

Cyberoam Endpoint Data Protection

Data Protection
& Encryption



Device
Management

Application
Control



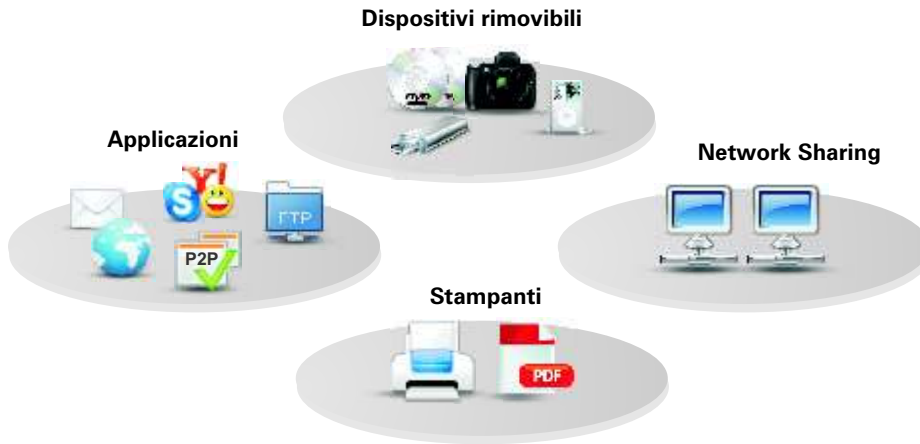
Asset
Management

Proteggi i tuoi dati. Proteggi le tue risorse.

Overview - Perdita accidentale dei dati

Oltre il 50% degli episodi di perdita dati ha origine agli end point. Le informazioni sensibili, quali i dati dei clienti, i segreti industriali, la proprietà intellettuale e i documenti legali, sono disponibili presso gli endpoint per l'utilizzo da parte degli utenti autorizzati. Tuttavia, l'accesso semplificato da parte degli utenti a dispositivi portatili come USB, DVD, MP3, ad applicazioni per il file sharing e la messaggistica istantanea e altro possono facilmente causare una perdita accidentale di tali informazioni. Oggi come oggi, il costo dei dati persi/sottratti a un'azienda di qualsiasi tipo è enorme e causa una riduzione del volume d'affari pari al 65% dei costi di violazione, secondo una ricerca. Da qui l'esigenza, da parte delle stesse aziende, di impedire che presso gli endpoint si verifichino condivisioni non autorizzate o si verifichino perdite accidentali ad opera dei dipendenti.

Dove si verifica la perdita accidentale dei dati



Inoltre, visti la presenza di un gran numero di utenti e filiali, l'incremento del numero di attacchi complessi e dei bug e le vulnerabilità conseguenti, è necessario implementare un sistema di gestione delle risorse (Asset Management) centralizzato e automatizzato presso gli endpoint stessi. La sicurezza degli endpoint per la protezione dei dati e degli asset aziendali è divenuta, quindi, un fattore cruciale e cresce sempre di più il numero di aziende che impiegano suite dedicate per la protezione dei dati in grado di assicurare controlli a livello di singolo utente nella gestione dei dati.

Endpoint Data Protection di Cyberoam

L'Endpoint Data Protection di Cyberoam protegge gli endpoint delle aziende dalla perdita accidentale di dati (data leakage) sfruttando controlli delle policy basati sull'identità e sui gruppi, la codifica, le copie nascoste, il logging, la reportistica e l'archiviazione. Cyberoam consente la protezione dei dati e la gestione degli assetti attraverso quattro moduli semplici da installare e utilizzare:



Data Protection and Encryption



Application Control



Device Management



Asset Management

Detti moduli consentono alle aziende di limitare l'accesso solo a dispositivi, applicazioni e destinatari affidabili nel momento in cui si condividono i dati. Il modulo di Asset Management sgrava il personale tecnico di molte incombenze, riducendo il numero di richieste di supporto dovute ad attacchi causati da malware, al rendimento, oppure a esigenze di system recovery. La semplicità di gestione dell'Endpoint Data Protection di Cyberoam permette alle aziende di prevenire la perdita di dati, migliorare la sicurezza e la produttività dei dipendenti, nonché di gestire efficacemente gli assetti informatici, preservando la flessibilità del business e rispettando i requisiti di sicurezza e le norme di legge.

