DeviceLock – Libro bianco (White paper)

Sommario:

- Perché scegliere DeviceLock?
- Quali sono le caratteristiche speciali di DeviceLock?
- A chi è destinato DeviceLock?
- Come funziona DeviceLock?
- Chi ha sviluppato DeviceLock?
- Dove è possibile ottenere il software DeviceLock?
- Assistenza tecnica DeviceLock
- Informazioni sui prezzi di DeviceLock
- Metodi di ordinazione e registrazione
- Informazioni di contatto

Perché scegliere DeviceLock?

Il controllo dei contenuti caricati e scaricati dalla rete informatica aziendale è un elemento essenziale ai fini della sicurezza IT. Tale controllo diventa ogni giorno una sfida più complessa. Una delle minacce più evidenti è rappresentata dalla crescente diffusione dei dispositivi portatili di memorizzazione USB. Questo mercato è caratterizzato da una crescita esponenziale[*] e i dispositivi vantano rapidità e capacità sempre maggiori e dimensioni sempre più contenute. Non vanno poi scordati i dispositivi Bluetooth che, per promuovere la semplicità d'uso, per impostazione predefinita comunicano con ogni client Bluetooth all'interno dell'area coperta dal segnale (e tali aree possono essere particolarmente estese). Allo stesso tempo, il mercato invoca a gran voce la necessità di migliorare l'accesso alla rete per i dispositivi wireless, il che probabilmente farà passare in secondo piano le problematiche legate alla protezione.

A breve termine, le forze di mercato hanno il sopravvento sui motivi di preoccupazione in tema di protezione. Il problema non è tanto la mancata consapevolezza dei problemi di vulnerabilità da parte delle imprese. I mezzi di comunicazione infatti danno ampio risalto agli attacchi sferrati da utenti malintenzionati che, operando sia all'interno sia all'esterno delle aziende, scaricano ed estraggono informazioni riservate per servirsene ai fini di spionaggio industriale, estorsione e terrorismo. Allo stesso tempo è importante sottolineare che le imprese sono impegnate attivamente nel settore della protezione. Sono infatti in crescita gli investimenti in firewall, crittografia e altre tecnologie e l'adozione di controlli volti a proteggere i dati in rete dai furti operati tramite Internet. Ciò nonostante, queste misure sono scarsamente efficaci qualora vi siano porte e dispositivi locali privi di protezione. In particolare non sono in grado di impedire a un dipendente armato di una piccola unità da 2 GB di inserirla in una porta USB e iniziare a scaricare dati riservati, né di impedire a un dipendente insoddisfatto di utilizzare un analogo dispositivo per caricare in rete un trojan o un programma dannoso. Per arginare questi problemi è necessario che gli amministratori siano in grado di controllare tanto gli utenti che hanno accesso ai supporti esterni quanto gli orari di accesso.

DeviceLock di DeviceLock, Inc. offre questo livello di controllo per le reti basate su Microsoft Windows. Questa soluzione basata esclusivamente su software consente agli amministratori di rete di assegnare le autorizzazioni per le porte USB e Firewire, gli adattatori WiFi e Bluetooth, così come per le unità floppy, le unità CD-ROM, le periferiche a nastro e altri supporti rimovibili. DeviceLock risolve i problemi di protezione fisica senza ricorrere a lucchetti fisici.

NetworkLock, un'estensione di DeviceLock, fornisce un controllo sulle comunicazioni di rete. Gli amministratori possono specificare l'accesso degli utenti ai protocolli FTP, HTTP, SMTP e Telnet, alla messaggistica immediata (ICQ/AOL Instant Messenger, Windows Live Messenger e Windows Messenger, Jabber, IRC, Yahoo!

[*] Secondo lo studio Semico Research Corp "Will USB Flash Drives Change Our Lives?", il numero di unità USB Flash Drive passerà da circa 10 milioni di articoli venduti nel 2002 a 50 milioni nel 2006.

Messenger e Mail.ru Agent), alla Webmail e alle applicazioni delle reti sociali (Gmail, Hotmail, Yahoo! Mail, mail.ru, web.de, gmx.de, Facebook, Myspace, LinkedIn, LiveJournal, Odnoklassniki, Vkontakte e Twitter).

ContentLock, altra estensione di DeviceLock, estrae e filtra il contenuto dei dati copiati sulle unità rimovibili e sulle periferiche di memorizzazione Plug-and-Play e dei dati trasmessi sulla rete. Gli amministratori possono creare regole per specificare il tipo di contenuto che può essere copiato e trasmesso.

Quali sono le caratteristiche speciali di DeviceLock?

Consentendo il controllo in rete degli utenti autorizzati ad accedere a porte e dispositivi di un computer locale, DeviceLock risolve in modo semplice ed economico un problema di protezione potenzialmente molto grave. Si tratta pertanto di una misura estremamente efficace. Se confrontata con le soluzioni fisiche che prevedono conservazione e gestione di chiavi e lucchetti hardware, DeviceLock è una soluzione più economica e più facile da implementare nell'ambito dell'intera azienda. Rispetto alle altre soluzioni applicate dagli amministratori basate esclusivamente su software che consentono il controllo dell'hardware locale (per esempio la modifica del BIOS), DeviceLock è una soluzione più elegante e più facilmente scalabile.

DeviceLock vanta un'interfaccia utente snella e intuitiva che offre semplici procedure di installazione guidata e una serie di visualizzazioni grafiche delle informazioni. Inoltre gli amministratori di rete possono configurare e mantenere DeviceLock in remoto sulle workstation. Questa soluzione, sviluppata per i sistemi operativi Windows NT/2000/XP/Vista/7 e Windows Server 2003/2008, supporta l'esecuzione automatica delle procedure di installazione e disinstallazione.

DeviceLock inoltre può essere gestito e distribuito tramite Criteri di gruppo in un dominio Active Directory. Criteri di gruppo utilizza l'appartenenza a gruppi di protezione e servizi di directory per garantire la flessibilità e supportare informazioni di configurazione esaustive. Le impostazioni dei criteri sono create tramite lo snap-in Microsoft Management Console (MCM) per Criteri di gruppo. La più serrata integrazione con Active Directory facilita la distribuzione e la gestione delle autorizzazioni di DeviceLock nel caso delle reti di ampie dimensioni, oltre a semplificare le mansioni degli amministratori di sistema. L'integrazione con Active Directory elimina la necessità di installare altre applicazioni di terzi per centralizzare gestione e distribuzione. DeviceLock non necessita di una specifica versione basata su server per controllare l'intera rete, poiché fa leva sulle funzioni standard fornite da Active Directory.

Nelle aziende che usano soluzioni di crittografia standardizzate basate su software e hardware come PGP Whole Disk Encryption, TrueCrypt, Windows BitLocker To Go, DriveCrypt e le unità USB Lexar JumpDrive SAFE S3000 e SAFE PSD S1100, DeviceLock consente agli amministratori di definire centralmente e controllare in remoto i criteri di crittografia da rispettare durante l'utilizzo dei dispositivi rimovibili da parte dei dipendenti, per attività di memorizzazione e recupero dei dati aziendali. Ad esempio, è possibile autorizzare determinati dipendenti o gruppi per la scrittura e la lettura da unità USB flash crittografate specifiche, mentre altri per la sola lettura da dispositivi rimovibili non crittografati.

Oltre a proteggere i computer di rete e locali contro il furto di dati e gli errori di rete, DeviceLock consente di creare un registro completo delle attività delle porte, delle periferiche e della rete.

La funzionalità opzionale di data shadowing di DeviceLock ottimizza il controllo IT aziendale, facendo in modo che i dati riservati non escano dalla sede aziendale. Vengono eseguite compie complete di tutti i dati trasferiti su dispositivi rimovibili e PDA/smartphone Windows Mobile autorizzati, masterizzati su CD/DVD, trasferiti sulla rete o stampati da utenti finali autorizzati. Le copie ombra sono memorizzate in un'ubicazione centralizzata sul server esistente o su un'infrastruttura SQL conforme a ODBC scelta dal cliente.

DeviceLock Search Server consente di eseguire ricerche full-text tra i dati memorizzati in DeviceLock Enterprise Server. La funzionalità di ricerca full-text è particolarmente utile nelle situazioni in cui il revisore IT aziendale deve cercare le copie shadow dei documenti sulla base del loro contenuto. DeviceLock Search Server può riconoscere, indicizzare, cercare e mostrare automaticamente i documenti in numerosi formati, tra cui: Adobe Acrobat (PDF), Ami Pro, archivi (GZIP, RAR, ZIP), Lotus 1-2-3, Microsoft Access, Microsoft Excel, Microsoft PowerPoint, Microsoft Word, Microsoft Works, OpenOffice (documenti, fogli elettronici e presentazioni), Quattro Pro, WordPerfect, WordStar e tanti altri ancora.

A chi è destinato DeviceLock?

La base clienti in rapida espansione di DeviceLock include aziende oggetto di verifiche volte ad accertare la sicurezza della gestione dei dati aziendali e dei clienti, agenzie governative che gestiscono informazioni riservate, società di servizi professionali e altre piccole-medie imprese che necessitano di controllo sull'accesso ai dispositivi.

Il seguente elenco riporta alcuni esempi di utilizzo di DeviceLock:

- Consente di controllare gli utenti o i gruppi autorizzati ad accedere a porte USB, FireWire, a infrarossi, COM e LPT, adattatori WiFi e Bluetooth, qualsiasi tipo di stampante (incluse le stampanti locali, di rete e virtuali), PDA e smartphone Windows Mobile, BlackBerry, iPhone, iPod Touch, iPad e Palm OS, DVD/CD-ROM, unità floppy e altre periferiche rimovibili e Plug-and-Play.

- Consente di controllare gli utenti o gruppi autorizzati ad accedere ai protocolli e alle applicazioni di rete (FTP, HTTP, SMTP, Telnet, messaggistica immediata, servizi Webmail e reti sociali).

- Consente di concedere o negare in maniera selettiva l'accesso alle informazioni in base ai tipi di file reali, ai motivi di espressioni comuni con condizioni numeriche e alle combinazioni booleane di criteri e parole chiave corrispondenti.

- Consente di controllare l'accesso alle immagini contenenti testo (ad esempio documenti sottoposti a scansione e schermate di documenti) e immagini che non contengono testo.

- Consente di controllare l'accesso alle periferiche e ai protocolli in base all'ora del giorno e al giorno della settimana.

- Definire i tipi di dati (file, calendari, e-mail, attività, note, ecc.) per cui autorizzare la sincronizzazione tra PC aziendali e dispositivi mobili personali.

- Definire diversi criteri di sicurezza online od offline per lo stesso utente o gli stessi gruppi di utenti.

- Consente di rilevare dischi crittografati PGP, DriveCrypt e TrueCrypt (unità USB flash e altre periferiche rimovibili), unità flash crittografate Lexar SAFE PSD e Lexar JumpDrive SAFE S3000 e unità crittografate BitLocker To Go, e applicare autorizzazioni "crittografate" speciali a tali dischi e unità.

- Autorizzare solo dispositivi USB specifici che non sono bloccati indipendentemente da qualsiasi altra impostazione.

- Concedere agli utenti l'accesso temporaneo ai dispositivi USB in assenza di connessione di rete (si forniscono agli utenti codici di accesso speciali tramite telefono che sbloccano temporaneamente l'accesso ai dispositivi richiesti).

- Identificare univocamente un determinato disco DVD/CD-ROM mediante la firma dei dati e autorizzare l'accesso allo stesso, anche nel caso in cui DeviceLock abbia bloccato l'unità DVD/CD-ROM.

- Fornire protezione nei confronti degli utenti dotati dei privilegi di amministratore locale cosicché non possano disattivare DeviceLock Service o rimuoverlo dai propri computer se non sono inseriti nell'elenco degli amministratori di DeviceLock.

- Eseguire ricerche di testo tra i file shadow e i registri di controllo memorizzati nel database centralizzato.

- Impostare i dispositivi in modalità di sola lettura.

- Proteggere i dischi da formattazioni accidentali o intenzionali.

- Rilevare e bloccare keylogger hardware (USB e PS/2).
- Implementare autorizzazioni e impostazioni tramite criteri di gruppo in un dominio Active Directory.
- Utilizzare lo snap-in RSoP standard di Windows per visualizzare i criteri di DeviceLock attualmente applicati e per conoscere i criteri giusti da applicare in una determinata situazione.
- Controllare qualsiasi elemento in remoto tramite la console di gestione centralizzata.
- Consente di creare un registro completo delle attività delle porte, delle periferiche e della rete, ad esempio operazioni di caricamento e scaricamento in base a utenti e nomi file nel registro standard degli eventi di Windows.
- Consente di eseguire il mirroring (shadowing) di tutti i dati copiati in periferiche di memorizzazione esterne (rimovibili, floppy, DVD/CD-ROM), PDA e smartphone Windows Mobile, iPhone, iPod Touch, iPad e Palm OS, trasferiti tramite porte COM e LPT o stampati.
- Memorizzare le copie ombra in un'ubicazione centralizzata sul server esistente e su qualsiasi infrastruttura esistente conforme a ODBC.
- Monitorare i computer remoti in tempo reale, verificando lo stato di DeviceLock Service (attivo o meno) e l'uniformità e l'integrità dei criteri.
- Generare un report sulle autorizzazioni e le impostazioni configurate.
- Creare report grafici basati sui registri (di controllo e shadow) memorizzati sul server.
- Generare un report che visualizzi i dispositivi USB, Firewire e PCMCIA tuttora e precedentemente collegati ai computer.
- Creare un pacchetto MSI personalizzato per DeviceLock Service seguendo criteri predefiniti.

Come funziona DeviceLock?

DeviceLock è compatibile con i computer dotati di sistema operativo Windows NT 4.0/2000/XP/Vista/7 o Windows Server 2003/2008. Supporta le piattaforme a 32 e 64 bit.

DeviceLock è costituito da tre elementi: l'agente, il server e la console di gestione:

1. DeviceLock Service (l'agente) è il cardine della soluzione DeviceLock. DeviceLock Service è installato su tutti i sistemi client, viene eseguito automaticamente e assicura la protezione delle periferiche e della rete sul computer client, risultando invisibile per gli utenti del computer locale.

