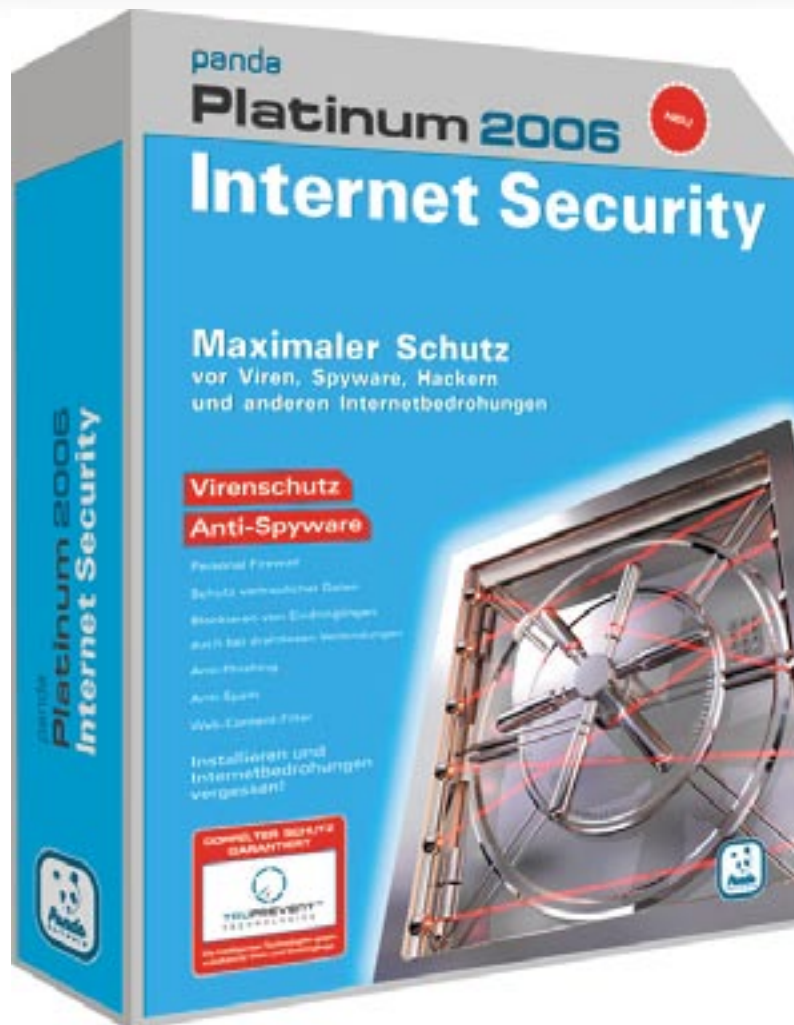


**PROTECTSTAR<sup>®</sup>**

**AWARD  
2006**

[www.protectstar.com](http://www.protectstar.com)



***Panda***  
***Platinum 2006***

**PROTECTSTAR<sup>®</sup>**  
for your security

## EINLEITUNG

Platinum 2006 Internet Security von Panda Software ist die vollständige Sicherheitslösung für alle Einzelplatz-Systeme und serverlose Netzwerke (peer-2-peer) zum Schutz vor allen Bedrohungen des Internets.

Unter einer übersichtlichen Oberfläche vereint Panda's Internet Security Suite 2006 den Schutz vor Viren, Würmern, Trojanern, Dialern, Hacking- und Phishing-Attacken, Spam-Mails, unerwünschten Web-Inhalten und bisher noch unbekannter Malware.

Quelle: [www.panda-software.de](http://www.panda-software.de)

## SICHERHEIT

**Platinum 2006 Internet Security** zeichnet sich durch eine Vielzahl an integrierten Schutzmodulen aus. Zu diesen Modulen gehören Antivirus, TruPrevent™ Technologien, Anti-Spyware, Anti-Phishing, Anti-Pharming, Anti-Spam, Anti-Dialer, Personal Firewall, Privacy Control, und Web Content Filter.

In den Testreihen wurde **Platinum 2006 Internet Security** sowohl unter Laborbedingungen, als auch unter **realen Bedingungen** gleichermaßen getestet.

