



Seqrite Endpoint Security

Sicurezza aziendale integrata e console unificata di gestione degli endpoint.

Principali caratteristiche del prodotto

Innovativa soluzione per la sicurezza degli endpoint che previene la perdita di dati, monitora le attività e il trasferimento dei file e fornisce robuste funzionalità antivirus e per una sicura navigazione sul web.

- » Protezione malware integrata, protezione web, del browser e dei dati (DLP) in una unica licenza.
- » Soluzione di gestione delle patch centralizzata per tutte le necessità di patching delle vulnerabilità dei prodotti Windows.
- » Informazioni complete e cumulative per gli endpoint Windows, Mac e Linux grazie alla funzione migliorata per la Gestione Risorse
- » Gli amministratori possono specificare i nomi dei dispositivi e le fasce orarie di accesso, assicurando così un totale controllo dell'interfaccia USB.
- » Solida protezione per gli endpoint con piattaforme Windows, Mac e Linux con una sola console di gestione.
- » Report di ogni attacco ransomware avvenuto attraverso la rete aziendale.

Caratteristiche



CONTROLLO DISPOSITIVI

Consente di gestire i vari dispositivi esterni usati dai dipendenti. Permette alle organizzazioni di controllare, configurare, definire diverse policy di accesso per i vari tipi di dispositivi su SO Windows e Mac. Grazie a questa funzione, l'Amministratore IT è in grado di:

- » Permettere l'accesso temporaneo ad un dispositivo, per una durata stabilita, per uno specifico client.
- » Permettere l'accesso a specifici dispositivi di storage in base al nome del modello.
- » Permette la criptazione totale del dispositivo per i file di sistema.
- » Bloccare l'interfaccia USB per tutti i dispositivi, escludendo i dispositivi di archiviazione di massa e di input.

In aggiunta a questi miglioramenti, si possono garantire ad ogni device di storage esterno i seguenti tipi di accesso:

- Consenti – I dati possono essere trasferiti da e verso il dispositivo.
- Blocca – I dati non possono essere trasferiti da e verso il dispositivo.
- Sola lettura – I dati possono essere letti solo dal dispositivo.



ANTI RANSOMWARE

La funzione Anti Ransomware utilizza la tecnologia di individuazione comportamentale (BDS) di Seqrite, che analizza il comportamento dei programmi in tempo reale. Questo aiuta a individuare e bloccare minacce come i ransomware. Come un vero e proprio livello di protezione aggiuntivo, questa caratteristica esegue il backup dei vostri dati in una location sicura: questo renderà possibile il ripristino dei file in caso di attacco ransomware.

La funzione Anti Ransomware di Seqrite è più efficace e avanzata di altri tool anti-ransomware.

- » Individuazione in base alle firme: permette l'individuazione dei ransomware già conosciuti che provano a entrare nel sistema tramite email infette, dispositivi USB o altri sistemi infetti nella rete.
- » Monitoraggio proattivo del sistema contro infezioni da nuovi ransomware: monitora le attività dei file scaricati i cui componenti potrebbero tentare un potenziale attacco ransomware.
- » Motore di individuazione comportamentale: analizza in tempo reale il comportamento dei programmi, così da poterli bloccare prima che producano qualsiasi danno.
- » Strumento di Backup& Restore integrato: lo strumento di backup e restore esegue proattivamente il backup di tutti i dati più importanti in una location sicura. Questi file possono essere ripristinati in caso di attacco da ransomware.



DATA LOSS PREVENTION

Arresta la fuga di dati all'interno o all'esterno dell'organizzazione regolando i canali di trasferimento dati quali dispositivi rimovibili, la condivisione di rete, applicazioni web, servizi online, stampa dello Screen e Appunti. Permette anche di monitorare i dati in base alla loro natura. I seguenti canali possono essere regolati attraverso DLP:

- » Possono essere monitorati file di Office, file grafici, file di programmazione e altri.
- » Possono essere sorvegliati dati confidenziali come i dati relativi alle carte di credito e i file personali.
- » Può essere implementato un dizionario personalizzato definito dall'utente. Inoltre possono essere creati avvisi istantanei e report

Per una trattazione più specifica del DLP, fare riferimento a questo documento <http://www.seqrite.it/dlp>



MONITORAGGIO ATTIVITA' FILE

Verifica i file riservati in modo da monitorare azioni sospette, quali la copia, la rinomina o l'eliminazione di file. In questo modo, le minacce esterne o interne possono essere bloccate e inoltre possono essere monitorate le perdite di dati riservati. Tutti i file che vengono trasferiti alle unità locali, unità rimovibili o unità di rete possono così essere sorvegliati.

