



PANORAMICA

VULNERABILITY & PATCH MANAGEMENT

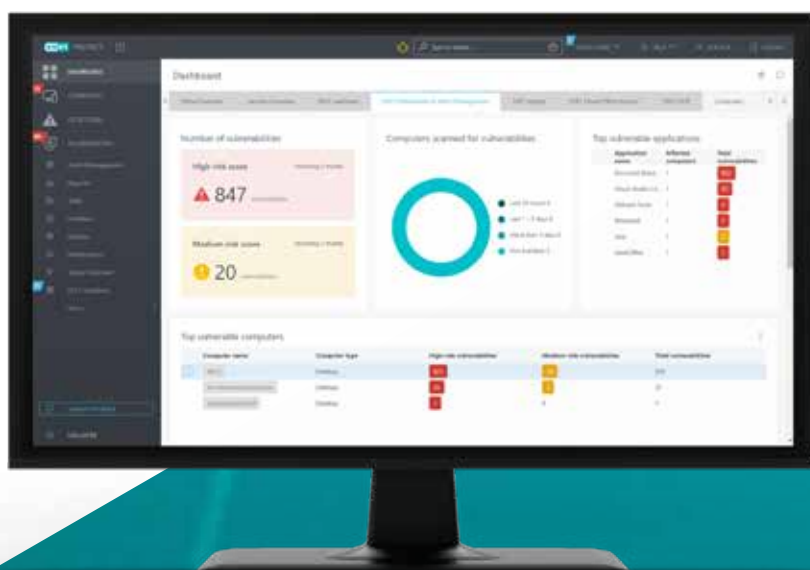
Traccia e risolve attivamente le
vulnerabilità su tutti gli endpoint.

Progress. Protected.

Che cos'è l'ESET Vulnerability and Patch Management?

ESET Vulnerability & Patch Management tiene attivamente traccia delle vulnerabilità nei sistemi operativi e nelle applicazioni più comuni e consente di eseguire patch automatiche su tutti gli endpoint gestiti attraverso la nostra piattaforma unificata.

La scansione automatica del software degli endpoint e delle applicazioni di terze parti, con segnalazione immediata alla console, fornisce una visibilità immediata delle vulnerabilità. Per garantire una protezione continua all'azienda, è possibile configurare l'auto-patching selezionando una strategia di patch (tutte, solo quelle consentite o applicare specifiche esclusioni) e definendo determinate fasce orarie per l'esecuzione delle patch.



Patching tempestivo di sistemi operativi e applicazioni

La correzione delle falle di sicurezza nei sistemi operativi e nelle applicazioni è fondamentale ma resta una delle attività più dispendiose in ambito IT. ESET Vulnerability & Patch Management offre un ulteriore livello di sicurezza alle organizzazioni che necessitano di applicazioni aggiornate, ma che non dispongono di risorse IT. Rileva le vulnerabilità ed elimina o riduce le possibilità di violazione installando le patch più recenti per le applicazioni e i sistemi operativi su tutti gli endpoint.

ESET Vulnerability & Patch Management utilizza tecniche avanzate di definizione delle priorità e

strumenti per l'automazione dei flussi di lavoro in grado di soddisfare al meglio le vostre esigenze infrastrutturali.

È incluso nella piattaforma ESET PROTECT e, come tale, non solo offre una valutazione continua delle vulnerabilità con classificazione e rimedio basati sul rischio, ma protegge anche dalle minacce che vanno ben oltre le vulnerabilità del software. Offre una protezione di livello enterprise contro tutti i tipi di malware, compresi i ransomware, e la prevenzione delle minacce zero-day su tutti gli endpoint, i server e le e-mail, il tutto attraverso un'unica soluzione.

