UNA PANORAMICA DELLE SOLUZIONI

DYNAMIC THREAT DEFENSE

Blocca le minacce zero-day grazie a una potente sandbox basata su Cloud

CYBERSECURITY
EXPERTS ON YOUR SIDE

Che cos'è una **security sandbox basata su Cloud?**

Una security sandbox basata su cloud è un ambiente di test isolato in cui un programma sospetto viene eseguito e in modo del tutto automatizzato ne osserva, annota e poi analizza il comportamento.

ESET Dynamic Threat Defense garantisce un ulteriore livello di sicurezza per i prodotti ESET, come la Mail Security e le soluzioni per gli Endpoint, utilizzando una tecnologia sandbox basata sul Cloud. In questo modo è possibile individuare nuove tipologie di minacce e quelle non ancora identificate. Questa sandbox è costituita da diversi tipi di sensori che si aggiungono all'analisi statistica del codice, a un'ispezione dettagliata del campione attraverso il machine learning, alla verifica della memoria e alla rilevazione basata sul comportamento.

Perché una **Security Sandbox basata su Cloud ?**

RANSOMWARE

Il Ransomware continua a rappresentare una delle principali minacce per le organizzazioni di tutto il mondo sin dai tempi di Cryptolocker nel 2013. Nonostante il Ransomware esista da molto più tempo, non è mai stato considerato un vero pericolo 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 rende immediatamente conto che i backup di cui dispone non sono abbastanza recenti, e si sente quasi obbligata a pagare il riscatto.

Una security sandbox basata su cloud fornisce un ulteriore livello di difesa al di fuori della rete aziendale per evitare che il ransomware venga eseguito in un ambiente di produzione.

