



Orientarsi nel panorama del ransomware:

spunti e strategie di prevenzione

spunti e strategie di prevenzione



Cybersecurity
Progress. Protected.

Il panorama del ransomware, prevenzione e orizzonti futuri

Il ransomware rimane una delle minacce alla cybersecurity più pressanti del 2025 e continua a evolversi sia in termini di sofisticazione che di impatto. Nonostante negli anni siano stati compiuti progressi nel campo della sicurezza informatica, al di là del settore di appartenenza e dell'ordine di grandezza, tutte le organizzazioni si trovano alle prese con attacchi incessanti capaci di aggirare i loro meccanismi di difesa con tecniche sempre più raffinate. Tra le ultime novità di questo conflitto in atto si osserva l'uso degli **EDR killer**, malware appositamente progettati per disabilitare le soluzioni di rilevamento e risposta degli endpoint (EDR) prima di distribuire il ransomware. Ciò dimostra come gli attori delle minacce si adattino ai progressi della sicurezza per sfruttare i punti deboli della difesa aziendale.

La motivazione alla base degli attacchi ransomware rimane viva, ed è animata non solo da incentivi finanziari ma anche da obiettivi tattici e strategici. Mentre i gruppi di criminali informatici utilizzano il ransomware principalmente a scopo di lucro, i gruppi APT possono servirsene per coprire le tracce o come strumento distruttivo per intaccare le infrastrutture critiche, non di rado con implicazioni geopolitiche. L'evoluzione dell'uso del ransomware aggiunge ulteriore complessità al panorama delle minacce. Sia i gruppi di ransomware a scopo di lucro che gli attori delle APT affinano continuamente le loro tecniche, sfruttando le compromissioni della catena di approvvigionamento,

gli [exploit zero-day](#) e il phishing assistito dall'intelligenza artificiale per massimizzare la loro portata e il loro impatto.

In questo panorama di minacce in continua evoluzione, la **prevenzione** rimane la misura più efficace che le organizzazioni possono adottare per rafforzare la propria posizione di sicurezza. Se da un lato la risposta agli incidenti e il recupero sono fondamentali, spegnere sul nascere il

ransomware riduce sia le interruzioni operative che le perdite finanziarie.

Una strategia di sicurezza preventiva che includa una solida gestione delle patch, un'architettura zero-trust, la protezione AI-native, criteri di gestione delle password, autenticazione a più

4.91 milioni di \$

è il costo medio di un attacco ransomware nel 2024.

Fonte: [IBM: Cost of a Data Breach Report 2024](#)

fattori (MFA), consapevolezza dei dipendenti e monitoraggio continuo delle minacce può ridurre significativamente il rischio di infiltrazione di ransomware.

Nel 2025, la capacità di anticipare, prevenire e neutralizzare le minacce ransomware prima che si concretizzino è più che mai fondamentale. Ciò include la disponibilità di una potente **tecnologia di remediation** attiva 24 ore su 24, 7 giorni su 7, 365 giorni all'anno.

Ultime osservazioni sul ransomware

Diverse tendenze che hanno caratterizzato il ransomware nel 2024 sono destinate a plasmare il panorama delle minacce e le strategie di difesa anche nel 2025. Tenerlo a mente è essenziale per essere al passo con l'evoluzione dei rischi.

Uno degli eventi più rilevanti del 2024 è stato lo [smantellamento di LockBit](#), che fino a quel momento era stato il gruppo di ransomware-as-a-service (RaaS) responsabile della distribuzione della variante di ransomware più diffusa in tutto il mondo. Venuto meno LockBit, si è creato un vuoto significativo nel panorama dei ransomware. Questa lacuna è stata rapidamente colmata da altri attori di ransomware, **primo fra tutti RansomHub**.

Alla fine del 2024 RansomHub contava quasi 500 vittime, affermandosi come attore dominante nell'ecosistema del ransomware. Ad oggi RansomHub [ha criptato ed estratto i dati](#) delle proprie vittime in svariati settori: IT, servizi e strutture governative, sanità, servizi di emergenza, alimentazione e agricoltura, servizi finanziari, strutture commerciali, produzione critica, trasporti o settori di infrastrutture critiche come le comunicazioni.

Sebbene il RaaS sia un ambiente altamente competitivo per i criminali informatici, caratterizzato da continua innovazione e adattamento dei programmi di affiliazione volti ad aumentare il numero dei partner e la redditività, ESET prevede che RansomHub manterrà la sua posizione dominante. Ciò è dovuto non solo alle sue **tattiche aggressive** e ai suoi metodi sofisticati per mantenere il controllo su reti compromesse e sfruttare le vulnerabilità dei sistemi, ma anche alla sua **capacità di attrarre affiliati** precedentemente afferenti a LockBit e BlackCat.