Im Testlabor von ProtectStar® konnte **Platinum 2006 Internet Security** in der aktuellen Softwareversion **10.01.02** getestet werden. Turnusmäßig musste die Sicherheitslösung umfassende Testreihen durchlaufen.

Die in **Platinum 2006 Internet Security** integrierte **Personal Firewall** kommt seit der Version 2006 nicht mehr von Sygate, sondern ist eine **Eigenentwicklung** aus dem Hause **Panda Software**. Die Personal Firewall schützt den PC vor unbefugten Zugriffen Dritter, ist intuitiv zu bedienen und individuell konfigurierbar. So ist beispielsweise der Netzwerkzugriff auf Basis von Mac- oder IP- Adressen möglich. Der Internetzugriff (erlaubt, verboten, auf Nachfrage) jeder einzelnen Applikation kann individuell festgelegt werden.

Die Personal Firewall hat an den Tagen der Testverfahren alle zum Zeitpunkt bekannten **9940** verschiedenen **Angriffs- und Sicherheitstests** erfolgreich abgewehrt.

Die Sicherheitstests enthielten alle bekannten **Denial of Service (DoS)** – Angriffsarten, sowie die **Ausnutzung** aller zum Zeitpunkt der Testverfahren bekannten **Schwachstellen** von Betriebssystemen, Anwendungen, CGI abuses, Useless services, Backdoors, Sicherheitschecks, uvm.

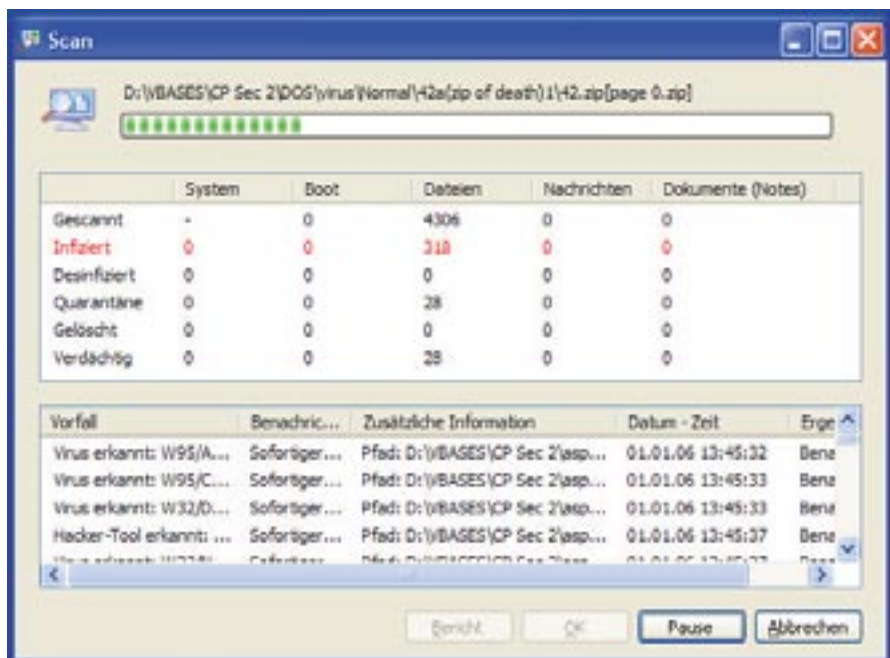
In einer weiteren Testphase wurde die Personal Firewall in den **Werkseinstellungen** betrieben und mit standardisierten Portscans nach eventuell geöffneten TCP- und UDP- Ports gescannt. Dabei wurden alle Ports (0 – 65535) gescannt. Im **zweiten Schritt** wurde die Firewall einem SYN-Portscan (half-open) - dem so genannten Stealth-Scan - unterzogen.

Im Rahmen der durchgeführten Portscans (tcp-connect und syn/half-open) fanden sich **keine** geöffneten Ports und **keine** unnötigen Dienste, die für gewöhnlich zu Sicherheitsproblemen führen können. Sowohl durch die **automatisch** ablaufenden Testreihen des hauseigenen **ProtectStar® Security-Scanners**

(zusätzlich **7014** weitere Sicherheitstests und Angriffstaktiken) als auch durch die **manuell** durchgeführten Prüfungen konnten **keine** sicherheitsrelevanten Schwachstellen festgestellt werden.

