



Protezione completa degli endpoint:
protezione di livello aziendale, individuazione
e risposta alle minacce per workstation,
laptop e server.



Perché la protezione degli endpoint **rappresenta il futuro della cybersecurity?**

Con gli attacchi informatici in continua evoluzione, il notevole incremento dell'adozione del cloud e il ricorso sempre più frequente alla forza lavoro da remoto, i metodi tradizionali di sicurezza degli endpoint non sono più sufficienti.

Nonostante i notevoli investimenti nella sicurezza informatica, le aziende spesso faticano a proteggere le risorse digitali e i loro dati dagli attacchi contro gli endpoint. Con il ricorso allo smart working / lavoro remoto mettere in sicurezza le tecnologie utilizzate dalla forza lavoro remota diventa imperativo!

Per garantire una sicurezza degli endpoint adeguata e al passo con i tempi, le aziende devono disporre di una soluzione di sicurezza che trascenda i confini fisici dell'azienda e che copra tutti i moderni endpoint remoti. In cloud o on-premise? Decidi tu! Noi ti offriamo una soluzione di sicurezza end-to-end semplice e completa che ti garantisce una protezione su tutti gli endpoint.



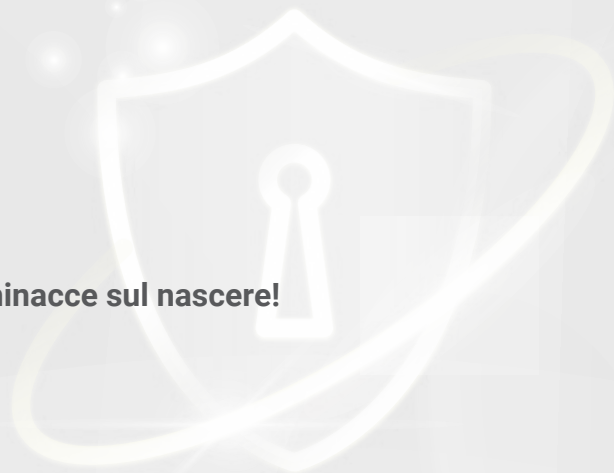


Seqrite Endpoint Protection per le aziende

Un'unica soluzione integrata per bloccare le minacce sul nascere!

Seqrite Endpoint Protection è una piattaforma semplice e completa che integra tecnologie innovative come Anti Ransomware e Sistema di Individuazione Comportamentale per proteggere la tua rete dalle minacce avanzate di oggi.

