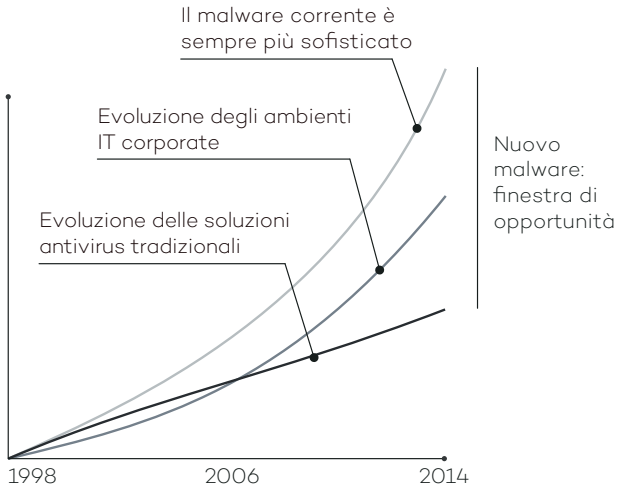
Adaptive Defense 360

Trova le risposte, risolvi il problema

DIFESA COMPLETA PER ENDPOINT INTEGRANTE PROTEZIONE, RILEVAZIONE, RISPOSTA E BONIFICA IN UN'UNICA SOLUZIONE

Difendere gli endpoint contro gli attacchi è difficile. La protezione deve comprendere un'ampia gamma di difese che comprenda i tradizionali antivirus/anti-malware, il personal firewall, il filtro su navigazione web e posta elettronica e il controllo dei dispositivi. Inoltre qualsiasi difesa deve fornire garanzie supplementari contro attacchi mirati e zero-day difficili da rilevare. Fino ad ora il personale IT doveva acquisire e gestire diversi prodotti di diversi fornitori per difendere gli endpoint.

Adaptive Defense 360 è la prima e unica offerta che integra le funzionalità Endpoint Protection (EPP) ed Endpoint Detection & Response (EDR) in un unica soluzione. **Adaptive Defense 360** automatizza diverse funzioni di sicurezza riducendo il carico sulle risorse IT. **Adaptive Defense 360** nasce da Panda Endpoint Protection, la migliore soluzione EPP nella sua categoria, che comprende: la gestione semplice e centralizzata della sicurezza, le azioni correttive, il monitoraggio e la reportistica in tempo reale, la protezione basata sui profili, il controllo centralizzato dei dispositivi e il monitoraggio e filtraggio del traffico web.

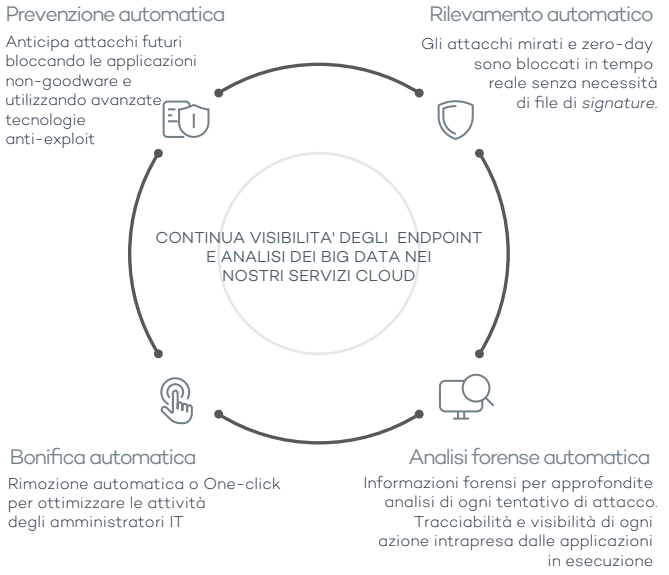


Tuttavia, questo è solo l'inizio. Il malware e gli ambienti di sicurezza IT hanno subito grandi cambiamenti incrementali in termini di volume e complessità. Con oltre 200.000 nuovi virus che compaiono ogni giorno e con la raffinatezza delle tecniche per penetrare le difese e occultare il malware, le reti aziendali sono più vulnerabili che mai ad attacchi mirati e zero-day.

Le soluzioni tradizionali di protezione degli endpoint sono efficienti nel bloccare malware noto mediante tecniche di rilevamento basate su database di *signature* e algoritmi euristici.

Tuttavia, esse non sono un'idonea difesa contro gli attacchi mirati e zero-day che sfruttano la 'finestra di opportunità per il malware', ovvero il tempo intercorso tra la comparsa di nuovi malware e il rilascio dell'antidoto da parte delle società di sicurezza: un divario crescente che viene sfruttato dagli hacker per introdurre virus, ransomware, trojan e altri tipi di malware nelle reti aziendali. Queste minacce possono crittografare i documenti riservati e richiedere un riscatto per la decifrazione o semplicemente raccogliere dati sensibili per spionaggio industriale.