Con la continua evoluzione del modello RaaS, gli attori delle minacce ransomware adottano sempre più spesso tecniche specializzate per eludere il rilevamento e aumentare i danni. Sebbene gli EDR killer (Endpoint Detection and Response) siano utilizzati già da tempo dai gruppi di ransomware, la loro diffusione è aumentata e oggi si assiste all'offerta di strumenti personalizzati sviluppati dalle bande criminali all'interno dei loro programmi RaaS. Allo stesso tempo, molti

attori di ransomware che fanno ingresso nell'ecosistema RaaS seguono le tendenze stabilite dai gruppi già affermati, codificando spesso la crittografia in Rust o Go per garantirne la compatibilità multiplatforma e una portata più ampia.

GLI EDR KILLER sono malware specializzati progettati per disabilitare le soluzioni di sicurezza sfruttando le tecniche BYOVD. Gli aggressori installano prima driver legittimi ma vulnerabili e poi li sfruttano per eseguire azioni privilegiate dallo spazio kernel. In questo modo possono aggirare i controlli, arrestare i processi di sicurezza e disattivare i meccanismi di rilevamento e protezione.

Poiché gli EDR killer sono diventati ormai comuni negli attacchi ransomware, ESET prevede che gli attori più avanzati miglioreranno nel corso dei mesi questo tipo di strumenti, rendendoli sempre più sofisticati, protetti e difficili da rilevare. Questa tendenza dimostra che gli strumenti di sicurezza come l'**EDR sono una spina nel fianco dei criminali informatici**, che cercheranno in tutti i modi di eliminarli o almeno di disattivarli.

Non si può parlare di RaaS e di tecniche avanzate senza riconoscere il coinvolgimento e il ruolo dei gruppi di Advanced Persistent Threat (APT). Con il ransomware questi gruppi non perseguono solo il guadagno finanziario, ma anche obiettivi strategici più ampi. Si segnalano i seguenti gruppi APT recentemente coinvolti in attacchi ransomware:



CHAMELGANG (ALLINEATO ALLA CINA)

È stato osservato che questo gruppo utilizzava il ransomware per distrarre

dalle proprie operazioni segrete, rendendo più difficile il rilevamento delle sue attività primarie.

Questo gruppo, che a volte si fa chiamare anche CamoFei, ha utilizzato il [ceppo di ransomware CatB](#) in attacchi diretti contro organizzazioni di alto profilo in tutto il mondo, comprese organizzazioni governative come la Presidenza del Brasile o infrastrutture critiche come l'All India Institute of

Medical Sciences (AIIMS), ospedale universitario pubblico e centro di ricerca medica.



MOONSTONE SLEET (ALLINEATO ALLA COREA DEL NORD)

Nota per aver sviluppato e distribuito il proprio

ransomware FakePenny, [Moonstone Sleet](#) utilizza il ransomware principalmente per scopi finanziari. Precedentemente noto come Storm-17, Moonstone Sleet sceglie i propri bersagli nei settori finanziario e dello spionaggio informatico. Tra i suoi metodi si osservano l'utilizzo di software troianizzato come PuTTY per l'accesso

→ iniziale, la distribuzione di giochi dannosi e pacchetti Node Package Manager (NPM), l'implementazione di caricatori di malware personalizzati e la creazione di [false società di sviluppo software](#) come StarGlow Ventures e C.C. Waterfall.

Queste false aziende si mettono in contatto con le potenziali vittime attraverso piattaforme come LinkedIn, Telegram, reti di freelance ed e-mail.



PIONEER KITTEN
(ALLINEATO CON
L'IRAN) E **ANDARIEL**
(ALLINEATO CON LA
COREA DEL NORD)

A questi gruppi sono stati ricondotti attacchi ransomware, soprattutto come fornitori di accesso iniziale. Probabilmente

Le aziende e le varie organizzazioni non sono probabilmente l'unico obiettivo degli attacchi ransomware. Gli attori delle minacce stanno nuovamente valutando e prendendo sistematicamente di mira gli **utenti privati**. Nell'agosto del 2024, il ransomware Magniber ha lanciato una [campagna globale](#) su larga scala criptando i dispositivi di normali utenti di tutto il mondo.

