DeviceLock®

PREVENZIONE DLP CONTRO LA SOTTRAZIONE DEI DATI, INTEGRATA CON LE GROUP POLICY, PER LA PROTEZIONE DI INFORMAZIONI RISERVATE

Perché prendere in considerazione una Soluzione DLP per gli Endpoint

Per quanto si cerchi di proteggere le vostre informazioni con firewall e password, queste possono sempre scivolare via dalle mani. La fuga di dati può avere origine da impiegati inconsapevoli o da utenti malintenzionati che copiano dati riservati o informazioni sensibili dai loro PC e MAC su flash memory, smartphones, macchine fotografiche, PDA, DVD/CD o su qualsiasi altro supporto di memoria esterna portabile.
La sottrazione di dati potrebbe avvenire anche attraverso messaggi di posta elettronica come pure con l'uso di applicazioni di instant messanging, web form, social network, servizi di file sharing o sessioni telnet.
Interfacce wireless come Wi-Fi, bluetooth e infrarossi o la sincronizzazione degli smartphone offrono altre opportunità per la sottrazione dei dati.
Analogamente i PC possono essere infettati da malware dannosi o keylogger che catturano quanto digitato dell'utente e inviano attraverso canali SMTP o FTP i dati sottratti nelle mani di criminali.
Mentre queste minacce possono eludere sia le soluzioni convenzionali di sicurezza di rete che i controlli nativi di Windows/Apple OS X, la soluzione DeviceLock DLP (Data Leak Prevention) è capace di intercettarle.
DeviceLock DLP rinforza le policy di protezione e di auditing riconoscendo sia il contesto sia il contenuto del flusso di dati trasferiti sui canali di scambio delle informazioni.
La capacità d'intercettazione dei contenuti offerta dal modulo indipendente DeviceLock Discovery previene la perdita dei dati archiviati nei computer aziendali, nelle condivisioni di rete e nei sistemi di archiviazione. DeviceLock rilascia anche un DLP Virtuale che estende la prevenzione a una varietà di sessioni, macchine virtuali e dispositivi BYOD che utilizzano architetture di virtualizzazione per applicazioni e desktop.

Sicurezza DLP centrata su Contesto & Contenuto

La miglior prevenzione contro la fuga dei dati inizia dal controllo contestuale - esso agisce bloccando o permettendo flussi di dati attraverso il riconoscimento dell'utente, i tipi di dati, l'interfaccia, il dispositivo o il protocollo di rete, la direzione del flusso, lo stato dei media o della crittografia SSL, la data e l'ora, etc.

Molti scenari richiedono altresì un più profondo livello di attenzione che il solo contesto non riesce a soddisfare. Ad esempio collaboratori affidabili possono maneggiare dati sensibili che contengono informazioni di natura personale (PII), finanziaria, medica, "Riservata" o di proprietà intellettuali (IP). I responsabili della sicurezza possono lavorare con maggiore dimestichezza e migliore aderenza alla sicurezza aziendale, assoggettando il flusso di dati, prima di consentirne il trasferimento e che potrebbe contenere uno degli elementi prima citati, all'analisi del contenuto e a regole di filtrazione.

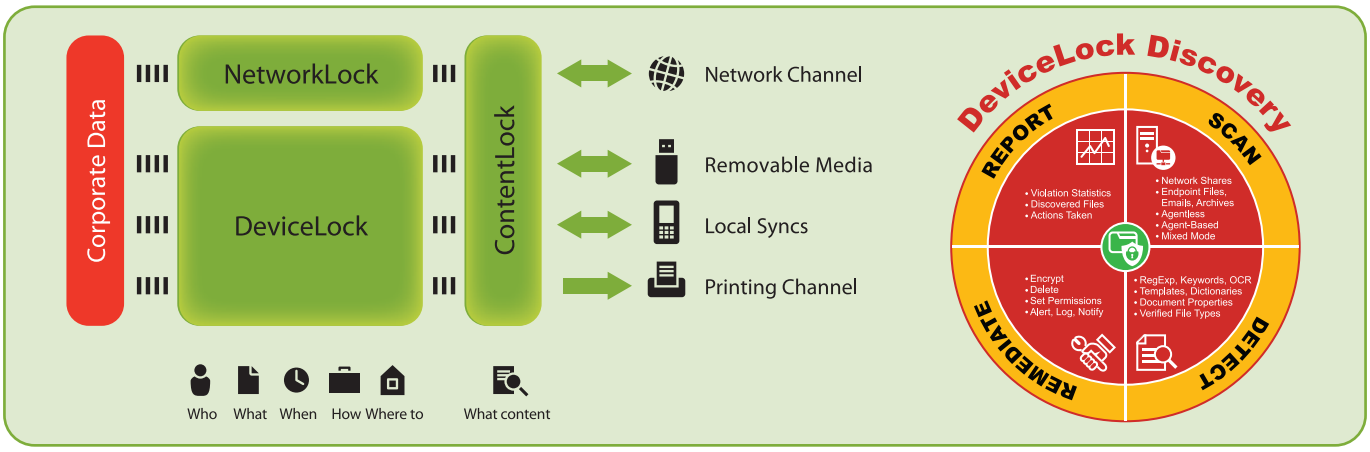
DeviceLock DLP assicura sia il controllo contestuale sia quello dei contenuti in una ottica di massima prevenzione al minor costo. Il suo motore multistrato d'ispezione e intercettazione fornisce un fine controllo granulare su una gamma completa di percorsi per scenari sia di "data-in-use" sia di "data-in-motion" per garantire che i dati definiti come sensibili non possano scappare. DeviceLock applica l'analisi e la filtrazione dei contenuti sui dati che gli endpoint scambiano con media rimovibili, dispositivi Plug-n-Play, stampanti, email, web, Skype, sessioni di IM e altre comunicazioni di rete. Inoltre l'attenzione ai contenuti è fondamentale per la prevenzione "data-at-rest" - una critica funzione DLP che DeviceLock fornisce con il modulo Discovery per ispezionare i dati residenti nei computer, nelle condivisioni di rete e nei sistemi di archiviazione aziendali.

