Protezione degli endpoint

EMOTET È DAVVERO SCOMPARSO PER SEMPRE?

Esamineremo un caso reale per illustrarti i rischi: EMOTET

Introduzione

Emotet è un trojan bancario polimorfo che è difficile da rilevare utilizzando le firme. Il suo obiettivo è trafugare i dati, incluse le credenziali degli utenti memorizzate nei browser, spiando il traffico Internet.

Considerata la sua efficacia in termini di persistenza e propagazione in rete, Emotet è spesso utilizzato per scaricare altro malware ed è particolarmente apprezzato come strumento per la diffusione di trojan bancari come Qakbot e TrickBot.

I server di comando e controllo di Emotet contattano regolarmente i sistemi compromessi per trovare aggiornamenti, inviare informazioni dai computer compromessi ed eseguire attacchi senza file con il malware scaricato.

Dopo aver infettato un computer su una rete, Emotet sfrutta la vulnerabilità EternalBlue per diffondersi e introdursi negli endpoint in cui sono presenti sistemi non sottoposti a patch.

Emotet: in che modo si diffonde e persiste?

Propagazione

Emotet **in genere si diffonde tramite allegati infetti o URL malevoli di messaggi e-mail.**

I messaggi e-mail sembrano provenire da fonti affidabili, perché Emotet assume il controllo degli account e-mail delle vittime, inducendo altri utenti inconsapevoli a scaricare il trojan nel proprio sistema.

Considerato il modo in cui Emotet si diffonde in una rete aziendale, qualsiasi computer infetto in una rete infetterà altri che, nel momento in cui erano stati aggiunti alla rete, risultavano puliti.

Persistenza

Emotet è progettato in modo da rimanere sul sistema infetto e attivarsi anche quando il sistema viene riavviato o si chiude la sessione. A questo scopo, crea:

- Copie di se stesso
- Chiavi di registro con nomi casuali
- Servizi che rimangono attivi

Danni

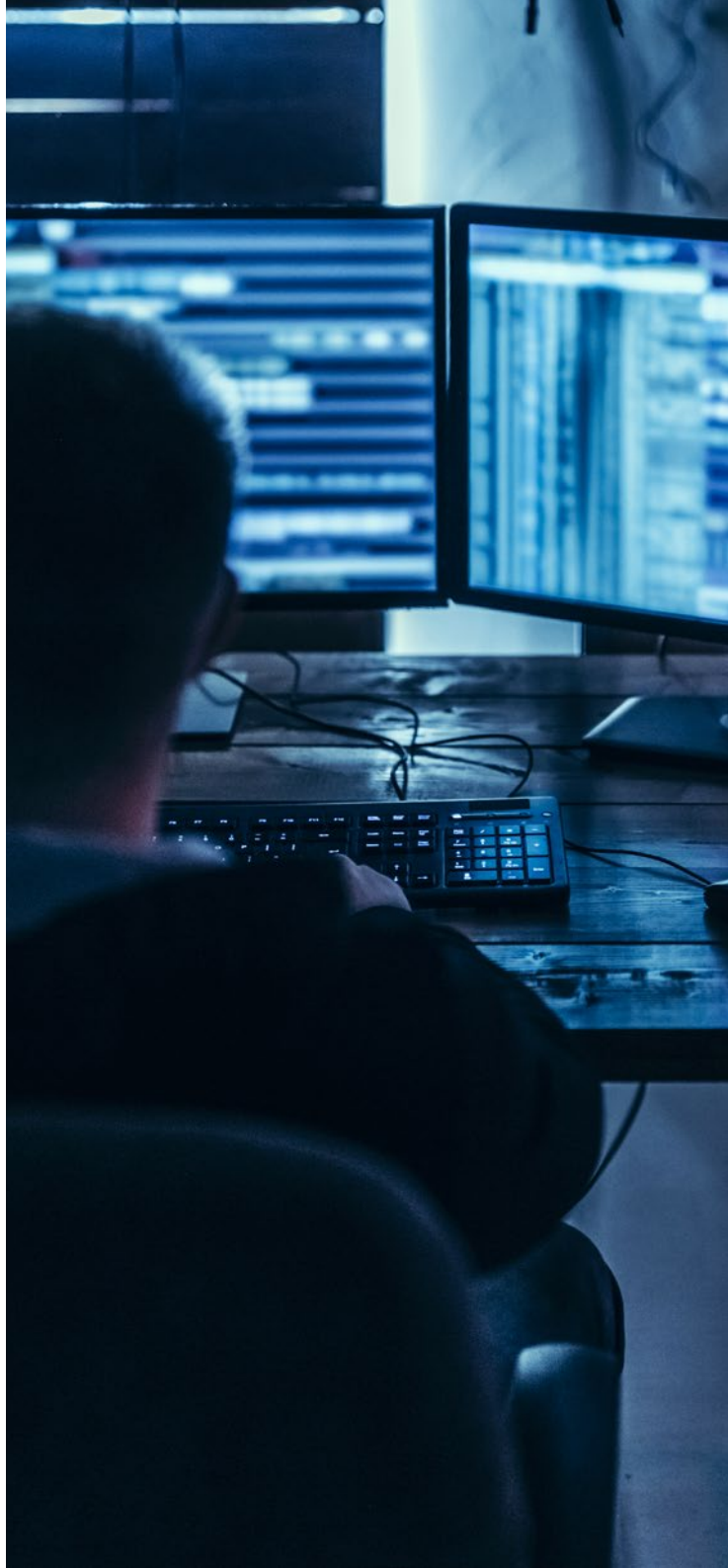
Emotet è pericoloso non solo a causa della sua capacità illimitata di diffondersi sfruttando la vulnerabilità EternalBlue, ma anche perché scarica e installa altro malware, consentendo l'accesso a qualsiasi tipo di trojan, spyware o persino ransomware.