Il Monitoraggio Attività File è uno strumento prezioso per la revisione di tutti i file che si muovono all'interno e all'esterno della rete e anche per l'individuazione di tutte le azioni volte contro i file riservati di ogni tipo all'interno di un'organizzazione. L'amministratore può specificare i percorsi delle cartelle da escludere dal monitoraggio.



GESTIONE RISORSE

Fornisce una visione dettagliata e cumulativa riguardo alla configurazione hardware e software di ogni endpoint. Gli amministratori possono facilmente vedere dettagli come la configurazione degli hardware, le informazioni di sistema, gli aggiornamenti installati e le modifiche hardware/software per ogni sistema. Vengono inviate notifiche alla email configurata ogni qual volta che, in ogni sistema, avviene una modifica hardware/software.

- » Per esempio, se in un computer si aumenta la RAM viene inviata una notifica, così come al rilevamento di nuovi dispositivi hardware aggiunti/rimossi e per modifiche avvenute all'hardware. Ciò consente agli amministratori di essere informati su tutto quello che c'è da sapere per ogni endpoint in qualsiasi momento.



GESTIONE PATCH

Strategia di gestione delle patch centralizzata per rimediare con successo alle vulnerabilità di sicurezza. Consente agli amministratori IT di verificare e installare le patch mancanti per le applicazioni Microsoft installate sugli endpoint aziendali. Un approccio semplice e centralizzato per garantire che tutte le patch siano installate al fine di ridurre i rischi di sicurezza e ottimizzare la produttività della rete.



ANTI-PHISHING

Gli attacchi di phishing originati da codici dannosi provenienti da Internet sono bloccati prima che possano entrare nella rete e diffondersi.



PROTEZIONE DALLO SPAM

Esegue la scansione della posta in arrivo negli endpoint in cerca di spam, tentativi di phishing o email inaspettate che provano a insinuarsi attraverso le difese della rete.



PIATTAFORMA ROAMING

La piattaforma roaming di Seqrite è una soluzione basata sul cloud che consente alle imprese di restare connesse e gestire gli endpoint in qualsiasi momento, anche quando gli endpoint sono fuori dalla rete locale aziendale. Con l'aiuto di questa funzione gli amministratori della rete possono essere sempre a conoscenza dello stato della rete e eseguire facilmente le seguenti attività sugli endpoint non collegate alla rete:

- » Controllare lo stato di conformità
- » Applicare policy di sicurezza
- » Scansionare in cerca di rischi per la sicurezza
- » Avviare il tune-up per migliorare la performance
- » Applicare service pack
- » Visualizzare notifiche e report
- » Reindirizzare i client roaming



IDS / IPS

Difesa avanzata contro attacchi provenienti da varie fonti, quali gli attacchi di tipo Port Scanning, Distributed Denial of Service (DDoS) e altri. Questo rilevamento aumenta il livello di sicurezza del sistema dalle intrusioni indesiderate.

- » Prevenzione dalle intrusioni – Blocca le attività di rete di maleintenzionati che tentano di sfruttare le vulnerabilità del software delle applicazioni installate.
- » Prevenzione attacchi Port Scanning – In sostanza, un attacco di tipo Port Scanning consiste nell’invio di un messaggio ad ogni singola porta trovata. In base alla risposta ricevuta l’attacco determina se la porta è in uso e se può essere indagata ulteriormente per scoprirne la vulnerabilità. La funzione blocca i tentativi degli intrusi volti ad attaccare qualsiasi porta aperta nella rete.
- » Prevenzione attacchi DDoS– DDoS è un tipo di attacco DoS in cui più sistemi compromessi – che di solito vengono infettati da malware - prendono come bersaglio un altro sistema, sovraccaricandolo di richieste e mandandolo in blocco. Seqrite



FIREWALL INTELLIGENTE

Blocca l’accesso non autorizzato alla rete aziendale. Permette di personalizzare le regole impostandole su diversi livelli, basandosi sul traffico di rete osservato. Gli amministratori possono anche configurare delle eccezioni per indirizzi o porte IP specifici.