Con DeviceLock, gli amministratori della sicurezza possono incrociare con precisione i diritti di accesso con la funzione aziendale ricoperta dall'utente per quanto riguarda il trasferimento, la ricezione e la memorizzazione dei dati sui dispositivi connessi ai computer aziendali o attraverso i protocolli di rete. Il risultato è un ambiente informatico sicuro che consente all'utente di svolgere senza impedimenti tutte le azioni consentite, mentre blocca ogni tentativo accidentale o intenzionale di eseguire operazioni non autorizzate. DeviceLock permette un approccio immediato alla gestione DLP consentendo agli amministratori della sicurezza l'uso delle Microsoft Active Directory® Group Policy Objects (GPO) e delle console snap-in di DeviceLock. Le policy DLP definite a livello centrale nelle Active Directory sono automaticamente trasferite agli agenti presenti sugli endpoint Windows e Apple, fisici o virtuali, per una loro costante applicazione.

Gli amministratori di DeviceLock controllano a livello centrale i file log, le copie shadow, gli avvisi e analizzano i dati trasferiti dagli utenti su tutti i tipi di periferiche, sulle porte e attraverso le comunicazioni di rete dei computer aziendali. Inoltre, l'agente installato sui computer è in grado di rilevare e bloccare i keylogger hardware per impedire il furto di password o di altre informazioni proprietarie o personali. L'agente DeviceLock installato sull'endpoint utilizza uno spazio minimo del disco e della memoria, è trasparente per l'utente e utilizza una modalità che non consente la sua manomissione neanche nel caso che l'utente sia un amministratore locale.

DeviceLock Discovery estende la protezione delle informazioni oltre il "data-in-use" e "data-in-motion" riferite agli endpoint, scansionando e ispezionando il contenuto dei file presenti nei server Windows, negli archivi dati accessibili in rete e nelle periferiche dell'ambiente IT aziendale per identificare e bonificare violazioni delle policy "data-at-rest" di archiviazione.

Con il suo controllo granulare del contesto completato dalla filtrazione dei contenuti sui più vulnerabili canali di scambio dei dati, DeviceLock DLP riduce significativamente il rischio di fuga d'informazioni sensibili dai computer aziendali, dovuta a semplice negligenza o dolo. DeviceLock DLP è una piattaforma di sicurezza che offre modelli di policy di protezione e promuove l'adeguamento alle norme aziendali di gestione delle informazioni, così come alle disposizioni ufficiali HIPAA, Sarbanes-Oxley, e PCI DSS.

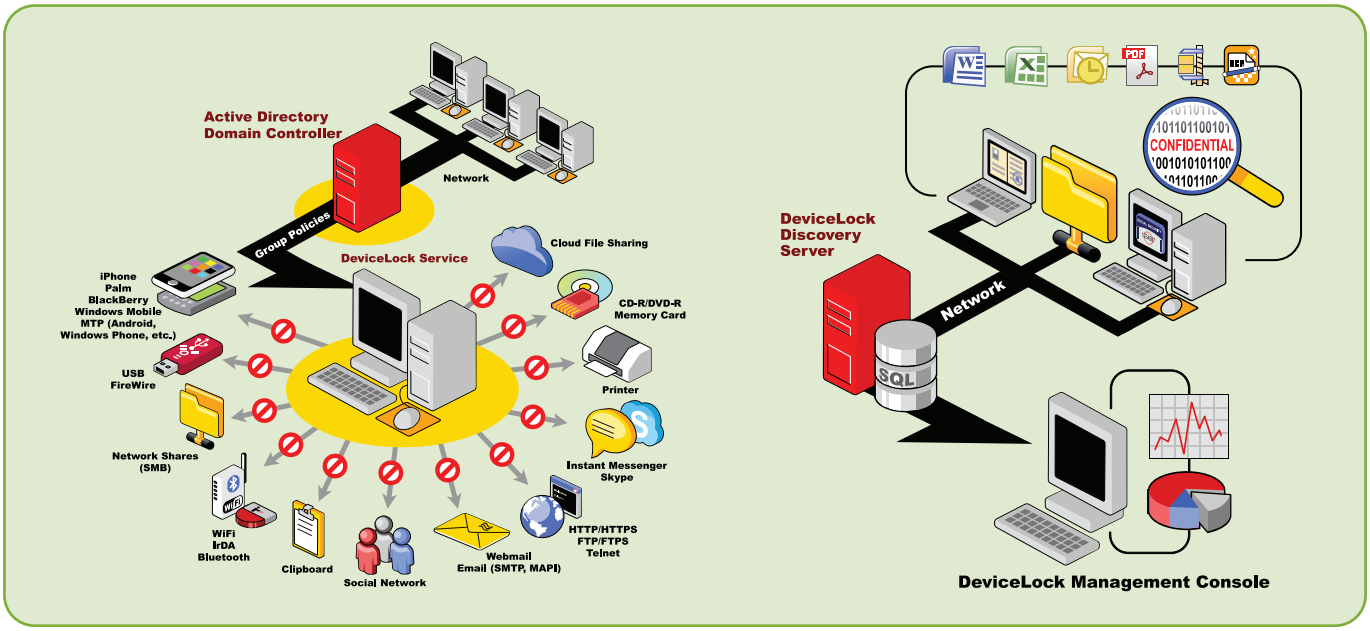


La funzionalità del modulo di base DeviceLock rinforza le policy di accesso ai dispositivi. Il modulo NetworkLock amplia il controllo del contesto ai protocolli e alle applicazioni utilizzati nelle comunicazioni di rete. Il modulo ContentLock fornisce regole avanzate di filtrazione dei contenuti per tutti i canali gestiti da DeviceLock e NetworkLock. DeviceLock Discovery individua i documenti con contenuti sensibili, abilita azioni di protezione e bonifica e può avviare procedure d'incident management inviando in tempo reale avvisi ai sistemi aziendali di Security Information ed Event Management (SIEM).

Struttura modulare e Licenze

DeviceLock Endpoint DLP Suite è costituita da un insieme modulare di componenti complementari e funzionalmente specifici che possono essere approvvigionati separatamente o combinati tra loro per soddisfare le distinte esigenze di sicurezza. I nostri clienti hanno a disposizione uno strumento sicuro per l'aggiornamento delle funzionalità di DeviceLock e la possibilità di espandere la propria sicurezza con la scelta di nuovi moduli. Allo stesso modo, i nuovi clienti possono spostarsi in modo incrementale da una soluzione base a una più completa implementando le funzionalità in accordo con le necessità e la disponibilità di budget.