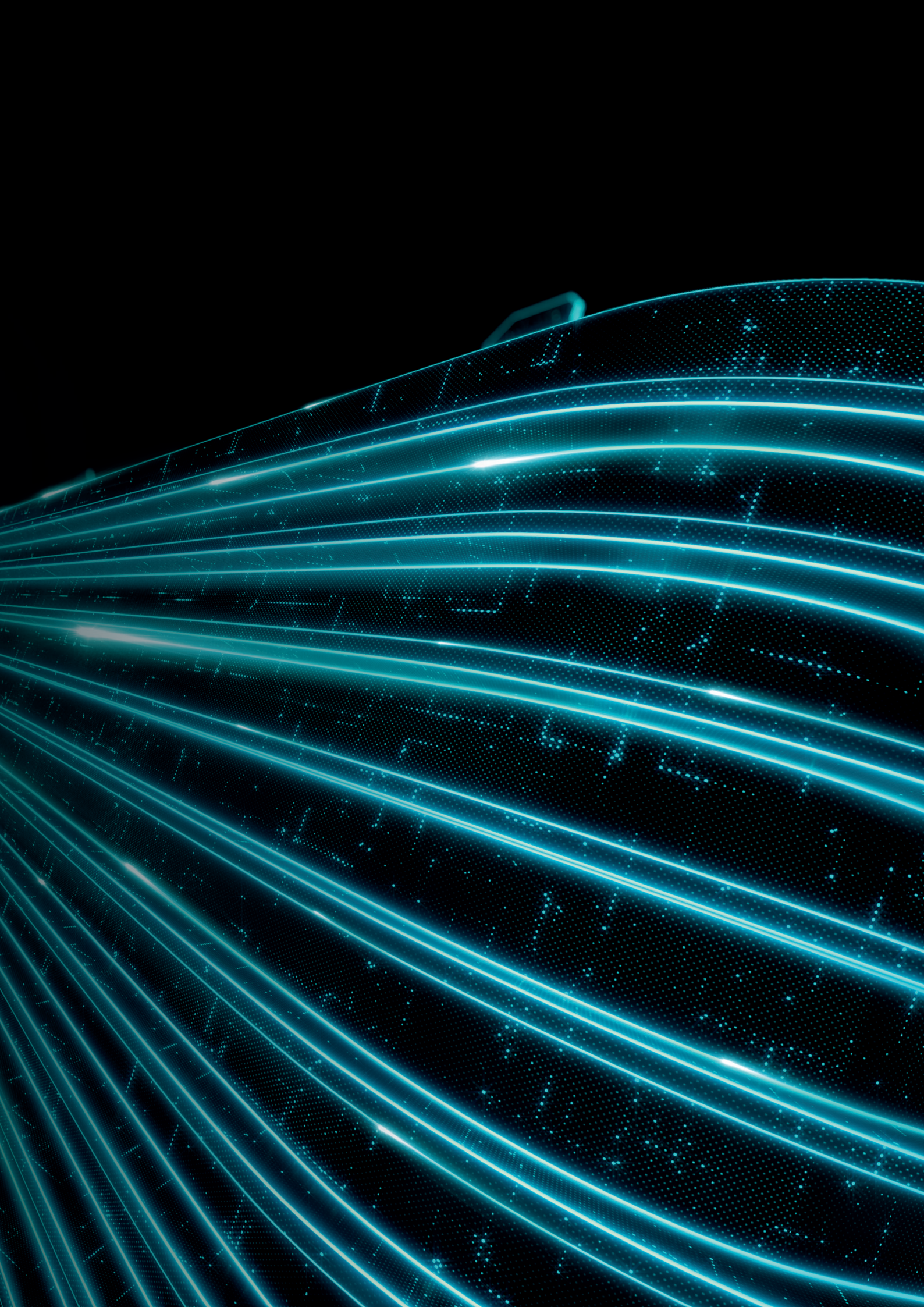
ATTACCHI MIRATI E VIOLAZIONI DI DATI

L'attuale panorama della sicurezza informatica è in costante evoluzione con nuovi metodi di attacco e minacce mai viste prima. 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. Una volta scoperto, le aziende mettono prontamente in atto delle misure di protezione per evitare che si ripeta. Tuttavia, questo non li protegge da un attacco successivo che potrebbe utilizzare un diverso e nuovo vettore.

L'approccio di una security sandbox basata su cloud è molto più efficace rispetto a una semplice osservazione della potenziale minaccia, perché va oltre la semplice apparenza e ne analizza anche il comportamento. Questo permette di essere molto più decisivi nel determinare se si tratta di un attacco mirato, una minaccia persistente o di nulla di pericoloso.

Una security sandbox basata su cloud fornisce un ulteriore livello di protezione al di fuori della rete aziendale.

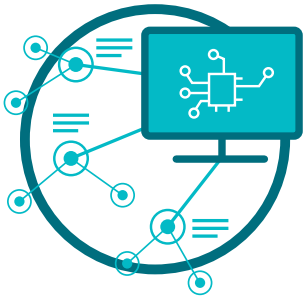
Una security sandbox basata su cloud va oltre la semplice apparenza e analizza il comportamento della potenziale minaccia.



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 innoquo, potenzialmente indesiderato o pericoloso.

ESPERIENZA UMANA

I migliori ricercatori di sicurezza informatica di tutto il mondo condividono il proprio know-how e le proprie analisi per garantire la condivisione di minacce note 24 ore su 24.

ESET fa la differenza

PROTEZIONE MULTILIVELLO

Grazie a ESET Dynamic Threat Defenses, ESET utilizza 3 differenti modelli di machine learning per l'analisi dei file. Dopo questo processo, viene eseguito un campione attraverso una sandbox che simula il comportamento degli utenti al fine di ingannare le tecniche anti-elusione. Successivamente, viene utilizzata una rete neurale di deep learning per confrontare il comportamento visto rispetto a dati comportamentali storici. Infine, ma non meno importante, viene utilizzata l'ultima versione del motore di scansione ESET per analizzare ogni singola componente alla ricerca di qualcosa di sospetto.