Alcune delle possibili conseguenze sono:

- Furto di informazioni di identificazione personale (PII)
- Perdita di informazioni finanziarie e riservate, che possono essere utilizzate per scopi di ricatto
- Furto di credenziali di accesso, che rende vulnerabili altri account
- Periodi di correzione più lunghi per gli amministratori di rete
- Perdita di produttività per i dipendenti i cui endpoint sono stati isolati dalla rete

Dai un'occhiata all'infografica sul flusso di un attacco EMOTET >

WatchGuard



Adaptive Defense 360 automatizza una difesa su più livelli contro il **flusso di un attacco Emotet**

1 ATTACKER

2 Victim receives a spam with **WORD attachment**

3 Victim opens **the email and the attachment**

4 Victim **clicks away protected view** and **macro warnings**

5 Macro downloads **EMOTET** from compromised website

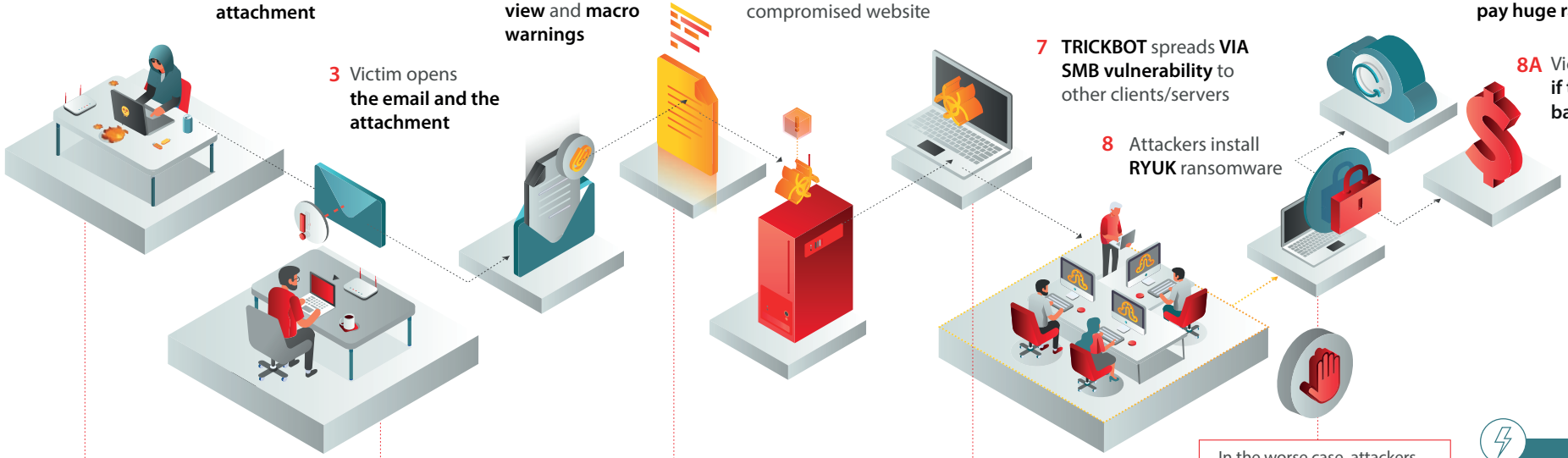
6 EMOTET drops TRICKBOT

7 TRICKBOT spreads **VIA SMB vulnerability** to other clients/servers

8 Attackers install **RYUK** ransomware

8A Victim can restore files **if they have offline backups**

8B If all backups are encrypted, **victim might pay huge ransom**



AD360 approach to defense:

Blocks malicious **email with antispam.**

Prevents access to known malicious URLs with URL filtering.

80%

AD360 approach to defense:

Blocks script execution with **macro detection and context-based detection**.

70%

AD360 approach to defense:

Blocks threats after lookup to the **Collective Intelligence** – the WatchGuard Cloud-based repository of malware and legitimate apps.

Blocks known/unknown threats with **generalist signatures & heuristics.**

60%

AD360 approach to defense:

Blocks known browser exploitation with **anti-exploit technology.**

Blocks unknown exploitation with **in-memory anti-exploit technology.**

50%

In the worse case, attackers are stopped here.

AD360 approach to defense:

The zero-trust model blocks any unknown binary coming from "outside" (email, web, network, device) until classified.

The Zero-Trust Application Service automatically classifies the payload **in a Cloud-based machine-learning system.**

0%

Ransomware begins process of encrypting files on the endpoint.

Message displayed confirms the presence on the endpoint and **provides intructions for paying the ransom.**

0% chance of success

WatchGuard

Emotet: in che modo si diffonde e persiste?

Proteggersi da una campagna Emotet non è particolarmente difficile perché il trojan si diffonde utilizzando **spam dannoso.** Ciononostante, gli utenti nella tua organizzazione possono diventare facilmente vittime delle **tecniche di phishing e di social engineering** che sono utilizzate con una frequenza elevata.

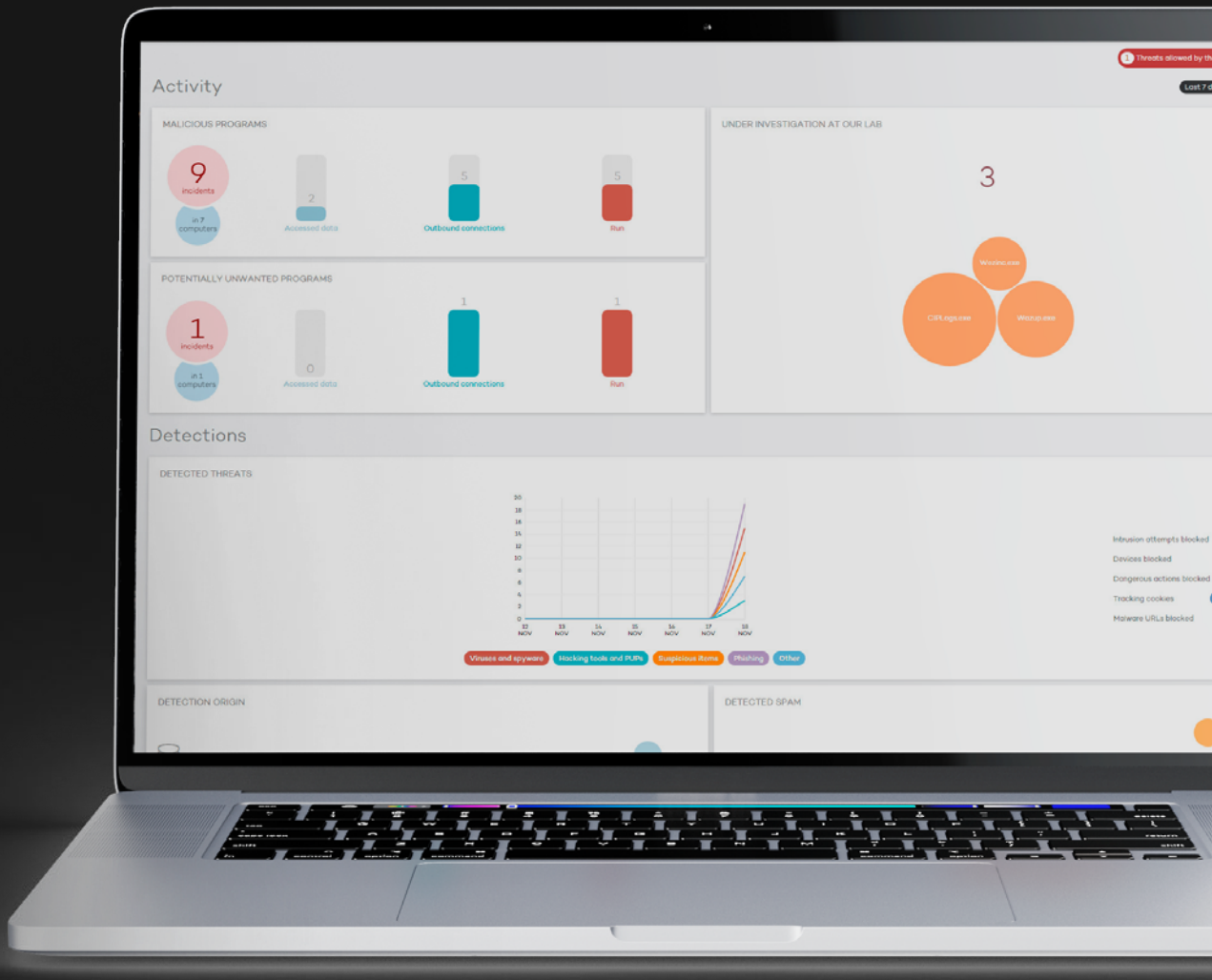
Ciò che rende questo trojan davvero pericoloso è la sua capacità di modificare automaticamente il proprio codice, diventando molto più difficile da rilevare con un antivirus tradizionale.