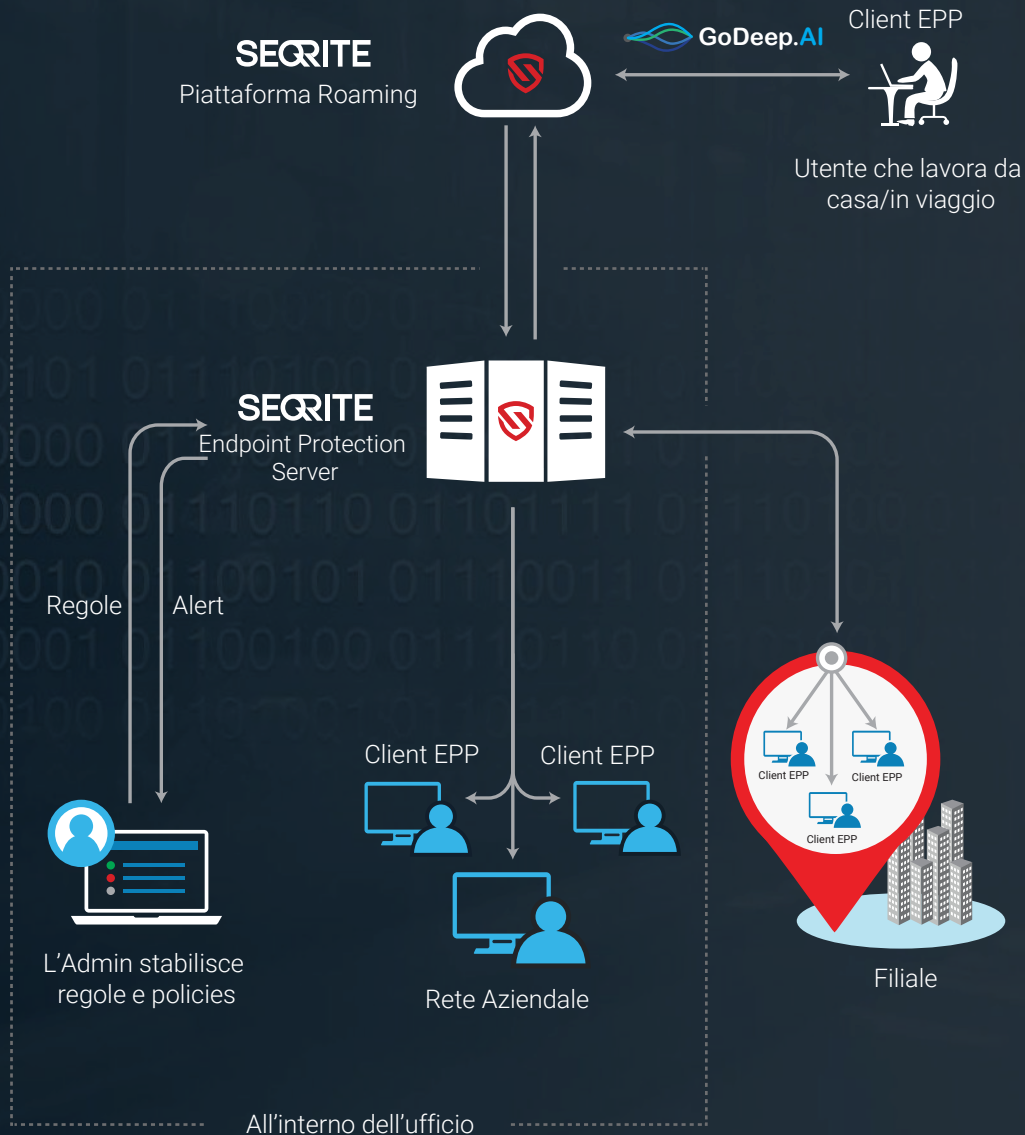
Offre una vasta gamma di funzionalità avanzate come il Controllo Avanzato dei Dispositivi, il DLP, la Scansione delle Vulnerabilità, la Gestione delle Risorse, il Filtro Web, la Gestione delle Risorse, l'Endpoint Threat Hunting, ecc., per garantire una protezione completa agli asset digitali delle aziende.





Un'unica piattaforma Per risolvere molti problemi

Seqrite Endpoint Protection





Perché scegliere Seqrite **Endpoint Protection?**

1

Sicurezza completa e Controllo per gli Endpoint

Una piattaforma semplice ma potente per gestire la sicurezza e rafforzare il controllo sui dati, le applicazioni, l'accesso al web: è dotata di una vasta gamma di funzioni come il Controllo Dispositivi Avanzato, il DLP, la Gestione delle Risorse, il Controllo delle Applicazioni ecc...

2

Protezione Multilivello

Garantita da numerose certificazioni di settore, integra tra loro innovative tecnologie come la Scansione Vulnerabilità, il Sistema di Analisi Comportamentale, l'Endpoint Threat Hunting e l'Anti Ransomware per proteggere il tuo sistema da malware e minacce avanzate su più e differenti livelli.

3

Scansione e patch delle vulnerabilità

Permette di individuare le vulnerabilità delle applicazioni e del sistema operativo e aiuta a risolvere le falle individuate tramite l'installazione delle relative patch. L'update regolare delle applicazioni rende la rete aziendale meno vulnerabile agli attacchi malware

4

Gestione e Controllo Centralizzati

Interfaccia user-friendly per il monitoraggio, la configurazione e la gestione dei sistemi nella rete grazie anche alla dashboard grafica e a dettagliati report.





Descrizione delle funzioni

Core Protection



Antivirus

Protezione Anti Malware garantita dalle più importanti certificazioni di settore.



Anti Ransomware

Protezione da attacchi ransomware e backup automatico dei file selezionati.



File Sandboxing

Integrazione con Seqrite Cloud Sandbox per l'analisi dei file sospetti alla ricerca di malware. Non ci sarà bisogno di acquistare e attivare hardware o software per l'analisi malware.

Controllo Dispositivi e DLP



Controllo Dispositivi Avanzato

Garantisce il rispetto delle policy riguardo l'uso dei dispositivi di storage, mobile e dispositivi removibili, wireless, interfacce di rete collegati agli endpoint.



Data Loss Prevention

Previene la perdita di dati monitorando quelli confidenziali e definendo le modalità di condivisioni dati degli utenti attraverso drive removibili, app ecc..

Protezione Web



Protezione Navigazione

Blocca i siti dannosi.



Antiphishing

Blocca i siti di phishing



Filtro Web

Blocca i siti in base alle categorie di appartenenza.



Accesso a Internet pianificato

E' possibile limitare l'accesso a Internet in base a precise fasce orarie.



Controllo Accesso a Google e YouTube

Blocca l'accesso personale a Google e consente quello aziendale. Blocca i video di YouTube a seconda della categoria di contenuto, nome del publisher, ecc.

Protezione della Rete



IDS/IPS

Individua le attività dannose nella rete, come i tentativi di exploit delle vulnerabilità delle app. Blocca i tentativi di intrusione e accesso non autorizzato alla rete.



Firewall

Monitora il traffico in entrata e in uscita seguendo precise regole preimpostate.



Prevenzione Attacco Port Scan

Avvisa quando la rete sta subendo uno scanning delle porte.



Prevenzione Attacchi DDoS

Avvisa quando è in corso un attacco DDoS.

Monitoraggio e Controllo



Scansione Vulnerabilità

Fornisce una panoramica delle vulnerabilità presenti nella rete, classificate secondo il loro livello di gravità.



Gestione Patch

Soluzione centralizzata di gestione delle patch per risolvere le falle delle app Microsoft e non.



Monitoraggio Attività File

Monitora i file riservati dell'azienda e notifica agli amministratori quando questi sono copiati, rinominati oppure cancellati.

Gestione e Controllo



Amministrazione Centralizzata

Console web con dashboard grafica, gestione gruppi e policy, notifiche email e SMS, facile implementazione.



Piattaforma Roaming

Gestisce i client anche quando si spostano fuori dalla rete fisica aziendale.



Migrazione da EPS v7.6

Facilita la migrazione di endpoint, utenti, gruppi e policy alla nuova configurazione del server EPS. Consente inoltre la migrazione di gruppi di endpoint.



High Availability (HA)

L'High Availability garantisce l'accesso ininterrotto dell'utente ai servizi, applicazioni e dati anche durante i guasti hardware e malfunzionamenti dei software, riducendo al minimo l'inattività del sistema.



Descrizione delle funzioni

Gestione e Controllo



Crittografia BitLocker per la sicurezza dei dati

Consente la gestione centralizzata dei criteri di crittazione BitLocker, delle chiavi e delle opzioni di ripristino, garantendo una solida sicurezza dei dati e la conformità ai requisiti normativi.

Endpoint Detection and Response (EDR)



Interrogazione rapida degli endpoint

Interroga gli endpoint in tempo reale per raccogliere informazioni da fonti predefinite sugli endpoint stessi.



Ricerca automatica Indicatori di Compromissione (IoC)

Integrazione con il server MISP per i feed delle minacce. Questi file hash presi dal server MISP saranno ricercati regolarmente (giornalmente / settimanalmente): i risultati saranno visibili nei report.



Blocco IoC in tempo reale

Ricerca continuamente questi file hash in cerca di contenuti dannosi: sarà possibile così bloccarli in tempo reale.



Endpoint Threat Hunting

Endpoint Threat Hunting (ETH) è il sistema più efficace per cercare, su tutti gli endpoint, corrispondenze tra i file e gli hash dannosi. ETH individua così anche attacchi nascosti in base agli hash forniti dall'utente e aiuta a bloccarli prima che possano causare danni al sistema.

Gestione Applicazioni e Risorse



Controllo Applicazioni

Limita l'accesso alle applicazioni basandosi sulla metodologia Zero Trust. Consente di definire le autorizzazioni delle applicazioni in base al sistema operativo, comprese le applicazioni predefinite del SO e di Segrite. Offre la modalità "solo monitoraggio" che permette, senza blocchi, di registrare l'accesso alle applicazioni consentendo agli amministratori di rete visibilità continua.