Benefici

- Previene la perdita accidentale dei dati presso l'endpoint
- Estende la sicurezza dei dati oltre la rete fisica
- Accresce la produttività dei dipendenti bloccando le applicazioni non autorizzate
- Semplifica la gestione dell'infrastruttura di IT
- Riduce il costo totale di possesso (TCO) dell'infrastruttura di IT
- Riduce la penetrazione di malware grazie alla gestione delle patch
- Soddisfa le norme di sicurezza grazie alla gestione assetti informatici
- Riduce la responsabilità legale e le perdite nel business

Endpoint Data Protection di Cyberoam: i moduli



Data Protection and Encryption

L'accesso di utenti interni a documenti sensibili, o il trasferimento accidentale o doloso di file rappresentano le principali cause di perdita di dati. Grazie al modulo di protezione e codifica dei dati di Cyberoam, le aziende possono controllare i dati trasferiti a dispositivi rimovibili e stampanti, o veicolati come allegati a e-mail o messaggi istantanei. È possibile controllare le operazioni sui documenti, la loro condivisione ed effettuare copie nascoste nel momento in cui si compiono azioni specifiche su un documento. Le aziende possono eliminare il rischio di perdita di dati a causa dello smarrimento di dispositivi rimovibili codificandone i dati e i file nel momento in cui vengono trasferiti al dispositivo stesso. Inoltre, è possibile garantire che i dati nei dispositivi siano accessibili solo agli utenti autorizzati attraverso impostazioni basate sull'utente che permettono la decodifica dei file encrypted.

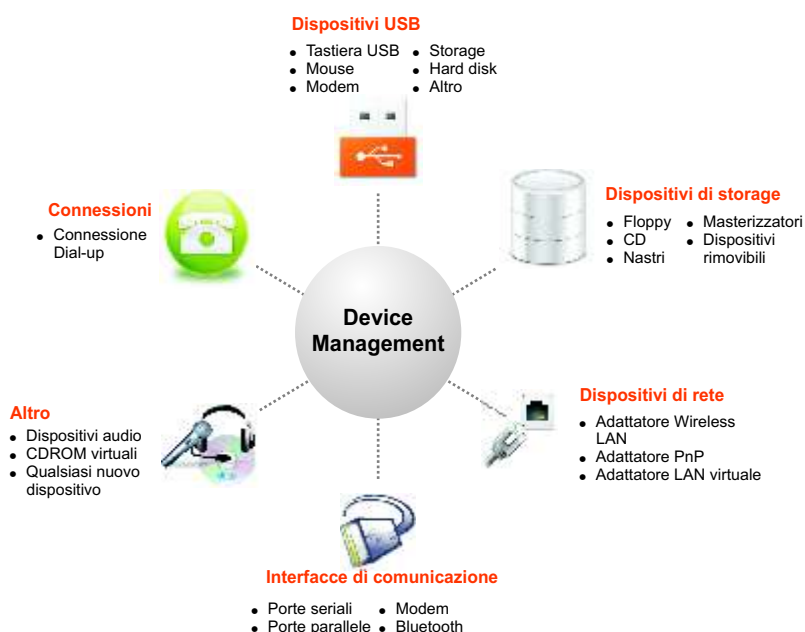
Caratteristiche

- Blocca il trasferimento dei file in base al nome o all'estensione in:
 - Dispositivi rimovibili
 - Applicazioni per chat, e-mail e file sharing
 - Reti condivise
 - Stampanti
- Specifica i permessi di lettura-scrittura per dispositivi rimovibili inseriti in white list.
- Offre la codifica e decodifica per file e dispositivi rimovibili.
- Controlla il trasferimento dei file via e-mail e sistemi di messaggistica istantanea in base a nome, estensione o dimensione del file, all'interno o all'esterno della rete.
- Controlla l'accesso alle stampanti.
- Crea copie nascoste dei file durante la creazione, la modifica, il trasferimento, o la stampa.
- Permette di personalizzare gli allarmi diretti agli amministratori e gli avvisi per gli utenti.
- Genera report relativi alle attività di accesso, utilizzo, modifica, trasferimento e cancellazione di file.



Device Management

I dispositivi attraverso cui è più facile perdere dei dati sono proprio quelli rimovibili, a causa delle ridotte dimensioni, della considerevole capacità di storage e della difficoltà nel tenerne traccia. Il modulo Device Management (gestione dispositivi) di Cyberoam consente alle aziende di tenere traccia e controllare tutti i dispositivi rimovibili presso il rispettivo endpoint. Le aziende possono consentire l'accesso solo ai dispositivi inseriti in white list, come dispositivi USB, porte di storage, dispositivi di rete/Wi-Fi, di interfaccia per la comunicazione, dial-up e altri.



