panda
a WatchGuard brand

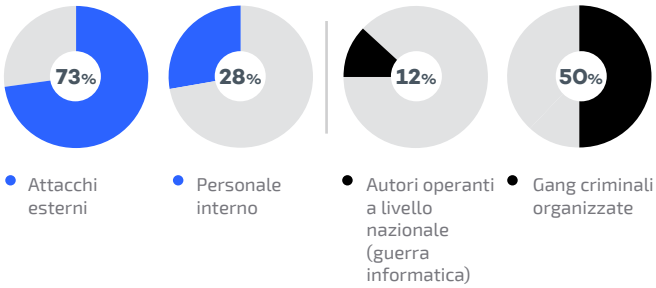
Dati a supporto dell'intelligence: per la massima protezione dalle violazioni

Panda Adaptive Defense 360 unisce la tradizionale tecnologia antivirus al modello di protezione avanzato con rilevamento degli endpoint e relativa risposta in un'unica soluzione mirata a contrastare le minacce note e non note.

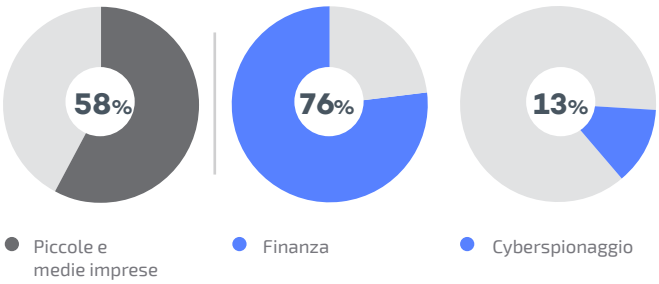
Panda Adaptive Defense 360

Panorama delle minacce

Da dove arrivano gli attacchi?[1]



Chi sono le vittime? Quali sono i motivi?[1]



Quali sono i costi per le aziende?

- **Costi globali:** $600.000 M[2]
- **Costi di una violazione dei dati:** $3,86 M[3]

L'evoluzione degli hacker

Gli hacker sono **sempre più sofisticati** e **sempre più numerosi**: una conseguenza della loro professionalizzazione, della condivisione delle tecnologie e delle tante lacune della cyber intelligence.

Eliminazione della superficie di attacco

Le minacce informatiche di prossima generazione che stanno mettendo in atto sono progettate per aggirare le **soluzioni tradizionali** passando completamente inosservate e rendendo le reti del tutto vulnerabili senza le opportune difese.

Le piattaforme di protezione tradizionali non sono sufficienti contro gli attacchi avanzati perché non forniscono visibilità e dettagli sufficienti in relazione ai processi e alle applicazioni in esecuzione nelle reti aziendali. Per risolvere questo problema, i reparti IT stanno aggiungendo un ulteriore livello di protezione introducendo le soluzioni di difesa degli endpoint e relativa risposta (EDR). Le funzionalità EDR includono il monitoraggio costante e l'analisi dei dati dell'attività di rete, offrendo ai reparti IT i dati e le opzioni di rilevamento di cui hanno bisogno per difendersi dalle minacce avanzate.

Gestione del carico di lavoro IT

Con l'aumento della quantità di macchine distribuite nelle infrastrutture aziendali, che di anno in anno è sempre maggiore, i team addetti alla sicurezza sono in difficoltà nel gestire e difendere i dispositivi sia interni che esterni alla rete. E per quanto le soluzioni EDR siano componenti fondamentali della protezione dalle minacce avanzate, la maggior parte di esse contribuisce ad aumentare le difficoltà di gestione dell'ambiente IT. Ciò accade principalmente perché la gestione della piattaforma non è automatizzata ed è, quindi, il team a dover gestire gli alert generati e classificare manualmente le minacce.

Soluzioni di rilevamento degli endpoint e relativa risposta (EDR)

Qual è la funzione principale delle soluzioni EDR?

Le soluzioni EDR consentono di monitorare, registrare e archiviare i dettagli delle attività di un endpoint, tra cui eventi degli utenti, processi, modifiche al registro di sistema, utilizzo della memoria e della rete. Questa visibilità mette in luce minacce che altrimenti passerebbero inosservate.

Quali sono i limiti delle soluzioni EDR?

Per individuare anomalie di sicurezza negli eventi e confermare o respingere gli alert, vengono utilizzate molteplici tecniche e strumenti, e tutto ciò richiede l'intervento umano.

