Adaptive Defense 360

Sicurezza di nuova generazione per eliminare tutte le minacce informatiche

panda a WatchGuard brand

Soluzione di cybersecurity che assicura protezione ottimale con il minimo sforzo gestionale

La mobilità, l'elaborazione e l'archiviazione in cloud hanno rivoluzionato la struttura delle reti aziendali, tuttavia, nonostante i progressi compiuti, gli attacchi degli hacker continuano ad andare a buon fine. I reparti IT ricevono ogni settimana migliaia di avvisi relativi ai malware, di cui soltanto il 19% viene reputato affidabile, mentre solo il 4% diventa oggetto di ulteriori indagini. Non c'è da stupirsi se due terzi del tempo di un comune amministratore della sicurezza informatica siano dedicati alla sola gestione degli avvisi.

Le soluzioni per la sicurezza degli endpoint devono affrontare non solo le minacce provenienti da un attacco informatico, ma anche la mancanza di risorse per gestire il processo di risposta. La prevenzione e il rilevamento sono fondamentali, ma è altrettanto importante garantire che il reparto IT guadagni tempo prezioso per concentrarsi su altre aree critiche, automatizzando le attività di gestione della soluzione implementata.

I problemi delle soluzioni avanzate di protezione dalle minacce informatiche

Gli attacchi informatici più all'avanguardia sono progettati per aggirare la protezione fornita dalle soluzioni di sicurezza tradizionali. Questi tipi di attacchi sono sempre **più frequenti** e **sofisticati** per via delle competenze professionali acquisite nel tempo dagli hacker e sono anche il risultato di una mancata correzione delle **vulnerabilità di sicurezza nei sistemi**.

Le piattaforme di endpoint protection tradizionali (EPP) non sono sufficienti a contrastare questo tipo di attacchi, poiché non sono in grado di fornire abbastanza visibilità e dettagli sui processi e sulle applicazioni in esecuzione sulle reti aziendali. Per affrontare il problema, i reparti IT aggiungono un'ulteriore protezione tramite soluzioni di rilevamento e risposta degli endpoint (Endpoint Detection and Response, EDR). La maggior parte delle piattaforme EDR, tuttavia, richiede all'amministratore della sicurezza di gestire gli avvisi e di classificare manualmente le minacce, aumentando il carico di lavoro fino a dieci volte e lasciando l'intera gestione sulle sue spalle.

Adaptive Defense 360, la soluzione avanzata per la sicurezza informatica

Panda Adaptive Defense 360 (AD360) è una soluzione di sicurezza informatica avanzata per le workstation, i laptop e i server basata su cloud, che **automatizza la prevenzione, il rilevamento, il contenimento e la risposta** contro minacce avanzate, malware zero-day, ransomware, phishing, exploit in memoria e attacchi malwareless. Questo livello di protezione garantisce l'eliminazione delle minacce presenti e future, indipendentemente dal fatto che risiedano all'interno o all'esterno della rete aziendale.

A differenza di altre soluzioni che si concentrano esclusivamente sull'EDR, AD360 combina protezione degli endpoint (EPP) tradizionale con le funzionalità EDR automatizzate di nuova generazione, fornendo un modello di sicurezza completo per affrontare minacce sia note che sconosciute. Gli aspetti chiave che differenziano maggiormente AD360 dalle soluzioni dei competitor risiedono in due servizi che non necessitano di alcuna gestione da parte del reparto IT:

- **classificazione del 100% dei processi**
- **ricerca e indagine delle minacce (Threat Hunting and Investigation Service, THIS)**

Questo agent leggero non influenza negativamente le prestazioni degli endpoint, i quali sono gestiti attraverso un'unica architettura cloud anche quando sono isolati.

Panda Adaptive Defense 360 è accessibile da una singola console web e presenta una piattaforma integrata di protezione e gestione basata su cloud (Aether), che massimizza e automatizza la prevenzione, il rilevamento e la risposta, riducendo al minimo lo sforzo richiesto.