Sebbene azioni di questo tipo siano state già osservate in passato, questa campagna ha segnato un cambiamento significativo nella scelta strategica dei target dei ransomware, soprattutto a causa della portata e dell'ampia distribuzione dell'attacco rivolto ai singoli utenti, spesso privi di solide misure di sicurezza informatica.

Il ransomware Magniber è stato distribuito attraverso download di software dannoso, falsi aggiornamenti e generatori di chiavi, richiedendo riscatti compresi tra i 1.000 e i 5.000 dollari per la decriptazione. Tra i metodi utilizzati per distribuire Magniber vi sono zero-days di Windows, falsi aggiornamenti di Windows e del browser, crack di software troianizzati e generatori di chiavi.

vendono questo accesso ad altri criminali informatici per ottenere un guadagno economico. Il primo di questi gruppi citati colpisce soprattutto settori come la difesa, l'istruzione, la finanza e la sanità, mentre il secondo prende di mira le infrastrutture critiche e le organizzazioni sanitarie, principalmente negli Stati Uniti.

[Pioneer Kitten](#) si fa chiamare anche Fox Kitten, UNC757, Parisite, RUBIDIUM e Lemon Sandstorm e utilizza una vasta gamma di [tecniche](#). [Andariel](#) è considerato un sottoinsieme del Gruppo Lazarus ed è stato attribuito al Reconnaissance General Bureau della Corea del Nord.

Le richieste di riscatto rivolte ai singoli utenti sono aumentate fino a

\$5,000

nel 2024.

Fonte: [BleepingComputer: Surge in Magniber ransomware attacks impact home users worldwide](#)

Prevenire è meglio che curare

Gli utenti domestici devono quindi rimanere vigili e proattivi nelle loro pratiche di sicurezza informatica. Adottando misure preventive è dunque possibile ridurre significativamente il rischio di cadere vittime di attacchi ransomware.

Il [ransomware è in genere](#) il colpo finale preceduto da altre minacce, tra cui phishing, sfruttamento, attacchi brute force, credenziali compromesse, downloader o malware personalizzato. Molti attacchi ransomware potenziali vengono intercettati nelle prime fasi del loro ciclo di vita e si può parlare di attacco ransomware vero e proprio solo se gli aggressori riescono ad aggirare le difese delle vittime e a compiere un tentativo di distribuzione.

Per prevenire efficacemente gli attacchi ransomware, le organizzazioni dovrebbero adottare un approccio alla sicurezza a più livelli che affronti ogni fase del ciclo di vita dell'attacco, integrando anche elementi di automazione. Questo può essere considerato un [approccio orientato alla prevenzione](#), per ovvi motivi già riconosciuto da molte organizzazioni e aziende per il notevole potenziale strategico.

Prima di tutto, la **formazione e la consapevolezza dei dipendenti** sono fondamentali, poiché il phishing rimane uno dei principali vettori del ransomware. I dipendenti devono essere consapevoli dei segnali comuni del phishing e capire l'importanza di non cliccare su link sconosciuti o scaricare allegati non richiesti.

La formazione regolare del personale sul riconoscimento dei tentativi di phishing, sull'uso di password forti e sull'abilitazione dell'autenticazione a più fattori può ridurre significativamente i rischi. Anche la **protezione degli endpoint** attraverso solide soluzioni antivirus, antimalware e strumenti di rilevamento e risposta degli endpoint (EDR) è essenziale per rilevare e bloccare le attività dannose.

Nessuna soluzione EDR è del tutto immune dagli EDR killer, in quanto gli aggressori sfruttano le vulnerabilità nei driver legittimamente firmati per eseguire codice dannoso nello spazio kernel. Questi driver, una volta caricati in Windows, possono essere utilizzati per disabilitare gli strumenti di sicurezza. I prodotti ESET bloccano efficacemente molti di questi driver vulnerabili e gli analisti e gli esperti ESET possono aiutare i clienti a rafforzare ulteriormente le loro difese. Configurando impostazioni rigorose di PUA sono consentiti solo i driver più recenti, in modo da trarre beneficio dalla guida di un esperto.

È importante anche proteggere il sistema operativo con regole WDAC, volte a rafforzare una strategia di prevenzione a lungo termine di per sé necessaria. Avvalersi di un esperto può rivelarsi decisivo per contrastare efficacemente gli EDR killer.

Ulteriori provvedimenti da adottare riguardano la **sicurezza della rete** per mezzo di firewall, sistemi di rilevamento delle intrusioni (IDS) e la segmentazione della rete, tutte misure che consentono di controllare e monitorare il traffico, prevenire gli accessi non autorizzati e limitare la diffusione del ransomware.