Den **zweistündigen** Dauer-**Penetrationstest** konnte die Personal Firewall ebenfalls **erfolgreich** absolvieren. Mit Hilfe der so genannten „**Leaktests**“ wurde weiterhin überprüft, ob die Personal Firewall Techniken erkennt, um Informationen (Passwörter, persönliche Daten, usw.) von einem Computer aus in das Internet vorbei an der Firewall zu schleusen:

Bei detaillierter Analyse stellten die Sicherheitsexperten von ProtectStar® fest, dass bereits der in Platinum 2006 Internet Security integrierte **Antiviren-Scanner**



die bekannten **Leaktest-Programme** als **Malware** einstuft und entsprechend den Zugriff auf die Dateien blockiert.

So wurden folgende Meldungen vom Antiviren-Scanner ausgegeben:

- **CopyCat** (Hacker-Tool erkannt!)
- **DNSTESTER** (Tracking-Programm erkannt!)
- **FireHole** (Tracking-Programm erkannt!)
- **Ghost** (Tracking-Programm erkannt!)
- **Leaktest 1.2** (Tracking-Programm erkannt!)
- **PCAudit** (Tracking-Programm erkannt!)
- **PCAudit 2** (Tracking-Programm erkannt!)
- **Surfer** (Tracking-Programm erkannt!)
- **Tooleaky** (Tracking-Programm erkannt!)
- **Yalta** (Tracking-Programm erkannt!)

Da die Leaktest-Programme ebenfalls in der „**Virus Encyclopedia**“ von **Panda Software** entsprechend gelistet sind, ist davon auszugehen, dass lediglich die **bekanntesten Signaturen** der öffentlich zugänglichen Leaktest-Programme in der AntiViren-Datenbank von Panda Software gespeichert sind. Eigens programmierte Leaktest-Programme werden **nicht** mehr als Malware erkannt.

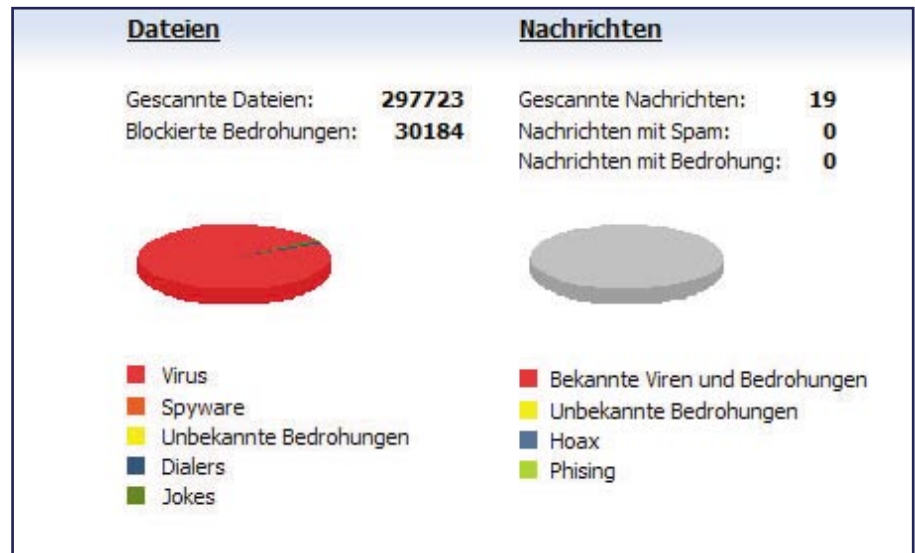
Auf der einen Seite bedeutet diese Art der Prävention von Panda Software eine **höhere Schutzfunktion**, da die bekannten Leaktest-Programme vor deren Ausführung von dem integrierten Antiviren-Scanner als Schadware erkannt werden und der Zugriff entsprechend verhindert wird. Andererseits wird hierdurch das Hauptproblem der Personal Firewall – die Schwachstellen der Anwendungssteuerung der Firewall – **nicht behoben**, sondern lediglich das Schutzniveau der Personal Firewall von Panda Software mit Hilfe des Antiviren-Scanners **scheinbar** ergänzt.