I tre livelli di personalizzazione del Firewall sono:

- » Basso – In configurazione di tipo Basso il firewall permette l’accesso a tutti in entrata e in uscita.
- » Medio – Permette tutto il traffico in uscita, ma blocca il traffico in entrata.
- » Alto – Blocca tutto il traffico, sia quello in uscita sia quello in entrata, escluse le eccezioni indicate

» Blocca tutto - Blocca tutto il traffico in entrata e in uscita

Questa funzione dà anche la possibilità di configurare eccezioni alle regole del firewall. Per esempio, se la configurazione firewall è impostata sul livello Alto, si può consentire ugualmente la connessione a un determinato indirizzo IP o a una porta specifica.



SICUREZZA WEB

Blocca malware infetti impedendo l'accesso a siti web dannosi o di phishing che potrebbero minacciare gli endpoint presenti all'interno della rete. Previene le minacce trasferite attraverso siti web che ospitano codici maligni quando si accede a Internet.

- » Protezione Navigazione – Contrasta gli attacchi trasferiti attraverso i siti web maligni.
- » Protezione Phishing – Esegue la scansione delle pagine web mentre si naviga per intercettare attività fraudolente e proteggere da attacchi di phishing.



WEB FILTERING

Consente il blocco di particolari categorie di siti web (es. social network, siti di intrattenimento, ecc.) o siti web specificati dall'utente per limitare l'accesso al web e aumentare la produttività.

- » Filtra rapidamente e con precisione milioni di siti web per più di 40 diverse categorie quali criminalità, violenza, pornografia,
- » Permette di gestire l'accesso degli utenti a Internet. Abbatte il tempo sprecato su siti di social network, media, streaming, ecc.
- » Gli amministratori possono ugualmente consentire l'accesso a determinati siti web che appartengono a categorie bloccate creando un elenco di esclusione. Ad esempio, se le categorie dei social network e delle chat sono bloccate, comunque l'amministratore può consentire l'accesso a Facebook.



CONTROLLO APPLICAZIONI

Intere categorie di applicazioni possono essere autorizzate o meno per poter essere eseguite all'interno della rete. Questa caratteristica offre anche la flessibilità per aggiungere determinate applicazioni a una lista già esistente di categorie non autorizzate.

- » Permette di autorizzare o meno categorie di applicazioni.
- » Applicazioni personalizzate che non esistono tra le applicazioni bloccate possono essere aggiunte in un secondo momento.
- » Fornisce una vasta panoramica di tutte le applicazioni (autorizzate o non autorizzate) installate in rete.



AGGIORNAMENTO

I computer in rete possono essere aggiornati da una postazione centrale ed anche in un momento specifico.



GESTIONE POLICY DI GRUPPO

Possono essere definiti gruppi diversi di client all'interno della rete e possono essere definite policy per ogni gruppo.



RIMOZIONE ANTIVIRUS DI TERZE PARTI

Se, durante l'installazione del client di EPS, viene individuata un'altra soluzione antivirus, ne verrà avviato l'uninstaller oppure sarà automaticamente disinstallata. L'installazione di Seqrite EPS non procederà fino a quando il precedente antivirus non sarà disinstallato dal sistema.



SCANSIONE EMAIL

Esegue la scansione delle caselle di posta elettronica per proteggere da spam, attacchi phishing e messaggi di posta elettronica non desiderati. Permette la creazione di Whitelist e di Blacklist e dispone di una funzione di auto-apprendimento.



NOTIFICHE EMAIL

Questa funzione invia notifiche agli indirizzi email o i numeri di telefono preconfigurati.