Vantaggi

Semplifica e riduce al minimo i costi per la sicurezza

- I servizi gestiti consentono di ridurre i costi del personale qualificato necessario, poiché non implicano task da delegare o falsi allarmi da gestire
- I servizi gestiti si basano sull'apprendimento automatico delle minacce, senza alcuna necessità di perdere tempo con le impostazioni manuali
- Migliori attività di prevenzione sugli endpoint riducono o azzerano i costi operativi
- Nessuna necessità di installare, configurare o mantenere un'infrastruttura di gestione
- L'agent leggero e l'architettura basata su cloud non influenzano negativamente la performance degli endpoint

Automatizza e riduce al minimo il tempo di rilevamento

- Le applicazioni che rappresentano un rischio per la sicurezza vengono bloccate (tramite hash o nome del processo)
- Blocco delle minacce nei processi in esecuzione, dei malware di tipo zero-day, degli attacchi fileless/malwareless, dei ransomware e dei tentativi di phishing
- Rileva e blocca l'attività dannosa in memoria (exploit) prima che possa diventare pericolosa
- Rileva i processi dannosi che hanno aggirato le misure preventive
- Rileva e blocca tecniche, tattiche e procedure di intrusione

Automatizza e riduce al minimo il tempo di risposta e indagine

- Soluzione e risposta tramite analisi forense per indagare su ogni tentativo di attacco e strumenti per mitigarne gli effetti (disinfezione)
- Capacità di tracciare tutte le azioni e l'attività dell'aggressore, facilitando le indagini forensi
- Miglioramento e perfezionamento delle policy di sicurezza grazie alle conclusioni dell'analisi forense

WatchGuard

Numero verde Italia 800.911.938 VENDITE INTERNAZIONALI +1.206.613.0895 www.watchguard.it | www.pandasecurity.com/it/business/

Non si fornisce alcuna garanzia esplicita o implicita. Tutte le specifiche sono soggette a modifiche e tutti i prodotti, le caratteristiche o le funzionalità future verranno forniti a seconda della disponibilità.
©2020 WatchGuard Technologies, Inc. Tutti i diritti riservati. WatchGuard, il logo WatchGuard e Panda Security sono marchi o marchi registrati di WatchGuard Technologies, Inc. negli Stati Uniti e/o in altri paesi. Tutti gli altri marchi registrati o marchi commerciali sono di proprietà dei rispettivi proprietari. WGCE67329_060420

Adaptive Defense 360

panda a WatchGuard brand

Sicurezza degli endpoint avanzata e automatizzata

Le tecnologie di protezione degli endpoint (EPP) tradizionali, incentrate sulla prevenzione, sono misure a basso costo, utili ma non sufficienti per minacce note e comportamenti dannosi. Per eliminare definitivamente le minacce informatiche è necessario passare dalla prevenzione tradizionale a un modello di prevenzione, rilevamento e risposta continui, presupponendo in ogni momento che la rete sia stata compromessa e che tutti gli endpoint siano costantemente sotto attacco.

Panda Adaptive Defense 360 consente ai reparti IT di garantire la protezione integrando le tradizionali tecnologie EPP con le funzionalità EDR in un'unica soluzione e rendendo la rete impenetrabile contro minacce sia note che sconosciute.

Tecnologie di prevenzione tradizionali

- Firewall personale o gestito e IDS
- Controllo dei dispositivi
- Anti-malware multivettoriale permanente e scansione on-demand
- Blacklisting/Whitelisting gestito
- Intelligenza collettiva
- Euristica pre-esecuzione
- Filtro degli URL e della navigazione web
- Anti-spam e anti-phishing
- Anti-tampering
- Filtro dei contenuti delle e-mail
- Correzione e rollback

Tecnologie di sicurezza avanzate

- EDR: monitoraggio continuo degli endpoint
- Blocco dell'esecuzione di processi sconosciuti
- Machine learning basato sul cloud che classifica il 100% dei processi (APT, ransomware, rootkit, ecc.)
- Sandboxing in ambienti reali
- Analisi comportamentale e rilevamento degli IOA (indicatori di attacco) come script, macro, ecc.
- Rilevamento e risposta automatici per attacchi mirati ed exploit in memoria
- Ricerca delle minacce e analisi forense