- Il modulo **DeviceLock® Core** include, per tutti i canali locali dei computer protetti, la completa funzionalità dei controlli di contesto e l'archiviazione sia dei file log, che dei file shadow come pure degli avvisi. Esso gestisce i dispositivi periferici e le porte, le azioni di copia/incolla, gli smartphone e i palmari, i dispositivi abilitati MTP (Android, Windows Phone etc.), dispositivi a controllo virtuale remoto, printscreen e la stampa dei documenti. DeviceLock Core è il cuore della piattaforma, ne permette la gestione centralizzata e assicura la gestione amministrativa di tutti gli altri moduli funzionali compresi nella DeviceLock Endpoint DLP Suite.
- Il modulo **NetworkLock™** svolge tutte le funzioni di controllo del contesto per le comunicazioni di rete come web, email e altro. Realizza il riconoscimento e il controllo selettivo di protocolli e applicazioni, messaggi e ricostruzione di sessioni con estrazione di file, dati e parametri così come la registrazione di eventi, degli avvisi e dati shadowing.
- Il modulo **ContentLock™** implementa la filtrazione dei contenuti dei file trasferiti da e verso i supporti rimovibili, i dispositivi Plug-n-Play, così come di vari oggetti nelle comunicazioni di rete ricostruite e gestite da NetworkLock. Questi comprendono e-mail, instant message, web form, allegati, scambi sui social media e trasferimento di file.
- **DeviceLock® Discovery** è un modulo funzionale separato. Consente alle organizzazioni di migliorare la visibilità e il controllo sui dati riservati "data-at-rest" archiviati nel proprio ambiente IT al fine di proattivamente prevenire la sottrazione degli stessi e uniformarsi alle norme e specifiche di sicurezza aziendali. Eseguendo automaticamente la scansione sulle condivisioni di rete, sui sistemi di archiviazione e sugli endpoint Windows all'interno del proprio network (o anche esternamente utilizzando l'Agente DeviceLock), DeviceLock Discovery localizza la posizione di documenti con contenuto sensibile e ne esegue l'eventuale bonifica per rimetterli in sicurezza. DeviceLock Discovery può anche avviare le procedure d'incident management inviando in tempo reale avvisi ai sistemi aziendali di Security Information, Event Management (SIEM) e/o di data security personnel.
- **DeviceLock® Search Server (DLSS)** è un altro modulo addizionale con il quale sono indicizzati ed eseguite ricerche full-text dei dati presenti nel database centrale in cui sono archiviati i file log e shadowing. DLSS è progettato per rendere più precise, meno laboriose e più veloci le impegnative attività di auditing della sicurezza, di analisi degli incidenti e di analisi forense.
- **Licensing.** Il modulo DeviceLock Core è indispensabile per qualsiasi configurazione di DeviceLock Endpoint DLP e può implementarsi con i restanti moduli opzionali NetworkLock, ContentLock e DeviceLock Search Server. DeviceLock Discovery, che può essere impiegato indipendentemente da qualsiasi altro modulo DeviceLock, comprende Discovery Server e l'Agente Discovery può altresì integrarsi con qualsiasi combinazione dei moduli di DeviceLock Endpoint DLP della versione 8 o successive sfruttando le pre-impostate capacità di filtrazione dei contenuti dell'Agente DeviceLock. Questa struttura modulare del prodotto e il flessibile sistema di licensing consentono ai clienti DeviceLock di implementare in modo conveniente e graduale le diverse funzionalità. Si può iniziare con le funzioni per il controllo delle porte e dei dispositivi offerte dal modulo base, aggiungere in modo incrementale le funzionalità specifiche dei restanti moduli e infine estendere la soluzione al modulo di discovering delle informazioni "data-at-rest" sensibili in accordo con la crescita delle necessità e dei requisiti di sicurezza.



Con DeviceLock DLP le imprese possono mettere in sicurezza qualsiasi numero di endpoint sfruttando la sua integrazione nativa con le Active Directory e Windows Group Policy Management Console. DeviceLock Discovery scansiona automaticamente i dati residenti nelle condivisioni di rete, nei sistemi di archiviazione e nei computer presenti all'interno e all'esterno del proprio network aziendale.

Caratteristiche e Vantaggi di DeviceLock

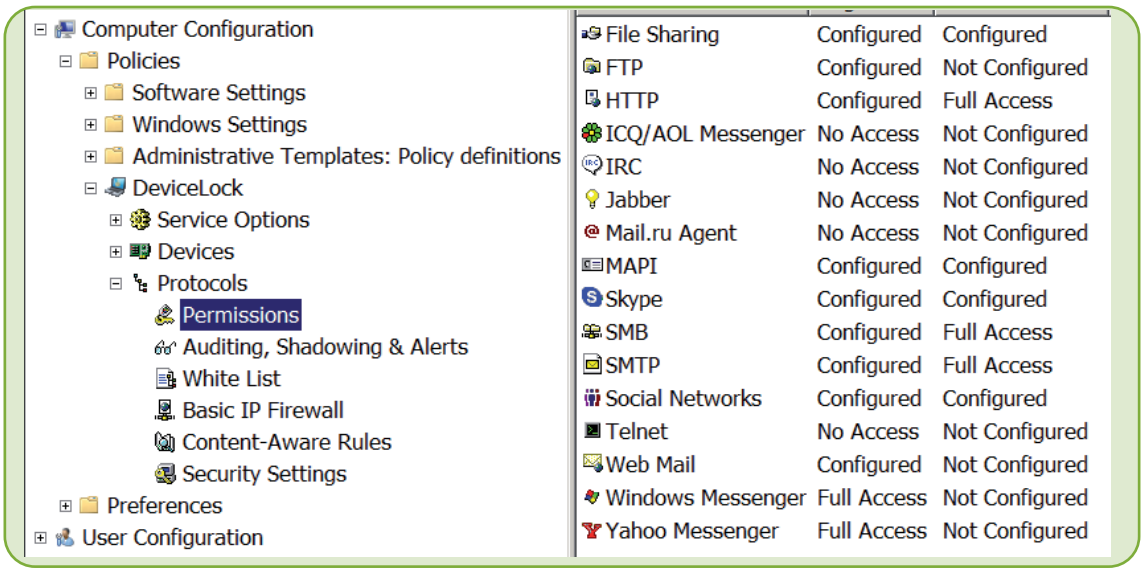
DeviceLock DLP assicura essenziali capacità di filtrazione dei contenuti e di discovery, il controllo fattivo delle comunicazioni di rete qualificandosi a livello industriale al top dei migliori controlli basati sul contesto per i quali gli accessi alle porte locali e ai dispositivi periferici sono gestiti centralmente dagli amministratori di DeviceLock

