

Ogni giorno vengono registrati più di 350.000 nuovi programmi dannosi (malware) e applicazioni potenzialmente indesiderate (PUA).<sup>1</sup> Gli hacker prendono di mira gli endpoint vulnerabili, nei quali le aziende archiviano le loro risorse più preziose. Il motivo? Il **ritorno economico**, naturalmente.

Le **aziende** dipendono sempre più dalle nuove tecnologie e sono quindi più **esposte** ai nuovi tipi di malware che ne **mettono in pericolo** la sicurezza. Ovviamente questa situazione impone l'adozione degli approcci di sicurezza più idonei a **ridurre la superficie di attacco**.

## EVOLUZIONE DEGLI AMBIENTI IT AZIENDALI

Negli ultimi anni l'evoluzione della tecnologia, associata alla grande diffusione di Internet, dei dispositivi mobili e dell'uso del cloud per l'archiviazione e le app, ha provocato una vera e propria rivoluzione per le aziende. È però una rivoluzione non priva di rischi, che se avvantaggia le imprese offre però grandi opportunità anche ai criminali informatici.

L'aumento del numero degli attacchi informatici è da mettere in relazione con il maggior valore delle risorse digitali di proprietà delle aziende nelle quali i criminali informatici scorgono un potenziale incremento del proprio ritorno economico. Il malware e il ransomware sono le minacce più frequenti, sebbene paradossalmente il problema principale non sia costituito dai costi diretti quanto piuttosto dall'interruzione delle attività che queste minacce provocano. Questa situazione impone alle aziende di adottare provvedimenti che rafforzino la protezione.

## PROTEZIONE DELL'AZIENDA DA MALWARE E RANSOMWARE

Panda Endpoint Protection Plus è una soluzione completa e avanzata per la sicurezza di PC desktop, laptop e server. Gestisce da una posizione centrale la sicurezza degli endpoint sia all'interno sia all'esterno della rete aziendale.

Il servizio offre una serie di tecnologie EPP per il controllo di malware, ransomware e minacce che sfruttano le vulnerabilità sconosciute (zero-day). Non è necessario installare o gestire nuove risorse hardware nell'infrastruttura aziendale.

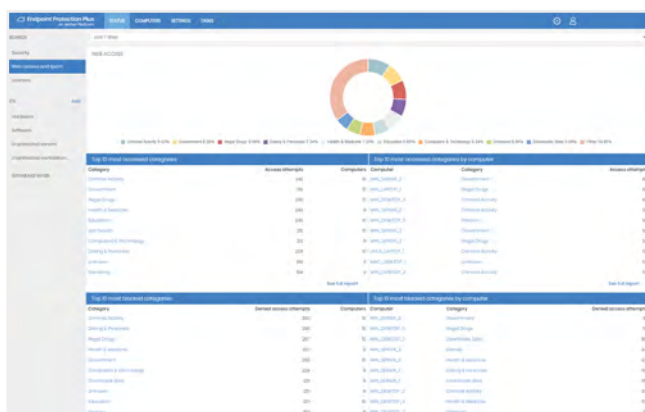


Figura 1: accesso al Web e dashboard per lo spam.

## VANTAGGI

### Sicurezza multiplatforma

- Sicurezza rispetto a minacce avanzate sconosciute: rilevamento e blocco di malware, trojan, phishing e ransomware.
- Sicurezza per tutti i vettori di attacco: browser, e-mail, file system e dispositivi esterni collegati agli endpoint.
- Analisi e disinfezione automatiche dei computer. Analisi del comportamento per rilevare malware noto e sconosciuto.
- Sicurezza per sistemi Windows, Linux, macOS, iOS, Android e ambienti virtuali (VMware, Virtual PC, MS Hyper-V, Citrix), nonché per infrastrutture di virtualizzazione (VDI) sia persistenti che non persistenti.

### Maggiore produttività

- Sorveglianza e filtra il traffico sul Web, impedendo ai dipendenti di assumere comportamenti improduttivi o subire minacce per la sicurezza sotto forma di bot o phishing.
- Non sono necessarie infrastrutture specifiche o particolari operazioni di manutenzione; il reparto IT può concentrarsi su attività più importanti.

### Gestione semplificata

- Facilità di gestione: non è necessaria alcuna infrastruttura specifica per la soluzione; il reparto IT può concentrarsi su attività più importanti.
- Facilità di protezione degli utenti remoti: ogni computer protetto da Panda Endpoint Protection Plus comunica con il cloud. Gli utenti e gli uffici remoti vengono protetti rapidamente e con facilità, senza installazioni aggiuntive.
- Facilità di distribuzione: più metodi di distribuzione, con programmi di disinstallazione automatici per i prodotti della concorrenza, per facilitare la migrazione da soluzioni di altri fornitori.