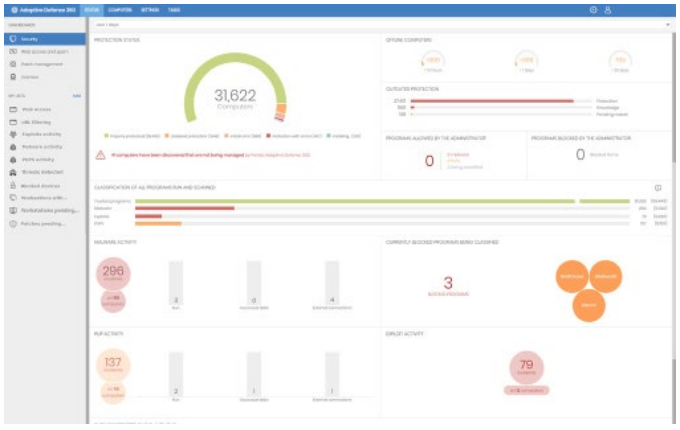

Figura 1: Dashboard principale di Panda Adaptive Defense 360

Modello Zero Trust

AD360 opera secondo il "modello Zero Trust", il cui principio fondamentale consiste nell'accordare zero fiducia, da parte delle organizzazioni, a entità interne o esterne al perimetro in qualsiasi momento. Questa metodologia si concretizza attraverso un servizio gestito che classifica il 100% dei processi, monitora l'attività degli endpoint e blocca l'esecuzione delle applicazioni e dei processi dannosi. Ogni esecuzione viene classificata in tempo reale come dannosa o legittima, senza possibilità di errore e senza l'intervento del personale IT, grazie alla capacità, alla velocità, all'adattabilità e alla scalabilità dell'intelligenza artificiale e dell'elaborazione su cloud.

Il servizio integra le tecnologie dei **big data** e le tecniche di **machine learning** multilivello, compreso il **deep learning**, che sono il risultato di una continua verifica e automazione dell'esperienza e delle conoscenze accumulate dal team di sicurezza interno di Panda.

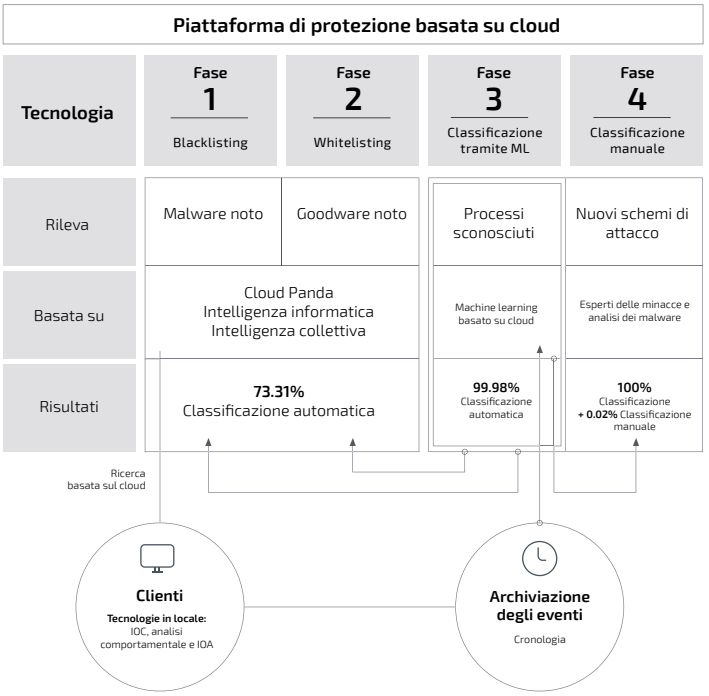

Figura 2: Fasi del servizio di classificazione in cloud.

Il servizio gestito di ricerca delle minacce e analisi forense è condotto da un team di esperti che utilizzano strumenti di profilazione in tempo reale e in retrospettiva e l'analisi della correlazione di eventi per scoprire in modo proattivo nuove tecniche e tattiche di intrusione e di elusione.

Gli addetti al threat hunting del Panda Intelligence Center lavorano partendo dal presupposto che le aziende siano costantemente compromesse.

PREMI E CERTIFICAZIONI

Panda Security partecipa regolarmente ai confronti in termini di protezione e prestazioni condotti da Virus Bulletin, AV-Comparatives, AV-Test e NSSLabs conquistando diversi premi. Panda Adaptive Defense ha ottenuto la certificazione EAL2+ nella sua valutazione per lo standard Common Criteria.