Bei weiterer Analyse mit Hilfe der Leaktests an **Platinum 2006 Internet Security** stellten die Sicherheitsexperten von ProtectStar® fest, dass es **nicht möglich** ist, **einzelne Schutzmodule** in Platinum 2006 Internet Security zu aktivieren bzw. zu deaktivieren. Es ist deshalb während dieser Testreihen nicht möglich gewesen, die Personal Firewall als **einzigste Schutzinstanz** zu aktivieren – alle anderen Schutzmodule sollten deaktiviert sein – um eine Durchführung der Leaktest-Programme dennoch zu ermöglichen.

Es ist zwar möglich **alle Schutzmodule** gleichzeitig zu **deaktivieren**, wird jedoch versucht ein beliebiges Schutzmodul (bspw. Personal Firewall) zu aktivieren,

schalten sich alle anderen Schutzfunktionen wieder automatisch an. Hier sollte Panda Software nachbessern, damit Anwender einzelne **Schutzmodule** entsprechend manuell **aktivieren** und/oder **deaktivieren** können.

Der in Platinum 2006 Internet Security integrierte **Antiviren-Scanner** ist seit der Version 2005 zusätzlich mit einer **Antispyware Engine** ausgestattet. Dadurch ist Platinum Internet Security



in der Lage, nicht nur bekannte Viren, Würmer und Trojaner, sondern auch **Spionage**-Programme zu erkennen und zu beseitigen.

Beide Schutzmodule – sowohl Antiviren-Scanner als auch Anti-Spyware Engine – arbeiten auf der **Winsock Ebene** und ermöglichen, dass Daten direkt in allen Bereichen des Systems überprüft werden, unabhängig davon, ob Dateien aus dem Internet heruntergeladen werden, E-Mails empfangen oder per CD/DVD oder USB transferiert werden.

Um die Schutzfunktionen des integrierten Panda **Anti-Virenschanners** testen zu können, wurden acht umfangreiche Viren- und Malwarearchive erstellt. Diese Archive umfassten insgesamt über **dreißigtausend** verschiedene Schädlinge. Von ganz neuen und aktuellen Viren, Würmern, Trojanern, Dialern und Spyware, bis hin zu alten MS-Dos Bootviren und selbstentwickelten unbekanntem Schädlingen.

Zusammenfassend konnte die **Virenerkennungsrate** des in Platinum 2006 Internet Security integrierten Virenschanners auf **98,20%** bestimmt werden. Im Vergleich zu den durchgeführten Testreihen zur Vorgängerversion Platinum 2005 Internet Security im **April 2005**, konnte festgestellt werden, dass sich die Virenerkennungsrate der Version 2006 um knapp **5%** verbessern konnte.

Um einige Resultate des Antiviren-Scanners von Panda Software zu verdeutlichen, werden anbei folgende Referenzwerte aus zwei beliebigen ProtectStar®-Testarchiven angegeben aus denen ersichtlich ist, wie viele **Schadprogramme** (inkl. Virenerkennungsrate in %) der Antiviren-Scanner der jeweiligen **Referenzprodukte** und der von **Platinum 2006 Internet Security** erkannte:

<b>Archiv „Objekte 1“ (1950 Schadprogramme):</b>			
1.	<b>Platinum 2006 Internet Security:</b>	1936	[99,28%]
2.	Norton Internet Security 2006	1931	[99,03%]
3.	Kaspersky AV PRO 5.0	1927	[98,82%]
4.	PC-cillin Internet Security 14	1920	[98,46%]
5.	GData AVKIS 2006	1908	[97,85%]
6.	F-Secure AV 2006	1906	[97,74%]
7.	NOD32 v2.5	1861	[95,44%]

<b>Archiv „Objekte 2“ (3100 Schadprogramme):</b>			
1.	Kaspersky AV PRO 5.0	3029	[97,71%]
2.	<b>Platinum 2006 Internet Security</b>	2990	[96,45%]
3.	Norton Internet Security 2006	2968	[95,74%]
4.	NOD32 v2.5	2913	[93,97%]
5.	F-Secure AV 2006	2873	[92,68%]
6.	PC-cillin Internet Security 14	2861	[92,29%]
7.	GData AVKIS 2006	2366	[76,32%]

Weitere Resultate können unter [testcenter@protectstar.com](mailto:testcenter@protectstar.com) angefragt werden Angaben ohne Gewähr. Irrtümer vorbehalten.

