



Endpoint Protection

Enkelt och lätt säkerhetsskydd för endpoint



HANTERA SÄKERHETEN FÖR ALLA DATORER NI DRIF TAR UTAN ATT PÅVERKA ER PRESTANDA OCH TILL LÄGSTA MÖJLIGA KOSTNAD

Panda Security erbjuder er det enklaste och lättaste skyddet för endpoint. Endpoint Protection ger ett centraliserat och oavbrutet skydd för alla era Windows, Mac och Linux arbetsstationer, laptops och servrar, samt de ledande virtualiseringssystemen och Android-enheter.

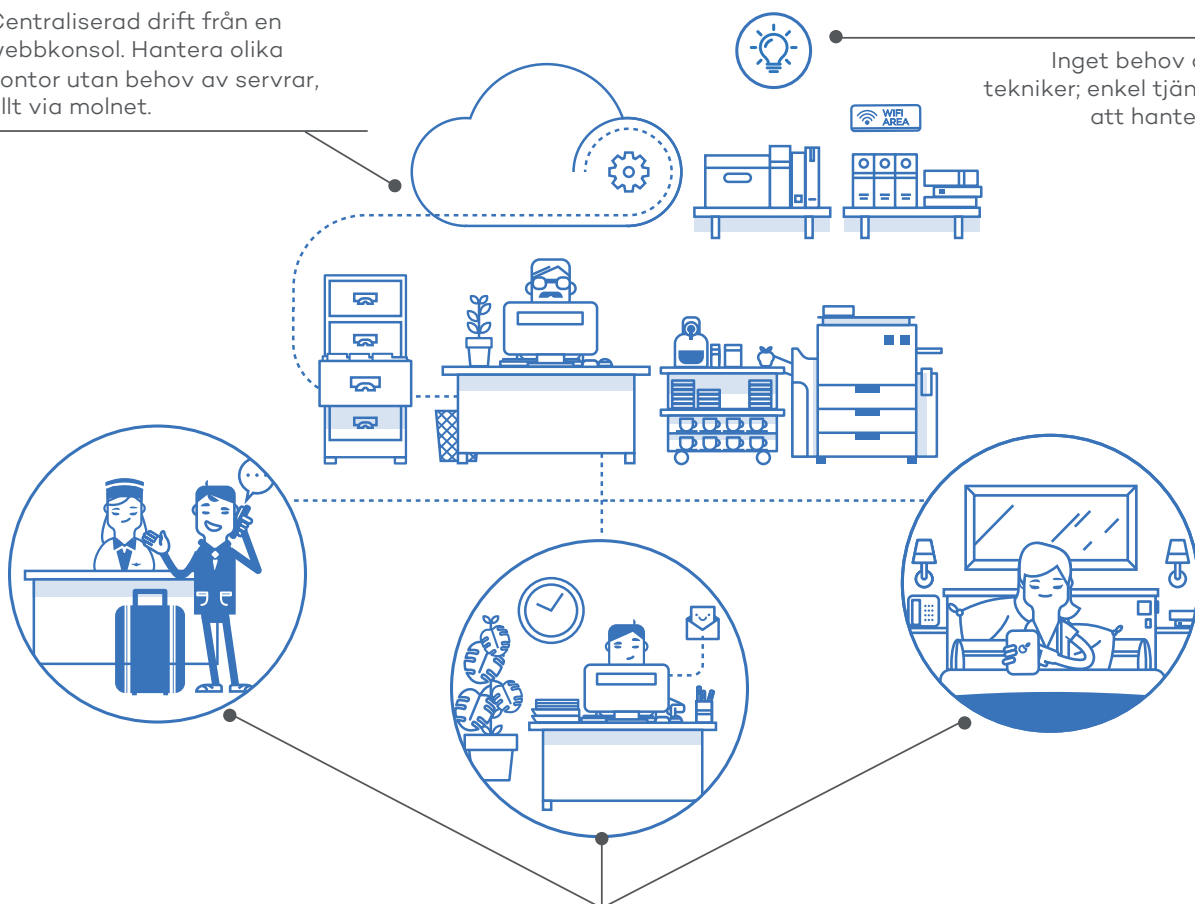
Panda Securitys teknologi Collective Intelligence skyddar alla era datorer och servrar mot hot och attacker som utnyttjar okända zero-day sårbarheter i realtid, utan behov av installation av ytterligare servrar eller IT-infrastruktur.

Med Endpoint Protection, hanteras skyddet enkelt och bekvämt från en webbkonsol, vilket möjliggör centraliserad administration närifrån och varifrån som helst, utan att ni behöver särskild teknisk kunskap.

Centraliserad drift från en webbkonsol. Hantera olika kontor utan behov av servrar, allt via molnet.



