



Endpoint Protection Plus

Soluzione di sicurezza e di produttività per endpoint semplice e leggera

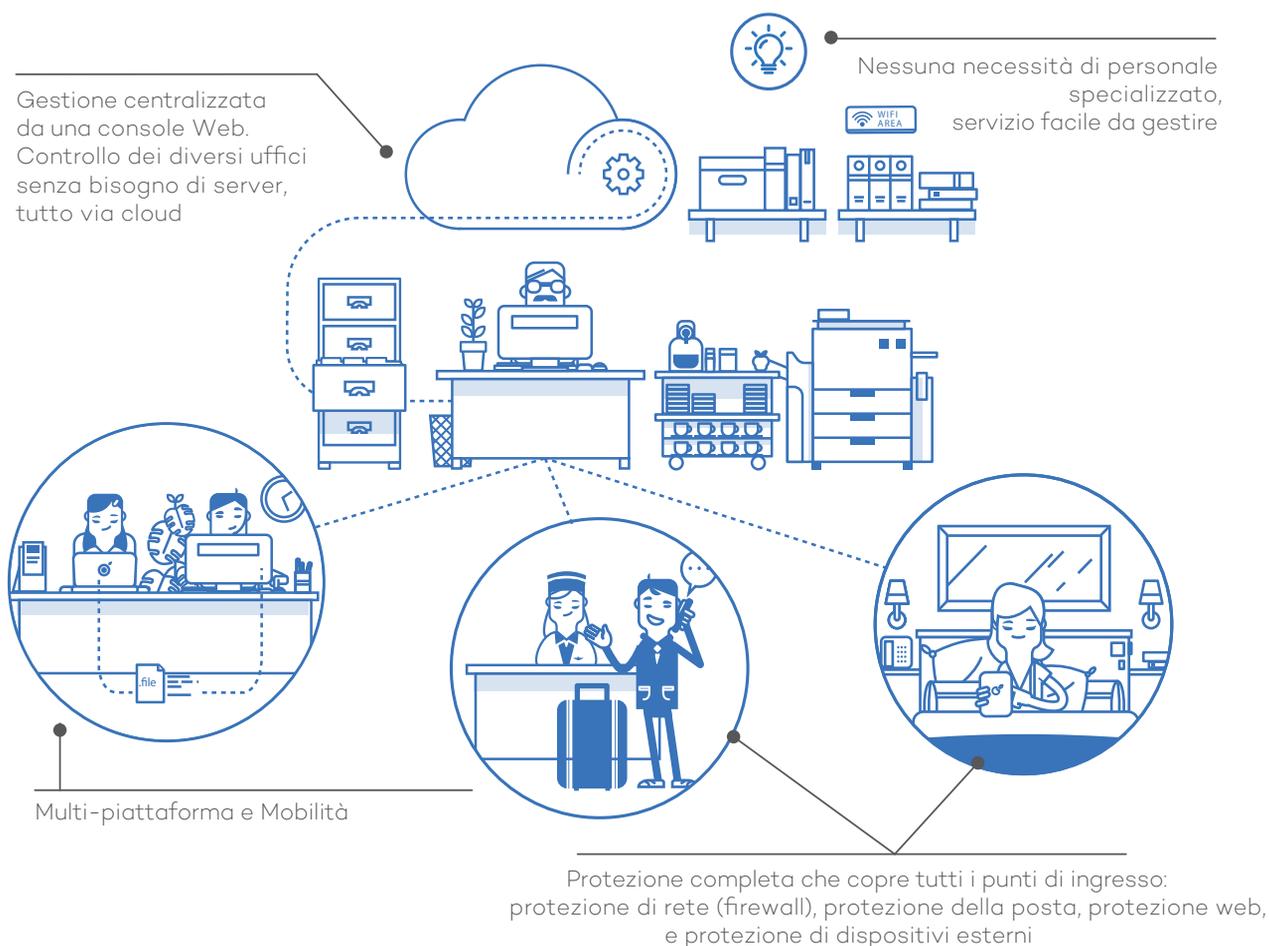


GESTITE LA SICUREZZA DI TUTTI I COMPUTER IN RETE E CONTROLLATE LA PRODUTTIVITA' DEGLI UTENTI AL PIU' BASSO COSTO DI GESTIONE POSSIBILE

Panda Security migliora la sua soluzione di sicurezza e produttività semplice e leggera. **Endpoint Protection Plus** fornisce protezione centralizzata e continuativa per tutte le postazioni di lavoro Windows, Mac, Linux, compresi laptop e server, oltre ai dispositivi Android™ e ai principali sistemi di virtualizzazione.