Per fortuna, le aziende che utilizzano Panda Security sono protette persino se i dipendenti aprono il messaggio e-mail e scaricano il documento.

Inoltre, le organizzazioni che si avvalgono di **Panda Adaptive Defense e Panda Adaptive Defense 360** sono anche protette da qualsiasi variante nota o sconosciuta, trojan o malware che sfrutta la **vulnerabilità EternalBlue.**

Il suo servizio di attestazione gestito per la classificazione di tutte le applicazioni e di tutti i processi impedisce l'esecuzione di questi elementi fino a quando non vengono classificati come affidabili.

Per maggiori informazioni su Panda Adaptive Defense 360 scarica il datasheet del prodotto.



Risposta a incidenti e correzione

Correzione

La pulizia di una rete infettata da Emotet **comporta l'esecuzione tempestiva di alcuni passaggi chiave.**

La cui implementazione, **in assenza degli strumenti adeguati** che vengono automatizzati e integrati nella soluzione di sicurezza, comporta rischi molto elevati ed è una procedura che può richiedere anche diversi mesi. Durante questo periodo, **un'organizzazione si espone al grave rischio di diventare vittima di questo o di altri attacchi informatici.**

Persistenza

Oltre a fornire protezione da Emotet e da tutte le sue varianti, Panda Adaptive Defense 360 ti fornisce tutti gli altri strumenti che facilitano e accelerano la risposta a un potenziale incidente:

- **Correzione automatizzata che distrugge tutte le tracce di Emotet.**
- **Per ogni rilevamento, puoi accedere alla cronologia delle azioni intraprese durante l'incidente, che ti consente di identificare la posizione e il momento in cui è avvenuto l'attacco, la modalità di ingresso e le azioni eseguite dal malware o dall'aggressore mentre il malware era attivo negli endpoint.**

Passaggi chiave >

1. Identifica i computer colpiti da Emotet.
2. Elimina i file eseguibili dannosi ed esegui il rollback delle modifiche apportate al sistema.
3. Trova (o richiedi al team IT) l'elenco dei computer vulnerabili a EternalBlue.
4. Isola i computer vulnerabili.
5. Riconnetti i computer alla rete.