Le soluzioni EDR richiedono una supervisione 24 ore su 24, 7 giorni su 7, e una risposta rapida da parte di personale altamente qualificato.

Queste risorse sono costose e difficili da trovare. Le organizzazioni a corto personale con budget limitati non sono preparate a sfruttare da sole i vantaggi offerti dalle soluzioni EDR. Il personale si trova con maggiori carichi di lavoro derivanti dall'implementazione e dall'utilizzo di queste soluzioni, che finiscono quindi per non essere di supporto in ciò che conta: ottimizzare la protezione delle organizzazioni.

La risposta a questo problema?

Panda Adaptive Defense 360.

1 "2018 Data Breach Investigation report" (Report di indagine del 2018 sulle violazioni di dati). Verizon

2 "2018 Economic Impact of Cybercrime — No Slowing Down" (L'impatto economico degli attacchi informatici: non accenna a rallentare). CSIC/McAfee
3 "2018 Study on Global Megatrends in Cybersecurity" (Studio del 2018 sui megatrend internazionali in materia di sicurezza informatica). Ponemon Institute
4 "2018 Cost of a Data Breach Study: Global Overview" (Studio del 2018 sui costi di una violazione di dati: una panoramica globale). Ponemon Institute/IBM Security

Panda Adaptive Defense 360

Panda Adaptive Defense 360 è un'innovativa soluzione per la sicurezza informatica pensata per PC desktop, laptop e server, il tutto su cloud. Automatizza la prevenzione, il rilevamento, il contenimento e la risposta a eventuali attacchi avanzati, malware zero-day, ransomware, phishing, exploit della memoria e attacchi privi di malware presenti o futuri, sia all'interno che all'esterno della rete aziendale.

Grazie alla sua architettura cloud, il software agent è a basso impatto e non influisce sulle prestazioni degli endpoint, che sono gestiti mediante un'unica console cloud anche quando non sono connessi a Internet.

Panda Adaptive Defense 360 integra le piattaforme di protezione e gestione del cloud (Aether), che consentono di ottimizzare la prevenzione, il rilevamento e la risposta automatica, riducendo al minimo le risorse necessarie.

Si differenzia da altre soluzioni in quanto combina la più ampia gamma di tecnologie di protezione (EPP) con le funzionalità automatiche di EDR, grazie a un servizio gestito dagli esperti di Panda Security e fornito come funzionalità della soluzione, vale a dire il servizio di classificazione 100%, che automatizza la gestione degli alert e il processo decisionale che ne consegue.