- » Queste notifiche avvisano gli amministratori su una serie di eventi critici come ad esempio il rilevamento di virus, tentativi di accesso di un dispositivo non autorizzato, la data di scadenza della licenza, ecc.



TUNEUP

Questa caratteristica migliora le prestazioni dei sistemi dei computer presenti nella rete, effettuando la pulizia dei file spazzatura ed eliminando le voci di registro non valide.

- » Tuneup può essere eseguito su tutti gli endpoint dal Server Endpoint Security.
- » La manutenzione può anche essere programmata in data e orari specifici.



SCANSIONE VULNERABILITA'

Questa funzione scansiona le vulnerabilità conosciute delle applicazioni installate e dei sistemi operativi in rete. Accresce le misure di sicurezza contro le vulnerabilità conosciute e protegge contro le violazioni della sicurezza da varie minacce.

- » Effettua la scansione di vulnerabilità in applicazioni come Adobe, Mozilla, Safari, Oracle, ecc.
- » Invia notifiche riguardanti i sistemi operativi non aggiornati sui computer interni alla rete.



REPORT

Questa funzione permette di generare report grafici e tabellari partendo da un livello più generale fino a dettagli più approfonditi.

- » I report possono essere esportati e salvati in vari formati come PDF e CSV.
- » I report possono essere programmati secondo requisiti personalizzabili.
- » I report possono essere inviati automaticamente a determinati indirizzi email predefiniti.

ALTRE FUNZIONI

Altre funzioni presenti nelle versioni client di Quick Heal sono integrate anche in Seqrite Endpoint Security 6.0.

- » Impostazioni Behavior Detection System – Queste impostazioni rilevano minacce sconosciute
- » Impostazioni Safe Mode Protection – Queste impostazioni aiutano ad evitare l'accesso non autorizzato ai computer quando sono in modalità provvisoria.

Certificazioni:



Comparazione Versioni

Funzionalità	Versioni			
	Business	Total	Suite	Educational
Protezione IDS/IPS	✓	✓	✓	✓
Firewall	✓	✓	✓	✓
Antiphishing	✓	✓	✓	✓
Protezione Navigazione	✓	✓	✓	✓
Notifiche eMail	✓	✓	✓	✓
Scansione Vulnerabilità (VS)	✓	✓	✓	✓
Roaming Client	✓	✓	✓	✓
Antispam	✓	✓	✓	✓
Web Security	✓	✓	✓	✓
Controllo Dispositivi Avanzato	✓	✓	✓	✓
Gestione Attività	✓	✓	✓	✓
Controllo Applicazioni	X	✓	✓	X
Tuneup	X	✓	✓	X
PC2Mobile	X	✓	✓	X
Monitoraggio Attività File	X	✓	✓	X
Gestione Patch	X	✓	✓	X
DLP (Data Loss Prevention)	X	X	✓	X

Requisiti di Sistema

I requisiti di sistema per Seqrite Endpoint Security Server sono i seguenti:

Requisiti generali

Componenti	Requisiti
Processore	1 GHz 32-bit (x86) or 64-bit (x64) Intel Pentium o superiore
RAM	2 GB – 4 GB
Spazio in hard disk	4800 MB
Display	1024 x 768 in modalità 256 colori
Web browser	<ul style="list-style-type: none">• Internet Explorer 7, 8, 9, 10, o 11• Google Chrome 45, 46, o 47• Mozilla Firefox 38, 39, o 40

Nel caso di più di 25 client, Seqrite suggerisce di installare EPS Server e Patch Management server sul sistema operativo Windows Server

Per più di 500 client, Seqrite raccomanda inoltre:

- Un Web server dedicato (IIS)
- Processore 2 GHz o superiore
- 4 GB RAM o superiore

Sistemi operativi compatibili

Seqrite Endpoint Security server può essere installato con uno qualsiasi dei sistemi operativi seguenti:

- » Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- » Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- » Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- » Microsoft Windows 7 Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- » Microsoft Windows Vista Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- » Microsoft Windows XP 32-bit SP3, 64-bit SP1 and SP2 / Professional Edition (32-bit / 64-bit)
- » Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- » Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- » Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- » Microsoft Windows »Server 2012 R2 Standard / Datacenter (64-bit)
- » Microsoft Windows SBS 2011 Standard / Essentials
- » Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- » Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- » Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- » Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)



Software aggiuntivi necessari per il server EPS

Seqrite EPS server necessita sia di Microsoft IIS Web sia di Microsoft NET Framework 4.0 sul sistema del computer.