Il 67%

dei CISO ha dichiarato di aver aumentato i budget per la cybersecurity nel 2024 rispetto al 2023.

Fonte: [IANS, 2024 Security Budget Benchmark Report](#)

Tutto ciò presuppone una regolare **gestione delle patch**, aggiornando tutti i sistemi e i software con le ultime patch di sicurezza per chiudere le vulnerabilità che gli aggressori potrebbero sfruttare.

L'implementazione di controlli di accesso basati sul principio del minimo privilegio e l'adozione di un **modello di sicurezza zero-trust** riducono ulteriormente il rischio di accesso non autorizzato e appartengono oggi a uno standard comune nell'ambito della prevenzione della cybersecurity. Lo stesso vale anche per i **backup regolari** dei dati critici, da archiviare offline o in ambienti cloud sicuri, in quanto sono fondamentali per il ripristino in caso di attacco. Naturalmente, questi backup devono essere regolarmente testati per garantirne l'efficacia.

Per quanto riguarda la prevenzione durante le operazioni quotidiane, le misure di **sicurezza delle e-mail** come i filtri antispam aiutano a bloccare le e-mail e gli allegati dannosi prima che raggiungano gli utenti. Molti incidenti si verificano ancora a causa di errori umani e le e-mail rimangono i vettori di attacco più importanti.

Dato l'alto numero di applicazioni utilizzate quotidianamente, anche stilare una **whitelist delle applicazioni** è di grande importanza. Ciò fa sì che solo le applicazioni approvate

possano essere eseguite sulla rete, impedendo l'esecuzione di software non autorizzato.

Disporre di un **piano di risposta agli incidenti** ben articolato, affiancato da simulazioni regolari, consente alle organizzazioni di essere pronte a rispondere efficacemente agli attacchi ransomware.

Tutte queste misure rafforzano la cybersecurity attraverso strategie di difesa proattive basate sul principio "prevenire è meglio che curare".

Perché non pagare il riscatto?

Tuttavia, nemmeno un forte approccio preventivo può escludere al cento per cento il verificarsi di un attacco ransomware. Gli attori delle minacce affinano costantemente le loro tattiche, sfruttando vulnerabilità zero-day, debolezze della catena di approvvigionamento o errori umani per aggirare anche le difese più valide. Tuttavia, persino a un attacco dirompente è possibile porre rimedio. Le organizzazioni che agiscono rapidamente, attivando i piani di risposta agli incidenti e facendo affidamento su backup sicuri, possono riprendersi senza cedere alle estorsioni.

63%

è la quota di vittime di ransomware che hanno allertato le forze dell'ordine invece di pagare un riscatto nel 2024.

Fonte: [IBM, Cost of a Data Breach Report 2024](#)

Questo ci porta a un punto critico: perché pagare il riscatto non è la soluzione giusta.

- Si sostiene il modello di business alla base del crimine.
- Si incoraggiano ulteriori attività criminali finanziandole inavvertitamente.
- Si permette alle bande di ransomware di ricercare le vulnerabilità zero-day e di sviluppare nuovi exploit.
- Ci si espone a divenire nuovamente bersaglio di attacchi futuri e di ulteriori richieste di denaro.

Pagare i criminali che hanno criptato i vostri dati non significa ottenere la garanzia di ricevere una chiave di decrittazione funzionante: dopotutto, non c'è modo di denunciarli

o di adire le vie legali contro di loro. Ci sono diversi motivi per cui il pagamento potrebbe non portare al recupero dei dati.

- Alcuni dati potrebbero essere stati danneggiati durante la cifratura, rendendoli comunque irrecuperabili.
- Lo strumento di decriptazione fornito potrebbe essere integrato con malware aggiuntivo, funzionare male o essere significativamente più lento del ripristino dai backup.
- Il buon esito della consegna della chiave di decriptazione può essere compromesso in diversi modi, tra cui bug nel codice di decriptazione, schema di [crittografia troppo complicato](#), disguidi nell'elaborazione dei pagamenti (soprattutto con le criptovalute) o tattiche di doppia estorsione che richiedono pagamenti ulteriori.
- È possibile inoltre che si agisca in malafede, senza l'intenzione di fornire una chiave di decriptazione.