Inget behov av tekniker; enkel tjänst att hantera



Kross-plattform och mobilitet
Komplett skydd som täcker allt: nätverksskydd, brandvägg, mailskydd, webbskydd, skydd av externa enheter

Enkelt och centraliserat skydd för alla enheter

Centraliserad drift av säkerhets- och produktuppdateringar genom en enkel webbläsare för alla nätverkets arbetsstationer och servrar. Hantera ert skydd för Windows, Linux, Mac OS X eller Android från en enda administrationskonsol.

Avhjäljande funktioner

Kör Cleaner Monitor på distans och reparera infekterade arbetsstationer.

Starta om servrar och arbetsstationer fjärrstyrt för att säkerställa att de senaste produktuppdateringarna är installerade.

Realtidsövervakning och rapportering

Noggrann övervakning av er IT-infrastruktur i realtid tack vare lättförståeliga och intuitiva instrumentpaneler.

Rapporter kan genereras och skickas automatiskt, med uppgifter om skyddsstatus, detektioner och olämplig användning av resurserna .

Profilbaserat skydd

Tilldela profilbaserade skyddspolicies, för att rätt personer ska ha rätt skydd.

Centraliserad enhetskontroll

Möjlighet att hantera alla eller specifika enheter (externa hårddiskar, kameror, DVD/CD-enheter, USB-modem, Bluetooth etc.) för att göra det möjligt att förhindra att skadlig kod kommer in eller att information läcks ut, samtidigt som det ökar produktiviteten. Ni kan även neka eller tillåta handlingar (läsa/skriva) för särskilda enheter.

Flexibel, snabb installation i ett svep

Skyddet rullas ut på en gång och kan göras på det sätt du föredrar på bara några minuter. Antingen genom att skicka e-post med nedladdningslänk, eller utan att det märks och utan att användaren blandas in via distributionsverktyget som ingår. Det finns också ett MSI-paket för distribution via inloggningsscript, Active Directory eller andra administrationsverktyg (Tivoli, SMS, etc.).

Malware Freezer

Bli aldrig mer bränd av falskpositiver. Malware Freezer fryser detekterad skadlig kod i 7 dagar ifall det finns en falskpositiv. I så fall är det möjligt att enkelt åter skapa filen i systemet. Ni har alltid möjlighet att återställa allt det som klassificerats som skadlig kod.

ISO27001, SAS 70 garanterad tillgänglighet dygnet runt

Lösningens plattform körs med Microsoft Azure och underhålls av Panda Security vilket garanterar att informations-säkerheten är under total kontroll och datacentrat är ISO 27001- och SAS 70-certifierat. Tjänsten är godkänd av Datainspektionen och i enlighet med PUL (personuppgiftslagen).

TEKNISKA KRAV

Webbkonsol

- Internetuppkoppling
- Internet Explorer
- Firefox 3.0
- Google Chrome

För arbetsstationer / filservrar

- Minst en med internetuppkoppling
- Operativsystem (arbetsstationer): Windows XP SP0 & SP1 (32 and 64-bitar) SP2 eller mer Vista & Windows 7 & Windows 8.1 (32 och 64 bitar). Windows 2000 Professional, Windows XP SP0 & SP1 (32 och 64-bitar).
- RAM (arbetsstationer): 64 MB
- Windows Internet Explorer 6.0 eller senare
- Operativsystem (servrar): Windows 2003 (32 bitar & R2) SP1 eller mer, Windows 2008 32 & 64 bitar, Windows 2008 R2 (64 bitar), Windows Server 2012 (64 bitar). Windows 2000 Server. Windows 2003 (64-bitar). Windows Home Server. bit and R2).

För MAC arbetsstationer / filservrar

- Mac OS X 10.6 Snow leopard, Mac OS X 10.7 Lion, Mac OS X 10.8 Mountain Lion, Mac OS X 10.9 Mavericks, Mac OS X 10.10 Yosemite

För Linux workstations / file servers

- Ubuntu 12 32/64 bitar eller senare
- Red Hat Enterprise Linux 6.0 64 bitar eller senare
- CentOS 6.0 64 bitar eller senare
- Debian 6.9 Squeeze eller senare
- OpenSuse 12 32/64 bitar eller senare
- Suse Enterprise Server 11SP2 64 bitar eller senare

För Androidenheter

- Android (från 2.3)

Virtual motor certifierad

- VMWare ESX 3.x,4.x, 5,x
- VMWare Workstation 6.0, 6.5, 7.x, 8.x och 9.x
- Virtual PC 6.x
- Microsoft Hyper-V Server 2008 R2 och 2012 3.0
- Citrix XenDesktop 5.x, XenClient 4.x, XenServer och XenApp 5.x and 6.x

Kompatibel med



Certifieringar:

