



PANORAMICA

CLOUD WORKLOAD PROTECTION

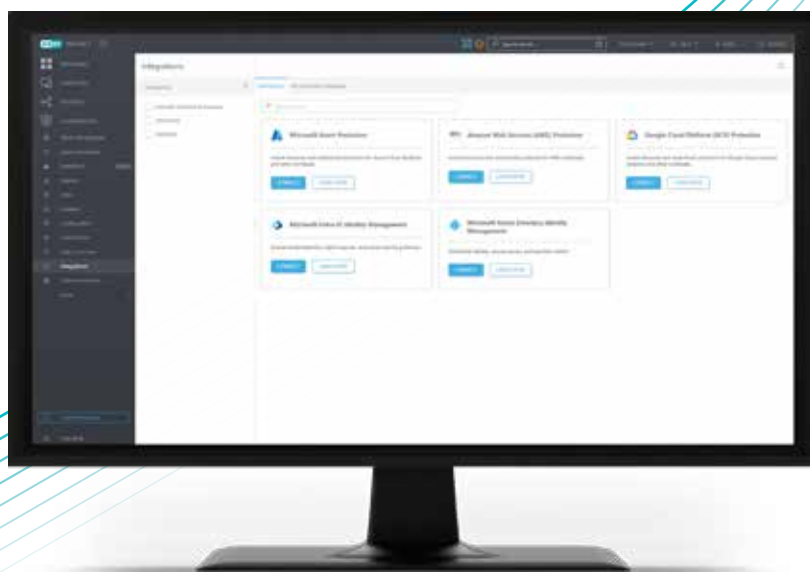
Proteggi le macchine virtuali nel cloud
dalle minacce informatiche avanzate

Progress. Protected.

Che cos'è **ESET Cloud Workload Protection**?

ESET Cloud Workload Protection (CWP) offre una protezione multilivello basata sull'intelligenza artificiale per le macchine virtuali (VM) in ambienti cloud, al fine di prevenire i malware, bloccare gli attacchi informatici e ridurre al minimo i tempi di inattività dei carichi di lavoro.

Si tratta di una soluzione di sicurezza informatica progettata per proteggere i carichi di lavoro, in particolare le macchine virtuali, in esecuzione negli ambienti Amazon Web Services, Microsoft Azure o Google Cloud Platform. CWP garantisce visibilità, rilevamento delle minacce e protezione in fase di esecuzione contro le vulnerabilità e gli attacchi informatici rivolti alle applicazioni ospitate nel cloud.



Questa soluzione viene fornita come servizio ed è gestita tramite la console web unificata ESET PROTECT, accessibile da qualsiasi luogo.

Perché è fondamentale rafforzare la sicurezza del cloud?

L'80% delle organizzazioni¹ considera il cloud pubblico fondamentale per le proprie iniziative di trasformazione digitale. L'utilizzo del cloud continua a crescere e sta rapidamente diventando la nuova normalità. Da recenti studi di settore emerge che la maggior parte delle organizzazioni ha già subito violazioni della sicurezza legate al cloud. Considerando che il costo medio di una violazione dei dati nel cloud pubblico raggiunge i 5,17 milioni di dollari², la sicurezza del cloud non è più un optional, ma è fondamentale per la sopravvivenza dell'azienda.

Gli ambienti cloud offrono un'agilità straordinaria, ma comportano anche una complessità sempre maggiore. I carichi di lavoro sono dinamici, distribuiti e spesso invisibili agli strumenti di sicurezza tradizionali. Gli hacker lo sanno bene. Prendono di mira i carichi di lavoro nel cloud con metodi sempre più sofisticati, causando interruzioni del servizio, perdita di dati e danni duraturi alla reputazione.

Principali punti critici da affrontare

- Livello di sicurezza non uniforme tra i vari ambienti
- Rapida diffusione delle minacce informatiche provenienti dal cloud
- Sfide in materia di efficienza e conformità

I vantaggi principali

✓ SEMPLICITÀ

Perfetta integrazione con i fornitori di cloud (AWS, Azure e GCP). Utilizza la console ESET PROTECT per una gestione centralizzata e semplificata delle macchine virtuali nel cloud e degli endpoint. Ottenere la licenza è semplice: basta sottoscrivere un unico abbonamento per la sicurezza degli endpoint e delle macchine virtuali nel cloud, a seconda delle esigenze.

✓ EFFICACIA

Una tecnologia collaudata garantisce il rilevamento in tempo reale e la prevenzione automatizzata delle minacce, andando ben oltre la sicurezza nativa del cloud. Sulle macchine virtuali viene installato un agente leggero per garantire una maggiore sicurezza delle risorse senza compromettere le prestazioni del sistema.

✓ FLESSIBILITÀ

Adatta il sistema di sicurezza alla crescita della tua azienda e all'evoluzione delle esigenze. Combina liberamente le licenze per le macchine virtuali cloud e gli endpoint all'interno di infrastrutture ibride o ambienti multi-cloud.

¹ Gartner: Solution Path for Security in the Public Cloud Report, March 2025

² 2025 IBM Cost of a Data Breach Report

Casi pratici

Interruzioni costose o tempi di inattività?

I benefici dell'agilità e della potenza del cloud senza un'adeguata protezione possono essere vanificati anche da un solo attacco di ransomware o malware, che rischia di bloccare le operazioni e causare costosi tempi di inattività.

Problema: Le macchine virtuali su cloud non protette sono vulnerabili alle infezioni da ransomware e malware. Una singola violazione può bloccare le operazioni, causare la perdita di dati e comportare costosi tempi di inattività.

Soluzione: ESET Cloud Workload Protection offre una protezione in tempo reale basata su agenti per le macchine virtuali basate sul cloud Azure, AWS e GCP. Le funzionalità XDR integrate consentono di individuare tempestivamente le anomalie, riducendo al minimo il rischio operativo.

PROTEZIONE APPLICATA:

- Rilevamento avanzato dei malware e blocco degli exploit
- Monitoraggio XDR delle esecuzioni di file sospetti
- Politiche di correzione automatizzate o servizio MDR dedicato

Violazioni dei dati e rapida escalation degli attacchi?

Senza misure di sicurezza rigorose e una visibilità in tempo reale nel cloud, gli aggressori possono compromettere rapidamente i carichi di lavoro esposti.

Problema: Le PMI che trasferiscono i propri carichi di lavoro su macchine virtuali nel cloud corrono rischi simili a quelli degli endpoint tradizionali, ma sono spesso più esposte a causa della connettività costante. Senza un monitoraggio costante dei processi, dei comportamenti

e dei tentativi di movimento laterale, gli attacchi avanzati possono intensificarsi rapidamente.

Soluzione: ESET Cloud Workload Protection estende le funzionalità XDR complete alle macchine virtuali basate su cloud. Offre una panoramica accurata grazie alla raccolta continua di dati di telemetria dettagliati e di basso livello e di segnali di sicurezza, consentendo ai team di sicurezza di individuare e analizzare in tempo reale malware avanzato, attacchi fileless, uso improprio di strumenti legittimi e comportamenti sospetti da parte di utenti o applicazioni.

PROTEZIONE APPLICATA:

- Host Intrusion Prevention System (HIPS)
- Correlazione XDR tra tentativi di accesso e modifiche dei privilegi
- Protezione dagli attacchi di rete per bloccare il traffico in uscita sospetto

Perdita di visibilità e controllo?

Gli ambienti ibridi aumentano la complessità. Garantire la sicurezza degli endpoint locali e delle macchine virtuali nel cloud senza gli strumenti adeguati comporta lacune nel monitoraggio e nella gestione, rendendo più difficile bloccare le minacce prima che si concretizzino.

Problema: Le PMI spesso non dispongono di una panoramica centralizzata dei carichi di lavoro sia on-premise che nel cloud, creando così dei punti ciechi di cui gli hacker approfittano. La frammentazione degli strumenti di sicurezza rende impossibile valutare l'intera superficie di attacco.

Soluzione: ESET CWP si integra con ESET PROTECT in un'unica console che garantisce visibilità e controllo completi su tutti i carichi di lavoro (on-premise e nel cloud). La gestione automatizzata garantisce una protezione uniforme in tutti gli ambienti.

PROTEZIONE APPLICATA:

- Gestione centralizzata della sicurezza di tutte le macchine virtuali e degli endpoint
- Distribuzione automatizzata basata su criteri
- Telemetria XDR per il rilevamento delle minacce

Caratteristiche principali

GESTITO DA UNA CONSOLE UNIFICATA

Tutte le macchine virtuali, gli endpoint e i dispositivi mobili ESET nel cloud possono essere gestiti da ESET PROTECT, la nostra console di gestione unificata basata su cloud o on-premise.

PROTEZIONE CONTRO IL RANSOMWARE E RIPRISTINO

Livello di protezione ulteriore che tutela gli utenti dal ransomware, integrato con un ripristino completo grazie al recupero automatico e senza interruzioni dei file da backup sicuri.

PROTEZIONE DA ATTACCHI MIRATI

ESET utilizza 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.

TECNOLOGIA MULTISTRATO INCENTRATA SULLA PREVENZIONE

La tecnologia basata sull'intelligenza artificiale di ESET sviluppata nel corso di decenni offre un motore di rilevamento pluripremiato e un nucleo di protezione apprezzato dai clienti di tutto il mondo.

ADVANCED THREAT DEFENSE

Una tecnologia basata sul cloud che dispone di scansione avanzata, machine learning all'avanguardia, sandboxing basato su cloud e analisi comportamentale approfondita per prevenire gli attacchi mirati e i nuovi tipi di minacce mai visti prima. ESET LiveGuard Advanced garantisce una prevenzione proattiva delle minacce contro gli attacchi zero-day con correzione autonoma.

INTEGRAZIONE PERFETTA

Attivazione in 1-2-3 clic della soluzione di sicurezza sulle macchine virtuali basate sul cloud selezionate. È sufficiente collegarsi all'integrazione di ESET PROTECT con Amazon Web Services, Microsoft Azure o Google Cloud Platform.

VISIBILITÀ ESTESA E XDR

I dati di telemetria provenienti dalle macchine virtuali e dal cloud stesso vengono acquisiti nel modulo ESET PROTECT XDR della piattaforma, consentendo agli amministratori di gestire e automatizzare le azioni di risposta agli incidenti e l'individuazione delle minacce.

ADD-ON MDR SERVICE

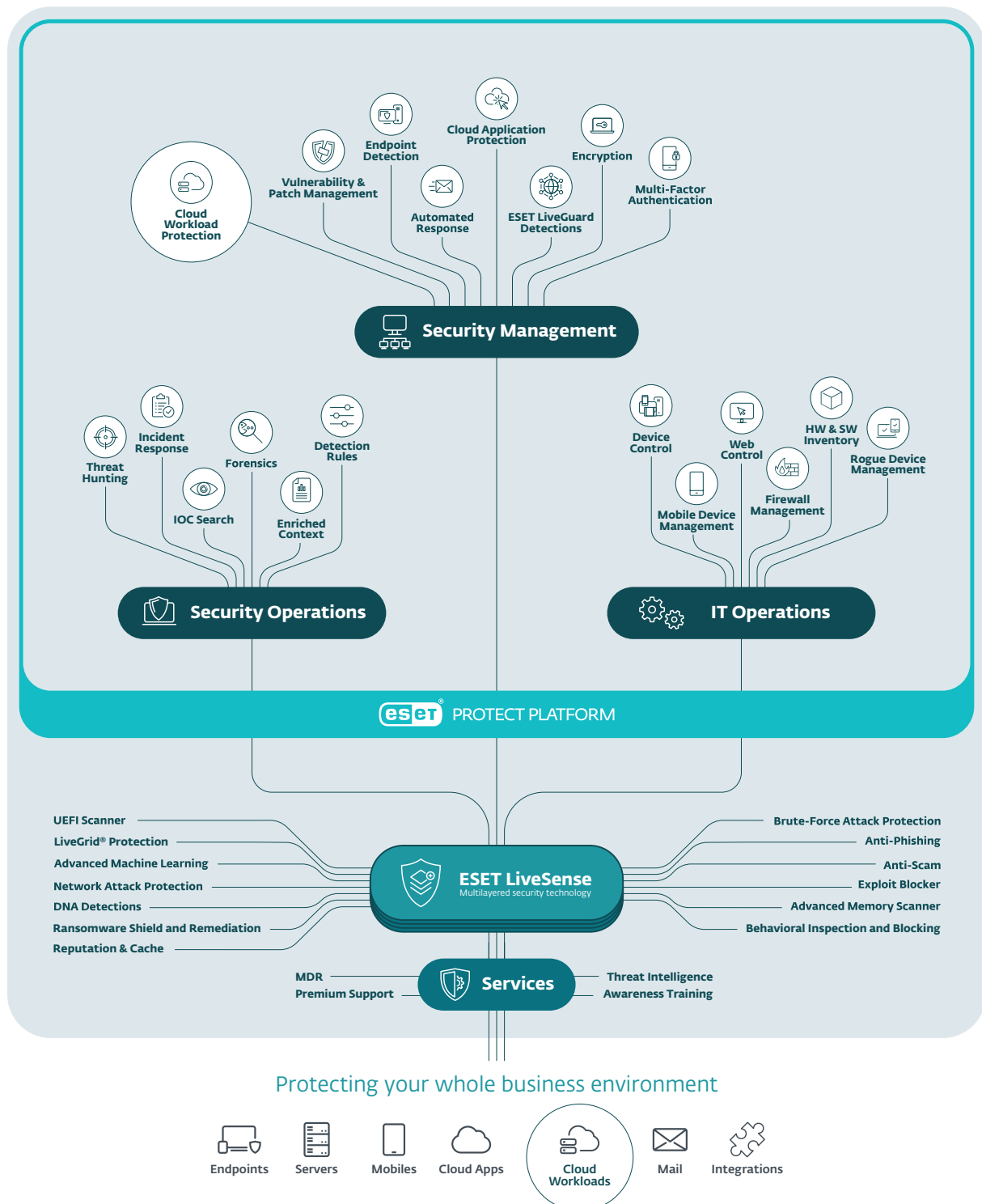
RILEVAMENTO E RISPOSTA GESTITI PER IL CLOUD

Affidatevi agli esperti ESET per monitorare l'ambiente ibrido o cloud 24 ore su 24, 7 giorni su 7, beneficiando del servizio di risposta agli incidenti in modo da bloccare le minacce o le attività dannose quasi istantaneamente. Colmate le lacune nelle competenze in materia di sicurezza informatica liberando risorse IT affinché possano concentrarsi sulle attività principali.



ESET PROTECT Platform ecosystem

Come si inserisce Cloud Workload Protection nell'ecosistema della sicurezza e quali esigenze in materia di sicurezza informatica è in grado di soddisfare questa piattaforma.



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, orientato alla 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.