2. DeviceLock Enterprise Server è il componente opzionale per la raccolta e la memorizzazione centralizzate dei dati shadow e dei registri di controllo. DeviceLock Enterprise Server utilizza MS SQL Server per archiviare i propri dati.

   DeviceLock Content Security Server è inoltre il componente opzionale che include DeviceLock Search Server, che consente di eseguire ricerche immediate di testo tra i file shadow e altri registri memorizzati su DeviceLock Enterprise Server.

3. La console di gestione è l'interfaccia di controllo utilizzata dagli amministratori di sistema per gestire in remoto ogni sistema dotato di DeviceLock Service. DeviceLock è fornito con tre diverse console di gestione: DeviceLock Management Console (lo snap-in MMC), DeviceLock Enterprise Manager e DeviceLock Group Policy Manager (che si integra con l'editor Criteri di gruppo di Windows).

Chi ha sviluppato DeviceLock?

DeviceLock è stato sviluppato da DeviceLock, Inc. Sin dalla sua fondazione risalente al 1996, DeviceLock, Inc. (in precedenza SmartLine Inc) fornisce soluzioni per la protezione delle informazioni e la gestione della rete alle organizzazioni che si avvalgono delle tecnologie Microsoft Windows. La comprovata esperienza di DeviceLock nel settore delle tecnologie di controllo dell'accesso consente ai clienti di migliorare la protezione, la produttività e la disponibilità dei sistemi. I professionisti IT scelgono le soluzioni DeviceLock, Inc. per amministrare, controllare e proteggere i sistemi chiave. Tra i clienti dell'azienda si annoverano BAE SYSTEMS, AEROTEC Engineering GmbH, HSBC Bank, Barclays Bank, Chase Manhattan Bank e numerose agenzie e dipartimenti governativi statali e federali. DeviceLock, Inc. è un'organizzazione internazionale con filiali a San Ramon (California), Londra (Regno Unito), Ratingen (Germania), Mosca (Russia) e Milano (Italia).

Dove è possibile ottenere il software DeviceLock?

Una demo gratuita completamente funzionante è disponibile al seguente indirizzo:

http://www.devicelock.com/it/dl/download.html

Assistenza tecnica DeviceLock

I clienti DeviceLock possono usufruire di assistenza tecnica inviando un messaggio di posta elettronica all'indirizzo support@devicelock.com. Il seguente sito Web offre una notevole mole di informazioni di natura tecnica, incluse le procedure di risoluzione dei problemi noti e le risposte alle domande più frequenti: http://www.devicelock.com/it/support.html

È inoltre possibile contattare il reparto del supporto tecnico al seguente numero: +1-925-231-0042, dal lunedì al venerdì, dalle 8 alle 17 PT (Pacific Time).

Informazioni sui prezzi di DeviceLock

Una licenza di base di DeviceLock per un singolo utente costa € 40 (Euro). Sono disponibili sconti per gli istituti di istruzione e per l'acquisto di licenze multiutente. Per ottenere informazioni sui prezzi delle licenze multiutente consultare la seguente pagina Web: www.devicelock.com/it/dl/register.html

Per utilizzare le funzionalità di NetworkLock e ContentLock, è necessario acquistare le licenze di NetworkLock e ContentLock, oltre alle licenze di base di DeviceLock.

Metodi di ordinazione e registrazione

Sono disponibili numerosi metodi di ordinazione / registrazione di DeviceLock:

Sul World Wide Web tramite un sito Web protetto (mediante carta di credito)
Per telefono (mediante carta di credito)
Per fax (mediante carta di credito)
Per posta ordinaria (mediante assegno)
Tramite ordine di acquisto

Per ottenere ulteriori informazioni su come collocare un ordine consultare la seguente pagina Web: http://www.devicelock.com/it/dl/register.html

Informazioni di contatto

DeviceLock Germany:

Halskestr. 21, 40880 Ratingen, Germania
TEL: +49 (2102) 89211-0
FAX: +49 (2102) 89211-29

DeviceLock Italy:

Via Falcone 7, 20123 Milano, Italia
TEL: +39-02-86391432
FAX: +39-02-86391407

DeviceLock UK:

The 401 Centre, 302 Regent Street, London, W1B 3HH, Regno Unito
TEL (numero verde): +44-(0)-800-047-0969
FAX: +44-(0)-207-691-7978

DeviceLock USA:

2010 Crow Canyon Place, Suite 100, San Ramon, CA 94583, USA
TEL (numero verde): +1-866-668-5625
FAX: +1-646-349-2996

Sales@devicelock.com
Support@devicelock.com

http://www.devicelock.com/it

