

# Panda GateDefenderIntegra

Unified Business Protection



Bedrohungen aus dem Internet nehmen dramatisch zu und werden immer komplexer. Um schwerwiegende Folgen zu vermeiden, müssen Eindringlinge blockiert werden, noch bevor sie ins System eindringen.

99% aller Gefahren für Unternehmensnetzwerke stammen aus dem Internet. Das Gateway ist daher bei der Netzwerksicherheit ganz besonders zu beachten. Schutzmodule, die dort platziert sind, können schädliche Prozesse stoppen, bevor Sie die interne Netzwerkumgebung erreichen.

Internet-Gefahren werden in zwei Gruppen unterteilt:

- Netzwerk basierte Bedrohungen (unauthorisierte Verbindungen, Eindringlinge, Datendiebstahl).
- Content basierte Bedrohungen (Viren, Würmer, Spyware, Spam).

**"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, analyst of Yankee Group*



## Die Lösung: Panda GateDefender Integra

Panda GateDefender Integra vereint leistungsstarken Perimeterschutz in einer einzigen, einfach zu bedienenden Oberfläche. Auf diese Weise ist die Netzwerkumgebung von Unternehmen jederzeit umfassend und proaktiv vor allen Bedrohungen geschützt. Dies sind die integrierten Schutzmodule:

- **Firewall:** Passt die interne und externe Kommunikation der Sicherheitsrichtlinien an.
- **Intrusion Prevention System (IPS):** Schützt Netzwerke vor unbekanntem Angriffen.
- **VPN:** Schützt sensible Daten, die via Internet versendet werden.
- **Anti-Malware:** Schutz gegen alle Internet-Bedrohungen.
- **Content-Filter:** Konfigurierbarer Inhaltsfilter ermöglicht die Anpassung an interne Sicherheitsrichtlinien.
- **Web-Filter:** Verweigert den Zugriff auf nicht unternehmensrelevante Webseiten.



Zwei verschiedene Hardware-Modelle für die Sicherheitsbedürfnisse von KMU's:

| Hardware Model                                                                          | Recommended Number of users | Firewall Throughput | Concurrent Sessions | 10/100/1000 Eth ports |
|-----------------------------------------------------------------------------------------|-----------------------------|---------------------|---------------------|-----------------------|
|  SB  | Up to 50                    | 400 Mbps            | 180.000             | 4                     |
|  300 | Up to 250                   | 850 Mbps            | 550.000             | 8                     |

### Main benefits

- **Plug 'n' Protect.** Sie müssen keine Konfiguration vornehmen. Einfach anschließen und sofort geschützt sein.
- **Reduziert die Komplexität.** Alle notwendigen Funktionen in einem einzigen, benutzerfreundlichen Interface.
- **Minimiert die Verwaltungskosten** durch wartungsfreien Schutz, automatische Updates und Echtzeit-Reports.
- **Entspricht den Sicherheitsvorschriften des Unternehmens,** indem es kritische Dateien nach ihrem Inhalt oder User spezifisch filtert.
- **Steigert die Produktivität** dank eines Spam-Filters und dem beschränkten Zugang zu unproduktiven Webseiten.
- **Verhindert den Verlust sensibler Daten** durch die Kontrolle ein- und ausgehender Daten sowie die Verschlüsselung von Informationen im Internet.

### Key features

- **Die einzige "Install and Protect" UTM.** Dies beinhaltet „Best-of-breed“-Technologien gegen alle Malware-Arten und potentiell gefährliche Inhalte (Panda), Spam (Cloudmark) oder unerwünschte Web-Inhalte (IBM/Cobion). Diese werden mit einer Deep Packet Inspection Firewall, einem leistungsstarken IPS sowie einem VPN Server in einem einzigen Modul zusammengefasst.
- **Umfassender 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). Diese werden mit einer Deep Packet Inspection Firewall, einem leistungsstarken IPS sowie einem VPN Server in einem einzigen Modul zusammengefasst.
- **Dauerhafte, automatische Updates:** Updates von Regeln und Finger-Prints werden für Malware, IPS und Web-Filter alle 15 Minuten, für Spam jede Minute durchgeführt.
- **Optimierte Netzwerkressourcen:** Eingeschränkter Web-Zugriff auf unproduktive Seiten garantiert die volle Produktivität der Mitarbeiter. Die 98%ige Spamererkennung befreit Email-Server und interne Netzwerke von Junk Mails.
- **Proaktiver Content-Filter** scannt ein- und ausgehenden Traffic auf der Grundlage der jeweilig definierten Sicherheitsrichtlinien des Unternehmens. Jede Kommunikation kann mit Hilfe eines VPNs verschlüsselt werden.

## Gateway Level Protection

Hard- und Software des Panda GateDefender Integra garantieren bestmögliche Schutzfunktionen direkt am Gateway. Sie scannen die gängigen Protokolle in Echtzeit:

- HTTP, FTP, SMTP, IMAP4, POP3 und NNTP
- IP, TCP, UDP und ICMP
- IPSec, SSL, L2TP und PPTP

## Größere Kontrolle



Die Firewall kontrolliert die Kommunikation zwischen Netzwerk und Internet oder zwischen allen Netzwerkebenen, Usern, Gruppen usw.