Caratteristiche principali

Valutazione della vulnerabilità

- Esegue la scansione di migliaia di applicazioni, come Adobe Acrobat, Mozilla Firefox e Zoom Client, e supporta diverse versioni di Windows, Linux e macOS
- Rileva oltre 35.000 vulnerabilità e esposizioni comuni (CVE), a cui vengono aggiunte di nuove man mano che vengono individuate
- Scansioni automatiche con possibilità di impostare pianificazione personalizzabili
- Classifica e filtra le vulnerabilità in base al punteggio di esposizione e alla gravità
- Rapporti sulla vulnerabilità dei software e dei dispositivi più vulnerabili
- Supporta la multitenancy in ambienti di rete complessi; consente la visibilità delle vulnerabilità in parti specifiche dell'organizzazione
- Vista unificata tramite la console ESET PROTECT con supporto multilingue e requisiti di sistema minimi per l'infrastruttura IT

Gestione delle patch

- Avvio immediato di aggiornamenti e patch manualmente o tramite opzioni personalizzabili
- Semplificazione del processo di patching: assegnazione delle priorità per le risorse critiche e possibilità di programmazione delle rimanenti per le ore con minor traffico, per evitare interruzioni.
- Possibilità di registrare e tenere traccia delle eccezioni per le patch delle applicazioni selezionate.
- Inventario aggiornato delle patch con il nome della patch, la nuova versione dell'applicazione, CVE, gravità/importanza della patch, applicazioni interessate.
- Tutte le patch sono disponibili tramite la console di ESET PROTECT

Come funziona?



Casi pratici

Anche se l'aumento del numero di lavoratori remoti e la crescente adozione di servizi cloud implica una diversificazione dell'esposizione alle minacce che va oltre la vulnerabilità del software, la patch tempestiva delle applicazioni e dei sistemi operativi rimane fondamentale per prevenire violazioni alla sicurezza.

Come ogni amministratore sa, il patching delle vulnerabilità è uno dei compiti più dispendiosi in termini di tempo nell'IT. Quando le risorse sono limitate, le patch tendono a essere rimandate e le vulnerabilità possono svilupparsi quasi inosservate. La crescente complessità dei sistemi IT potrebbe comportare delle difficoltà di coordinamento tra i team interdisciplinari, a lacune nell'inventario e a una visibilità limitata del panorama delle minacce.

In ritardo con le patch

PROBLEMA

Il team IT è sovraccarico e quindi in ritardo con le patch

SOLUZIONE

Beneficiare di tecniche avanzate di classificazione e automazione

- ✓ Impostare la frequenza di scansione ottimale e sincronizzarla impostando i criteri di patching per gestire le vulnerabilità più rilevanti e potenzialmente sfruttabili senza sovraccaricare il team IT
- ✓ Filtrare le vulnerabilità in base alla loro gravità dando priorità a quelle che potrebbero rappresentare rischi aziendali significativi
- ✓ Personalizzare i vostri criteri di patch. Dare priorità agli asset critici, risolvere manualmente le vulnerabilità più gravi e automatizzare il patching degli altri asset in modo che avvenga in orari con minor traffico per evitare interruzioni
- ✓ Registrare e tenere traccia delle eccezioni per le patch; evitare di dover tenere traccia di ogni singola patch

Carenza di risorse IT

PROBLEMA

Le applicazioni dovrebbero essere aggiornate, ma mancano le risorse IT

SOLUZIONE

Approfittate delle soluzioni di valutazione delle vulnerabilità e della gestione delle patch completamente automatizzate e del supporto di ESET:

- ✓ Scansione automatica dei software degli endpoint e delle applicazioni di terze parti, con segnalazione immediata alla console, per una visibilità immediata delle vulnerabilità
- ✓ Per garantire una protezione continua all'organizzazione, è possibile configurare l'auto-patching selezionando una strategia di patch (tutte, solo quelle consentite o applicare specifiche esclusioni) e definendo determinate fasce orarie per l'esecuzione delle patch

Crescente complessità, esigenze di coordinamento

PROBLEMA

La complessità del sistema IT continua a crescere, rendendo più difficile il coordinamento tra i team interdisciplinari

SOLUZIONE

La nostra piattaforma ESET PROTECT permette di gestire ESET Vulnerability & Patch Management e offre la più ampia sicurezza per asset digitali e inventari.