La soluzione Panda a questi tipi di attacchi è la **Difesa Adattiva.** Essa fornisce un servizio EDR che può classificare con precisione ogni applicazione in esecuzione in un'organizzazione, consentendo la corretta esecuzione dei soli programmi legittimi. Le funzionalità EDR di **Panda Adaptive Defense 360** si basano su un modello di sicurezza basato su tre principi: il monitoraggio continuo delle applicazioni sui computer e server di un'azienda, la classificazione automatica tramite un Sistema Esperto che inferisce sulla nostra piattaforma Big Data in Cloud e, infine, il nostro team di esperti tecnici che analizzano quelle applicazioni che non sono state classificate automaticamente per essere certi del comportamento di tutto ciò che viene eseguito sui sistemi aziendali.



Queste funzionalità sono ora combinate nella nostra soluzione EPP al top della sua categoria, che completa il ciclo di protezione adattiva da malware e che comprende ora le funzioni di prevenzione, individuazione, analisi e bonifica automatizzate

- Copy Service s.r.l. - Aprilia (LT) Via Pontina Km 46600 - Tel 0692060064 - e-mail commerciale@copyservicesrl.com -

L'UNICA SOLUZIONE CHE GARANTISCE LA SICUREZZA DI TUTTE LE APPLICAZIONI IN ESECUZIONE

PROTEZIONE COMPLETA E ROBUSTA GARANTITA

Panda Adaptive Defense 360 offre due modalità operative:

• La **modalità standard** consente a tutte le applicazioni catalogate come goodware di essere eseguite, insieme alle applicazioni che devono ancora essere catalogate dai sistemi automatizzati di Panda Security.

• La **modalità estesa** consente solo l'esecuzione di goodware. Questa è la forma ideale di protezione per le aziende con un approccio a 'rischio zero' per la sicurezza.

INFORMAZIONI FORENSI

• **I grafi di correlazione degli eventi** permettono di acquisire una chiara comprensione di tutte le azioni causate da malware.

• Si possono ottenere informazioni visive, attraverso le mappe di intensità, sull'origine geografica delle connessioni stabilite dai malware, sui i file creati e altro ancora.

• E' possibile individuare i software con vulnerabilità note installati sulla vostra rete.

PROTEZIONE PER SISTEMI OPERATIVI E APPLICAZIONI VULNERABILI

Sistemi come Windows XP che non sono più supportati da MS e sono quindi vulnerabili perché non più patchati diventano facile preda per le nuove generazioni di attacchi zero-day Inoltre, le vulnerabilità nelle applicazioni come Java, Adobe, MS Office e di diversi browser sono sfruttate dal 90 per cento dei malware.

Il modulo di protezione delle vulnerabilità in Adaptive Defense 360 utilizza regole contestuali e comportamentali per garantire che le aziende possano lavorare in un ambiente sicuro, anche se utilizzano sistemi non più aggiornati.

COMPLETE FUNZIONALITÀ EPP

Adaptive Defense 360 integra Panda Endpoint Protection Plus, la più sofisticata soluzione EPP Panda, fornendo così una piena capacità EPP che comprende:

- Misure correttive
- Controllo centralizzato dei dispositivi per prevenire l'immissione di malware e la perdita di dati, bloccando tipologie di dispositivi USB esterni
- Monitoraggio e filtraggio della navigazione Web
- Antivirus e anti-spam per server Exchange
- Endpoint Firewall, e molti altri...

INFORMAZIONI CONTINUE SULLO STATO DI TUTTI GLI ENDPOINT NELLA RETE

Ricezione di avvisi immediati nel momento in cui il malware viene individuato sulla rete, con una relazione completa che dettaglia la posizione, i computer infetti e le azioni intraprese dal malware.
Ricezione via e-mail di rapporti sull'attività quotidiana del servizio.

FUNZIONI SIEM (Security Information and Event Management)

Adaptive Defense 360 si integra con soluzioni SIEM per fornire dati dettagliati sull'attività di tutte le applicazioni eseguite sui vostri sistemi.

Per i clienti senza una propria soluzione SIEM, **Adaptive Defense 360** può includere un proprio sistema per memorizzare e gestire eventi di sicurezza e per analizzare tutte le informazioni raccolte in tempo reale.

SERVIZIO GESTITO AL 100%

Dimenticatevi di dover investire in personale tecnico per gestire la quarantena o i file sospetti o per disinfettare e ripristinare i computer infetti. **Adaptive Defense 360** classifica tutte le applicazioni automaticamente grazie ai Sistemi Esperti implementati nei nostri ambienti Big Data sotto la continua supervisione degli esperti dei PandaLabs.

REQUISITI TECNICI

Web Console di monitoraggio

- Connessione Internet
- Internet Explorer 7.0 o successivo
- Firefox 3.0 o successivo
- Google Chrome 2.0 o successivo

Agente

- Sistema operativo (workstation): Windows XP SP2 e successivo, Vista, Windows 7, 8 & 8.1, 10
- Sistema operativo (server): Windows Server 2003, Windows Server 2008, Windows Server 2012
- Connessione Internet

Supporto parziale (solo funzioni EPP):

- Sistemi operativi Linux, Mac OS X e Android

Copy Service s.r.l. Via Pontina, Km 46600 Aprilia (LT)

Tel- 06-92060064
www.copyservicesrl.com
commerciale@copyservicesrl.com