Integrazione con Active Directory Group Policy.
La console principale di DeviceLock si integra direttamente con l'interfaccia Microsoft di Management Console (MMC) Active Directory (AD) Group Policy. Di conseguenza gli amministratori IT operano con interfacce in stile MMC di cui hanno assoluta dimestichezza e non devono installare e apprendere nuove interfacce o dispositivi proprietari per gestire centralmente tutti i computer. La semplice console MMC snap-in di DeviceLock presente sul computer dell'amministratore che gestisce le Group Policy consente l'integrazione immediata con le console Group Policy Management (GPMC) o Active Directory Users & Computers (ADUC) evitando qualsiasi script, modelli ADM o modifiche degli schemi già impostati. Gli Amministratori possono gestire dinamicamente le policy sia in ambiente Windows sia in ambiente Apple OS X contemporaneamente ad altre operazioni automatiche di Group Policy. Nel caso non si utilizzassero le Group Policy DeviceLock impiega classiche console in stile Windows e una web console per gestire centralmente gli agenti su Novell, LDAP o IP "workgroup" per computer Windows e Apple OS X. I modelli di policy in formato XML possono essere condivisi tra tutte le console DeviceLock.

Whitelist dei Dispositivi. Tra i molteplici livelli di controllo dei dispositivi Windows e Apple OS X supportati da DeviceLock, i livelli basati su dispositivo USB e su ID del dispositivo sono gestiti con un approccio di tipo whitelist. In questo modo l'Amministratore può inserire nella whitelist specifiche periferiche USB aziendali e DeviceLock permetterà l'accesso a esse solo agli utenti o gruppo di utenti esplicitamente autorizzati. Tutti gli altri dispositivi e utenti non elencati risulteranno dunque bloccati per default. È inoltre possibile inserire nella whitelist un dispositivo in modo univoco utilizzando il suo ID e bloccare altri dispositivi del medesimo modello a patto che il produttore lo abbia dotato di un preciso identificativo.

Eccezioni alle Policy di Sicurezza.
DeviceLock utilizza anche una potente applet che l'utente può lanciare per richiedere in modo sicuro l'accesso temporaneo a un dispositivo USB altrimenti bloccato dalle policy locali di DeviceLock … anche se il laptop Windows si trova all'esterno del network aziendale. Lo specifico dispositivo USB è montato e selezionato dall'applet che genera un codice univoco legato a dispositivo, computer e utente che ne ha fatta richiesta. Il codice deve essere sottoposto a valutazione e approvazione da parte di un Amministratore di DeviceLock. Se approvato allora, viene generato per l'utente un nuovo codice dispositivo che ne autorizza l'uso per una durata massima di un mese. La policy di sicurezza originale rimane dunque intatta ma rinforzata dall'utilizzo di questo dispositivo per il periodo stabilito.

Controllo delle Comunicazioni di Rete. Il modulo NetworkLock aggiunge un completo controllo sul contesto delle comunicazioni di rete che avvengono sui computer aziendali come il riconoscimento di protocolli, applicazioni web e di Instant Messenger come Skype. Le comunicazioni email regolari e protette SSL (SMTP, Exchange-MAPI e servizi di web-mail elencati) sono gestite separatamente per messaggio e per allegato. NetworkLock controlla anche gli accessi web e altre applicazioni su base HTTP con la capacità di estrarre il contenuto da sessioni HTTPS crittografate. Applicazioni web e accessi web a social network, file sharing e servizi webmail sono protetti separatamente dal controllo HTTP per facilitarne la configurazione mentre possono essere inseriti in whitelist i siti, gli URL, gli indirizzi email e gli ID mittenti/destinatari per gli utenti autorizzati. Consulta la sezione Specifiche di Prodotto per un elenco dei servizi web mail, social networks, file sharing e instant messenger supportati da NetworkLock.



Con NetworkLock è possibile impostare le autorizzazioni per l'accesso degli utenti alle comunicazioni di rete come Web mail/SMTP/MAPI, social network, instant messaging, trasferimento file e altro

Filtrazione dei contenuti. Questa funzionalità estende le capacità dei moduli DeviceLock e NetworkLock oltre i meccanismi di sicurezza basati sul contesto. Il modulo ContentLock può filtrare il contenuto dei file copiati su unità rimovibili e altri dispositivi di archiviazione Plug-n-Play, utilizzando le clipboard, i dati in stampa perfino altri dati che potrebbero altrimenti essere celati negli screenprint, in file grafici o immagini nidificate nei documenti. ContentLock filtra anche i dati di oggetti e sessioni concernenti le attività sulle comunicazioni di rete.
Questi includono e-mail, accessi al web e altre popolari applicazioni basate su HTTP come servizi webmail, social network, servizi di file sharing, instant messenger, allegati, web form/post e trasferimenti file FTP. Il motore di analisi dei testi può estrarre informazioni di testo da più di 160 formati file e tipi di dati e dunque applicare un efficace e affidabile metodo di filtrazione dei contenuti basato su modelli di Regular Expression (RegExp), dizionari e parole chiave specifiche (HIPAA, PCI etc.) proprietà dei documenti, tipi di file e altro. Questi modelli possono essere modificati abbinando condizioni numeriche e operatori Booleani (AND/OR/NOT) per massimizzarne il controllo.