VISIBILITÀ COMPLETA

Per ogni campione analizzato, è possibile visualizzare il verdetto finale in ESET Security Management Center o in ESET Cloud Administrator. Inoltre i clienti con una licenza con più di 100 postazioni ricevono un rapporto comportamentale completo con informazioni dettagliate sui campioni e sul loro comportamento osservato durante l'analisi nella sandbox .Tutte le informazioni vengono mostrate in maniera chiara e comprensibile. Non ci limitiamo ad mostrare i campioni inviati a ESET Dynamic Threat Defense, ma anche tutto ciò che viene inviato a ESET's Cloud Malware Protection System – ESET LiveGrid®.

MOBILITÀ

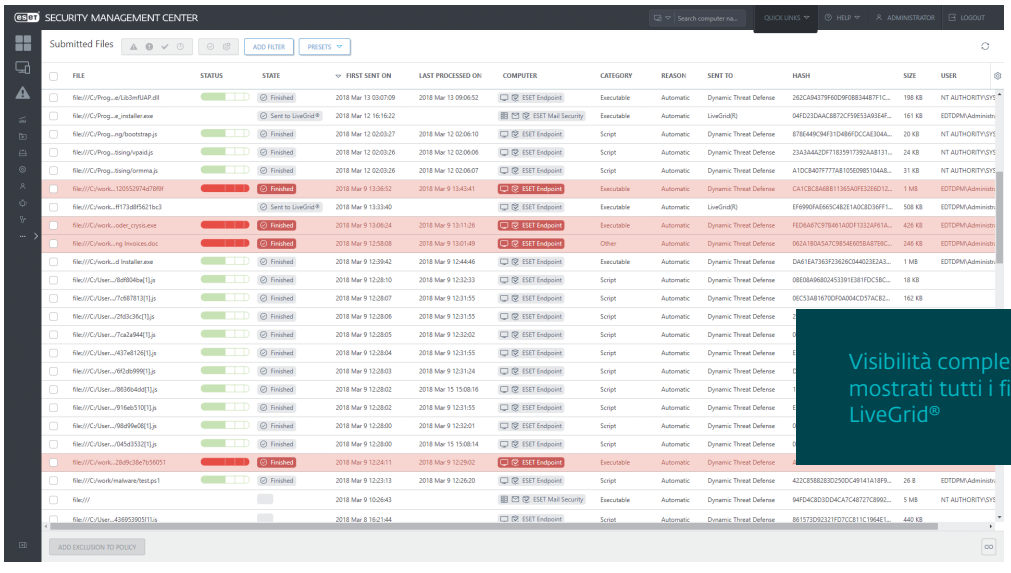
Al giorno d'oggi i dipendenti sono costantemente in viaggio e non si trovano sempre in sede. Per questo motivo ESET Dynamic Threat Defense è in grado di analizzare i file indipendentemente da dove si trovino gli utenti. La cosa più interessante è che se vengono individuate delle minacce, l'intera azienda viene immediatamente protetta.

VELOCITÀ SENZA PARI

Ogni singolo minuto è importante. Per questo motivo, ESET Dynamic Threat Defense è progettato per analizzare la maggior parte dei campioni in meno di 5 minuti. Se i campioni erano già stati analizzati in precedenza, avrà bisogno di pochi secondi per garantire protezione a tutti i dispositivi della vostra azienda.

COLLAUDATO E AFFIDABILE

ESET opera nel settore della sicurezza da oltre 30 anni e continuiamo ad evolvere la nostra tecnologia per essere sempre un passo avanti rispetto alle nuove minacce. Questo ci ha permesso di ottenere la fiducia di oltre 110 milioni di utenti in tutto il mondo. La nostra tecnologia è costantemente esaminata e provata da test di organizzazioni indipendenti che dimostrano quanto sia efficace il nostro approccio per fermare le minacce più recenti.