In pratica, sono due le argomentazioni principali a favore del pagamento del riscatto. La prima è l'impossibilità di ripristinare i dati crittografati dai backup quando questi ultimi non esistono, sono incompleti o sono stati danneggiati. Tuttavia, possono esserci delle alternative al pagamento. Prima di effettuare qualsiasi pagamento, consultate il vostro fornitore di software di sicurezza:

(a) verificare se è disponibile uno strumento di decriptazione per la specifica variante di ransomware, che potrebbe consentire il recupero senza pagamento, e

(b) verificare se ci sono notizie circa l'inefficacia del pagamento del riscatto per quella particolare variante.

Il secondo argomento comune a favore del pagamento del riscatto è che è più economico del ripristino dai backup. Sebbene ciò possa essere tecnicamente vero in termini di tempo e lavoro, rimane una decisione fondamentalmente sbagliata per diversi motivi.

Come già detto, le promesse di decriptazione sono inaffidabili, c'è un'alta probabilità di essere presi di mira di nuovo dopo aver effettuato il primo pagamento - non si dimentichi che non si tratta di individui rispettosi della legge - e pagando si sostiene un'operazione criminale, aumentando in ultima analisi la probabilità di ulteriori attacchi contro altri. Il pagamento è talvolta addirittura illegale e uno dei motivi è che gli aggressori potrebbero essere soggetti a [sanzioni](#).

Qual è il supporto che ESET offre per proteggersi dagli attacchi ransomware? Quali i rimedi?

Uno strumento **di remediation affidabile**, nell'ambito di una strategia proattiva e orientata alla prevenzione, può essere la migliore difesa contro le decisioni più difficili: cioè se investire pesantemente nel recupero dei dati o prendere in considerazione il pagamento di un riscatto. Grazie alla potente tecnologia di remediation, sarete sempre un passo avanti.

Ransomware Remediation di ESET è un livello di sicurezza completamente automatizzato all'interno del moderno modulo di protezione degli endpoint della [Piattaforma ESET PROTECT](#). Progettato per migliorare la difesa contro i ransomware, insieme a [Ransomware Shield](#) rileva e blocca i comportamenti sospetti. Combina prevenzione e rimedio in un'unica soluzione, fornendo un approccio completo a più fasi per contrastare la crittografia.

Il 94%

delle organizzazioni intervistate ha riferito di tentativi da parte di criminali informatici di compromettere i loro backup nel 2024.

Fonte: [SC World, Compromised backups send ransomware recovery costs soaring](#)

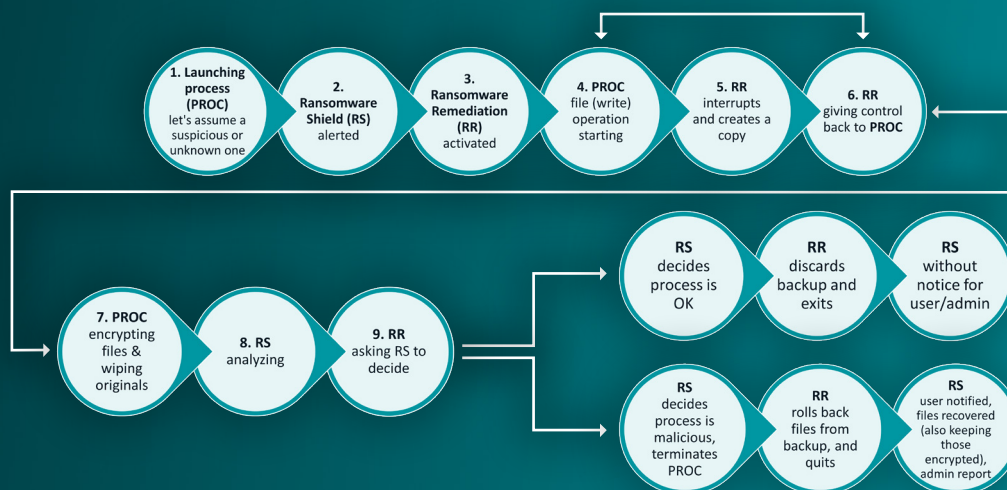
A differenza delle tradizionali soluzioni di rimedio e rollback basate sul Volume Shadow Copy Service del sistema operativo - spesso un obiettivo primario per gli aggressori - **ESET utilizza una soluzione proprietaria di caching dei file**, che offre maggiore flessibilità e affidabilità. Gli operatori di ransomware spesso eliminano o sovrascrivono le copie shadow per impedire il recupero, rendendo inefficaci i metodi di rollback tradizionali.