Description	Type	Action(s)	Applies To	Device Type(s)	Send Alert	Log Event	Profile
Executable	File Type Detection	Deny: Write, Write Encrypted, Read, Read Encrypted	Permissions	Removable	Enabled	Enabled	Regular
HIPAA ICD9	Keywords	Deny: Read	Permissions	Optical Drive	Enabled	Enabled	Regular
Password Protected	Document Properties	Allow: Write, Write Encrypted	Shadowing	Removable	Disabled	Disabled	Regular
Phone Numbers and Emails	Complex	Deny: Clipboard Outgoing Text, Clipboard Incoming T...	Permissions	TS Devices	Disabled	Enabled	Regular
US Social Security Number	Pattern	Deny: Write, Write Encrypted, Read, Read Encrypted	Permissions	Removable	Disabled	Enabled	Offline
US Social Security Number	Pattern	Deny: Print	Permissions, Shadowing	Printer	Enabled	Disabled	Regular

Description	Type	Action(s)	Applies To	Protocol(s)	Send Alert	Log Event	Profile
Bank ABA	Keywords	Allow: Outgoing Messages, Outgoing Files	Shadowing	Social Networks	Disabled	Disabled	Regular
Credit Card Number	Pattern	Deny: POST Requests, Outgoing Files, Encrypted PO...	Permissions	HTTP	Enabled	Disabled	Regular
Images, CAD & Drawing	File Type Detection	Deny: Outgoing Files, Encrypted Outgoing Files	Permissions	FTP	Enabled	Disabled	Regular
Password Protected	Document Properties	Allow: Outgoing Messages, Outgoing Files	Permissions, Shadowing	MAPI	Enabled	Enabled	Regular
PCI GLBA	Keywords	Deny: Outgoing Messages, Outgoing Files	Permissions	Skype	Disabled	Enabled	Offline
Phone Numbers and Emails	Complex	Deny: POST Requests, Outgoing Files, Encrypted PO...	Permissions	File Sharing	Enabled	Enabled	Regular
US Phone Number	Pattern	Deny: Outgoing Messages, Outgoing Files	Permissions	Yahoo Messenger	Enabled	Enabled	Regular

Le schermate di configurazione mostrano esempi di alto livello delle regole di gestione dei contenuti per specifici dispositivi (sopra) e per specifici protocolli di rete (sotto). L'intuitiva interfaccia del modulo ContentLock facilita la definizione delle policy di filtrazione per i contenuti.

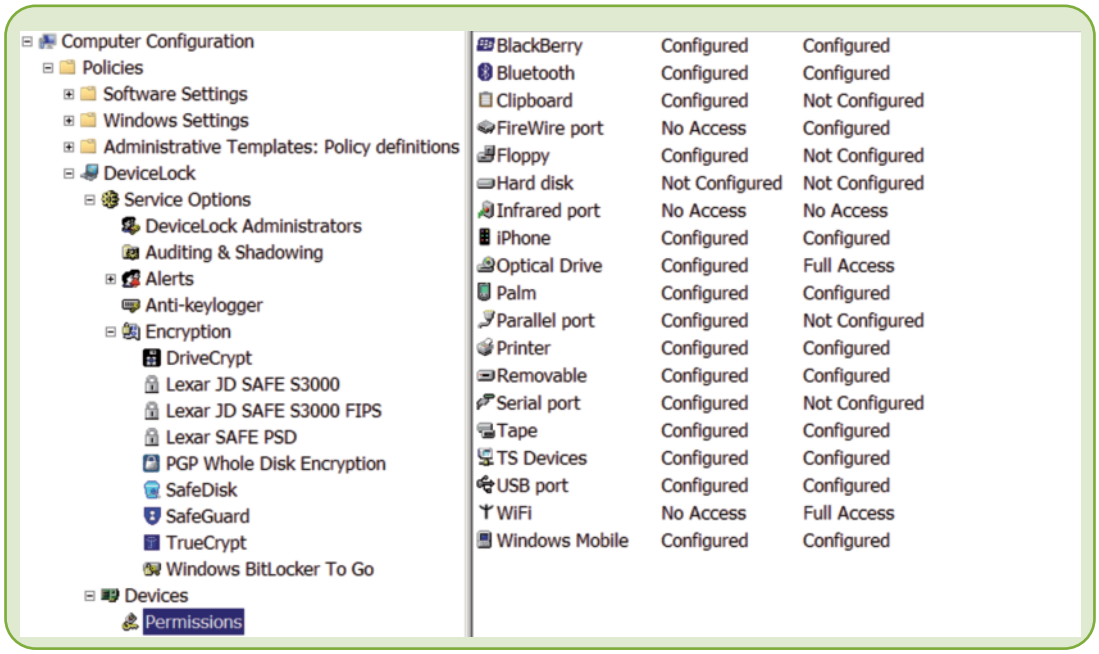
OCR residente. Un motore di riconoscimento ottico dei caratteri (OCR) si accompagna alla filtrazione dei contenuti degli oggetti di natura testuale permettendo l'estrazione e l'ispezione veloce, efficiente e accurata dei testi presenti nelle immagini di documenti e file grafici di diversi formati. Questo efficiente OCR, attivo su più di 25 lingue, utilizza regular expression, dizionari di parole chiavi e altri avanzati metodi per migliorare il riconoscimento individuando e proteggendo le informazioni riservate presentate in forma grafica. L'esclusività di DeviceLock DLP è che il modulo OCR lavora su ciascuno dei suoi componenti applicativi: DeviceLock Agent, DeviceLock Discovery Server e DeviceLock Discovery Agent. Questa architettura OCR distribuita massimizza le caratteristiche complessive della soluzione in quanto gli oggetti grafici archiviati nei pc possono essere scansionati e ispezionati dai moduli OCR residenti localmente. Essa inoltre riduce significativamente il carico sul Discovery Server, come pure riduce il traffico "di scansione" sul network aziendale.

Content Discovery. DeviceLock Discovery migliora la visibilità e il controllo delle informazioni riservate "data-at-rest" archiviate in tutto l'ambiente IT prevenendone la possibile sottrazione e garantendo la conformità con le norme e i requisiti di sicurezza dell'Azienda.
Realizzando automaticamente la scansione dei dati residenti nelle condivisioni di rete, nei sistemi di archiviazione e negli endpoint Windows interni o esterni alla rete aziendale, DeviceLock Discovery individua i documenti con contenuti sensibili o riservati, permette la loro eventuale bonifica e avvia le procedure di Incident Management con avvisi in tempo reale ai sistemi SIEM e al personale della sicurezza. Utilizzando il set completo di funzionalità di ContentLock, che ora comprende anche la funzione OCR, DeviceLock può individuare contenuti testuali in più di 120 formati file e 40 tipi di archivi nidificati, come pure all'interno di immagini in documenti e file grafici.
In funzione della topologia e delle specifiche di rete DeviceLock Discovery può eseguire scansioni nelle modalità senza agente, con agente o mista. La scansione può essere lanciata sui pc, sulle condivisioni di rete e sui sistemi di archiviazione aziendali in modalità manuale o in maniera programmata. L'Agente Discovery di DeviceLock può essere installato e rimosso da remoto sui pc da ispezionare utilizzando DeviceLock Discovery Server in maniera automatica e completamente trasparente. Quando abbinato agli altri componenti DeviceLock DLP, DeviceLock Discovery utilizza la preimpostata capacità degli Agenti di DeviceLock di scansionare i dati archiviati nei computer e nelle condivisioni di rete.