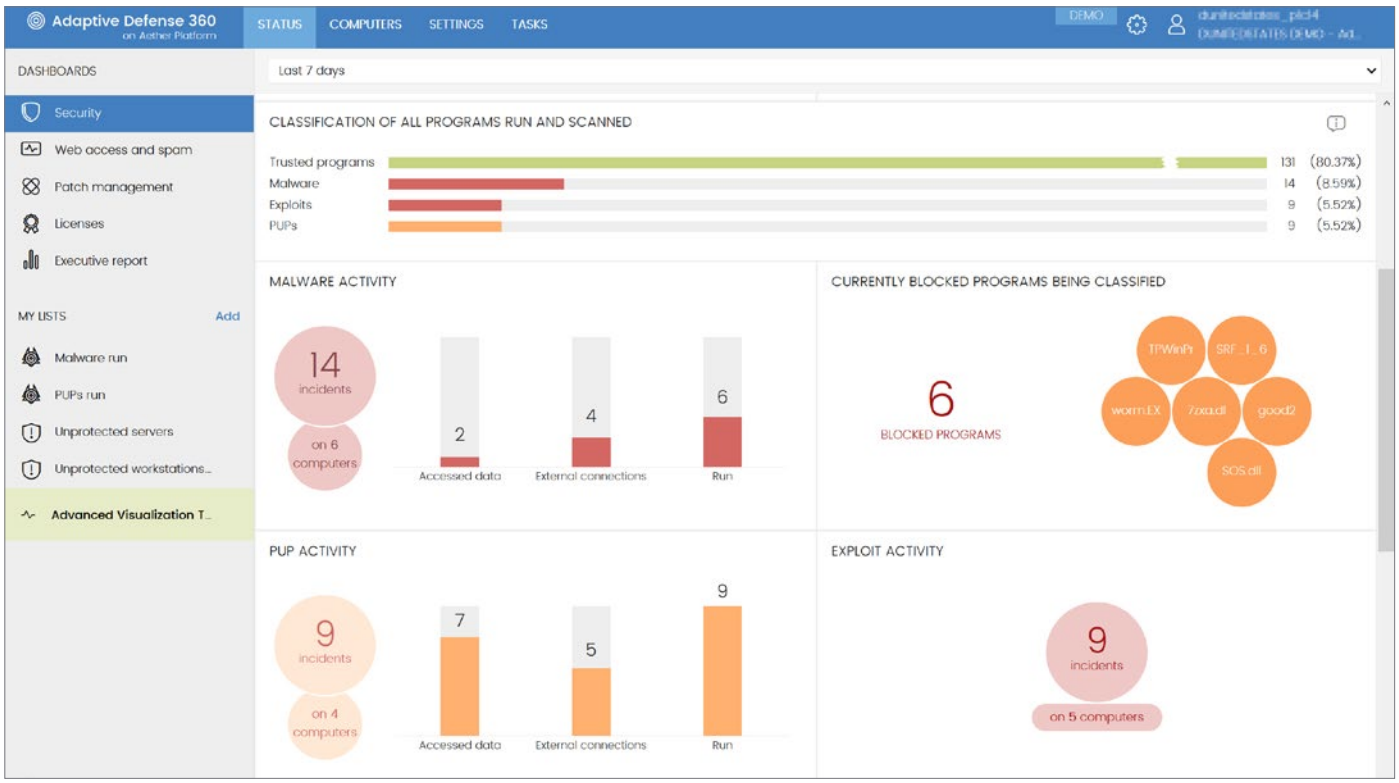


Figura 1: Un unico dashboard offre una visione globale e una gestione consolidata che dà priorità alle minacce rilevate

Vantaggi Panda Adaptive Defense 360

Semplificazione e riduzione del costo della sicurezza avanzata e adattiva

- I servizi gestiti riducono il costo del personale esperto, eliminando la responsabilità di gestire gli alert e il processo decisionale che ne consegue
- I servizi gestiti apprendono automaticamente dalle minacce e consentono di non perdere tempo con le impostazioni manuali
- La massima prevenzione sull'endpoint riduce i costi operativi pressoché a zero
- Non è necessario installare, configurare o manutenere infrastrutture di gestione
- Le prestazioni degli endpoint non sono intaccate in quanto si basano su un agent a basso impatto e su un'architettura cloud

Automazione e riduzione del rilevamento e del tempo di esposizione (tempo di permanenza)

- Blocco dell'esecuzione di minacce, malware zero-day, ransomware e phishing
- Rilevamento e blocco dell'attività dannosa nella memoria (exploit) prima che possa causare danni
- Rilevamento dei processi dannosi che aggirano le misure preventive
- Rilevamento e blocco delle tecniche e procedure di hacking

Automazione e riduzione dei tempi di risposta e di indagine

- Correzione automatica e trasparente
- Ripristino dell'attività dell'endpoint e ripristino immediato delle normali attività
- Informazioni utili sugli hacker e sulla relativa attività, per accelerare le indagini forensi
- Riduzione della superficie di attacco, ottimizzazione immediata della protezione

Riduzione del carico di lavoro IT con il servizio di classificazione 100%

Il servizio di classificazione 100% consente di monitorare e impedire l'esecuzione di applicazioni e processi dannosi sugli endpoint. Per ogni esecuzione, viene generata in tempo reale una classificazione **dannoso/non dannoso** che elimina la necessità dell'intervento umano. Tutto ciò è possibile grazie alla velocità, capacità, flessibilità e scalabilità dell'IA e dell'elaborazione cloud.

Il servizio combina Big Data e apprendimento automatico multilivello, incluso Deep Learning, ed è supportato dalla costante supervisione e automazione dell'esperienza, dell'intelligenza e delle competenze acquisite nel tempo degli esperti in materia di sicurezza e minacce del centro di intelligence di Panda Security.

Il servizio di classificazione 100% è in grado, come nessun'altra soluzione sul mercato, di evitare che i reparti IT eseguano malware sugli endpoint all'interno e all'esterno della rete aziendale.

