SEQRITE

SEQRITE
Data Loss Prevention

www.seqrite.it

Panoramica

Al giorno d'oggi un volume crescente di dati aziendali è in formato digitale. Le aziende devono contemporaneamente accelerare i processi aziendali. Se poi aggiungiamo il ricorso crescente al cloud e l'aumentare del lavoro remoto / smart working, il rischio di perdita di dati, dati leak o data breach, si fa sempre più pressante per le aziende di qualsiasi dimensione.

Seqrite DLP consente alle aziende di minimizzare il rischio di perdita dei dati regolando i canali di trasferimento dei dati come le unità rimovibili, le condivisioni di rete, le web app e servizi online, gli screen e gli appunti. Il DLP consente inoltre di monitorare i dati sensibili in base alla loro natura e tipologia. In questo modo, le aziende possono monitorare i file di Office, i file grafici, i file di programmazione, i dati riservati e implementare dizionari personalizzati definiti dall'utente per il monitoraggio dei dati.

Caratteristiche di Seqrite DLP

Protezione dei dati all'interno dell'azienda

Con Seqrite DLP, le aziende possono ora monitorare accuratamente e in tempo reale gli eventi riguardanti i dati aziendali e applicare politiche di sicurezza gestite a livello centrale. Questo aiuta le aziende a monitorare le modalità con cui i dipendenti accedono e trasferiscono informazioni senza limitare o ostacolare la produttività dei dipendenti. La funzionalità DLP consente alle aziende di proteggere i dati aziendali da minacce provenienti da fonti interne come le e-mail in uscita, la messaggistica istantanea, le applicazioni web e le chiavette USB. Non solo: DLP può bloccare i data breach dovuti a worm, trojan e altre minacce.

- DLP blocca tutti i canali attraverso i quali può avvenire una potenziale perdita di dati. Questi includono, ma non solo, le unità rimovibili, la condivisione di rete, la cattura dello schermo, gli appunti, le applicazioni basate sul web, i servizi di archiviazione cloud e gli allegati di posta elettronica.
- Il DLP identifica i documenti Office in base alla loro origine o in base alle regole impostate dagli amministratori IT. In questo modo si evita che le informazioni sensibili vengano copiate tramite le applicazioni web o altre tecnologie di condivisione.
- Il DLP fornisce notifiche regolari e tempestive agli utenti, in modo da rafforzare la conformità ai criteri di sicurezza preimpostati e regolare il comportamento degli utenti in base alla strategia scelta dall'azienda.

Gestione centralizzata e visibilità

La console di gestione centralizzata di SEQRITE Endpoint Protection consente alle aziende di elencare le varie politiche di sicurezza DLP e i report su numerosi endpoint, anche in sedi fisiche diverse. DLP offre anche l'ulteriore vantaggio di ridurre i costi rendendo la gestione della sicurezza il più semplice possibile e di consentire la visibilità dei dati sensibili in tutta l'azienda. I clienti aziendali possono inoltre accedere a report e audit di sicurezza dettagliati tramite l'infrastruttura di sicurezza e la console di gestione integrate. L'integrazione con Seqrite DLP consente inoltre alle aziende di monitorare gli eventi in tempo reale e di disporre di una postazione centralizzata per la gestione efficace degli incidenti.

Tutti questi aspetti offrono inoltre alle aziende la possibilità di raccogliere facilmente statistiche sull'accesso ai dati. Queste informazioni dettagliate possono essere condivise con revisori dei dati, amministratori di rete e stakeholder di alto livello all'interno o all'esterno dell'organizzazione stessa.

Riduzione della complessità e dei costi di implementazione

Seqrite DLP razionalizza la complessità dell'infrastruttura di sicurezza e minimizza il costo della protezione dei dati all'interno dell'azienda, integrando le funzionalità DLP con la soluzione Endpoint Protection esistente. Come pacchetto aggiuntivo a basso consumo di risorse, DLP consente di ottenere visibilità massima sui dati confidenziali e di bloccare la potenziale perdita di dati attraverso canali di trasferimento quali dispositivi USB, allegati di posta elettronica e altri canali web. Inoltre, il componente aggiuntivo DLP non richiede alcun hardware aggiuntivo. La soluzione DLP integrata di Seqrite consente alle aziende di migliorare la sicurezza per prevenire la fuga di dati a un prezzo minimo e senza ulteriori investimenti di tempo rispetto a quelli necessari per la soluzione tradizionale di sicurezza degli endpoint.

Principali vantaggi di Seqrite DLP

- Previene in modo proattivo la fuga di dati o il furto di proprietà intellettuale all'interno della tua azienda.
- Garantisce una visione di insieme e "dall'alto" della sicurezza dei dati e delle azioni che mettono a repentaglio la riservatezza dei dati.
- Fornisce notifiche immediate sulle fughe di dati non autorizzate attraverso unità rimovibili, condivisioni di rete, e-mail e altro ancora…
- I dati sensibili e confidenziali, nonché quelli riservati, non usciranno dalla tua azienda.

Segregazione dei dati aziendali

Le aziende hanno bisogno di strategie DLP efficaci e, a tal fine, è fondamentale separare i diversi tipi di dati e valutarne le caratteristiche peculiari.

Trasferimento dei dati attraverso applicazioni web

Seqrite DLP consente alle aziende di analizzare il traffico di rete per individuare i contenuti sensibili attraverso i canali di comunicazione stabiliti. Questi dati in movimento vengono analizzati passivamente o tramite inline proxy per analizzarli e impedire la fuga di dati importanti all'esterno dell'azienda.

Dati trasferiti tramite dispositivi fisici

I protocolli DLP emettono alert ogni volta che vengono eseguite azioni sui dati sensibili e riservati sui singoli endpoint dell'azienda. Sarà così possibile tracciare tutti i file copiati o trasferiti tramite applicazioni o dispositivi USB. Seqrite DLP assicura alle aziende di ricevere avvisi per ogni trasferimento non autorizzato di dati sensibili.

Piattaforme supportate

Workstation Windows supportate:

- Microsoft Windows 11
- 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/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows Vista Home Basic/ Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
- Microsoft Windows XP Home (32-bit) / Professional Edition (32-bit / 64-bit)
- Microsoft Windows Server 2022 Standard / Datacenter / Essentials
- Microsoft Windows Server 2019 Standard / Datacenter / Essentials
- Microsoft Windows Server 2016 Standard / Datacenter (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 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)

Workstation Mac supportate:

- Mac OS X 10.9, 10.10, 10.11, macOS 10.12, 10.13, 10.14, 10.15, 11 e 12

  Nota - Sui sistemi Mac è supportato solo il monitoraggio degli appunti e delle applicazioni.

Quick Heal Technologies Limited

Quick Heal Technologies Limited | Distribuito in Italia da s-mart.biz
seqrite.it | cs@s-mart.biz