DLP Virtuale per dispositivi BYOD. La caratteristica DeviceLock di Virtual DLP permette la protezione di qualsiasi dispositivo BYOD contro la sottrazione interna delle informazioni quando si utilizzano le più importanti soluzioni e applicazioni di virtualizzazione come Citrix XenApp/XenDesk/Top, Microsoft RDS e VMware Horizon View. Attivo con VDI Host o Terminal Server, DeviceLock avvia controlli DLP remoti di contesto e di contenuto sul dispositivo BYOD creando un agente DLP virtuale che impedisce lo scambio incontrollato delle informazioni verso le periferiche locali, le applicazioni residenti e le connessioni di rete del dispositivo BYOD durante la "sessione" di collegamento. Questo approccio unifica l'attività di DeviceLock DLP per ambienti fisici, virtuali e BYOD.

Controllo Clipboard. DeviceLock consente agli amministratori di bloccare efficacemente la sottrazione di dati fin dalla loro fase embrionale quando gli utenti con azioni di copia-incolla deliberate o accidentali trasferiscono dati non autorizzati tra diverse applicazioni e documenti sul proprio computer attraverso i meccanismi di clipboard e print-screen di Windows. DeviceLock può in maniera selettiva controllare gli accessi degli utenti/gruppi a oggetti di diversi tipi di dati che sono copiati nelle clipboard. Questi tipi comprendono file, testi, immagini, segmenti audio (ad esempio catturati con Windows Sound Recorder) ed anche dati di tipo "non identificato". Inoltre è possibile monitorare e filtrare il contenuto di testi copiati via clipboard. Per consentire il Virtual DLP in una terminal session DeviceLock DLP protegge e filtra in maniera separata e indipendente le operazioni con le clipboard quando reindirizzate a un dispositivo BYOD. Anche le operazioni di screenshot possono essere bloccate per specifici utenti/gruppi prevenendo uno dei vecchi metodi di furto delle informazioni. Queste comprendono il comando PrintScreen da tastiera e il cattura schermo di terze parti. Se gli screenshot sono contestualmente ammessi dalle policy allora l'ispezione OCR del modulo ContentLock può filtrare i contenuti di testo presenti nelle immagini catturate in accordo con le regole DLP.

Controllo Sincronizzazione Locale Smartphone. Gli Amministratori possono utilizzare la tecnologia di sincronizzazione locale brevettata da DeviceLock per impostare in modo granulare l'accesso, l'auditing e le regole di shadowing per i dati che gli smartphone Microsoft Windows Mobile®, Apple iPhone ®/ iPad®/iPod touch® e i palmari Palm® scambiano attraverso la sincronizzazione locale con i pc Windows. Le autorizzazioni sono assegnate con una fine granularità e definiscono quali tipi di dati (file, immagini, e-mail, contatti, calendari, ecc.) utenti e/o gruppi specifici sono autorizzati a sincronizzare tra il PC aziendale e i dispositivi mobili personali, indipendentemente dall'interfaccia di connessione. Riconoscimento della presenza, controllo dell'accesso e log degli eventi per Android®, Windows Phone, altri dispositivi MTP ed anche BlackBerry® sono specificatamente supportati a livello di tipo del dispositivo.



DeviceLock MMC snap-in per Group Policy Management: gli amministratori di DeviceLock hanno il completo controllo centrale agli accessi, audit, shadow, avvisi e alle regole sui contenuti per proteggere i possibili canali di fuga delle informazioni attraverso l'intero dominio gestito dalle Active Directory

Sicurezza delle stampe. DeviceLock pone la stampa locale e di rete degli endpoint sotto uno stretto controllo degli Amministratori. Intercettando le operazioni dello Spooler di stampa, DeviceLock permette agli amministratori di controllare a livello centrale gli accessi alle stampanti e i contenuti dei documenti inviati alle stampanti locali, di rete e virtuali da parte dei PC gestiti da DeviceLock. Inoltre le stampanti connesse via USB possono essere assegnate o per modello o in modo univoco a precisi utenti o gruppi. È possibile registrare gli eventi di stampa, raccogliere e archiviare a livello centrale e in formato PDF lo shadowing delle stampe eseguite, per successive verifiche e analisi.

Sicurezza Endpoint Offline. Gli Amministratori possono definire, per lo stesso utente e in funzione dello stato del laptop rispetto al network, differenti policy di sicurezza per la modalità online e offline. Ad esempio si potrebbe disabilitare il Wi-Fi quando connesso al network via cavo per evitare la sottrazione di dati attraverso il "bridging" di rete e invece abilitare il Wi-Fi quando sconnesso. Oppure, nello stato offline, può essere attivato il modulo NetworkLock per mimare le impostazioni DLP del perimetro di rete o altre condizioni di sicurezza.

Autoprotezione. Una caratteristica configurabile riservata agli "Amministratori di DeviceLock" previene per i sistemi operativi Windows e Apple OS X la manomissione delle impostazioni delle policy locali anche da parte di utenti con privilegi di amministratore locale. Grazie a questa caratteristica solo i ben identificati Amministratori di DeviceLock che lavorano dalla console di DeviceLock oppure dall'Editor delle Group Policy Object (GPO) possono disinstallare o aggiornare l'Agente o modificare le policy di DeviceLock in modo autonomo.

La Modalità Osservatorio di DeviceLock

Spesso DeviceLock è utilizzato in prima battuta per raccogliere e rivedere le informazioni relative agli oggetti che gli utenti stanno trasferendo verso media rimovibili, CD/DVD-ROM, PDA, attraverso Wi-Fi e via email, web form etc. I record di DeviceLock così raccolti (log/shadow) sono utili per comprendere l'attuale livello di esposizione alla non-conformità e possono essere utilizzati per fornire un non-ripudiabile strumento alle verifiche ufficiali di conformità. Quando si scopre che un'informazione è stata sottratta, oppure si è tentato di sottrarla o ancora ne esiste il solo sospetto allora DeviceLock offre gli strumenti corretti per catturare e giuridicamente mettere sotto osservazione gli oggetti e gli eventi a loro associati per essere usati come prove o per avviare azioni correttive o aggiornare le policy dei contenuti.