Gestione Risorse

Garantisce totale visibilità degli hardware e dei software in esecuzione sugli endpoint e aiuta a tracciarne ogni variazione avvenuta.





Comparazione Prodotti

| Funzioni | Business | Total | Enterprise Suite | EDR |
|------------------------------------|----------|--------|------------------|--------|
| Antivirus | ✓ | ✓ | ✓ | ✓ |
| Anti Ransomware | ✓ | ✓ | ✓ | ✓ |
| Protezione Email | ✓ | ✓ | ✓ | ✓ |
| IDS/IPS | ✓ | ✓ | ✓ | ✓ |
| Firewall | ✓ | ✓ | ✓ | ✓ |
| Protezione Phishing | ✓ | ✓ | ✓ | ✓ |
| Protezione Navigazione | ✓ | ✓ | ✓ | ✓ |
| Notifica SMS* | ✓ | ✓ | ✓ | ✓ |
| Scansione Vulnerabilità | ✓ | ✓ | ✓ | ✓ |
| Piattaforma Roaming | ✓ | ✓ | ✓ | ✓ |
| GoDeep.AI* | ✓ | ✓ | ✓ | ✓ |
| Gestione Risorse | ✓ | ✓ | ✓ | ✓ |
| Anti Spam | ✓ | ✓ | ✓ | ✓ |
| Filtro Web | ✓ | ✓ | ✓ | ✓ |
| Controllo Dispositivi | ✓ | ✓ | ✓ | ✓ |
| Integrazione SIEM | ✓ | ✓ | ✓ | ✓ |
| Controllo Applicazioni - Blocklist | | ✓ | ✓ | ✓ |
| Controllo Applicazioni - Safelist | | ✓ | ✓ | ✓ |
| Tuneup* | | ✓ | ✓ | ✓ |
| Monitoraggio Attività File | | ✓ | ✓ | ✓ |
| Gestione Patch | | ✓ | ✓ | ✓ |
| Controllo Accessi YouTube | | | ✓ | ✓ |
| Controllo Accessi Google | | | ✓ | ✓ |
| Disk Encryption Management | | | ✓ | ✓ |
| Rapid Query a Endpoints | | | | ✓ |
| Automated IoC Search | | | | ✓ |
| Realtime IoC Blocking | | | | ✓ |
| Endpoint Threat Hunting | Add-on | Add-on | Add-on | ✓ |
| Data Loss Prevention | Add-on | Add-on | ✓ | ✓ |
| File Sandboxing | Add-on | Add-on | Add-on | Add-on |

Nota: *Funzione presente solo in v7.x



Certificazioni




Seqrite Endpoint Protection è stato certificato come “Approved Corporate Endpoint Protection per Windows” da AV-Test.

Pronto per una demo?

[Clicca qui](#)

o scansiona






Info su Seqrite

Seqrite è un fornitore leader di soluzioni di cyber security aziendale. Avendo a mente, come primo obiettivo, quello di semplificare la sicurezza informatica e renderla accessibile alle PMI, Seqrite offre soluzioni e servizi completi mettendo a disposizione dei clienti tecnologie brevettate e i vantaggi dell'Intelligenza Artificiale (AI) e del Machine Learning (ML). Le soluzioni di sicurezza di Seqrite proteggono le aziende dalle minacce più avanzate grazie a più livelli di sicurezza posti a difesa di dispositivi, applicazioni, reti, cloud e dati. Seqrite è il ramo di sicurezza informatica per le aziende di Quick Heal Technologies Limited, l'unica società di prodotti e soluzioni di cybersecurity quotata in borsa in India.

Oggi, oltre 30.000 imprese in più di 76 Paesi si affidano a Seqrite per le loro esigenze di cybersecurity.

SEQRITE

Quick Heal Technologies Limited

Seqrite Italia www.seqrite.it | cs@s-mart.biz | +39 055 43 03 52 | Distribuito da s-mart.biz 

Tutte le Proprietà Intellettuai, compreso Marchio/i di Fabbrica, Logo/i, Copyright sono di proprietà dei rispettivi proprietari. Copyright©2024 Quick Heal Technologies Ltd. Tutti i diritti riservati