Aufgefallen ist während dieser Testreihen, dass der Antiviren-Scanner von Platinum 2006 Internet Security (Softwareversion: **10.01.02**) **Schwierigkeiten** mit so genannten „**Zip of Death**“ – Archiven hat. Zwar überprüft der Antiviren-Scanner ordnungsgemäß den Inhalt dieses Zip-Archivs, allerdings wird die Scangeschwindigkeit dermaßen **abgebremst**, dass der Antiviren-Scanner für unsere Testdatei namens „**protectstar-zod42.zip**“ mit einer Größe von **42KB** über **zwei Stunden** benötigte, um den Inhalt dieser Datei zu analysieren. Vergleichsweise benötigte die Scanengine des Produkts „**Kaspersky Anti-Virus Personal Pro 5.0**“ für dieselbe Datei weniger als **acht Sekunden**.

Der Hersteller **Panda Software** wurde über diesen Vorfall informiert und verspricht den Vorfall zu überprüfen und ein Patch bereitzustellen.

**Besonders erwähnenswert** sind die in Platinum 2006 Internet Security integrierten **TruPrevent™ Technologien**. Diese Technologien sind in der Lage, unbekannte Bedrohungen zu erkennen. Hierzu werden verdächtige Programme nach bestimmten Verhaltensmustern analysiert und automatisch

geblockt. So können beispielsweise **unbekannte Viren** und Eindringlinge ohne entsprechende Signaturdateien erkannt werden. Auch können Anwender mit Hilfe dieser Technologien vor „**Buffer-Overflow**“-Attacken geschützt werden.

Die **Heuristik** des Anti-Virenschanners, die auf Wunsch des Anwenders stufenweise eingeschaltet werden kann und die **TruPrevent Technologien** funktionieren **sehr gut** und erkannten an den Tagen der Testverfahren zusätzlich **44** von insgesamt **50** unbekanntem Viren, die speziell für diesen Test erstellt wurden.

**Nachteil** der TruPrevent Technologien ist, dass dieses Schutzmodul alle laufenden Hintergrundprozesse eines Betriebssystems **permanent** analysiert, um verdächtige Verhaltensweisen aufspüren zu können. Dies sorgt für eine **höhere Systembelastung** und Ressourcenverbrauch.

Dem zunehmenden Ansturm von betrügerischen E-Mail Nachrichten (**Phishing**) wirkt Panda Software mit dem integrierten **Phishing-Modul** entgegen. Es ist vor allem für Heimanwender oder für den unerfahrenen Anwender nützlich. Sobald diese Option aktiviert wurde, erkennt und neutralisiert dieses Schutzmodul E-Mails, die darauf abzielen, falsche Webseiten zu verwenden und vertrauliche Daten zu stehlen.

Wird eine solche Phishing-E-Mail erkannt, wird der Anwender **umfassend** über den Vorfall informiert. Ebenfalls neu in **Platinum 2006 Internet Security** sind die beiden Schutzmodule „**Anti-Pharming**“ und „**Schwachstellenscanner**“. **Pharming** basiert auf einem ähnlichen Prinzip wie Phishing, nutzt jedoch **keine** E-Mails um den Nutzer auf gefälschte Webseiten zu lenken, sondern verändert die Host Datei und sorgt so dafür, dass Anwender permanent auf falsche Webseiten weitergeleitet werden.

Der „**Schwachstellenscanner**“ ist eine nützliche Hilfe, um das System vor möglichen Schwachstellen zu überprüfen. Allerdings ist der „Schwachstellenscanner“ **nicht** direkt mit einem Scanner vergleichbar, der bekannte oder unbekannte Sicherheitslücken auf dem System des Anwenders aufspüren kann. Dieser Schwachstellenscanner dient lediglich dazu, um feststellen zu können, ob die **aktuellen Sicherheitsupdates** von Microsoft™ auf dem System des Anwenders ordnungsgemäß installiert sind.