Log di verifica. La capacità DeviceLock di auditing traccia, per un determinato computer, l'attività dell'utente e dei file verso specifici tipi di dispositivi, porte e protocolli. Può pre-filtrare per utente/gruppo gli eventi da osservare in base a giorno/ora, tipo di file, porta/tipo di dispositivo/protocollo, lettura/scrittura e a eventi autorizzati/bloccati. DeviceLock utilizza il subsystem standard di log degli eventi di Windows o Apple OS X. All'interno del visualizzatore a colonne di DeviceLock i log possono essere estratti per colonna e filtrati con criteri a stringa e operatori jolly per organizzare la vista desiderata dei dati raccolti. I record possono anche essere esportati in diversi formati per essere utilizzati in altre soluzioni di log management e reporting.

Shadowing dei dati. La funzione DeviceLock di shadowing può essere impostata per specchiare tutti i dati copiati su archivi esterni, stampati o trasferiti attraverso porte seriali, parallele e di rete (modulo Network Lock). DeviceLock può anche suddividere le immagini ISO create da masterizzatori CD/DVD/BD nei file originali grazie all'agente presente in DeviceLock Enterprise Server (DLES). Una copia completa dei file può essere salvata per eventuali verifiche forensi. I dati shadow possono essere pre-filtrati per utente/gruppo, giorno/ora, tipo di file e contenuto per meglio selezionare ciò che deve essere catturato e dunque collezionato. Le caratteristiche DeviceLock di auditing e shadowing sono progettate per un uso efficiente delle risorse di trasmissione e archiviazione dei dati comprimendo il flusso e modellando il traffico per impostare la qualità del servizio (QoS), le quote locali e un'ottimale auto-selezione del server DLES.

Agente di Monitoraggio. L'attività degli agenti di DeviceLock Enterprise Server può monitorare in tempo reale i computer Windows remoti controllando lo stato dell'agente DeviceLock sull'endpoint (attivo o meno), la versione, l'integrità e la consistenza delle policy. Dettagliate informazioni, sono riportate sul Monitoring log.

Avvisi. DeviceLock permette la notifica in tempo reale, attraverso l'invio di avvisi di tipo SNMP e SMTP, degli eventi definiti sensibili che gli utenti svolgono sugli endpoint Windows della rete.

Report Dispositivi Plug-n-Play. Il Report PnP consente ad amministratori e ispettori di generare un elenco dei dispositivi USB, FireWire e PCMCIA attualmente e storicamente connessi ai computer selezionati della rete. Il medesimo report permette inoltre il popolamento della whitelist dei dispositivi USB che andranno poi associati, per tipo o per dispositivo univoco, alle policy di accesso di DeviceLock.

Report Grafici. DeviceLock può generare preconfezionati report grafici nei formati HTML, PDF o RTF basati sull'analisi dei dati raccolti come log e shadow da DLES. Questi report, una volta generati, possono essere spediti automaticamente via email a un elenco di responsabili della gestione della sicurezza o dell'uniformità dei dati.

Ricerca di dati. Il modulo opzionale DeviceLock Search Server (DLSS) enfatizza le capacità forensi di DeviceLock indicizzando e permettendo la completa ricerca full-text all'interno dei dati di log e shadow raccolti centralmente. Il modulo DLSS facilita la complessa e pesante attività dei processi di verifica circa la conformità alla sicurezza informatica, l'analisi degli incidenti e l'analisi forense rendendo la ricerca più veloce, più precisa e più conveniente. Il modulo DLSS supporta l'indicizzazione e la ricerca su più di 80 tipi di formati file. Ricerche indipendenti dalla lingua utilizzata necessitano solo di pochi secondi una volta che il dato è stato indicizzato. Per parole e frasi in Inglese, Francese, Tedesco, Italiano, Giapponese, Russo e Spagnolo è automaticamente attivata la filtrazione dei derivati e delle parole di disturbo. DLSS utilizza "all words" (AND) logici con caratteri jolly per perfezionare o espandere le ricerche. Per impostazione i risultati sono ottenuti "per incrocio" mentre sono opzionali "per peso del termine" o "per peso del campo". DLSS supporta anche l'indicizzazione e la ricerca full-text delle stampe per verificare virtualmente tutti i documenti in stampa.

"Dopo mesi di valutazione riconosciamo come DeviceLock rappresenta la soluzione più efficace soprattutto in termini economici per la gestione periferica dei PC aziendali. Si è dimostrata la più interessante proposta tra i controlli di sicurezza informatica presente nei nostri archivi".

Data Security Specialist, University of Alabama at Birmingham Health System

Specifiche di Prodotto

Componenti Strutturali (installabili)

- Agente DeviceLock (Windows e Apple OS X)
- Agente DeviceLock Discovery (Windows)
- DeviceLock Enterprise Server (DLES)
- DeviceLock Content Security Server (Discovery Server, Search Server)
- Console: DeviceLock Group Policy Manager (MMC snap-in/ Microsoft GPMC), DeviceLock Management Console (MMC snap-in), DeviceLock Enterprise Manager, DeviceLock WebConsole w/Apache

Controllo delle Porte

- **Windows:** USB, FireWire, Infrarosse, Seriali, Parallele
- **Mac:** USB, FireWire, Seriali
- **Terminal Session/BYOD:** USB, Seriali

Controllo dei Dispositivi (elenco parziale)

- **Windows:** archivi rimovibili (flash drive, memory card, PC card, eSATA etc.), CD-ROM/DVD/BD, floppy, hard drive, nastri, adattatori WiFi e Bluetooth, Apple iPhone/iPod touch/iPad, Windows Mobile, Palm OS, BlackBerry, dispositivi MTP (come Android e Windows Phone), stampanti (locali, di rete e virtuali), modem, scanner e fotocamere.
- **Mac:** archivi rimovibili, hard drive, CD-ROM/DVD/BD, adattatori Wi-Fi e Bluetooth
- **Terminal Session/BYOD:** drive mappati (rimovibili, ottici, rigidi), dispositivi USB

