Panda Endpoint Protection

La sicurezza degli endpoint sta cambiando

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.

In effetti nel 2020 sono stati registrati **più di 350.000 nuovi programmi dannosi**[1] al giorno. Gli hacker prendono di mira gli endpoint vulnerabili, nei quali le aziende archiviano le loro **risorse più preziose**. Il motivo? Il ritorno economico, naturalmente. 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

La crescente esposizione delle aziende a nuovi tipi di malware e minacce ne mina i livelli di protezione e richiede nuovi approcci per ridurre l' impatto dei possibili attacchi.

Panda Endpoint Protection è un' efficace soluzione per la sicurezza basata su cloud pensata per PC desktop, laptop e server. Gestisce da una posizione centrale la sicurezza degli endpoint, sia all' interno sia all' esterno della rete aziendale.

Per impedire malware, ransomware e le minacce più recenti comprende una serie di tecnologie EPP, una delle quali consulta in tempo reale il Panda Threat Intelligence, un immenso repository basato sui più recenti algoritmi di apprendimento automatico, per rilevare più rapidamente gli attacchi dolosi.

In più non è necessario dotarsi di hardware e software. Il suo agente a basso impatto non incide sulle prestazioni degli endpoint, semplifica la gestione della sicurezza e aumenta l' efficienza operativa.

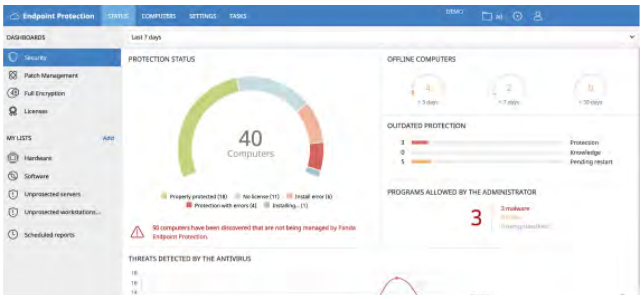

Figura 1: dashboard dello stato di protezione della rete.

[1] **Test AV:** https://www.av-test.org/en/statistics/malware/

VANTAGGI

Sicurezza multipiattaforma

- 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 tra piattaforme: sistemi Windows, Linux, macOS, iOS, Android e ambienti virtuali (VMware, Virtual PC, MS Hyper-V, Citrix). Gestione di licenze appartenenti a infrastrutture di virtualizzazione (VDI) sia persistenti che non persistenti.

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 comunica con il cloud. Gli uffici e gli utenti 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.
- Curva di apprendimento bassa: l' interfaccia di gestione basata sul Web è semplice e intuitiva, con opzioni di uso frequente attivabili con un solo clic.

Basso impatto sulle prestazioni

- L' agente richiede un utilizzo minimo di rete, memoria e CPU, poiché tutte le operazioni vengono eseguite sul cloud.
- Panda Endpoint Protection non richiede installazione, gestione o manutenzione di nuove risorse hardware nell' infrastrutturadell' organizzazione.

SICUREZZA CENTRALIZZATA DEI DISPOSITIVI

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 analizza i comportamenti e le tecniche di intrusione per rilevare e bloccare malware noto e sconosciuto, nonché ransomware, trojan e phishing.

DISINFEZIONE AVANZATA

Nell' eventualità di una violazione della sicurezza, Panda Endpoint Protection 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 IN TEMPO REALE E REPORT

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

I report generati automaticamente segnalano lo stato della protezione, i rilevamenti eseguiti e l' uso scorretto dei dispositivi.

CONFIGURAZIONE DETTAGLIATA DEI PROFILI

È possibile assegnare specifiche policy di protezione in base a profili utente, garantendo a ogni gruppo di utenti l' applicazione della policy più appropriata.

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 o configurando autorizzazioni di accesso in sola lettura, sola scrittura e lettura-scrittura.

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 distribuzionedella soluzione. Il programma di installazione MSI è compatibile con strumenti di altri fornitori (Active Directory, Tivoli, SMS, ecc.).

MALWARE FREEZER

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.

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

La soluzione risiede sulla piattaforma Aether 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 Plus**

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

VENDITE ITALIA: 800.911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 www.watchguard.com | pandasecurity.com