echtzeit.
- **Zentralisiertes Monitoring und Administration.** Der Administrator kann eigens definierte Reports der Schutzmodule zentralisiert über eine einzige Konsole erstellen.

## Perimeter-Schutz

Panda GateDefender Performa ist eine Appliance, die höchste Performance und bestmöglich Schutz am Haupteintrittspunkt für Malware in Netzwerke garantiert. Sie scannt die verbreiteten Protokolle HTTP, FTP, SMTP, POP3, IMAP4 und NNTP.

## Umfassender Proaktiv-Schutz



Panda GateDefender Performa entdeckt und blockiert alle Arten von Internet-Bedrohungen noch bevor sie ins Netzwerk eindringen. Es schützt vor

Viren	Würmern	Spyware
Phishing	Dialer	Hacking-Tools
Trojaner	Jokes	Sicherheitsrisiken

Dank seiner heuristischen Analyse und der „Collective Intelligence“ entdeckt es sogar unbekannte Malware Exemplare.

## Zombie-Erkennung



Mit der Erkennung von abgehendem SMTP-Verkehr können die Administratoren interne Computer ermitteln, die infiziert worden sind und ohne Kenntnis des Anwenders Spam und Malware an Kunden und Kontakte senden. Dies trägt zum Ansehen und Ruf des Unternehmens bei den Kunden bei.

## Spam-Filter



Das Anti-Spam-Modul der Appliance wehrt Junk Mails direkt am Haupteintrittspunkt des Netzwerks ab. Dies garantiert volle Mitarbeiterproduktivität.

## Optimierte Internetnutzung



Mit dem Web-Filtermodul können Administratoren den Zugriff auf nicht unternehmensrelevante Webseiten einschränken. Dies kann automatisch oder manuell nach definierten Kategorien geschehen.

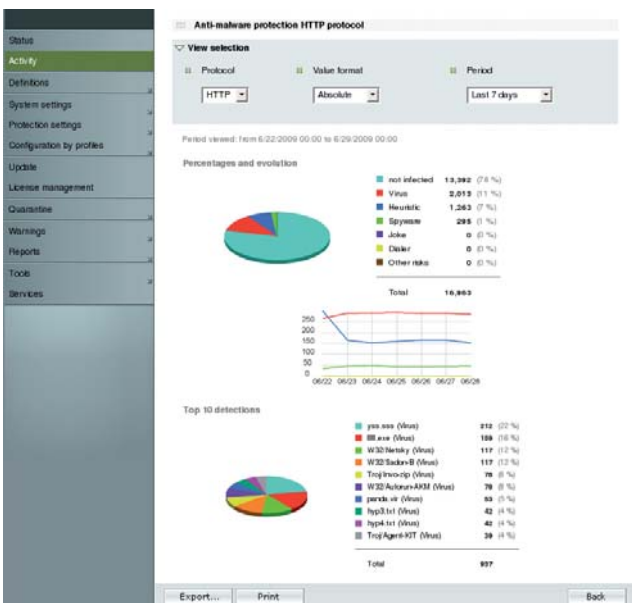
## Effektive Ressourcenauslastung



Panda GateDefender Performa kann den Zugriff auf Instant Messaging und Peer-to-Peer-Programme verweigern und den optimalen Gebrauch der Netzwerk-Ressourcen sichern.

## Real-Time Monitoring

Die Konsole ermöglicht es, den Sicherheitsstatus mit Echtzeit-Reporten zu dokumentieren. Der Administrator kann sowohl periodische Auswertungen als auch detaillierte Protokolle einzelner Schutzmaßnahmen erstellen.



Revision 4. 7 2009

## Zentralisierte Verwaltung

Alle Schutzmodule, die im Netzwerk angewendet werden, können über eine einzige Konsole administriert werden.

## Individuelle Sicherheitsrichtlinien

Panda GateDefender Performa integriert sich mit LDAP und Active Directory. Die optionale Definition von User-Profilen und –Gruppen erlaubt es Administratoren, individuelle Sicherheitsrichtlinien zu verfassen, die an die jeweiligen Bedürfnisse des Users angepasst sind.

## Kontrollierter Daten-Empfang

Panda GateDefender beinhaltet drei Quarantäne-Typen:

- Unbekannte oder nicht desinfizierbare Malware
- Spam-Mails
- Dateien, die den Sicherheitsrichtlinien nicht entsprechen

Die Dateien der Quarantäne-Ordner können entweder abgerufen oder direkt gelöscht werden. Verdächtige Dateien werden an die Panda Security Sicherheitslabore gesendet, damit sie desinfiziert und in die Signatur aufgenommen werden können.

## „Connect and forget“

Die Appliance arbeitet im transparenten Bridge-Modus. Der Netzwerk-Traffic muss nicht umgeleitet werden. Sie wird bereits vor der Installation konfiguriert und aktiviert ihre Schutz-Module über eine Web-Konsole.

## Zentralisiertes Monitoring

Das System sendet kundenspezifische Warnmeldungen durch SNMP, SNP und/oder Syslog. Die Administratoren können die Versand-Methode je nach Vorfall bestimmen.

## Hohe Skalierbarkeit

Panda GateDefender Performa garantiert mit automatischem Load-Balancing eine optimale Netzwerkleistung.



## Optimierter Datenfluss

Hardware-Modelle für große Unternehmen beinhalten eine Bypass-Option, die den unbeeinträchtigten Datenfluss auch bei Systemfehlern Aufrecht erhält.