Web Server	Requisiti
IIS	IIS Versione 10 su Windows 10
	IIS Versione 8.5 su Windows 8.1 e Windows Server 2012 R2
	IIS Versione 8.0 su Windows 8 e Windows Server 2012
	IIS Versione 7.5 su Windows 7 e Windows Server 2008 R2
	IIS Versione 7.0 su Windows Vista e Windows Server 2008
	IIS Versione 6.0 su Windows Server 2003
	IIS Versione 5.1 su Windows XP SP3

L'Installer di EPS installerà i componenti IIS necessari.

Requisiti Java Runtime Enviroments (JRE)

I Requisiti per eseguire l'installazione attraverso la pagina web, la notifica di installazione e la funzionalità di aggiunta del dispositivo come di cui sotto:

Versione OS	Requisiti	JRE
32-bit	32-bit	JRE 7, JRE 8
64-bit	32-bit	32-bit JRE 7, 32-bit JRE 8
	64-bit	64-bit JRE 7, 64-bit JRE 8

Requisiti di Sistema per Seqrite EPS Client

Componenti	Requisiti
Processore	1 GHz 32-bit (x86) o 64-bit (x64) per Windows Vista o successivi
RAM	1 GB
Spazio in hard disk	3200 MB
Web browser	Internet Explorer 5.5 or later

Seqrite Endpoint Security client può essere installato con uno qualsiasi dei sistemi operativi seguenti:

- » Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
- » Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)
- » Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
- » Microsoft Windows 7 Home Basic / Home Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)