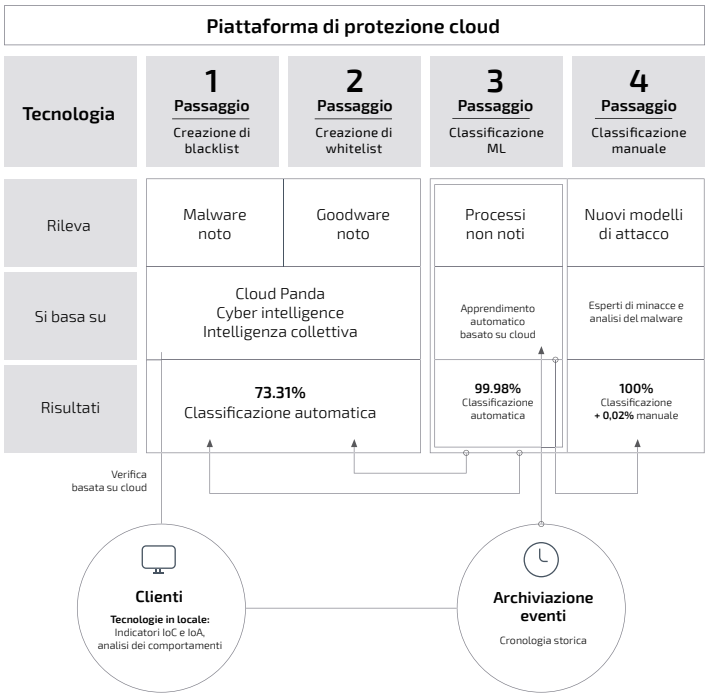


Figura 2: Workflow del servizio di classificazione cloud gestito

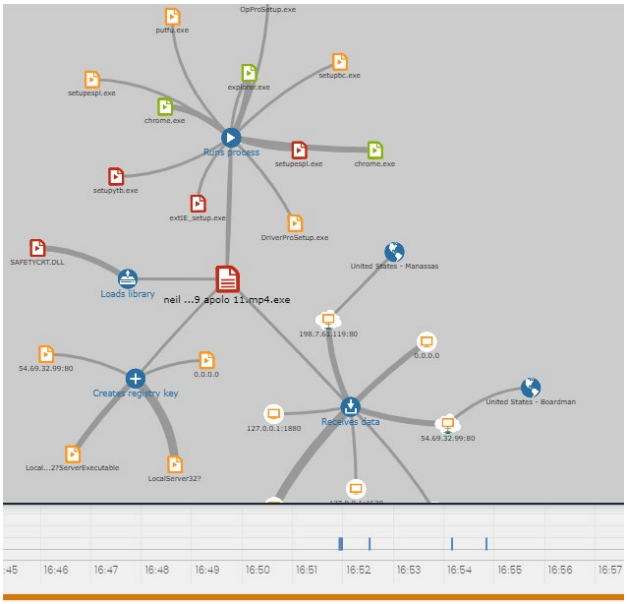


Figura 3: La cronologia degli incidenti fornita dalla console Panda Adaptive Defense 360 semplifica le indagini forensi, in quanto indica la data della prima visualizzazione nella rete, i nomi e il numero degli endpoint interessati, le modifiche alle impostazioni e i destinatari delle comunicazioni.

Sicurezza avanzata automatizzata sugli endpoint

Panda Adaptive Defense 360 integra, in un'unica soluzione, le tecnologie di protezione tradizionali con le funzionalità di nuova generazione per la prevenzione, il rilevamento e la risposta automatica a minacce informatiche avanzate.

Tecnologie di protezione tradizionali

- Firewall personale o gestito. IDS
- Controllo dispositivi
- Antimalware permanente multivettore e scansione on-demand
- Creazione di blacklist/whitelist gestita. Intelligenza collettiva
- Euristica pre-esecuzione
- Controllo dell'accesso al Web
- Antispam e antiphishing
- Soluzioni antimanomissione
- Filtro dei contenuti e-mail
- Correzione e rollback

Tecnologie di sicurezza avanzate

- EDR: monitoraggio costante delle attività degli endpoint
- Prevenzione dell'esecuzione di processi non noti
- Apprendimento automatico dei comportamenti basato su cloud, per classificare il 100% dei processi non noti (access point, ransomware, rootkit, ecc.)
- Sandboxing basata su cloud in ambienti reali
- Analisi dei comportamenti e rilevamento di IoA (script, macro, ecc.)
- Rilevamento automatico e relativa risposta a exploit della memoria

*TTP: tattiche, tecniche e procedure utilizzate dagli hacker

Piattaforma di gestione cloud: Aether

Sicurezza, visibilità e controllo di prossima generazione. Completa, scalabile e su cloud, per una convenienza immediata.

La piattaforma Aether e la relativa console cloud ottimizzano la gestione della sicurezza avanzata e adattiva all'interno e all'esterno della rete.