- ✓ Centralizzare e automatizzare molteplici attività di sicurezza e gestione dell'IT con ESET PROTECT Platform, che include ESET Vulnerability & Patch Management. Ridurre la complessità della gestione IT
- ✓ Sfruttare la funzionalità multitenancy di ESET Vulnerability & Patch Management: godendo di una visibilità completa sull'intera rete, ma concentrandosi sulla propria area dedicata
- ✓ Mantenere un inventario aggiornato e colmare eventuali punti ciechi dell'infrastruttura
- ✓ Approfittare delle strategie di prevenzione, rilevamento e risposta di ESET PROTECT per ridurre al minimo l'esposizione alle minacce che vanno oltre le vulnerabilità del software
- ✓ ESET Vulnerability & Patch Management semplifica la conformità a NIS2, FedRAMP, HIPAA, PCI DSS e altri requisiti di sicurezza dei dati da parte di aziende, governi ed enti normativi

Visibilità limitata del proprio sistema IT

PROBLEMA

Visibilità incompleta della sicurezza del sistema IT?

SOLUZIONE

Approfittate della panoramica unificata fornita dalla console di ESET PROTECT

- ✓ Visibilità completa degli endpoint dell'organizzazione, delle licenze e degli stati di vulnerabilità e patching del proprio inventario di asset, sempre aggiornati
- ✓ Visualizzazione in tempo reale dello stato della sicurezza IT tramite la console di ESET PROTECT
- ✓ Collegamento in qualsiasi momento e ovunque, dal proprio browser web preferito, consentendo di rispondere all'istante
- ✓ Creazione di report mirati per misurare l'efficacia e i progressi delle politiche di gestione delle vulnerabilità e delle patch

Questo è ESET

Difesa proattiva. Ridurre al minimo i rischi con la prevenzione.

Rimanere un passo avanti rispetto alle minacce informatiche note ed emergenti (attacchi mirati, minacce zero-day, ransomware, phishing e altro ancora) grazie al nostro approccio AI-Native, basato sulla prevenzione. ESET combina la potenza dell'intelligenza artificiale e l'esperienza umana per offrire una protezione semplice ed efficace.

Scoprite una sicurezza all'avanguardia, basata su un approccio scientifico e supportata da oltre 30 anni di analisi interna delle minacce informatiche a livello globale. La nostra vasta rete di ricerca e sviluppo, guidata da ricercatori di fama nel settore, è alla base della nostra pluripremiata piattaforma di sicurezza informatica

incentrata sul cloud. Le soluzioni ESET sono altamente personalizzabili, includono assistenza locale e hanno un impatto minimo sulle prestazioni.

ESET protegge la vostra azienda per consentirvi di sfruttare appieno il potenziale della tecnologia.

ESET IN NUMERI

1bn+

utenti internet
protetti

500k+

clienti
aziendali

178.

paesi

11.

centri
R&D globali

ALCUNI DEI NOSTRI CLIENTI



protetti da ESET dal 2017 più di 9.500 dispositivi



protetti da ESET dal 2019 più di 1.200 dispositivi e 2.700 mailbox



protetti da ESET dal 2016 più di 23.000 dispositivi



Partner di sicurezza ISP dal 2008 customer base di 2 milioni di clienti

RICONOSCIMENTI



Vincitore dei premi **Best Enterprise Endpoint** e **Best Small Business Endpoint** agli SE LABS Awards 2025



Nominato **Customers' Choice** su Gartner® Peer Insights™ report **"Voice of the Customer" Endpoint Protection Platforms** del 2026



Nominato **Leader** su Frost Radar: Endpoint Security 2025, un esempio di eccellenza in termini di crescita e innovazione

Gartner e Peer Insights™ sono marchi commerciali di Gartner, Inc. e/o delle sue affiliate. Tutti i diritti riservati. I contenuti di Gartner Peer Insights sono costituiti da opinioni di singoli utenti finali basate sulle proprie esperienze e non devono essere interpretati come dichiarazioni di fatto, né rappresentano le opinioni di Gartner o delle sue affiliate. Gartner non approva alcun fornitore, prodotto o servizio descritto in questo contenuto né fornisce alcuna garanzia, espressa o implicita, in merito a questo contenuto, alla sua accuratezza o completezza, comprese le garanzie di commerciabilità o idoneità per uno scopo particolare.