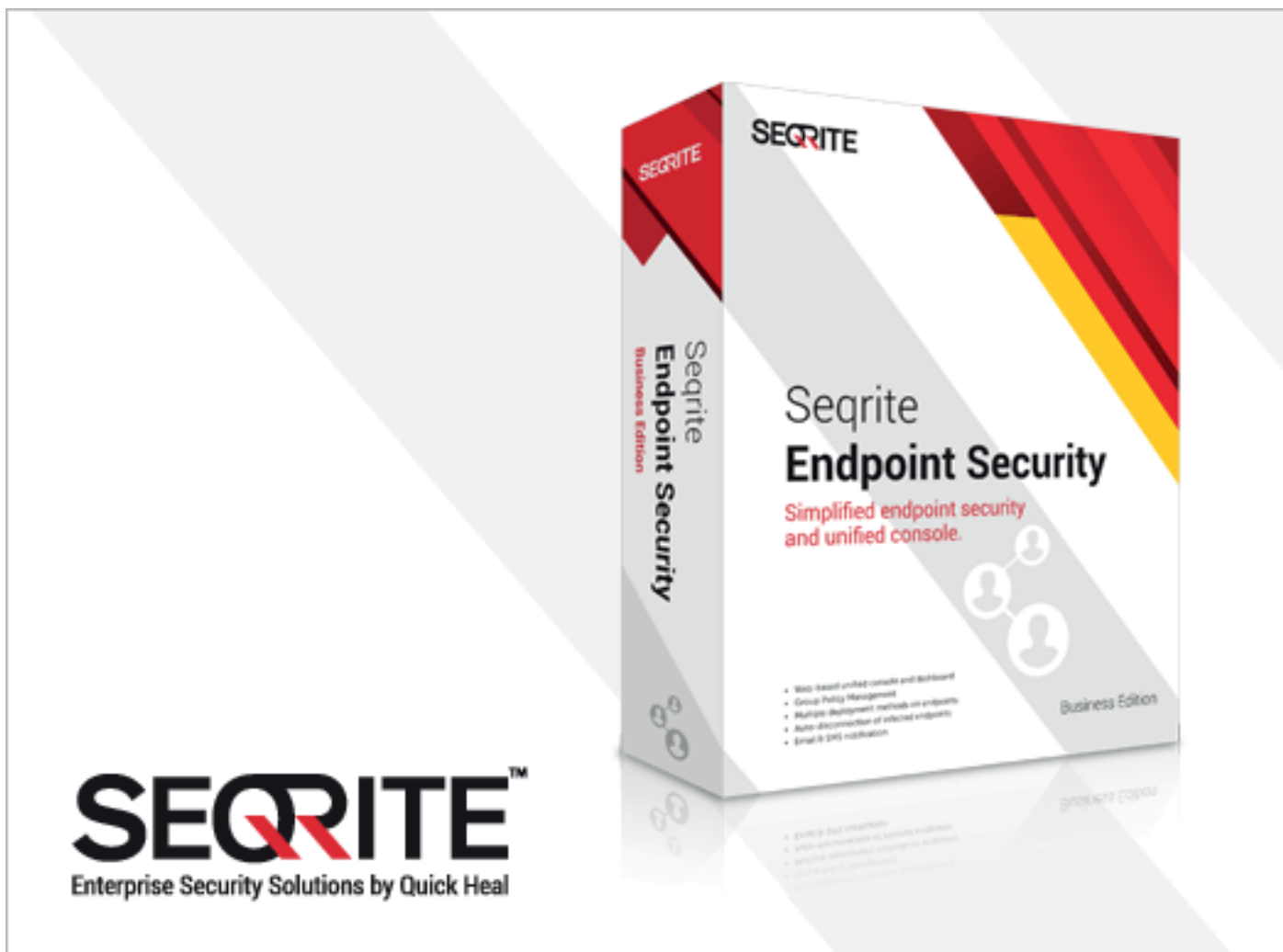
- » Microsoft Windows Vista Home Basic / Home Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- » Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit)
- » Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- » Microsoft Windows MultiPoint Server 2012 Standard (64-bit)
- » Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
- » Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
- » Microsoft Windows SBS 2011 Standard / Essentials
- » Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
- » Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
- » Microsoft Windows Server 2003 R2 Web / Standard / Enterprise /Datacenter
- » Microsoft Windows Server 2003 Web / Standard / Enterprise (32-bit/64-bit)
- » Microsoft Windows 2000 SP 4 Professional / Server / Advanced Server

Requisiti Minimi di Sistema per Endpoint Mac:

Componenti	Requisiti
MAC OS	Mac OS OS X, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11
Processore	Intel o compatibili
RAM	512 MB
Spazio in hard disk	1200 MB

Requisiti Minimi di Sistema per OS Linux:

Componenti	Versione OS Linux	Requisiti
Linux OS	32-bit	<ul style="list-style-type: none"> • BOSS 6 • RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8 • Fedora 14, 18, 19, 20, 21 • openSUSE 11.4, 12.2, 12.3 • Linux Mint 13, 14, 15, 16, 17.3 • Ubuntu 10.10, 11.4, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10 e 15.04 • CentOS 6.3, 6.4, 6.5
	64-bit	<ul style="list-style-type: none"> • RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 7.0, 7.1, 7.2 • Fedora 14, 18, 19, 20, 21 • openSUSE 11.4, 12.1, 12.2 • SUSE Linux 11.00, 12.00 • Linux Mint 13, 14, 15, 16, 17.3 • Ubuntu 10.10, 11.4, 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, and 15.04 • CentOS 6.3, 6.4, 6.5
Processore		Intel o compatibile
RAM		512 MB
Spazio in hard disk		300 MHz o superiore
Memoria		1200 MB



SEQRITE™
Enterprise Security Solutions by Quick Heal

Headquarter

Quick Heal Technologies (P) Ltd.

603, Mayfair Tower II, Wakdewadi, Shivajinagar, Pune - 411 005, India.

Tutti i diritti di proprietà intellettuale, inclusi marchi, loghi e copyright sono di proprietà dei rispettivi proprietari.. Copyright © 2014 Quick Heal Technologies (P) Ltd. Tutti i diritti riservati.

Distributore per l'Italia

somart

www.s-mart.biz