Visibilità completa - vengono mostrati tutti i file inviati a ESET LiveGrid®

Casi pratici

Ransomware

CASI PRATICI

Il Ransomware si diffonde solitamente nelle caselle di posta elettronica di utenti ignari .

SOLUZIONE

- ✓ ESET Mail Security invia automaticamente gli allegati delle email sospette a ESET Dynamic Threat Defense.
- ✓ ESET Dynamic Threat Defense analizza il campione, quindi invia i risultati a Mail Security soloitamente entro 5 minuti.
- ✓ ESET Mail Security rileva e filtra automaticamente gli allegati che contengono contenuti dannosi.
- ✓ L'allegato dannoso non raggiunge mai il destinatario.

Protezione granulare per i diversi ruoli aziendali

CASI PRATICI

Ogni ruolo in azienda richiede diversi livelli di protezione. Gli sviluppatori o il personale IT necessitano di restrizioni di sicurezza diverse rispetto al responsabile dell'ufficio o al CEO.

SOLUZIONE

- ✓ Configurare un criterio univoco per computer o per server in ESET Dynamic Threat Defense.
- ✓ Applicare automaticamente un criterio differente basato su un diverso gruppo di utenti statici o gruppo di Active Directory.
- ✓ Cambiare automaticamente le impostazioni di configurazione semplicemente spostando un utente da un gruppo a un altro.

File sconosciuti o sospetti

FILE BEHAVIOR REPORT

STATUS	Malicious
SHA-1	FED6A67C97B461A0DF1332AF61A89EA9FB5A540F
SIZE	436736B
CATEGORY	Executable

Detected Behaviors

BEHAVIOR	Malware detected after execution
EXPLANATION	Sample has been detected as malicious after execution
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware detected with ESET scanning engine after execution
BEHAVIOR	New files created in the Windows folder
EXPLANATION	Sample has created new files in the Windows folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Analyzed sample copied
EXPLANATION	Sample has been copied to a different location
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware tried to hide its presence
BEHAVIOR	Startup list modified
EXPLANATION	Sample has added a new entry to the Windows Startup application list
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Malware wants to run after a system reboot
BEHAVIOR	Machine Learning detection
EXPLANATION	Sample behaves very similarly to known malware
BENIGN CAUSES	Clean applications should not do this
MALICIOUS CAUSES	Malware has been detected by Neural network Machine Learning
BEHAVIOR	New files in Program Files folder created
EXPLANATION	Sample has created new files in the Windows Program Files folder
BENIGN CAUSES	This is standard behavior for some installers
MALICIOUS CAUSES	Sample may be a Potentially Unwanted Application

DYNAMIC THREAT DEFENSE

CASI PRATICI

A volte i dipendenti o il personale IT potrebbero ricevere un file che vogliono sottoporre a una doppia verifica.

SOLUZIONE

- ✓ Ogni utente può inviare un campione da analizzare direttamente da tutti i prodotti ESET.
- ✓ Il campione viene rapidamente analizzato da ESET Dynamic Threat Defense.
- ✓ Se un file è ritenuto dannoso, tutti i computer dell'azienda sono protetti.
- ✓ L'amministratore IT ha piena visibilità sull'utente che ha inviato il campione e sull'esito, negativo o positivo, dell'analisi.

ESET Dynamic Threat Defense Caratteristiche tecniche

PROTEZIONE AUTOMATICA

Una volta che tutto è impostato, non è necessaria alcuna azione da parte dell'amministratore o dell'utente. Il prodotto di sicurezza endpoint o server decide automaticamente se un campione è legittimo, pericoloso o sconosciuto. Se il campione è sconosciuto, viene inviato a ESET Dynamic Threat Defense per l'analisi. Al termine dell'analisi, il risultato viene condiviso e i prodotti ESET rispondono di conseguenza.

CONFIGURATO SU MISURA

ESET Dynamic Threat Defense consente di configurare dei criteri dettagliati anche per singolo computer in modo che l'amministratore possa controllare cosa viene inviato e cosa dovrebbe accadere in base al risultato ricevuto.