Die Panda Firewall kann zwei verschiedene Filterungen vornehmen:

- 1. Statische Filterung auf Netzwerkebene** basiert auf vom Administrator definierten Regeln für ein- und ausgehenden Traffic.
- 2. Dynamische Filterung auf Anwendungsebene** mit
  - a. Stateful Inspection** überwacht den Inhalt der Basis-Kommunikation in allen Protokollen. Für erweiterte Kommunikation kontrolliert er FTP, PPTP, L2TP und IPSEC.
  - b. Deep Packet Inspection** scannt den Inhalt von Paketen zur Untersuchung von Nachrichten in HTTP, FTP, SMTP, IMAP, POP3 usw., wenn andere Module aktiviert sind.

## Sichere Übertragung



VPN garantiert eine sichere Internet-Kommunikation mit Nutzern außerhalb des Netzwerks. Es verschlüsselt die Daten vor der Übertragung und entschlüsselt sie erst bei ihrer Ankunft. Dabei funktioniert es unter Host-to-Host-, Host-to-Net- und Net-to-Net-Konfigurationen. Unterstützt werden IPSec, SSL, L2TP und PPTP Protokolle sowohl im Server- als auch im definierbaren Client-Modus.

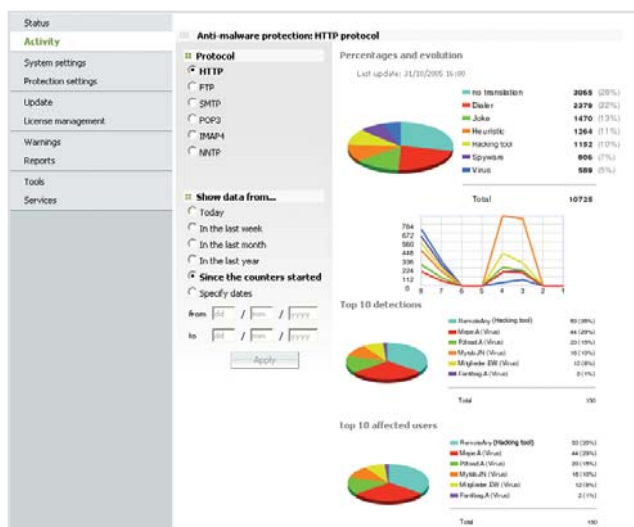
## Stärkerer Schutz



Das integrierte IPS schützt anhand von Sicherheitsrichtlinien gegen externe Attacks. Administratoren können das System so konfigurieren, dass erkannte Angriffe automatisch blockiert werden. Außerdem können sie für jede Regel bestimmte Schwellenwerte festlegen, um die Anzahl der Fehlalarme zu verringern.

## Gesteigerte Produktivität

Der Web-Filter beschränkt den Zugriff auf unangemessene oder nicht unternehmensrelevante Webseiten. Eine volle Produktivität am Arbeitsplatz wird somit gewährleistet.



Revision 1.06 2009

## Real-Time-Monitoring

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

## Vollständiger Schutz



Panda GateDefender Integra entdeckt und blockiert alle Arten von Internet-Bedrohungen, die in das Netzwerk eindringen können:

- |          |        |                    |
|----------|--------|--------------------|
| Viren    | Würmer | Spyware            |
| Phishing | Dialer | Hacking-Tools      |
| Trojaner | Jokes  | Sicherheitsrisiken |

Dank seiner heuristischen Scanmethoden auf Basis der "Collective Intelligence" werden auch unbekannte, noch nicht gelistete, Malware-Exemplare proaktiv abgewehrt.

## Security Compliance



Mit Hilfe des Content-Filter können Administratoren die Sicherheit für das jeweilige Unternehmen festlegen. So können sie definieren, welche Dateien und/oder E-Mails in dem Netzwerk empfangen oder aus dem Netzwerk versendet werden. Dies wirkt dem Verlust sensibler Daten und sonstigen Sicherheitsrisiken proaktiv entgegen.

## Spam-Filter



Der Spam-Filter wehrt Junk Mails direkt am Haupteintrittspunkt des Netzwerks ab und leitet unverzüglich die entsprechenden vordefinierten Maßnahme ein.

## Optimiertes Web-Surfing



Mit dem Web-Filter können Administratoren den Zugriff auf Webseiten mit unproduktiven Inhalten einschränken. Dies kann anhand vorgegebener Kategorien und/oder Black-/Whitelisting erfolgen. Dadurch wird die Verwendung der Ressourcen optimiert und die allgemeine Produktivität verbessert. GateDefender Integra stellt für die Restriktion eine Auswahl von 60 Kategorien.

## Zentralisiertes Monitoring

Das System sendet automatisch kundenspezifische Warnmeldungen durch SNMP, SNP und/oder Syslog. Die Administratoren können die Versandmethode je nach Vorfal bestimmen.

## Automatische Updates

Sowohl die Signaturdatei für Malware-Schutz und Content-Filter, als auch die Datenbank für den Web-Filter und das IPS-Regelwerk, werden alle 15 Minuten aktualisiert. Für den Spam-Fingerprint wird ein minutliches Micro-Update durchgeführt, um bestmögliche Erkennungsraten zu erzielen.