Al contrario, il processo di backup di Ransomware Remediation di ESET non è un servizio locale, ma opera all'interno della **propria sezione di archiviazione protetta** sull'unità, dove i file non possono essere modificati, danneggiati, né eliminati dagli aggressori.

La tecnologia monitora continuamente tutti i processi, intercettando le modifiche dei file in tempo reale. Nel momento in cui viene rilevato un processo di alterazione dei file, il sistema di backup rapido di ESET crea copie dei file originali, anche prima che i sistemi

di reputazione comportamentale come Ransomware Shield determinino se l'attività è dannosa. Il tutto funziona di concerto con le [tecnologie ESET LiveSense](#), che sezionano e analizzano il malware fino al suo nucleo.

ESET Ransomware Remediation, secondo un approccio proattivo, garantisce alle organizzazioni il recupero immediato dei file, eliminando la necessità di pagare il riscatto. ESET Ransomware Remediation è incluso in tutti i livelli della Piattaforma ESET PROTECT a partire da [ESET PROTECT Advanced](#). È disponibile anche una versione di prova completamente funzionale della durata di 30 giorni.



L'albero dei processi complessi di ESET Ransomware Shield e Ransomware Remediation

QUALI SONO I PRINCIPALI VANTAGGI DI ESET RANSOMWARE REMEDIATION?

- Lo strumento fornisce un rollback completo attraverso il ripristino automatico dei file dalla cache sicura
- Protegge solo i file interessati da un processo sospetto, riducendo i problemi dello spazio su disco
- A differenza di altre soluzioni, ESET utilizza una tecnologia proprietaria unica e non si affida alla funzione VSS (Volume Shadow Copy Service) presente nei sistemi operativi Windows di Microsoft
- La funzione è attiva per impostazione predefinita nei livelli di abbonamento ESET PROTECT idonei; non è richiesta alcuna interazione da parte dell'utente e gli amministratori possono configurare le cartelle e i tipi di file protetti

Conclusione

Il ransomware rimane una minaccia importante per la sicurezza informatica nel 2025, con tattiche in continua evoluzione e sempre più sofisticate. La caduta di LockBit e l'ascesa di RansomHub evidenziano le dinamiche mutevoli dell'ecosistema RaaS, dove il successo si misura spesso in termini di capacità di attrarre e mantenere affiliati.

In seguito alla rimozione di LockBit da parte delle forze dell'ordine, molti affiliati hanno perso la fiducia e sono passati a RansomHub, indebolendo in modo significativo la scala operativa di LockBit. Nel frattempo, tecniche avanzate come gli EDR killer, insieme al coinvolgimento di gruppi APT, continuano ad aggravare il livello di complessità a queste minacce.

Per combattere efficacemente il ransomware e le minacce che lo precedono, le organizzazioni devono adottare un approccio alla sicurezza a più livelli e di tipo preventivo. Ciò presuppone la formazione dei dipendenti, una solida protezione degli endpoint e dei dati, backup regolari e soluzioni di sicurezza avanzate come [MDR](#) o [XDR](#).

La suite completa di cybersecurity di ESET include la tecnologia Ransomware Remediation, una soluzione proattiva che consente un recupero rapido e riduce al minimo l'impatto degli attacchi, in modo da gestire anche le minacce ransomware più sofisticate.

ESET

Difesa proattiva. Il nostro obiettivo è ridurre al minimo la superficie di attacco.

Rimanete un passo avanti rispetto alle minacce informatiche note ed emergenti con il nostro **approccio prevention-first, basato sull'intelligenza artificiale e sull'esperienza umana.**

Avvalendovi del nostro supporto beneficiate di una protezione best-in-class, basata su un'**intelligence interna sulle minacce informatiche** globali maturata in oltre 30 anni all'interno della nostra rete di ricerca e sviluppo sotto la guida di **ricercatori rinomati nel settore.** ESET protegge la vostra azienda per consentirvi di sfruttare appieno il potenziale della tecnologia.



**Tecnologia
multilivello**



**L'Intelligenza
Artificiale
incontra
l'esperienza
umana**



**In prima linea
nella ricerca sulla
cybersecurity**



**Assistenza
personalizzata
e locale**



Cybersecurity
Progress. Protected.

© 1992–2025 ESET, spol. s r.o. – All rights reserved. Tutti i marchi commerciali qui utilizzati sono marchi commerciali o marchi registrati di proprietà di ESET, spol. s r.o. o ESET North America. Tutti gli altri nomi e marchi sono marchi registrati delle rispettive società.