Panda Adaptive Defense

Rilevamento di endpoint e risposta

panda
a WatchGuard brand

SICUREZZA INFORMATICA PER L'ORGANIZZAZIONE

La mobilità, l' elaborazione e l' archiviazione in cloud hanno rivoluzionato l' ambiente aziendale. **Le workstation sono l' obiettivo principale di gran parte degli attacchi informatici.** Per questo motivo le soluzioni per la sicurezza degli endpoint devono essere **avanzate, adattive e automatiche**, con i livelli più alti possibili di **prevenzione** e **rilevamento**.

Le organizzazioni 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. **Due terzi del tempo degli amministratori della sicurezza informatica** sono dedicati alla **gestione degli avvisi relativi a malware**.[1]

ATTACCHI INFORMATICI SEMPRE PIÙ SOFISTICATI

Difesa informatica dalle minacce avanzate

Gli attacchi informatici più all' avanguardia sono progettati per aggirare la protezione fornita dalle soluzioni di sicurezza tradizionali. **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**.

Alla luce di questa situazione, le piattaforme di protezione tradizionali sono insufficienti perché non forniscono una visibilità abbastanza dettagliata dei processi e delle applicazioni in esecuzione nelle reti aziendali.

Inoltre **alcune soluzioni EDR** invece di risolvere i problemi **creano ulteriore stress** e aumentano il **carico di lavoro degli amministratori della sicurezza** perché li investono della responsabilità di **gestire gli avvisi** e li obbligano a classificare **manualmente** le minacce.

PANDA ADAPTIVE DEFENSE

La soluzione EDR: rilevamento di endpoint e risposta

Panda Adaptive Defense è un' innovativa soluzione per la sicurezza informatica pensata per computer, laptop e server basata su cloud che **automatizza la prevenzione, il rilevamento, il contenimento e la risposta a qualsiasi minaccia avanzata, dal** malware zero day al ransomware, fino ai tentativi di phishing e agli exploit in memoria, compresi gli attacchi senza malware, sia attuali che futuri e sia all' interno che all' esterno della rete.

Panda Adaptive Defense unisce la più ampia gamma di **funzionalità automatiche di EDR**. Integra inoltre **due servizi, gestiti dagli esperti di Panda Security, che vengono resi disponibili come una funzione della soluzione:**

- **Servizio Zero Trust per le applicazioni**
- **Servizio di ricerca delle minacce**

Questo agente leggero non influenza negativamente le prestazioni dei dispositivi, i quali sono gestiti attraverso un' unica architettura cloud anche quando sono isolati.

Panda Adaptive Defense 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 suoi servizi innovativi riducono i costi del personale esperto. Non sono presenti falsi avvisi da gestire e non viene delegata alcuna responsabilità.
- I servizi apprendono automaticamente dalle minacce e consentono di non perdere tempo con le impostazioni manuali.
- Massima prevenzione sull' endpoint. Costi operativi quasi completamente azzerati.
- Non è necessario installare, configurare o manutenere infrastrutture di gestione.
- L' agente leggero e l' architettura nativa per il cloud non influenzano negativamente le prestazioni degli endpoint.

Automatizza e riduce il tempo di rilevamento

- Le applicazioni che rappresentano un rischio per la sicurezza vengono bloccate (tramite hash o nome del processo).
- Viene bloccata l' esecuzione di minacce, dei malware di tipo zero-day, degli attacchi senza file/malware, dei ransomware e dei tentativi di phishing.
- Viene rilevata e bloccata l' attività dannosa in memoria (exploit) prima che possa diventare pericolosa.
- Vengono rilevati i processi dannosi che hanno aggirato le misure preventive.
- Vengono rilevate e bloccate tecniche, tattiche e procedure di intrusione.

Automatizza e riduce il tempo di risposta e indagine

- Soluzione e risposta: analisi forense per indagare a fondo su ogni tentativo di attacco e strumenti per mitigarne gli effetti (disinfezione).
- Capacità di tracciare tutte le azioni; visibilità dell' aggressore e delle sue attività con la possibilità di intervenire direttamente, facilitando le indagini forensi.
- Miglioramento e perfezionamento delle policy di sicurezza grazie alle conclusioni dell' analisi forense.

[1] Il costo per il contenimento del malware secondo Ponemon Institute. Citato anche da Swimlane (https://swimlane.com/blog/cybersecurity-statistics-2017) e in altri studi indipendenti.

