

UNA PANORAMICA DELLE
SOLUZIONI



ENDPOINT SOLUTIONS

Il perfetto equilibrio dinamico tra tecnologia
multilivello, machine learning ed esperienza
umana rende ESET il partner n.1 per la sicurezza
degli endpoint nell'Unione Europea

CYBERSECURITY
EXPERTS ON YOUR SIDE



Cos'è una **Piattaforma di protezione endpoint?**

Una piattaforma di protezione endpoint (EPP) è una soluzione distribuita sui dispositivi endpoint per bloccare gli attacchi malware basati su file, rilevare attività pericolose e fornire funzionalità di analisi e risoluzione necessarie per rispondere agli incidenti e agli allarmi di sicurezza.

Le soluzioni di protezione endpoint di ESET utilizzano un approccio multilivello che impiega molteplici tecnologie in equilibrio dinamico per bilanciare costantemente le prestazioni, il rilevamento e i falsi positivi.

Perché scegliere le **soluzioni di Protezione Endpoint?**

RANSOMWARE

Il ransomware è una preoccupazione costante per le imprese di tutto il mondo sin dai tempi del Cryptolocker nel 2013. Nonostante il ransomware esista da molto più tempo, non è mai stato una delle minacce principali per le aziende. Tuttavia, oggi un singolo attacco di ransomware può facilmente compromettere l'operatività di un'azienda criptando file importanti o essenziali. Quando un'azienda subisce un attacco ransomware, si potrebbe rendere conto che i backup di cui dispone non sono abbastanza recenti, ed è tentata di pagare il riscatto.

Le soluzioni di protezione endpoint di ESET forniscono livelli di difesa non solo per bloccare preventivamente il ransomware, ma anche per rilevarlo nel caso fosse già presente nell'infrastruttura aziendale. È importante non solo prevenire ma anche rilevare il ransomware, poiché ogni volta che qualcuno paga il riscatto, incentiva i criminali a continuare a utilizzare questo tipo di attacco.

OBIETTIVI MIRATI E VIOLAZIONE DEI DATI

L'attuale panorama della sicurezza informatica è in costante evoluzione con nuovi metodi di attacco e minacce mai viste prima d'ora. Quando si verifica un attacco o una violazione di dati, le aziende sono in genere sorprese che le loro difese siano state compromesse o sono completamente inconsapevoli dell'avvenuto attacco. Dopo la scoperta della violazione le aziende implementano quindi delle soluzioni per impedire nuovi attacchi simili. Tuttavia, questo non li protegge da un attacco successivo che potrebbe utilizzare un diverso e nuovo vettore.

Le soluzioni di protezione endpoint di ESET utilizzano le informazioni della Threat Intelligence basate sulla propria esperienza a livello globale, in modo da dare priorità e bloccare efficacemente le minacce più recenti prima che vengano diffuse in altre reti. Inoltre, tutte le piattaforme di protezione degli endpoint dispongono di aggiornamenti basati su Cloud per rispondere rapidamente in caso di mancato rilevamento senza dover attendere un normale aggiornamento.

ATTACCHI FILELESS

Le minacce più recenti, chiamate malware fileless, vengono caricate esclusivamente nella memoria del computer, rendendo impossibile la rilevazione da parte delle protezioni basate sulla scansione dei file. Inoltre, alcuni attacchi fileless sfruttano le applicazioni attualmente installate e integrate nel sistema operativo per rendere ancora più difficile il rilevamento di un payload dannoso. Ad esempio, in questi attacchi è molto comune l'uso di PowerShell.

Le piattaforme di protezione endpoint ESET dispongono di strumenti per rilevare le applicazioni corrotte e per offrire protezione dagli attacchi fileless. ESET ha anche creato scanner dedicati al controllo costante della memoria che identificano tutto ciò che è sospetto. Utilizzando questo approccio multilivello, ci assicuriamo di essere sempre un passo avanti rispetto ai malware più recenti.



Le soluzioni di protezione endpoint di ESET forniscono livelli di difesa non solo per bloccare preventivamente il ransomware, ma anche per rilevarlo nel caso fosse già presente nell'infrastruttura aziendale.