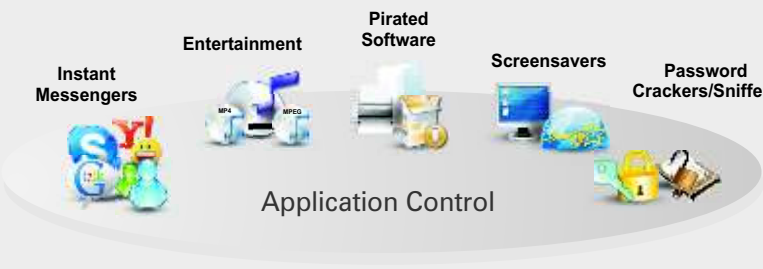
Caratteristiche

- Consente/blocca l'accesso a dispositivi rimovibili riservati
- Implementa la policy di controllo dei dispositivi, anche se offline
- Imposta una scadenza alla quale disabilitare automaticamente le policy



Application Control

Laddove non vengono stabilite regole per l'utilizzo delle applicazioni, si possono verificare accessi ad applicazioni non autorizzate, illegali o causate da malware che comportano la perdita di dati, di produttività, responsabilità legali e interruzioni nei collegamenti di rete. Il modulo per il controllo delle applicazioni (Application Control) consente alle aziende di prevenire la perdita di dati proprio permettendo o negando l'accesso ad applicazioni specifiche. I log delle applicazioni consentono di rilevare quali applicazioni sono state utilizzate presso gli endpoint e per quanto tempo, in tutta l'azienda.



Caratteristiche

- Implementazione granulare di controlli secondo policy predefinite per chat, webmail, giochi, file sharing, FTP e altro.
- Implementazione delle policy, anche se offline.
- Impostazione degli avvisi e del loro livello in caso di accessi non autorizzati alle applicazioni.
- Personalizzazione dei messaggi di avviso per gli utenti.
- Impostazione di una scadenza per disabilitare automaticamente le policy.



Asset Management

Gli uffici distribuiti e l'incremento degli attacchi dovuti a malware espongono le aziende a più alti livelli di rischio, mettendo il personale informatico in una sorta di stato di allarme continuo. Il modulo per la gestione degli assetti per Windows di Cyberoam consente alle aziende di semplificare la gestione della propria infrastruttura IT grazie ad operazioni centralizzate e automatizzate sugli assetti hardware e software comprendenti inventario, patch e aggiornamenti. Ciò permette di controllare i costi relativi all'hardware e al software, riducendo l'incidenza del malware e rispettando i requisiti di conformità in termini di sicurezza.

Caratteristiche

- Inventario dell'hardware e del software.
- Dislocazione, configurazione, storico delle versioni e delle informazioni per gli assetti hardware e software.
- Gestione automatizzata delle patch, aggiornamento del Sistema Operativo Microsoft e delle sue applicazioni.
- Gestione centralizzata.
- Installazione remota di pacchetti Microsoft Software Installation (MSI).

Prodotti Cyberoam

Cyberoam offre soluzioni complete per la vostra sicurezza tramite i seguenti prodotti:

- Unified Threat Management
- Central Console Cyberoam
- iView Cyberoam
- VPN SSL
- Endpoint Data Protection



Numeri Verdi:

USA : +1-877-777-0368

India : 1-800-301-00013

APAC/MEA : +1-877-777-0368

Europa : +44-808-120-3958

Copyright © Elitecore Technologies Ltd. Tutti i diritti riservati. Il marchio e il logo Cyberoam sono marchi registrati della Elitecore Technologies Ltd. La Elitecore fa del proprio meglio per fornire sempre informazioni accurate, ma non assume alcuna responsabilità in caso di inaccuratezza o incomplezza delle stesse, né considera la presente una dichiarazione vincolante. La Elitecore si riserva il diritto di cambiare, modificare, trasferire o rivedere la pubblicazione senza preavviso.



Distributore ufficiale per l'Italia:
Horus Informatica
Tel: (+39) 02 33510135
Fax commerciale: (+39) 02 33510199
Email: commerciale@horus.it
www.horus.it