WatchGuard

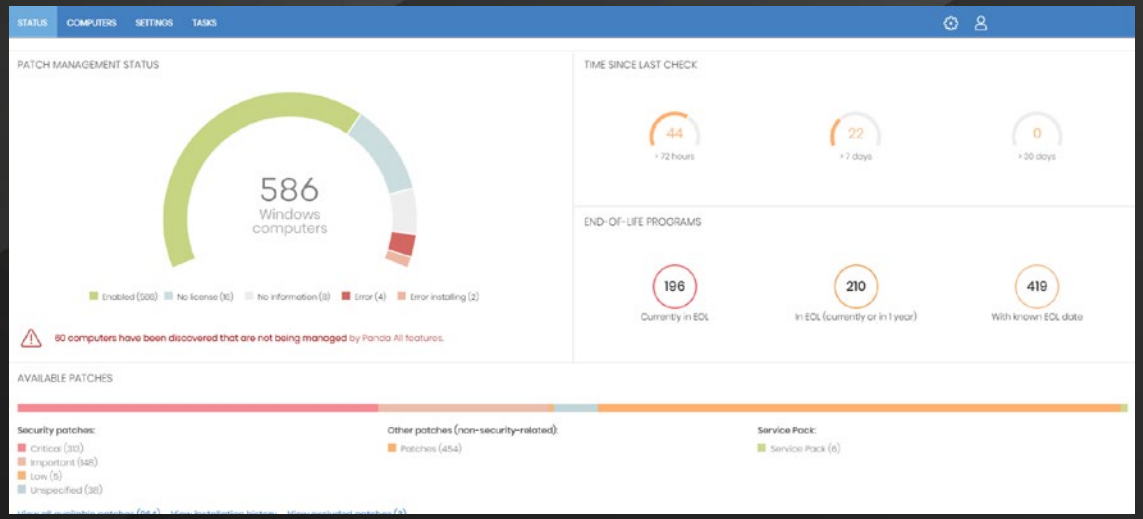
Non permettere che la tua organizzazione sia la prossima della lista.

Applicazione di patch e aggiornamento eseguiti in modo semplice da una singola console di gestione

Inoltre, **Panda Patch Management**, che è completamente integrato nella console di gestione di Panda Adaptive Defense 360, identifica automaticamente tutti i computer vulnerabili a EternalBlue o a qualsiasi altro sistema operativo o vulnerabilità di programma e li sottopone a patch in tempo reale dalla console con un semplice clic.

Non c'è dubbio che Panda Patch Management faciliti e acceleri questa attività sia per il team delle operazioni IT che per il team di sicurezza, che devono garantire l'applicazione sistematica di questa misura per ridurre la superficie di attacco.

Video: Panda Patch Management



Per maggiori informazioni su Panda Patch Management, [scarica il datasheet del prodotto](#).

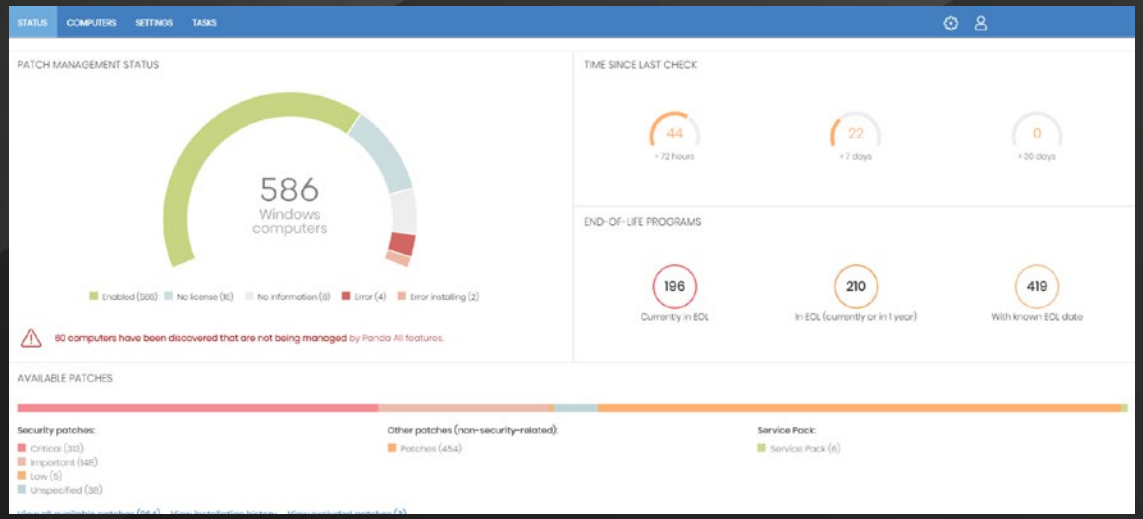
Panda Data Control

Infine, le **informazioni di identificazione personale (PII) o i dati sensibili che potrebbero attirare gli aggressori,** ad esempio informazioni finanziarie o riservate, presenti sugli endpoint degli utenti rappresentano un rischio latente per la sicurezza della tua organizzazione.

