SEQRITE

Seqrite
Data Loss Prevention (DLP)

Mantieni il controllo totale sui dati che ti appartengono

www.seqrite.it

Panoramica

Il volume di informazioni distribuite digitalmente è in continua crescita e le organizzazioni devono adeguarsi. Il fenomeno BYOD (Bring Your Own Device) e l'uso sempre più diffuso di servizi di archiviazione basati sul cloud contribuiscono ulteriormente a rendere sempre più alto il rischio di fuoriuscita di dati, un pericolo che sta sempre più sensibilizzando gli amministratori IT e i Chief Security Officer delle imprese.

Seqrite Data Loss Prevention (DLP) consente alle aziende di combattere le minacce di furto dei dati regolandone e controllandone il trasferimento tramite unità removibili, condivisioni di rete, servizi e applicazioni online ed anche tramite la funzione print screen e la copia in appunti.
Inoltre DLP dà la possibilità di monitorare i dati sensibili in base a natura e tipo. In questo modo le aziende possono controllare il flusso di ogni genere di file (documenti Office, grafici, di programmazione, confidenziali) e realizzare raccolte personalizzate definite dall'utente per il monitoraggio dei dati.

Come installare Seqrite DLP

Le funzione Seqrite Data Loss Prevention (DLP) è integrata nella versione Enterprise Suite. E' invece disponibile come opzione aggiuntiva nelle versioni Business e Total.

» Per gli utenti di Seqrite Endpoint Security Business Edition:

Per aggiungere la funzionalità DLP è necessario disporre (o eventualmente richiedere l'aggiunta) del pack Conformità.

» Per gli utenti di Seqrite Endpoint Security Total Edition

Gli utenti Seqrite Endpoint Security Total Edition possono aggiungere la funzionalità DLP subito, poichè il pack Conformità è già incluso all'interno della versione.

Caratterische di Seqrite DLP

Protezione Dati all'interno delle Imprese

Con Seqrite DLP, le aziende ora possono accuratamente controllare il flusso dei propri dati in tempo reale e rafforzare le policy di sicurezza.

Tutto ciò le aiuta ad avere una visione sui metodi di accesso ai dati e sul trasfermento delle informazioni. E possono raggiungere questo obiettivo senza interrompere il processo produttivo. DLP consente di contrastare il furto di dati tramite l'utilizzo di fonti interne (email in uscita, messaggistica istantanea, applicazioni online, unità USB) e allo stesso tempo da cause esterne (infezioni da Worm, Trojan e altre minacce).

- DLP blocca tutti i canali tramite i quali possono prendere forma potenziali furti di dati (unità removibili, reti di condivisione, screen capture, appunti, applicazioni online, archiviazioni in cloud e allegati email).
- DLP riconosce i documenti Office in base alla loro origine, o alle regole stabilite dall'amministratore. Ciò consente di prevenire che le informazioni sensibili vengano copiate attraverso applicazioni online o tecnologie di condivisione.
- DLP provvede a fornire notifiche regolari e tempestive agli utenti in modo da sensibilizzarli e renderli più consapevoli riguardo ai criteri di sicurezza stabiliti dall'azienda per cui essi lavorano.

Visibilità e Gestione Centralizzata

La console di gestione centralizzata di Seqrite Endpoint Security permette alle aziende di gestire le policy di sicurezza tramite la funzione DLP su ogni singolo computer della rete aziendale, anche se gli endpoint sono situati in sedi diverse. DLP permette anche di disabilitare la visibilità di determinati dati sensibili all'interno dell'azienda. E' anche possibile accedere a report dettagliati.

Seqrite DLP consente un monitoraggio in tempo reale e una facile gestione tramite la console centralizzata centrale per prevenire, monitorare e gestire efficacemente gli incidenti relativi al furto o perdita di dati.

Tutti questi aspetti danno la possibilità alle organizzazioni di raccogliere facilmente statistiche sugli accessi ai dati. Queste informazioni dettagliate possono essere poi condivise con revisori esterni, amministratori di rete ed esperti interni o esterni all'azienda.

Diminuzione della Complessità e Basso Costo di Gestione

Seqrite DLP facilita la gestione e riduce i costi della sicurezza nelle imprese integrando le funzioni DLP nelle già esistenti soluzioni Endpoint Security. Offerta come risorsa aggiuntiva del pacchetto, DLP permette di tenere al sicuro dalla visibilità pubblica i dati confidenziali e bloccare potenziali furti informatici attraverso il trasferimento non autorizzato di dati con unità USB, allegati email e altre applicazioni online. Consente alle imprese di impostare una prevenzione sulla fuoriuscita di informazioni in modo economico e senza un impiego di tempo superiore a quello normalmente richiesto per la gestione della sicurezza.

Vantaggi Chiave di Seqrite DLP

- Prevenzione dinamica da furto o perdita di dati riservati custoditi all'interno dell'azienda.
- Ampia visione di tutte le azioni promosse per tentare di trasferire file confidenziali fuori dall'azienda.
- Notifica fuoriuscite dati non autorizzate attraverso fonti come unità removibili, condivisoni di rete, email e altro.
- Garantisce che i dati confidenziali non fuoriescano dall'azienda.

Suddivisione dei Dati Aziendali

Le imprese necessitano di strategie di prevenzione efficaci e immediate contro la perdita di dati e per questo motivo la divisione tra differenti tipi di dati e la valutazione delle loro particolari caratteristiche è la prima attività fondamentale.

Trasfermento Dati attraverso Applicazioni Online

Seqrite DLP consente di filtrare il traffico in rete per individuare contenuti sensibili specifici che stanno attraversando i canali di comunicazione. Questi dati in movimento vengono analizzati passivamente al fine di ispezionarli e prevenirne la fuoriuscita. Frammenti di codice sono analizzati in vari protocolli come email e messaggistica.

Accesso o Transferimento Dati attraverso Dispositivi Fisici

DLP è in grado di avvisare ogni volta che un informazione importante viene trasferita su un dispositivo fisico. Possono essere tracciati tutti i file che vengono copiati o trasferiti tramite applicazioni o unità USB. Seqrite DLP garantisce che i dati trasferiti e sensibili siano riconosciuti e che l'amministratore di rete sia avvisato tempestivamente.

Benefici Aziendali nell'uso di Seqrite DLP

- Mantiene al sicuro gli archivi di dati relativi a proprietà intellettuali per mantenerne i benefici competitivi e reputazionali.
- Previene la fuga accidentale o intenzionale di dati attraverso attraverso canali come email, unità USB, applicazioni online e altro.
- Identifica gli archivi dati rispetto alle policy aziendali per ridurre rischi futuri e rafforzando i punti deboli rispetto alla protezione dei dati fondamentali
- Permette alle imprese di essere preparate per future modifiche e rinnovi delle policy. In questo modo la conformità viene mantenuta anche se cambiano le circostanze.

» Fornisce report in tempo reale sui tentativi di trasferimento non autorizzato di dati come promemoria utili a rafforzare la consapevolezza dei dipendenti sull'attenzione rivolta dall'impresa sulla protezione dei dati.

Seqrite DLP può anche essere usata insieme ad altre funzioni – Controllo Dispositivi Avanzato. Con l'aiuto di questa funzione, i client di Endpoint Security client possono ottenere i seguenti benefici:

» Configurare le policy di accesso per più di 25 differenti tipi di dispositivi

» Bloccare l'accesso alla rete di dispositivi non verificati

» Prevenire infezioni Autorun attraverso dispositivi sconosciuti

Headquarters

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

s-mart

www.s-mart.biz