Progettata in modo che i team addetti alla sicurezza possano concentrarsi esclusivamente sulla gestione della protezione aziendale, riduce la complessità ottimizzando flessibilità, granularità e scalabilità.

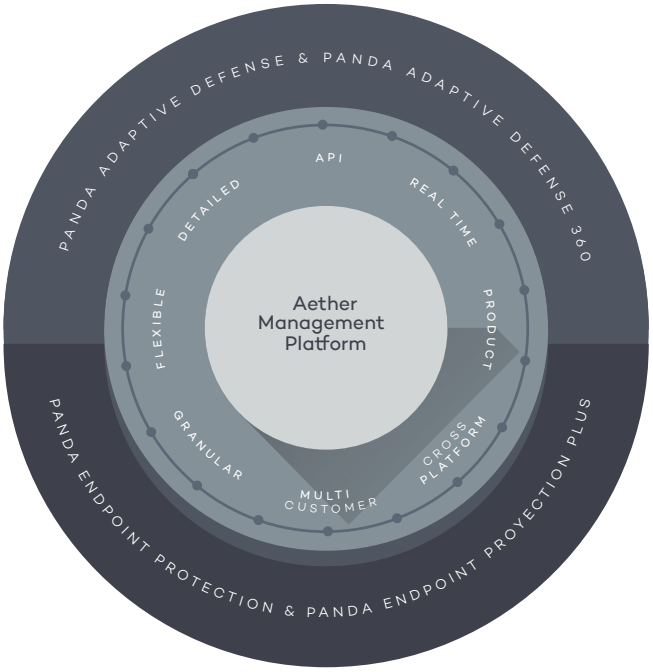


Figura 3: Un'unica piattaforma di gestione cloud: Aether

Vantaggi della piattaforma Aether

Maggiore convenienza in meno tempo grazie alla semplicità di implementazione che assicura visibilità immediata

- Distribuzione, installazione e configurazione in pochi minuti, per la massima convenienza fin dal primo giorno
- Agent a basso impatto multiprodotto e multimodulo distribuibile su tutte le piattaforme più comuni (Windows, Mac, Linux, Android)
- Rilevazione automatica di endpoint non protetti e installazione remota
- Tecnologia proxy proprietaria, anche su computer privi di connessione Internet
- Ottimizzazione del traffico, con tecnologia repository/cache proprietaria

Facilità d'uso e adeguamento alle esigenze aziendali

- Console Web intuitiva per una gestione flessibile e modulare
- Ruoli predefiniti e personalizzati
- Audit dettagliati delle azioni nella console
- Utenti con autorizzazioni e visibilità totali o limitate
- Policy di sicurezza per gruppi ed endpoint
- Inventari per hardware e software e registro delle modifiche

Monitoraggio semplificato per risposte più tempestive

- Dashboard e indicatori chiave con priorità
- Alert confermati e con priorità nel flusso di lavoro
- Cronologia incidenti completa e sfruttabile: processi interessati, fonte, tempo di permanenza, diffusione, ecc.
- Intervento sugli endpoint con un solo clic: riavvio, isolamento, applicazione di patch e scansione, accelerazione dei tempi di risposta

Premi e certificaciones

Panda Security partecipa regolarmente ai confronti in materia di protezione e prestazioni condotti da tutte le principali società di analisi, tra cui Virus Bulletin, AV-Comparatives, AV-Test e NSSLabs, ricevendo numerosi premi.

AV-Comparatives sostiene Adaptive Defense 360 "poiché questa soluzione classifica tutti i processi eseguiti e, quindi, non può non riuscire a registrare l'eventuale malware presente"

Piattaforme supportate e requisiti di sistema delle nostre soluzioni di sicurezza per endpoint

Le piattaforme supportate sono in continua evoluzione al fine di fornire la massima copertura possibile per i sistemi operativi più recenti. Dai link riportati n basso è possibile accedere al supporto online di ciascuno dei nostri prodotti:

Workstation e server Windows: http://go.pandasecurity.com/endpoint-windows/requirements
Dispositivi Mac OS: 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

Panda Patch Management: http://go.pandasecurity.com/patch-management/requirements
Gestione dei sistemi cloud Panda: http://go.pandasecurity.com/systems-management/requirements
SIEM Feeder: http://go.pandasecurity.com/siem-feeder/requirements
Advanced Reporting Tool: http://go.pandasecurity.com/reporting-tool/requirements
Panda Full Encryption: http://go.pandasecurity.com/full-encryption/requirements

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com pandasecurity.com/business