Quando si verifica un attacco o una violazione di dati, le aziende sono in genere sorprese che le loro difese siano state compromesse o sono completamente inconsapevoli dell'avvenuto attacco.

Le minacce più recenti, chiamate malware fileless, vengono caricate esclusivamente nella memoria del computer, rendendo impossibile la rilevazione da parte delle protezioni basate sulla scansione dei file.

"ESET è da anni la nostra soluzione di sicurezza e si è sempre rivelata affidabile. Sa quello che deve fare; non ti devi preoccupare. In breve, ESET sta per: affidabilità, qualità e servizio.

-Jos Savelkoul, Team Leader ICT-Department; Ospedale Zuyderland, Paesi Bassi;
oltre 10.000+ postazioni



Le soluzioni di protezione Endpoint di ESET

ESET Endpoint Security per Windows/Mac/Android

ESET Endpoint Antivirus per Windows/Mac/Linux

ESET File Security per Windows Server/Linux/Azure

ESET Mobile Device Management per Android e Apple iOS

ESET fa la differenza

PROTEZIONE MULTILIVELLO

ESET combina tecnologia multilivello, machine learning ed esperienza umana per fornire ai propri clienti il miglior livello di protezione possibile. La nostra tecnologia viene costantemente migliorata per ottenere soluzioni in cui il rapporto tra rilevazione, falsi positivi e prestazioni sia perfettamente bilanciato.

SUPPORTO MULTI-PIATTAFORMA

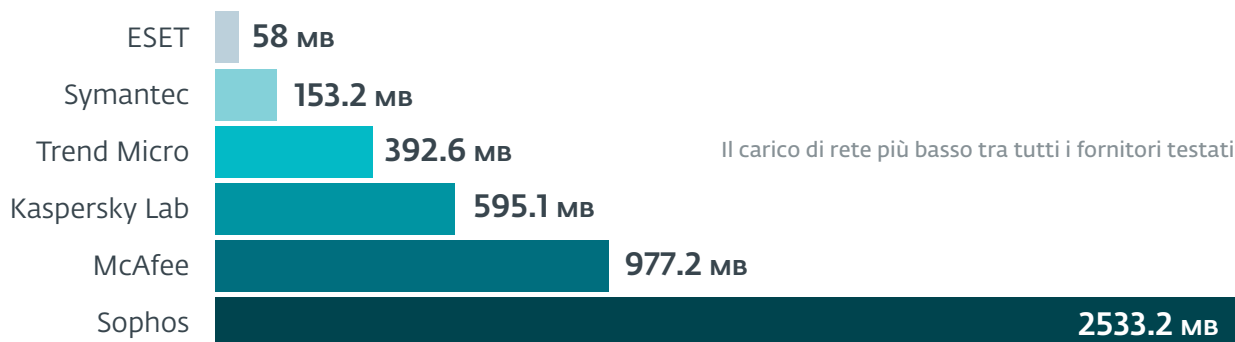
Le soluzioni di protezione per endpoint di ESET supportano tutti i sistemi operativi inclusi Windows, Mac, Linux e Android. Tutti i prodotti possono essere completamente gestiti da un'unica console che integra anche il Mobile Device Management per iOS e Android.

PERFORMANCE ASSOLUTE

La principale preoccupazione delle aziende è l'impatto che la soluzione di protezione degli endpoint può avere sulle prestazioni del sistema. I prodotti ESET continuano a eccellere in termini di performance vincendo i test di organizzazioni indipendenti che dimostrano il basso impatto dei nostri prodotti sui sistemi.

PRESENZA NEL TUTTO IL MONDO

ESET ha uffici in 22 paesi nel mondo, laboratori di ricerca e sviluppo in 13 ed è presente in oltre 200 paesi e territori. Questo ci permette di avere i dati per bloccare i malware prima che si diffondano in tutto il mondo ma anche di dare priorità alle nuove tecnologie basate sulle minacce più recenti o sui possibili nuovi vettori di infezione.