Panda Data Control aiuta le organizzazioni e l'amministratore dei dati a identificare queste informazioni in file non strutturati sugli endpoint in tutta l'organizzazione.

Questa valutazione rappresenta il primo passo nel programma di gestione del rischio di violazione dei dati. **La classificazione automatizzata** delle informazioni personali, la ricerca di informazioni sensibili sugli endpoint e **l'analisi dell'inventario e dell'evoluzione dei dati sono strumenti utili per ridurre questo rischio.**

Video: Panda Data Control



Per maggiori informazioni su Panda Data Control, scarica il datasheet del prodotto.

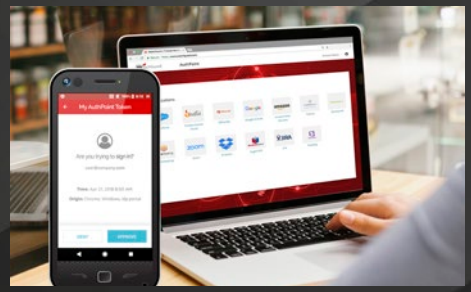
WatchGuard Unified Security Platform™

Sicurezza di rete

Le soluzioni per la sicurezza di rete di WatchGuard sono progettate da zero per offrire facilità di implementazione, uso e gestione, oltre a fornire la massima sicurezza possibile. Il nostro esclusivo approccio alla sicurezza di rete è incentrato sull'offerta di una sicurezza di livello enterprise e all'avanguardia a qualunque tipo di organizzazione, a prescindere dalle dimensioni o dalle competenze tecniche.

Wi-Fi sicuro

La soluzione Secure Wi-Fi di WatchGuard, rivoluzionaria per il mercato di oggi, è progettata per fornire sicurezza e protezione per gli ambienti Wi-Fi, eliminando al contempo le lungaggini amministrative e riducendo notevolmente i costi. Grazie all'ampia gamma di strumenti di coinvolgimento e alla visibilità dell'analisi aziendale, la soluzione offre il vantaggio competitivo di cui le aziende hanno bisogno per avere successo.



Autenticazione a più fattori

WatchGuard AuthPoint® è la soluzione giusta per gestire le lacune della sicurezza basata su password con l'autenticazione a più fattori tramite una piattaforma cloud facile da usare. L'approccio esclusivo di WatchGuard aggiunge il "DNA del cellulare" come fattore di identificazione, per garantire che solo le persone autorizzate possano accedere a reti sensibili e applicazioni cloud.

Sicurezza degli endpoint

WatchGuard Endpoint Security è un portafoglio di avanzate soluzioni native per il cloud ideato per la sicurezza degli endpoint e che protegge le aziende di qualsiasi tipo di attacco informatico attuale e futuro. Panda Adaptive Defense 360, la sua soluzione principale basata sull'intelligenza artificiale, migliora immediatamente la protezione delle organizzazioni. Combina funzionalità di protezione degli endpoint (EPP) e di rilevamento e risposta degli endpoint (EDR) con un'applicazione Zero Trust e servizi di ricerca delle minacce.

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella fornitura di servizi relativi a sicurezza di rete, sicurezza degli endpoint, Wi-Fi protetto, autenticazione a più fattori e intelligence di rete. I pluripremiati prodotti e servizi della nostra azienda hanno ottenuto la fiducia di oltre 18.000 rivenditori e fornitori di servizi che provvedono alla sicurezza di più di 250.000 clienti. WatchGuard persegue la missione di rendere la sicurezza accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, diventando in tal modo la soluzione ideale per le aziende del midmarket e distribuite. La sede centrale di WatchGuard si trova a Seattle (Washington, Stati Uniti); l'azienda dispone di uffici dislocati in Nord America, Europa, Asia e America Latina.

NUMERO VERDE ITALIA: **800.911.938** E-MAIL **italy@watchguard.com** SITO WEB **www.watchguard.it**

Cod. articolo WGCE67452_021721