<sup>1</sup> Test AV: <https://www.av-test.org/en/statistics/malware/>

## SICUREZZA CENTRALIZZATA DEGLI ENDPOINT

È inclusa la gestione centralizzata della sicurezza e degli aggiornamenti del prodotto per tutte le workstation e i server della rete aziendale. È possibile gestire la protezione dei dispositivi con Windows, Linux, macOS, iOS e Android da un'unica console di amministrazione basata sul Web.

## PROTEZIONE DA MALWARE E RANSOMWARE

Panda Endpoint Protection Plus analizza i comportamenti e le tecniche di intrusione per rilevare e bloccare malware noto e sconosciuto, nonché ransomware, trojan e phishing. Inoltre Malware Freezer mette in quarantena il malware rilevato per sette giorni e, in caso di un falso positivo, ripristina automaticamente il file interessato nel sistema.

## DISINFEZIONE AVANZATA

Nell'eventualità di una violazione della sicurezza, Panda Endpoint Protection Plus consente alle aziende di riportare i computer interessati allo stato in cui erano prima dell'aggressione con strumenti avanzati di disinfezione e con la quarantena, nella quale vengono inseriti gli elementi sospetti e quelli eliminati. Consente inoltre agli amministratori di riavviare da remoto le workstation e i server per assicurarsi che vi siano installati gli aggiornamenti più recenti.

## MONITORAGGIO E FILTRO WEB

I dashboard completi e alcuni grafici intuitivi assicurano un monitoraggio dettagliato in tempo reale della sicurezza della rete.

I filtri per il Web aumentano la produttività all'interno dell'azienda e sorvegliano l'attività per impedire l'accesso a URL pericolosi o improduttivi.

## CONTROLLO CENTRALIZZATO DEI DISPOSITIVI

È possibile fermare il malware e la fuga di informazioni bloccando intere categorie di dispositivi (unità flash, modem USB, webcam, DVD/CD, ecc.), inserendo i dispositivi consentiti in appositi elenchi, configurando autorizzazioni di accesso in sola lettura, sola scrittura e lettura-scrittura e bloccando le attività che vengono ritenute a rischio.

## INSTALLAZIONE VELOCE E FLESSIBILE

La distribuzione della protezione può avvenire via e-mail tramite un URL per il download oppure automaticamente in endpoint selezionati tramite lo strumento di distribuzione della soluzione. Il programma di installazione MSI è compatibile con strumenti di altri fornitori (Active Directory, Tivoli, SMS, ecc.).

## CONFORMITÀ ISO 27001 E SAS 70 - DISPONIBILITÀ 24/7 GARANTITA

La soluzione risiede su Aether, la piattaforma con protezione dei dati completa garantita. I nostri data center sono dotati di certificazione ISO 27001 e SAS 70 e permettono ai clienti di evitare costose interruzioni del servizio e infezioni da malware.



## RECUPERO E BONIFICA DI UN SISTEMA COLPITO DA UN RANSOMWARE

Per impedire il recupero di un sistema corrotto, i cyber criminali, oltre a crittografare i file, cercano di eliminare i file VSS e di backup creati dagli amministratori e di disattivare i servizi pensati per supportare il recupero.

Per consentire agli utenti di recuperare i propri dati in seguito a un attacco ransomware, il servizio di copia shadow incluso nelle nostre tecnologie di antimanomissione sfrutta la base tecnica del sistema operativo per proteggere quei file.

I professionisti IT utilizzano, infatti, le copie shadow per recuperare i file in caso di gravi malfunzionamenti del sistema, ma questa tecnologia è ottima anche per ripristinare i file crittografati dal ransomware.

### Soluzioni compatibili sulla piattaforma Aether:

 Panda Endpoint Protection  Panda Endpoint Protection

Workstation e server Windows:

<http://go.pandasecurity.com/endpoint-windows/requirements>

Dispositivi macOS:

<http://go.pandasecurity.com/endpoint-macos/requirements>

Workstation e server Linux:

<http://go.pandasecurity.com/endpoint-linux/requirements>

Dispositivi mobili Android:

<http://go.pandasecurity.com/endpoint-android/requirements>

Dispositivi mobili iOS:

<https://www.pandasecurity.com/support/card?id=700123>