Controllo Clipboard

- Operazioni di copia/incolla tra le applicazioni Windows
- Operazioni di copia delle clipboard tra OS host e guest
- Trasferimento di dati con clipboard nelle sessioni desktop/ application
- Operazioni con gli screenshot (PrintScreen e applicazioni di terzi)

Controllo Comunicazioni di Rete

- **Email:** SMTP/SMTPS, Microsoft Outlook (MAPI)
- **Web Mail:** AOL mail, Gmail, Hotmail/Outlook.com, GMX.de, Web.de, Yahoo!Mail, Mail.ru, Rambler Mail, Yandex Mail, Outlook WebApp/Access (OWA)
- **Social Network:** Facebook (+API), Twitter, Google+, LinkedIn, Tumblr, MySpace, Vkontakte (+API), XING.com, LiveJournal, MeinVZ.de, StudiVZ.de, Disqus, LiveInternet.ru, Odnoklassniki.ru,
- **Instant Messenger:** Skype, ICQ/AOL Messenger, IRC, Jabber, Windows Messenger, Yahoo! Messenger, Mail.ru Agent
- **Servizi di File Sharing:** Amazon S3, Dropbox, Google Docs/Google Drive, OneDrive/SkyDrive, Rusfolder.com, RapidShare, Yandex.Disk
- **Protocolli Internet:** HTTP/HTTPS, FTP/FTPS, Telnet
- **Altro:** condivisione dischi SMB, conversazioni Skype

Controlli dei Contenuti

- **Canali controllati:** Dispositivi di archiviazione (rimovibili, floppy, dischi ottici), stampanti (locali, di rete, virtuali), clipboard (Windows, sessioni desktop/application), comunicazioni di rete (email, webmail, IM, social network, servizi di file sharing, HTTP/HTTPS, FTP/FTPS)
- **Contenuti controllati:** contenuti testuali, tipi di dati
- **Oggetti di testo:** formati file (120+) & archivi (40+), dati di testo (email, messaggi, web form etc.), immagini (processo OCR), documenti combinati Oracle IRM, dati binari non identificati
- **Metodi di filtrazione dei contenuti Testuali:** parole chiavi e dizionari (160+ preimpostati e personalizzabili) con analisi morfologica (Inglese, Francese, Tedesco, Italiano, Russo, Spagnolo, Catalano, Portoghese, Polacco), modelli RegExp (90+ preimpostati, personalizzabili)
- **Tipi di dati controllabili:** tipi di file validati (5300+), proprietà di documenti/file, proprietà immagini nidificate, tipi di clipboard (file, testi, immagini, audio, non identificati), protocolli di sincronizzazione (Microsoft ActiveSync®, WMDC, Apple iTunes®, Palm® HotSync), documenti combinati Oracle IRM (sicurezza del contesto)
- **Shadowing dei contenuti:** per i canali e i tipi di contenuti gestiti
- **OCR:** operatività OCR residente sull'endpoint, 25+ lingue, parole chiave, dizionari e regular expression integrati, immagini ruotate/invertite/specchiate

Integrazione crittografica

- **Windows:** Windows 7 BitLocker To Go™, Sophos® SafeGuard Easy®, SecurStar® DriveCrypt® (DCPPE), TrueCrypt®, PGP® Whole Disk Encryption, Infotecs SafeDisk®, Lexar® Media S1100/S3000
- **Mac:** Apple® OS X FileVault

Discovery dei contenuti

- **Target:** endpoint Windows (file system, archivi email, periferiche collegate), condivisioni di rete, sistemi di archiviazione
- **Modalità scansione:** con e senza agente, mista
- **Operazioni di scansione:** esecuzioni manuali o programmate
- **Azioni di bonifica:** Cancella, Salva Cancella, Cancella il contenitore, Imposta autorizzazioni (per file NTFS), Log, Avvisi, Notifiche all'Utente, Crittografa (usando EFS per file NTFS)
- **Altre caratteristiche:** configurazione elenco degli obiettivi statici e dinamici, report attività, installazione/rimozione automatica dell'Agente Discovery su richiesta

Requisiti di Sistema

- **Agente:** Windows NT/2000/XP/Vista/7/8/8.1/Server 2003-2012 R2 (32/64-bit); Apple OS X 10.6.8/10.7/10.8/10.9 (32/64-bit); Microsoft RDS, Citrix XenDesktop/XenApp, Citrix XenServer, VMware Horizon View, VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC; CPU Pentium 4, 64MB RAM, HDD 100MB
- **Console:** Windows 2000/XP/Vista/7/8/8.1/Server 2003-2012 R2 (32/64-bit; CPU Pentium 4, 2GB RAM, HDD 600GB
- **DeviceLock Enterprise Server, DeviceLock Discovery Server, DeviceLock Search Server:** Windows Server 2003-2012 (32/64-bit); Microsoft RDS, Citrix XenServer, VMware vSphere Desktop; 2xCPU Intel Xeon Quad-Core 2.33GHz, RAM 8GB, HDD 800GB (se utilizza SQL DB altrimenti inferiore); MSEE/MSDE/SQL Express o MS SQL Server

AMERICHE
DeviceLock, Inc.
3130 Crow Canyon Place, Suite 215
San Ramon, CA 94583, USA

1066 West Hastings Street Ste 2300
Vancouver, BC, Canada V6E 3X2

e-mail: us.sales@devicelock.com
Toll Free: +1 866 668 5625
Phone: +1 925 231 4400
Fax: +1 925 886 2629

UNITED KINGDOM
DeviceLock, Inc.
The 401 Centre, 302 Regent Street
London, W1B 3HH, UK
Toll Free: +44 (0) 800 047 0969
Fax: +44 (0) 207 691 7978

ITALY
DeviceLock Italia Srl
Via Falcone 7
20123 Milano, Italia
Phone: +39 02 86391432
Fax: +39 02 86391407

GERMANY
DeviceLock Europe, GmbH
Halskestr. 21
40880 Ratingen, Germany
Phone: +49 2102 131840
Fax: +49 2102 1318429

RUSSIA
DeviceLock, Russia
M. Semenovskaya d. 9 st. 9 Office 140
107023 Moscow, Russia
Phone: +7 495 647 9937

[Per ulteriori informazioni: www.devicelock.com]