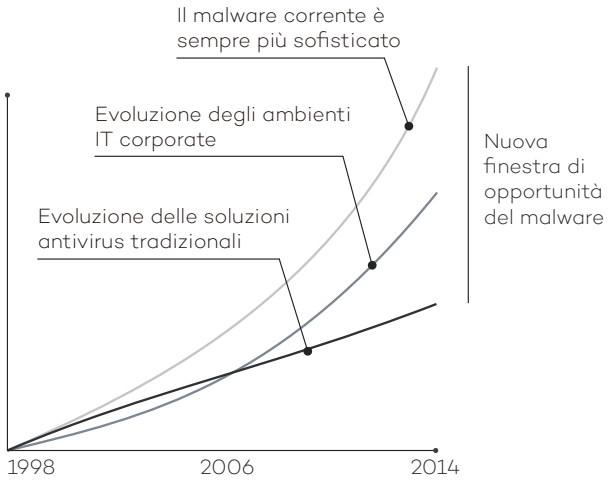
Adaptive Defense

Chiudere la finestra di opportunità alle minacce avanzate

PENSATE CHE LA VOSTRA ORGANIZZAZIONE SIA PROTETTA CONTRO ATTACCHI MIRATI E ZERO-DAY?

Gli scenari del malware e della sicurezza IT hanno subito un cambiamento importante in termini di volume e di sofisticazione. C'è stato un aumento esponenziale del numero di virus in circolazione (circa 200.000 nuovi virus appaiono ogni giorno); nuove tecniche tecniche per penetrare le difese e nascondere il malware permettono alle minacce di persistere sulle reti aziendali per lunghi periodi.



Allo stesso tempo, gli ambienti informatici sono diventati sempre più complessi, rendendo la gestione più difficile e i sistemi più vulnerabili.

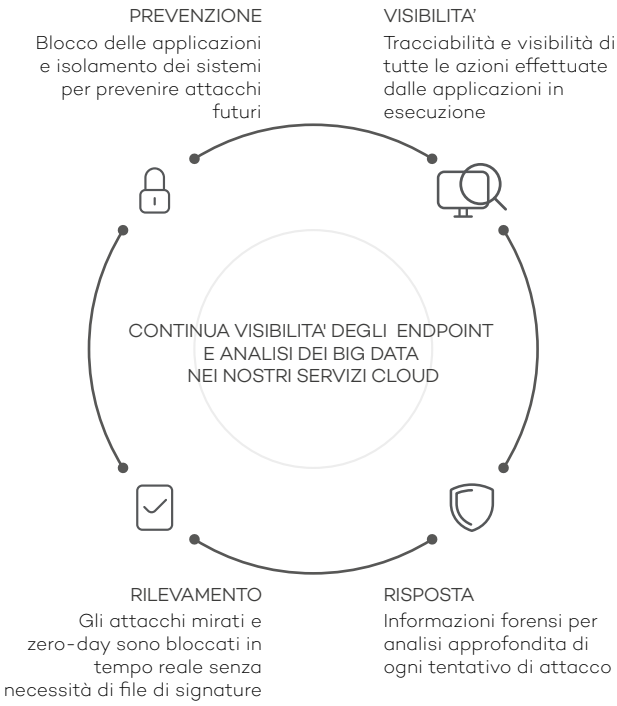
Le soluzioni antivirus tradizionali oramai non sono più al passo con la realtà. La loro evoluzione lineare continua a utilizzare obsolete tecniche di rilevamento basate su file di signature e algoritmi euristici. Ciò significa che i risultati sono inaccurati, ovvero che il malware può passare inosservato e vengono generati falsi positivi.

Questa discrepanza ha portato a quella che è stata definita la **'Finestra di opportunità per il malware':** il lasso di tempo che intercorre tra la comparsa di un nuovo virus ed il rilascio dell'antidoto dalle società di sicurezza. Un crescente divario che viene sfruttato dagli hacker per introdurre i virus, ransomware, Trojan e altri tipi di malware nelle reti aziendali. Tali minacce sempre più comuni possono crittografare documenti riservati e richiedere un riscatto, o semplicemente raccogliere dati sensibili per spionaggio industriale.

I governi, le banche e altre grandi aziende stanno sopportando il peso di attacchi che le soluzioni antivirus tradizionali non sono in grado di rilevare in tempo. Il nostro reparto di ricerca ha analizzato milioni di campioni di virus e i migliori prodotti antivirus presenti sul mercato per dimostrare che il 18 per cento del malware non viene rilevato nelle prime 24 ore dopo il rilascio e che anche dopo tre mesi queste soluzioni tradizionali non sono ancora in grado di rilevare il 2 per cento del malware.

La soluzione a questa situazione è **Adaptive Defense:** il servizio di Panda Security che può classificare con precisione ogni applicazione in esecuzione nella propria organizzazione, consentendo soltanto l'esecuzione di programmi legittimi.

Per raggiungere questo obiettivo, abbiamo lavorato per cinque anni su un nuovo modello di sicurezza basato su tre principi: il monitoraggio continuo delle applicazioni sui computer e server di una società, la classificazione automatica tramite Machine Learning sulla nostra piattaforma Big Data nel cloud e infine, il nostro team di tecnici esperti che analizzano quelle applicazioni che non sono state classificate automaticamente per essere certi del comportamento di tutto ciò che viene eseguito sui sistemi aziendali.



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

PROTEZIONE COMPLETA E ROBUSTA GARANTITA

Panda Adaptive Defense offre due modalità:

- **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.

COMPATIBILE CON LE SOLUZIONI ANTIVIRUS TRADIZIONALI

Adaptive Defense può coesistere con soluzioni antivirus tradizionali e assumere il ruolo di **strumento aziendale capace di bloccare ogni tipo di malware, tra cui attacchi mirati e zero-day** che tali soluzioni tradizionali non sono in grado di rilevare.

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** utilizza regole contestuali e comportamentali per garantire che le aziende possano lavorare in un ambiente sicuro, anche se utilizzano sistemi non più aggiornati.

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 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** 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 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 (solo 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