**Sehr gut** sind die in **Platinum 2006 Internet Security** integrierten Benachrichtigungs-funktionen: Anwender können sich bei der Erkennung eines Virus per E-Mails oder über das Netzwerk benachrichtigen lassen. Das **Pop-up-Warnsystem**, das bei Bedarf in der rechten unteren Ecke des Bildschirms angezeigt wird, informiert über alle Vorgänge (Updates, Scans,

erkannte Viren, Firewall-Aktivitäten, Serviceleistungen, uvm.), **und es werden Vorschläge aus dem Programm heraus gegeben, welche Aktionen als sinnvoll erachtet werden oder der Anwender wird auf entsprechende Webseiten von Panda Software verwiesen, welche verschiedene Problemlösungen enthalten.**

Die Updates der Virensignaturen stellt Panda Software **mindestens einmal täglich** zur Verfügung. Bei globalen oder lokalen Virenausbrüchen (Outbreaks), gibt es zudem **Eilupdates**, die in der Regel sofort für den Anwender bereit stehen.

Hier sollte **Panda Software** trotz seiner in Platinum 2006 Internet Security integrierten TruPrevent™ Technologien **nachbessern**, da bereits seit über einem Jahr mit großem Erfolg gegen Schadprogramme verschiedene Hersteller von Antiviren-Produkten **stündlich** Virensignaturupdates zur Verfügung stellen.

## BENUTZERFREUNDLICHKEIT

Die Installation von Platinum 2006 Internet Security verläuft **problemlos** und **anwenderfreundlich**. Während der Installation wird der Benutzer durch einen Wizard über bereits auf dem Computersystem installierte Sicherheitsprogramme, wie Anti-Virens Scanner und Personal Firewall informiert.

u.a. **keine** Updates der Virensignaturen herunter geladen werden. Nach erfolgter Registrierung erhält der Anwender einen **Benutzernamen** und ein **Passwort**, welche unter dem Menüpunkt „Service“ in Platinum 2006 Internet Security eingegeben werden.

**Benutzerfreundlich** sind ebenfalls die Optionen die Anwender festlegen können, wie sich das Programm zu einem bestimmten Zeitpunkt verhalten soll: was gescannt werden muss, wie und wann aktualisiert werden soll, ob eine Eigendiagnose durchgeführt werden soll, um zu überprüfen, dass das Schutzniveau Ihres Systems korrekt ist, ob man mit **Pop-Ups** oder mit **akustischen Signalen** bei der Erkennung von Vorfällen gewarnt werden soll, uvm.

Besonders erwähnenswert ist die Option **„Rettungsmedien“** mit aktuellen Virensignaturen zu erstellen. Seit der Version 2006 können Anwender nun nicht nur Rettungs-**Disketten** oder Rettungs-**CDs**, sondern auch Rettungs-**DVDs** erstellen, um in einer Notfallsituation den Computer von einer virenfreien Umgebung aus zu starten.

Die **Original-CD** von Platinum 2006 Internet Security kann standardgemäß ebenfalls als **Rettungs-CD** eingesetzt werden.

Praktisch und für die meisten Anwender einfach zu bedienen sind die beiden Schutzfunktionen **„AntiSpam“** (mailshell) und der **„Webfilter“** (Cobion).

Weniger gut hat uns das „Startfenster“ von Platinum 2006 Internet Security gefallen, welches immer dann für circa eine Sekunde lang erscheint, sobald Anwender den E-Mail Client Microsoft™ Outlook starten.

Für dieses Startfenster konnte – auch mit Hilfe des Handbuches - keine Option gefunden werden, um dieses zu deaktivieren.

Verzögerungen bei Seitenaufrufen im Internet unter Firefox 1.5 oder dem Internet Explorer konnten während der gesamten Testreihen **nicht** festgestellt werden.

Anwender können in Platinum 2006 Internet Security eine Vielzahl von weiteren **Einstellungsmöglichkeiten** an deren Bedürfnisse festlegen. Diese reichen von der Steuerung der CPU-Last bis hin zu individuellen Einstellungen bei der „Eigendiagnose“ oder Heuristiken des Antiviren-Scanners und TruPrevent™ Technologien.