SICUREZZA DEGLI ENDPOINT AVANZATA E AUTOMATIZZATA

Le tecnologie di protezione tradizionali, incentrate sulla prevenzione, sono misure a basso costo, utili ma non sufficienti per minacce note e comportamenti dannosi. Per difendere con efficacia un' organizzazione ed 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 l' organizzazione sia stata compromessa e che tutti gli endpoint siano costantemente sotto attacco.

Panda Adaptive Defense integra in un'unica soluzione le tecnologie di prevenzione tradizionali e le funzionalità innovative e adattive di prevenzione, rilevamento e risposta alle minacce informatiche più avanzate, sia presenti che future:

- Tecnologie di prevenzione tradizionali
- Antimalware multivettoriale permanente e scansione su richiesta
- Creazione di blacklist/whitelist gestita
- Intelligenza collettiva
- Euristica pre-esecuzione
- Soluzioni antimanomissione
- Correzione e rollback
- Tecnologie di sicurezza avanzate
- EDR: monitoraggio continuo degli endpoint
- Prevenzione dell' esecuzione di processi sconosciuti
- Apprendimento automatico basato su 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.
- Ricerca delle minacce e analisi forense

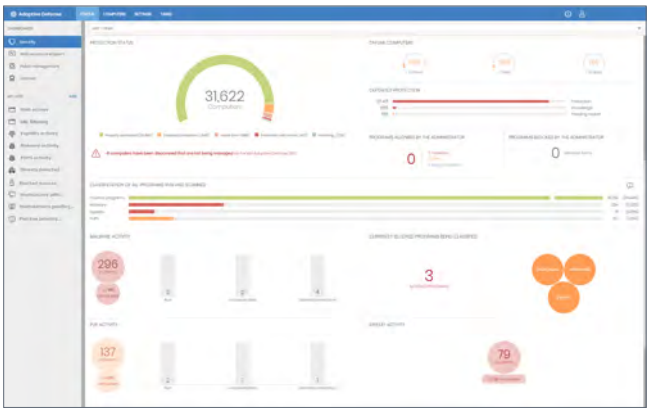

Figura 1: dashboard principale di Panda Adaptive Defense.

SERVIZIO ZERO TRUST PER LE APPLICAZIONI

Un servizio innovativo 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 incertezze e senza delegare alcuna responsabilità al client, 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 **apprendimento automatico** (o ML, Machine-Learning) multilivello, compreso il **deep learning**, che è il risultato di una continua verifica e automazione dell' esperienza e delle conoscenze accumulate dal team di sicurezza interno di Panda Security.

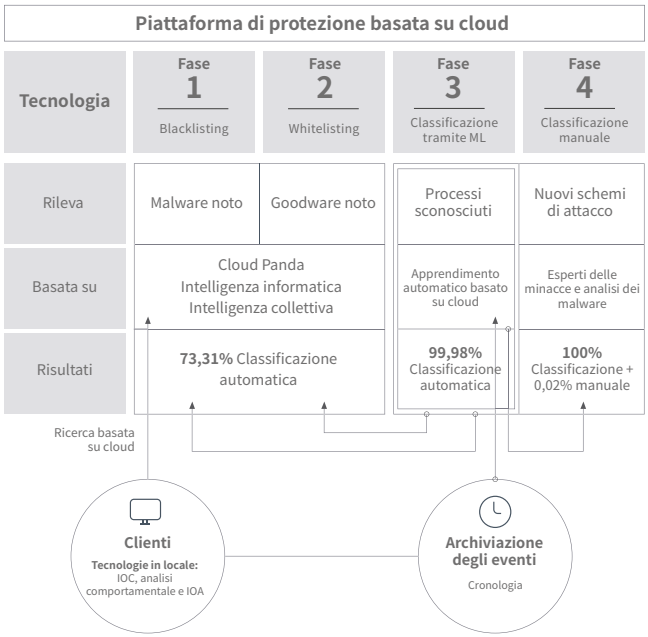

Figura 2: fasi del servizio di classificazione in cloud.

Il servizio di ricerca delle minacce è condotto da un team di esperti che utilizzano strumenti di profilazione, analisi e correlazione di eventi per scoprire in modo proattivo nuove tecniche di intrusione e di elusione.

Gli addetti alla ricerca delle minacce del Panda Intelligence Center lavorano partendo dal presupposto che le aziende siano costantemente compromesse.

Piattaforme supportate e requisiti di sistema di PANDA ADAPTIVE DEFENSE

Sistemi operativi supportati: Windows, macOS e Linux.
Le funzionalità EDR sono disponibili in Windows, macOS e Linux; Windows è la piattaforma che ne garantisce la piena operatività.

Elenco dei browser compatibili: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera.

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