Fonte: AV-Comparatives: Network Performance Test, Business Security Software

"La migliore testimonianza? Le statistiche del nostro helpdesk: da quando ci siamo affidati a ESET, i nostri ragazzi del supporto non registrano alcuna chiamata, non devono occuparsi di problemi relativi all'antivirus o ai malware!"

- Adam Hoffman, IT Infrastructure Manager; Mercury Engineering, Irlanda;
1.300 postazioni

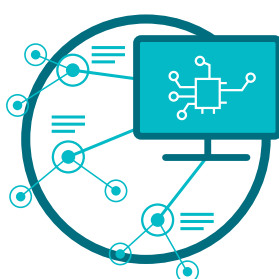
La tecnologia

I nostri prodotti e le nostre tecnologie poggiano su 3 pilastri



ESET LIVEGRID®

Quando una minaccia zero-day come un ransomware viene intercettata, il file viene inviato al nostro sistema di protezione malware su Cloud – ESET LiveGrid®- dove viene eseguito per controllarne il comportamento. I risultati vengono condivisi in tempo reale con tutti gli endpoint a livello globale senza dover attendere alcun aggiornamento.



MACHINE LEARNING

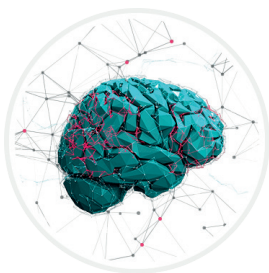
Usa il potere combinato di reti neurali e di algoritmi scelti con cura per stabilire se un campione è da considerarsi innocuo, potenzialmente indesiderato o pericoloso.



ESPERIENZA UMANA

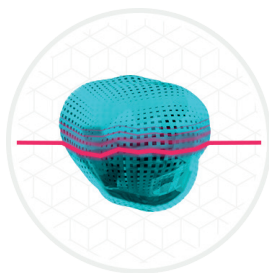
I ricercatori ESET di livello mondiale nel campo della sicurezza condividono il know-how e l'intelligenza dell'élite per garantire che i nostri utenti possano beneficiare di un'intelligence ottimale sulle minacce, 24 ore su 24.

Un unico livello di protezione non è sufficiente contro le attuali minacce in costante evoluzione. Tutti i prodotti ESET per Endpoint sono in grado di rilevare i malware prima, durante e addirittura dopo la loro esecuzione. Non concentrandosi solo su una parte specifica del ciclo di vita del malware, ESET è in grado di fornire il massimo livello di protezione possibile.



MACHINE LEARNING

Tutti i prodotti ESET Endpoint attualmente impiegano il machine learning combinato insieme a tutti i nostri altri livelli di protezione e lo fanno sin dal 1997. In particolare, il machine learning viene utilizzato sfruttando tecnologie consolidate e una vasta rete neurale. Per un'ispezione approfondita della rete, gli amministratori possono attivare una speciale modalità di machine learning aggressivo che funziona anche senza connessione internet.



SCANNER AVANZATO DI MEMORIA

ESET Advanced Memory Scanner controlla il comportamento di un processo dannoso e lo analizza una volta presente in memoria. Il malware fileless agisce senza la necessità di componenti persistenti nel file system che possono essere rilevati in modo convenzionale. Solo la scansione della memoria può scoprire e bloccare con successo tali attacchi dannosi.



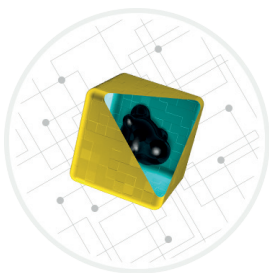
RANSOMWARE SHIELD

Eset Ransomware Shield offre un livello di protezione aggiuntivo per difendere gli utenti dai ransomware. La nostra tecnologia controlla e valuta tutte le applicazioni eseguite in base al loro comportamento e alla loro reputazione. È stato progettato per rilevare e bloccare i processi che si comportano come un ransomware.



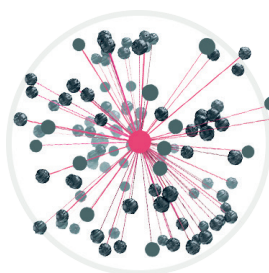
EXPLOIT BLOCKER

ESET Exploit Blocker controlla le applicazioni solitamente vulnerabili agli exploit (browser, lettori di documenti, programmi di posta, Flash, Java e altri ancora) e invece di occuparsi solo di specifici identificatori CVE, si concentra sulle tecniche exploit. Una volta attivato, sulla macchina viene bloccata immediatamente la minaccia.



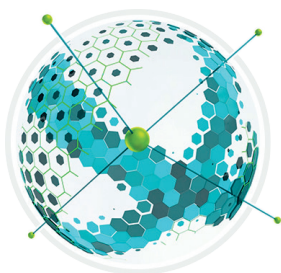
SANDBOX NEL PRODOTTO

Gli attuali malware spesso utilizzano tecniche di offuscamento nel tentativo di eludere la rilevazione. Per identificare il reale comportamento di un malware offuscato utilizziamo un sistema di sandbox in-product. Grazie a questa tecnologia, le soluzioni ESET imitano diverse componenti hardware e software di un computer per eseguire un campione sospetto in un ambiente virtualizzato e assolutamente isolato.



BOTNET PROTECTION

ESET Botnet Protection rileva le comunicazioni pericolose usate dalle botnet, e allo stesso tempo ne identifica i processi malevoli. Qualsiasi comunicazione dannosa rilevata viene bloccata e segnalata all'utente.



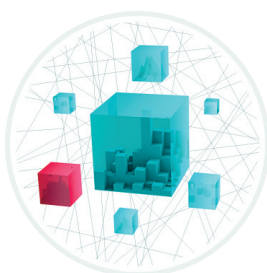
PROTEZIONE DA ATTACCHI DI RETE

Questa tecnologia migliora il rilevamento delle vulnerabilità note a livello di rete. Costituisce un altro importante livello di protezione contro la diffusione di malware, attacchi di rete e sfruttamento di vulnerabilità, per le quali non sia ancora stata rilasciata o installata una patch.



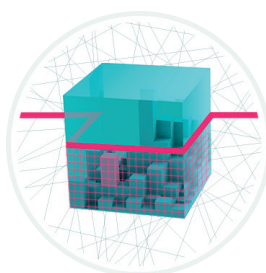
SECURE BROWSER

Progettato per proteggere le risorse aziendali attraverso uno speciale livello di protezione incentrato sul browser, e per essere lo strumento principale per accedere ai dati critici all'interno del perimetro dell'intranet e nel cloud. Secure Browser fornisce una maggiore protezione della memoria per il funzionamento del browser, associato alla protezione della tastiera, e consente agli amministratori di aggiungere URL da proteggere.



HIPS

Il Sistema di Prevenzione dalle Intrusioni basato su Host di ESET (HIPS) controlla le attività di sistema e utilizza un insieme di regole predefinite per riconoscere e bloccare comportamenti sospetti. Inoltre, il meccanismo di autoprotezione HIPS impedisce al processo incriminato di svolgere attività dannose.

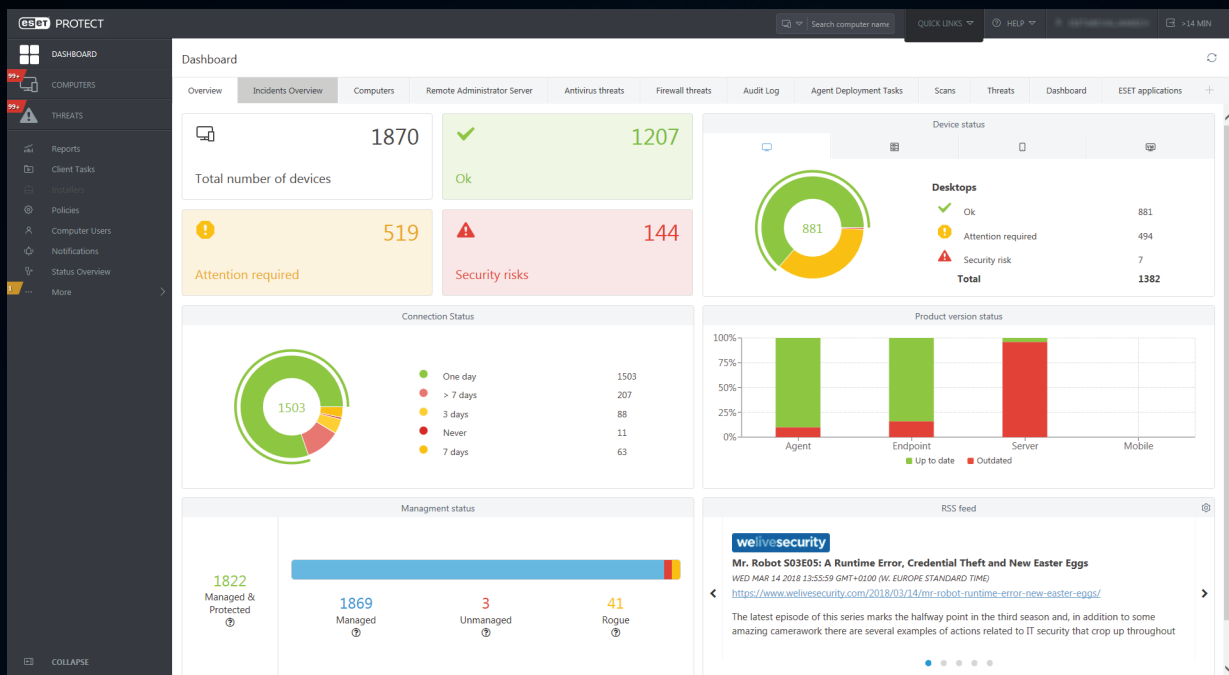


UEFI SCANNER

ESET è il primo produttore di sicurezza per endpoint ad aggiungere nella sua soluzione un livello di protezione dedicato all'Unified Extensible Firmware Interface (UEFI). ESET UEFI Scanner verifica e aumenta la sicurezza degli ambienti di preboot ed è progettato per controllare l'integrità del firmware. In caso di modifiche queste verranno notificate all'utente.

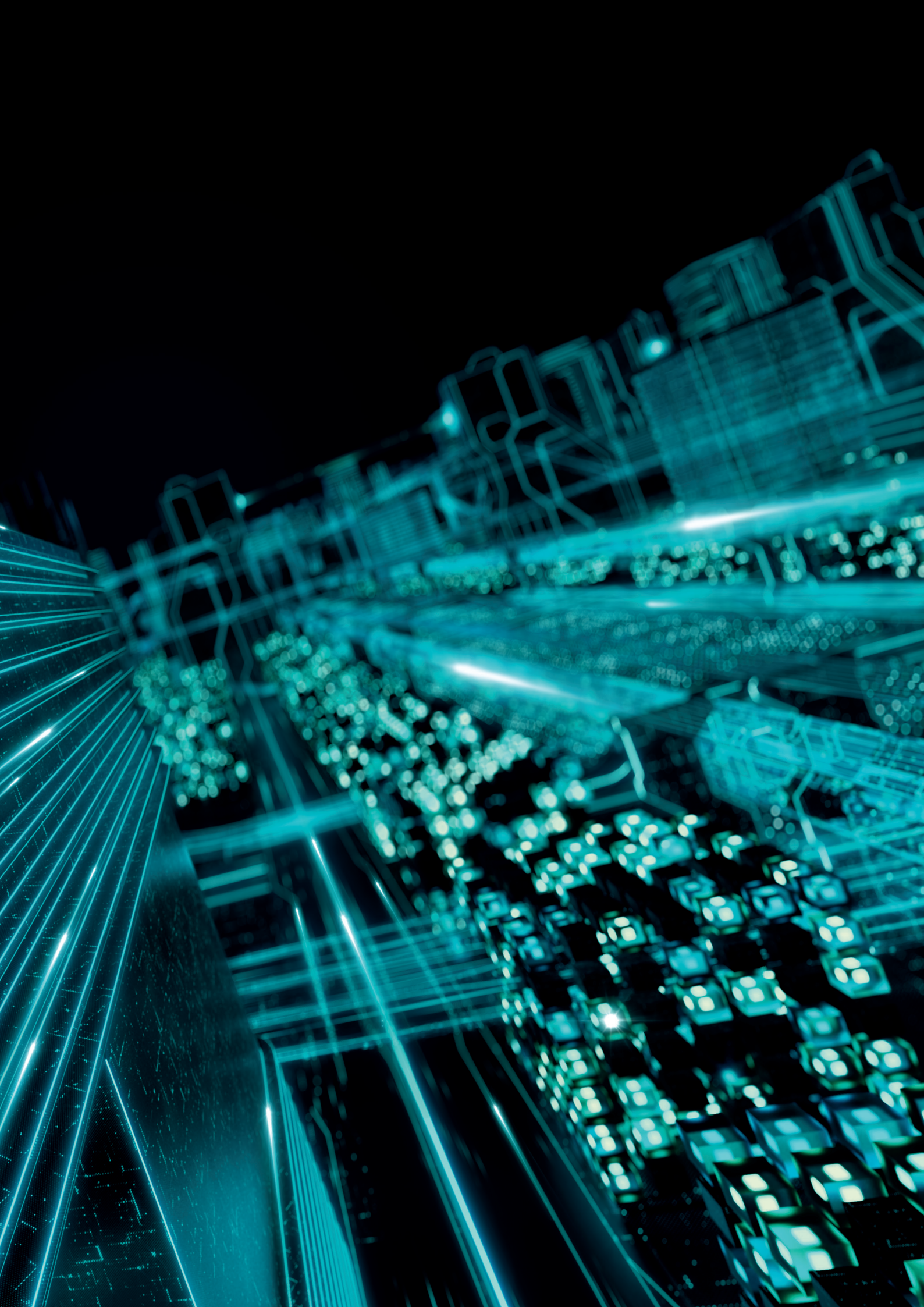
"Ciò che spicca maggiormente è il suo decisivo vantaggio tecnico rispetto ad altri prodotti sul mercato. ESET offre una sicurezza affidabile, il che significa che possiamo lavorare su qualsiasi progetto in qualsiasi momento, sapendo che i nostri computer sono protetti al 100%."

- Fiona Garland, Business Analyst Group IT; Mercury Engineering, Irlanda;
1.300 postazioni



PROTEZIONE ESET

Tutte le soluzioni endpoint ESET sono gestite da una console cloud disposta su un'unica, singola schermata, ESET PROTECT, che fornisce una panoramica completa della rete.



Casi pratici

Ransomware

Alcune aziende richiedono assicurazioni aggiuntive sulla protezione dagli attacchi ransomware.

SOLUZIONE

- ✓ Network Attack Protection ha la capacità di impedire ai ransomware di infettare un sistema bloccando gli exploit a livello di rete.
- ✓ La nostra difesa multilivello vanta una sandbox in-product che ha la capacità di rilevare i malware che usano tecniche di offuscamento.
- ✓ Il sistema di protezione dai malware in Cloud di ESET protegge automaticamente dalle nuove minacce senza dover attendere il nuovo aggiornamento delle firme antivirali.
- ✓ Tutti i prodotti includono il Ransomware Shield per garantire alle aziende protezione da file dannosi crittografati.

Malware fileless

I malware fileless sono minacce relativamente nuove e, risiedendo solamente nella memoria, richiedono un approccio differente rispetto ai tradizionali malware basati su file.

SOLUZIONE

- ✓ La tecnologia esclusiva di ESET, Advance Memory Scanner, protegge i sistemi da questo tipo di minacce monitorando il comportamento dei processi maligni e analizzandoli una volta presenti in memoria.
- ✓ Riduce i tempi di raccolta e analisi dei dati caricando la minaccia in ESET Threat Intelligence per ottenere informazioni su come agisce la minaccia.
- ✓ La tecnologia multilivello, il machine learning e l'esperienza umana garantiscono ai nostri clienti la miglior protezione possibile.

Minacce "Zero-day"

Le minacce zero-day sono una delle maggiori preoccupazioni per le aziende che non sanno come proteggersi da qualcosa che non hanno mai visto prima.

SOLUZIONE

- ✓ I prodotti ESET per endpoint sfruttano l'euristica e il machine learning come parte dell'approccio multilivello per prevenire e proteggere i sistemi dai nuovi malware appena diffusi in rete.
- ✓ I nostri 13 centri globali di Ricerca e Sviluppo ci consentono di rispondere rapidamente ai malware non appena iniziano a diffondersi nel mondo.
- ✓ Grazie al sistema di protezione dai malware in Cloud di ESET le macchine sono protette automaticamente dalle nuove minacce senza dover attendere il successivo aggiornamento delle firme antivirali.

"Quando abbiamo trovato ESET, ci siamo accorti subito che era la scelta giusta: tecnologia affidabile, ottima rilevazione, presenza locale e un'eccellente supporto tecnico, in poche parole tutto quello di cui avevamo bisogno."

— Ernesto Bonhoure, IT Infrastructure Manager;
Ospedale Alemán, Argentina,
1.500+ postazioni

Informazioni su ESET

Per oltre 30 anni, ESET® ha sviluppato software e servizi di sicurezza IT tra i migliori del settore, offrendo soluzioni di protezione immediate e complete contro le minacce di cybersecurity per aziende e consumatori di tutto il mondo.

ESET è un'azienda privata senza debiti e senza prestiti, per questo motivo abbiamo la libertà di fare ciò che deve essere fatto per la massima protezione di tutti i nostri clienti.

ESET IN NUMERI

110m+
utenti in
tutto il mondo

400k+
clienti
aziendali

**Oltre
200**
paesi e
territori

13
centri R&D
globali

ALCUNI DEI NOSTRI CLIENTI



Drive your Ambition

protetti da ESET dal 2017
più di 14.000 endpoint

Canon

Canon Marketing Japan Group

protetti da ESET dal 2016
più di 9.000 endpoint

Allianz 
Suisse

protetti da ESET dal 2016
più di 4.000 mailbox



Partner di sicurezza ISP dal 2008
2 milioni di customer base



ESET è conforme alla norma [ISO/IEC 27001:2013](#), uno standard di sicurezza internazionalmente riconosciuto e applicabile nell'implementazione e nella gestione dell'information security. La certificazione viene concessa dall'organismo di certificazione accreditato e indipendente [SGS](#) e dimostra la piena conformità di ESET alle best practice del settore.

MITRE

ATT&CK™

ESET è un importante collaboratore di MITRE ATT&CK. Essendo uno dei collaboratori più referenziati e attivi, ESET conferma il suo impegno a fornire la migliore protezione alla comunità e ai propri clienti.

RICONOSCIMENTI OTTENUTI



ANALYST RECOGNITION

Gartner

ESET è stato nominato unico Challenger nel Magic Quadrant 2018 di Gartner per Endpoint Protection Platforms, per il secondo anno consecutivo.

FORRESTER®

ESET è stato nominato Strong Performer nel The Forrester Wave(TM): Endpoint Security Suites, Q3 2019.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET è stato nominato "Top Player" nel 2019 Radicati Endpoint Security report per i due importanti criteri: funzionalità e visione strategica.

Gartner Inc, Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Lawrence Pingree, Dionisio Zumerle, Prateek Bhajanka, Paul Webber, 20 agosto 2019. Gartner non sostiene alcun fornitore, prodotto o servizio citato nelle sue pubblicazioni di ricerca. Le pubblicazioni di ricerca di Gartner sono costituite dalle opinioni dell'organizzazione di ricerca di Gartner e non devono essere interpretate come dati di fatto. Gartner declina ogni garanzia, espressa o implicita, in relazione alla presente ricerca, incluse eventuali garanzie di commerciabilità o di idoneità per un particolare scopo.

Gartner Peer Insights è una piattaforma gratuita di peer review e valutazione progettata per i responsabili delle decisioni in materia di software e servizi aziendali. Le valutazioni passano attraverso un rigoroso processo di verifica e di controllo per garantire l'autenticità delle informazioni. Le valutazioni Gartner Peer Insights costituiscono le opinioni soggettive dei singoli utenti finali sulla base delle loro esperienze e non rappresentano il punto di vista di Gartner o dei suoi affiliati.