Eine **übersichtliche, komfortable** und **verständliche** grafische Benutzeroberfläche mit Statusanzeigen lassen den Anwender alle Einstellungen auf einen Blick erkennen und vornehmen. Um das Programm mit seinen Serviceleistungen jedoch vollständig nutzen zu können, müssen sich Anwender registrieren. Ohne **Registrierung** können

**Anschaulich** sind seit der Version 2006 von Platinum Internet Security die Log-Dateien bzw. Berichte, die sich nun als **Grafiken und Statistiken** darstellen lassen. Die **Berichte** enthalten alle Vorfälle (erkannte Bedrohungen, blockierte Einbruchversuche, Updates, Scans, etc.) mit Zeitangaben, die sich während



## SUPPORT

Mit dem Erwerb von **Platinum 2006 Internet Security** erhalten Anwender **ein Jahr** lang Software- und Patternupdates sowie den Support von Panda Software inklusive.

Alle verfügbaren Serviceleistungen können Benutzer nach der **Registrierung** der Sicherheitslösung nutzen. Sie ermöglichen, das Programm automatisch zu aktualisieren, verdächtige Dateien zur Analyse und Untersuchung an Panda Software zu senden, technische Anfragen per E-Mail zu stellen sowie Feedback und Erfahrungen über das Produkt zu versenden.

der Verwendung des Programms ereignet haben. Diese **Berichte** können einfach per Mausklick als **grafische Informationen** aufbereitet werden. Sollten Anwender dennoch Probleme oder Fragen haben, helfen neben dem **Support** von Panda Software das über einhundertseitige **Handbuch** und die **Online-Programmhilfe**, in der Benutzer eine Vielzahl von Hilfestellungen, Tipps und eine ausführliche FAQ erhalten.

## PERFORMANCE

Aufgrund der Vielzahl an integrierten Schutzmodulen in **Platinum 2006 Internet Security** ist es für Anwender und Interessenten empfehlenswert **ausreichend** Prozessorleistung und Hauptspeicher in ihrem Computersystem zu besitzen, um ein reibungsloses Arbeiten mit der Sicherheitslösung gewährleisten zu können. Der Hersteller Panda Software gibt die empfohlenen Systemanforderungen für Platinum 2006 Internet Security mit **256 MB Hauptspeicher** und mindestens **500 MHz** Prozessor-Taktfrequenz an. Während der Testverfahren wurde Platinum 2006 Internet Security bezüglich der Performance **einwandfrei** auf unterschiedlichen Testsystemen zwischen **1200-3200 MHz** und **512-1500 MB** Hauptspeicher erfolgreich getestet.

Ebenfalls **sehr gute** Performancewerte erbrachte die vollständige Untersuchung der Test-Festplatten. Im Durchschnitt benötigte der Antiviren-Scanner für 10GB (~ 200.000 Dateien) zwölf Minuten, um alle Dateien auf Virenbefall hin zu überprüfen.

