

Suite DeviceLock® Endpoint DLP

Les modules additionnels ContentLock™ et NetworkLock™

La suite DeviceLock® Endpoint DLP comprend l'excellent logiciel de contrôle d'accès aux ports et aux périphériques de DeviceLock, associé aux modules sophistiqués ContentLock™ et NetworkLock™, pour une sécurité granulaire encore plus élevée sur les objets de données qui tentent de se déplacer d'un poste de travail à l'autre via des périphériques ou des communications réseau.

ContentLock™ et NetworkLock™ sont des options sous licence séparée qui s'appuient sur les informations détaillées fournies par DeviceLock®, et accroissent son efficacité dans la lutte contre les fuites de données au niveau des terminaux en ajoutant le filtrage du contenu et le contrôle des communications réseau.

ContentLock™

Pour certains experts, ce qui fait la force d'une solution DLP (*Data Leak Prevention* ou *Prévention des fuites de données*) est sa capacité à analyser les flux de données — ce qui s'est avéré très complexe et coûteux pour les premiers utilisateurs de solutions DLP.

Aujourd'hui, avec DeviceLock® et ContentLock™, les administrateurs peuvent analyser les contenus de façon sélective, selon le contexte, au niveau du poste de travail, via les paramètres de sécurité des objets de groupe de la console de gestion de DeviceLock®, basée sur Active Directory.

ContentLock™ prend en charge le filtrage des objets de données copiés vers des lecteurs amovibles, ou autres périphériques de stockage "plug and play", ou via des communications réseau sécurisées par le module NetworkLock™ au niveau local.

Capable de reconnaître plus de 80 formats de fichier et types de données, ContentLock™ extrait et filtre le contenu

des fichiers et autres types d'objets de données, dont les e-mails, les messages instantanés, les formulaires Web, les échanges sur les réseaux sociaux, les sessions Telnet, etc.

ContentLock™ filtre les flux de données en se basant sur les expressions régulières, la correspondance numérique et des conditions booléennes "et/ou". Il est ainsi possible d'utiliser plus de 50 paramètres textuels, dont les utilisateurs, les ordinateurs, les groupes, les ports, les types et la direction des flux de données, etc.

La technologie de filtrage de ContentLock™ rend la fonctionnalité de contrôle discret de DeviceLock® plus efficace, extensive et intelligente.

Le contrôle discret des données selon le contenu de tout type de supports est pris en charge, y compris les périphériques de stockage amovibles et "plug and play", les communications réseau, les synchronisations locales avec les smart



phones compatibles, et l'impression de documents.

Les transmissions entrantes et sortantes peuvent également être contrôlées selon des conditions. En pré-filtrant les objets de données potentiellement importants avant de les contrôler et de les journaliser, DeviceLock® réduit ces flux aux seuls objets contenant des informations pertinentes, et pour des tâches de post-analyse telles que les audits de conformité à la sécurité, les enquêtes après incident, et les recours légaux. Cette méthode réduit de façon significative les besoins en espace de stockage et en bande passante réseau.

Confidential	Keywords	Deny: Write	Permissions	Removable	Regular
Email Address	Pattern	Deny: Write	Permissions	Removable	Regular
Fax Documents	File Type Detection	Deny: Read	Permissions	Removable	Regular
Password protected	Document Properties	Deny: Read, Write	Permissions	Removable	Regular
Phone numbers & Emails	Complex	Deny: Write	Permissions	Removable	Regular
Archives	File Type Detection	Allow: Incoming Files	Permissions	HTTP	
Confidential	Keywords	Deny: Outgoing Files	Permissions	FTP	
Password protected	Document Properties	Deny: Outgoing Files	Permissions	SMTP	
Phone numbers & Emails	Complex	Deny: Outgoing Messages	Permissions	SMTP, Web Mail	
US Social Security Num...	Pattern	Allow: Incoming Messages	Permissions	ICQ/AOL Messenger	

Exemples de règles de contrôle de contenu par périphérique

Exemples de règles de contrôle de contenu par protocole réseau



L'interface de la console de gestion de ContentLock™ facilite la définition de règles de filtrage selon le contenu. À un niveau de configuration inférieur, des options détaillées utilisent les opérateurs logiques, des mots-clés prédéfinis spécifiques à l'industrie, ainsi que des modèles basés sur les expressions régulières. Ces méthodes sont utilisées pour sécuriser des données sensibles comme des coordonnées personnelles, des numéros de carte bancaire ou de sécurité sociale, etc.

DeviceLock®

Proactive Endpoint Security

Pour parer aux éventuelles fuites de données au niveau du poste de travail, la suite DeviceLock® Endpoint DLP permet en outre le contrôle contextuel et le filtrage de contenu des objets de données présents dans le trafic réseau entrant et sortant du PC.

NetworkLock™

La technologie de détection de NetworkLock™ est indépendante du port. Elle reconnaît les types d'application ainsi que les protocoles réseau concernés par des risques de fuite.

NetworkLock™ peut être configuré pour contrôler le courrier électronique, les communications sur les réseaux sociaux, la messagerie instantanée et les sessions Telnet.

Une fois le module installé, vous pouvez définir des règles de "listes blanches" basées sur l'adresse IP, l'adresse du

réseau, le masque de sous-réseau, les ports et les plages réseau, ainsi que des règles basées sur des critères de type "plus que/moins que".

NetworkLock™ peut intercepter, inspecter et contrôler séparément les messages e-mail SMTP et leurs pièces jointes, même cryptés avec SSL, ainsi que les accès internet, les applications basées sur HTTP ou les sessions HTTPS chiffrées.

Les messages et sessions sont reconstruits, les données et informations de paramétrage extraites et transmises au



module ContentLock™ pour filtrage de contenu. La journalisation d'événements et les traces du contrôle discret sont préservées et spécifiées de façon conditionnelle.

Name	Regular	Offline
FTP	Configured	Configured
HTTP	Configured	Configured
ICQ/AOL Messenger	Configured	Configured
IRC	Configured	Configured
Jabber	Configured	Configured
Mail.ru Agent	Configured	Configured
SMTP	Configured	Configured
Social Networks	Configured	Configured
Telnet	Configured	Configured
Web Mail	Configured	Configured
Windows Messenger	Configured	Configured
Yahoo Messenger	Configured	Configured

Applications et protocoles gérés par NetworkLock™

Communications réseaux contrôlées

- Clients mail : Gmail, Yahoo! Mail, Windows Live Mail
- Réseaux sociaux : Facebook, Twitter, LiveJournal,
- LinkedIn, MySpace, Odnoklassniki, Vkontakte
- Clients messagerie : ICQ/AOL, MSN Messenger,
- Jabber, IRC, Yahoo! Messenger, Mail.ru Agent.
- Protocoles Internet : FTP, FTP over SSL, HTTP/HTTPS, SMTP, SMTP over SSL
- Sessions Telnet

Pré-requis

ContentLock™ et NetworkLock™ nécessitent l'installation du module principal DeviceLock®.

NetworkLock™ nécessite ContentLock™ pour appliquer les règles basées sur le contenu des communications réseau.

Liste des revendeurs agréés sur
www.device-lock.fr

Importateur en France : ATHENA Global Services - www.athena-gs.com

Editeur : DeviceLock - www.device-lock.com/fr

VOTRE REVENDEUR :