INVIO MANUALE

In qualsiasi momento un utente o l'amministratore possono inviare dei campioni da analizzare attraverso un prodotto ESET compatibile e ricevere i risultati completi. Gli amministratori vedranno chi ha inviato cosa e i relativi risultati direttamente nell' ESET Security Management Center.

PROTEZIONE MAIL SECURITY

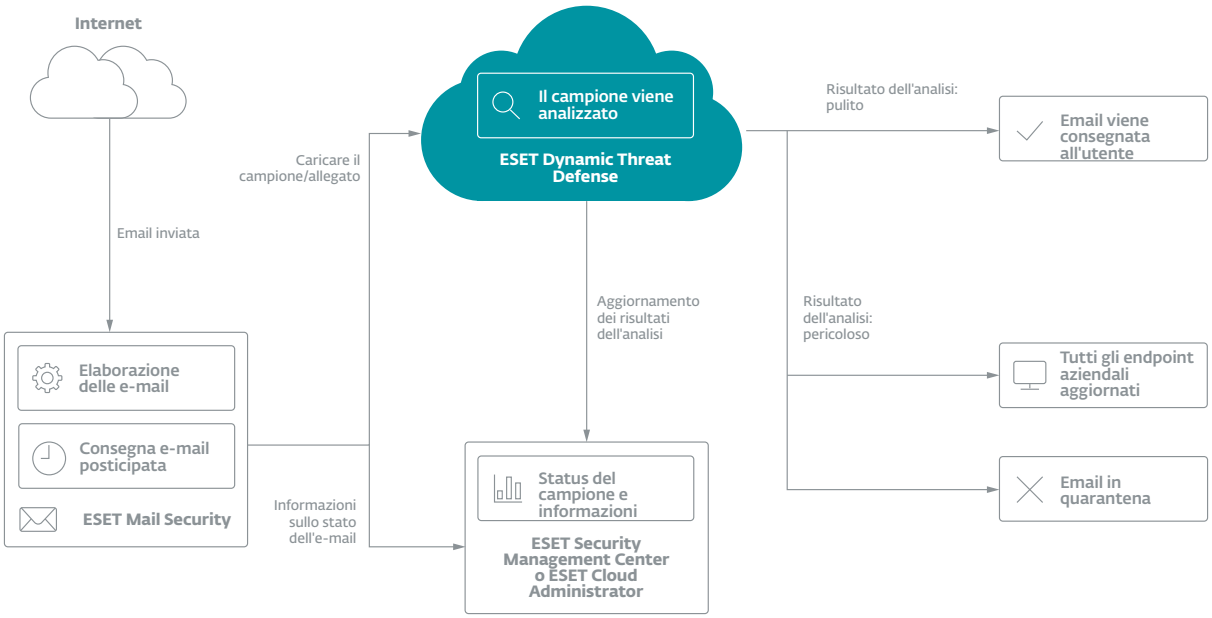
ESET Dynamic Threat Defense non solo funziona con i file, ma si integra anche con ESET Mail Security, per garantire che le e-mail pericolose non vengano consegnate all'interno dell'azienda. Per garantire la continuità produttiva, possono essere inviate per l'analisi a ESET Dynamic Threat Defense solo le e-mail provenienti dall'esterno dell'azienda.

"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

Come funziona **ESET Dynamic Threat Defense**

Con ESET Mail Security



"La nostra esperienza con ESET è stata più che soddisfacente, tanto che abbiamo rinnovato le nostre licenze per altri tre anni. Quindi, senza alcun dubbio, raccomandiamo le soluzioni ESET a tutte le aziende che vogliono aumentare i loro livelli di sicurezza"

— Ernesto Bonhoure, IT Infrastructure Manager;
Hospital 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

MITSUBISHI MOTORS
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.

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

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

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

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.

CYBERSECURITY
EXPERTS ON YOUR SIDE