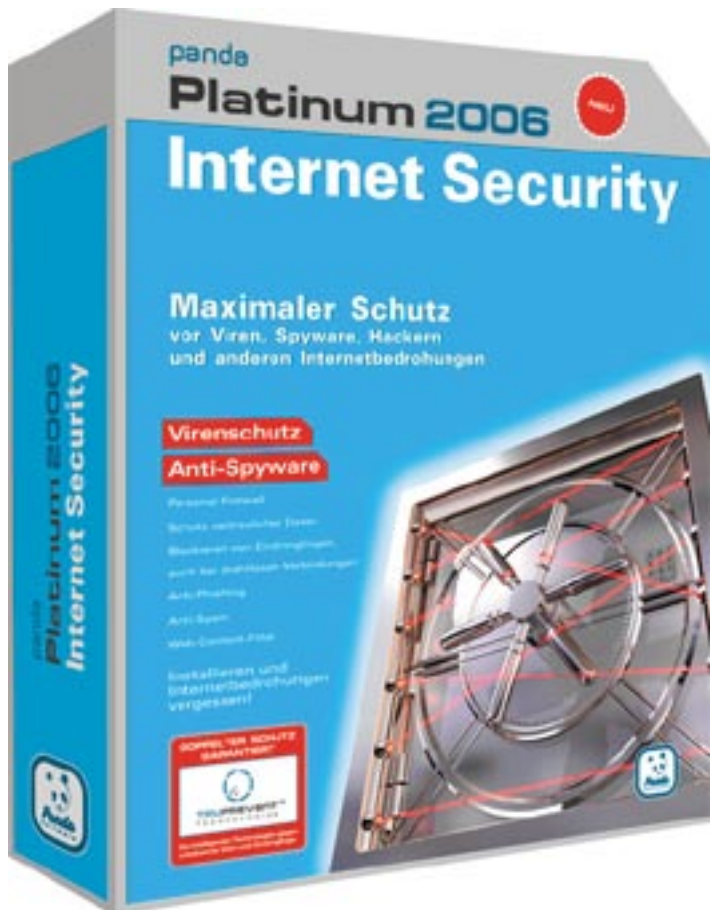
Während der Testreihen wurden von den Sicherheitsexperten des ProtectStar®-Testcenters insgesamt 58 Dateien zur Überprüfung an Panda Software eingesendet, die Platinum 2006 Internet Security als verdächtig einstufte. Obwohl pro Einsendung nur maximal **fünf Dateien** mit Hilfe des Assistenten zur Analyse versendet werden können, erhielten wir in der Regel nach durchschnittlich **acht Stunden** eine **ausführliche Rückantwort** per E-Mail. In diesem detaillierten Schreiben werden dem Anwender Informationen über die eingesendeten Dateien gegeben, dass es sich entweder um einen „falschen Alarm“ oder um „einen neuen Virus“ handelt, der unverzüglich in die Signaturdatenbank hinzugefügt wird. Zudem werden **hilfreiche Links** zu weiteren Informationen und evtl. benötigten **Entfernungstools** angegeben.



## PREIS- und LEISTUNG

Mit einem empfohlenen Verkaufspreis von **79,95 Euro** ist Platinum 2006 Internet Security von Panda Software in diesem Produktsegment das **teuerste Produkt** auf dem IT-Sicherheitsmarkt. Andere Hersteller verlangen für vergleichbare Internet Security Suites – wenn auch zum Teil mit weniger Schutzmodulen ausgestattet – durchschnittlich zwischen **59,95-69,95 Euro**.

Aufgrund der **überdurchschnittlichen** Anzahl an Schutzmodulen wie Antiviren-Scanner, Personal Firewall, TruPrevent Technologien, Anti-Spyware, Anti-Spam, Anti-Phishing, Anti-Pharming, uvm. ist Platinum 2006 Internet Security in Sachen Preis- und Leistungsverhältnis mit knapp achtzig Euro dennoch **gerechtfertigt** bewertet.



## FAZIT

Die Testreihen an **Platinum 2006 Internet Security** (10.01.02) zeigen, dass sich **Panda Software** mit seiner aktuellen 2006er Version im Vergleich zu seinen Vorgängerversionen um ein **Vielfaches** im Bereich der Systemsicherheit, Benutzerfreundlichkeit und Performance **verbessern** konnte.

Betrachtet man die Testergebnisse der Virenerkennungsrate wird zudem ersichtlich, dass Panda Software problemlos mit den äquivalenten Sicherheitslösungen von Kaspersky, Symantec, Gdata, uvm. mithalten kann.

Auf der technischen Seite konnte Platinum 2006 Internet Security ebenfalls überzeugen. Die Sicherheitslösung kombiniert **sehr guten Grundschutz** mit **guter Performance** und spricht nicht zuletzt aufgrund der Mehrzahl an Schutzmodulen sowohl den professionellen als auch unerfahrenen Anwender an.

Hervorzuheben sind die gute Virenerkennungsrate von **98,20%** und die **sehr guten** Schutzfunktionen von Platinum 2006 Internet Security. Die integrierten **TruPrevent Technologien** und **Heuristik** schützen ausreichend vor unbekanntem Bedrohungen, wenn Anwendern noch keine Virensignaturen zur Verfügung stehen.

Einem **sehr guten Gesamturteil** stehen lediglich die etwas **fragwürdige** „Zip of Death“-Problematik, die **Undurchführbarkeit** der Leaktests und die damit zusammenhängende **fehlende Option** einzelne Schutzmodule individuell ein- und auszuschalten, entgegen.

**Platinum 2006 Internet Security** von **Panda Software** wird mit dem „**ProtectStar® AWARD 2006**“ ausgezeichnet.