La tecnologia di **Intelligenza Collettiva** di Panda Security protegge in tempo reale tutte le workstation e i server dalle minacce ed exploit che utilizzano vulnerabilità zero-day sconosciute, senza bisogno di installare server aggiuntivi o infrastrutture IT. Essa controlla e filtra anche il traffico Web e lo spam, consentendo all'azienda di concentrarsi sul suo business ed evitando i comportamenti improduttivi dei dipendenti.

Con **Endpoint Protection Plus**, la protezione è gestita comodamente e facilmente da una singola console Web, consentendo l'amministrazione centralizzata sempre e ovunque, senza bisogno di conoscenze tecniche specifiche.



Sicurezza semplice e centralizzata per tutti i dispositivi

Gestione centralizzata della sicurezza e aggiornamento dei prodotti attraverso un semplice browser Web per tutte le workstation e server in rete. Gestione delle protezioni per Windows, Linux, Android o Mac OS X da una singola console di amministrazione.

Misure correttive

Esecuzione di Cleaner Monitor da remoto e ripristino di postazioni di lavoro infettate da malware avanzati o non convenzionali. Riavvio remoto di server e workstation per garantire l'installazione degli ultimi aggiornamenti di prodotti.

Monitoraggio e report in tempo reale

Monitoraggio dettagliato dell'infrastruttura IT in tempo reale grazie a dashboard complete e intuitive. I report possono essere generati e inviati automaticamente, dettagliando stato della protezione, rilevazioni e uso inadeguato di risorse.

Protezione basata su profili

Assegnazione di politiche di protezione basate sul profilo, garantendo che le politiche appropriate vengano applicate a ciascun gruppo di utenti.

Controllo centralizzato dei dispositivi

Blocco dei dispositivi (unità USB, modem, webcam, DVD/CD, ecc.) o definizione delle azioni consentite (accesso, blocco, lettura, scrittura) per evitare ingresso di malware o perdite di dati.

Monitoraggio e filtro Web

Incremento della produttività degli utenti mediante prevenzione e/o monitoraggio dell'accesso ai contenuti web appartenenti alle categorie considerate pericolose o improduttive in orario di lavoro, indipendentemente dal tipo di browser utilizzato.

Mai più caselle di posta sature

Riduzione del rischio di attacchi sui server Exchange con la funzionalità di filtro dei contenuti. Miglioramento della produttività e protezione degli utenti finali filtrando messaggi indesiderati e dannosi con i motori antimalware e antisipam.

Malware Freezer

Nessun pericolo di falsi positivi. Malware Freezer blocca il file sospetto per 7 giorni. Nel caso si riveli un falso positivo il file verrà automaticamente ripristinato nel sistema.

Conformità ISO 27001 e SAS 70. Disponibilità 24x7 garantita.

La soluzione è ospitata su Microsoft Azure con protezione completa e garantita dei dati. I nostri data center sono certificati ISO 27001 e SAS 70.

REQUISITI TECNICI:

Web Console

- Connessione a Internet
- Internet Explorer
- Firefox
- Google Chrome

Per workstation / file server Windows:

- Almeno un endpoint connesso a Internet.
- Sistema operativo (workstation): Windows 2000 Professional, XP SP0 e SP1 (32 / 64 bit), XP SP2 o successivi, Windows Vista, Windows 7 e Windows 8.1 (32 / 64 bit).
- Sistema operativo (server): Windows 2000 Server, Windows Home Server, Windows 2003/R2 (32 / 64 bit) SP1 e superiore, Windows 2008 (32 / 64 bit), Windows 2008 R2 (64 bit), Windows Small Business Server 2011, Windows Server 2012/R2 (64 bit).

Per workstation / file server Mac:

- 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

Per workstation / file server Linux

- Ubuntu 12 32/64 bit e successivo
- Red Hat Enterprise Linux 6.0 64 bit e successivo
- CentOS 6.0 64 bit e successivo
- Debian 6.0 Squeeze e successivo
- OpenSuse 12 32/64 bit e successivo
- Suse Enterprise Server 11SP2 64 bit e successivo

Per dispositivi Android

- Android (da 2.3)

Piattaforme di virtualizzazione certificate:

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

Compatibile con:



Certificazioni:

