DeviceLock®

ЦЯЛОСТНО *DLP РЕШЕНИЕ ЗА ПРЕДОТВРАТЯВАНЕ НА КРАЖБИ И СЛУЧАЙНО ИЗТИЧАНЕ НА ИНФОРМАЦИЯ ОТ "ВЪТРЕ НАВЪН" ВЪВ ВАШАТА ОРГАНИЗАЦИЯТА

- **Използването на стандартни средства за ИТ сигурност като антивирусни продукти и firewall за защита на информацията не работят, когато става дума за кражба от недобросъвестни служители вътре в организацията.**

Стандартния подход за предотвратяване на изтичане на информацията е нейният контекстен контрол, при който информацията се контролира чрез разрешаване и забрана на операции с нея в зависимост от потребителя, типа на данните, интерфейса, устройството или мрежовия протокол, посоката на движение на данните, криптиране и т.н.
Някои сценарии за защита от изтичане на чувствителна информация изискват по-задълбочено ниво на анализ – например, когато информацията съдържа атрибути за персонална идентификация (ЕГН, банкови и картови сметки) или, когато се работи с информация считана за високорискова. В тези случаи администраторите по ИТ сигурност могат да извършат допълнителен анализ на съдържанието преди информацията да протече по съответният канал и да бъде достъпната от съответния служител.

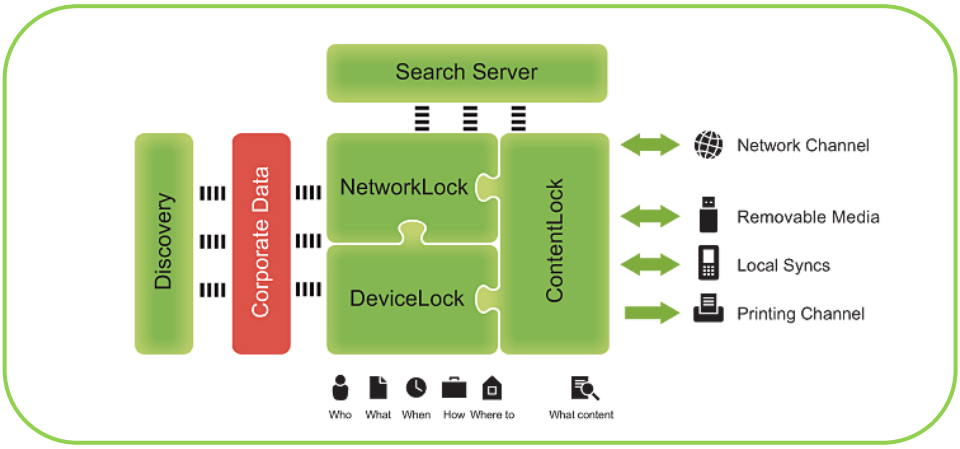
- **DeviceLock Endpoint DLP Suite** осигурява както стандартния контекстен контрол (потребител / файл/ устройство/ канал/ протокол), така и контрол по съдържание на информацията без значение от файловия формат, в които са опаковани данните. Ядрото на продукта осигурява анализ на съдържанието на информацията, прехващане на ключови фрази и изрази във всички възможни информационни канали, както и съответно филтриране.

- С **DeviceLock®** администраторите по ИТ сигурност имат възможността прецизно да управляват достъпа и операциите, които могат да се извършват с информацията отделните потребители.
Така изградената сигурна ИТ среда позволява безпрепятствена работа за легитимните потребители и прави невъзможно всяко преднамерено или инцидентно действие, извън границите установени с приетата политика за сигурност.
Продуктът позволява безпроблемна интеграция на Microsoft Windows Active Directory®, Group Policy Objects (GPOs) и **DeviceLock**-конзолите за динамично и централизирано управление на **DeviceLock**-агентите инсталирани в крайните точки (работни станции, лаптопи и т.н.) в съответствие с политика та за сигурност.

- **DeviceLock®** позволява централизирано да се контролират, описват в дневници, създават скрити копия на документите, да се анализира достъпа на крайните потребители до всички периферни устройства и портове, както и до мрежовите комуникации. В допълнение агентите инсталирани в крайните точки могат да откриват и блокират хардуерни кейлогери (keylogrers) и да предпазват от кражба на пароли или друга чувствителна информация.

DeviceLock®
Proactive Endpoint Security

***DLP решение работещо в над 100 държави и защитаващо над 5 милиона потребителя**



- **DeviceLock®** работи използвайки минимална системна памет и дисково пространство и остава прозрачен и невидим за крайните потребители.

- Комбинирането на прецизен контекстен контрол и филтриране по съдържание на информацията **DeviceLock Endpoint DLP Suite** значително редуцира риска от изтичане на чувствителна информация от компютрите (лаптопите, таблетите и мобилните телефони) на служителите независимо от причината – неволни или преднамерени действия.

- В същото време **DeviceLock** работи като платформа за ИТ сигурност, даваща възможност за изпълнение на избраната политика за сигурност, спазване на корпоративните правила за работа с информацията, както и да се постигне съответствие с изискванията на регулаторните органи като HIPAA, Sarbanes-Oxley и PCI DSS.

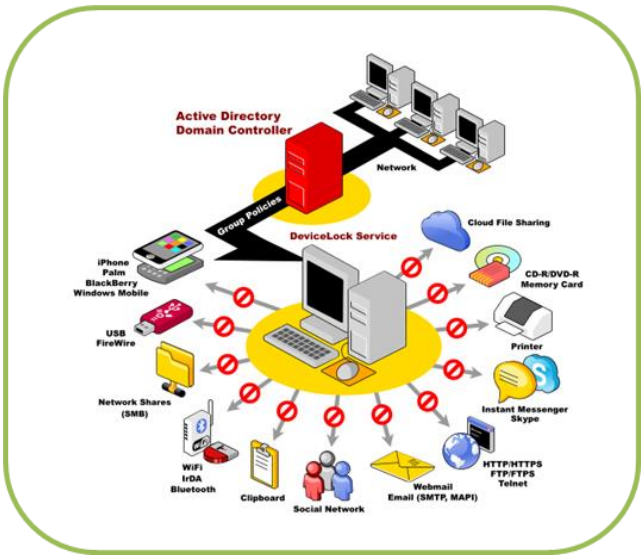
***DLP - Data Loss Prevention –** защита от изтичане на данни.

infinity Endpoint Security

DeviceLock Proactive Endpoint Security осигурява мониторинг, управление и контрол на всички периферни устройства по портове и интерфейси, класове, типове, модели, уникални ID тагове, седмичен график, часови график, както и по операции с данните (запис, четене, коригиране, изтриване и форматиране):

- **NetworkLock™** разширява обхвата на продукта чрез контрол на мрежовите комуникации;
- **ContentLock™** осигурява филтриране по съдържание на данните протичащи по информационните канали;
- **DeviceLock Discovery™** позволява да се идентифицира, класифицира и поеме контрола над поверителните данни "в покой" **"data at rest"**.

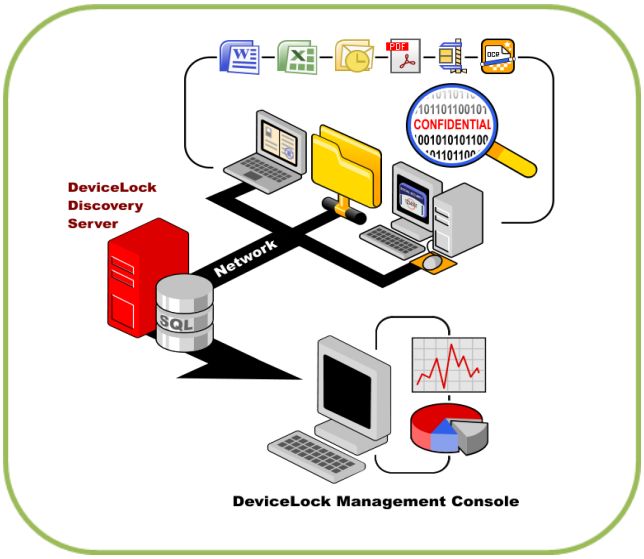
Модулна структура



- **DeviceLock Endpoint DLP Suite** е съставена от няколко взаимно допълващи се компонента, които се лицензират отделно или в комбинация според специфичните нужди. Съществуващите клиенти имат възможността за ъпгрейд на продукта с нови възможности, а новите потребители могат постепенно да изграждат цялостно DLP решение чрез добавянето на отделните модули, когато са им нужни или, когато го позволява бюджета им.
- **DeviceLock®** включват цялостен набор от компоненти, включващи инструменти за контекстен контрол, създаване на дневници със събития, създаване на скрити копия на документите (data shadow) за всички локални информационни канали. Те включват и периферните устройства и локални портове, свързаните смартфони и таблети, както и всички принтери и скенери. DeviceLock осигурява основната платформа, централното управление и всички административни компоненти за останалите модули от пакета.
- **NetworkLock™** е компонент с функции за контекстен контрол върху мрежовите комуникации чрез портово-независима детекция на протоколи и приложения, за реконструкция на сесии и съобщения, за извличане на данни и параметри, за създаване на дневници за събития и за скрито създаване на дубликати на файлове с данни.
- **ContentLock™** е компонент за извършване на мониторинг по съдържание на информацията и филтриране на файловете прехвърляни от и на преносими носители на данни, Plug-n-Play устройства, както и на различни данни преминаващи през мрежовите комуникации – имейли, съобщения през Skype, ICQ, web-форми, прикачени файлове в имейли, социални мрежи, трансфер на файлове и Telnet сесии.

- **DeviceLock Discovery™** е най-новият модул предлаган от DeviceLock, той позволява на организациите да идентифицират, класифицират и поемат контрол над поверителните си данни "в покой" ("data at rest"), съхранявани в техните сървъри, работни станции или системи за съхранение на данни с цел про-активно да се предотврати изтичането на поверителна информация и да се постигне съответствие с нормативните и корпоративни изисквания за сигурност на данните.

DeviceLock Discovery чрез автоматичното сканиране на данните, разположени на сървъри, работни станции, мрежови дялове или системи за съхранение на данни, вътре и извън корпоративната мрежа, DeviceLock Discovery локализирана документи с чувствително съдържание, предоставя възможности за класификация и последващи процедури за защита от изтичане на чувствителната за организацията информация като изпраща предупреждения в реално време към Security Information and Event Management (SIEM) системите, използвани в организацията.



В зависимост от топологията на мрежата, както и други особености на защитената IT среда, DeviceLock Discovery може да извърши сканиране в няколко режима:базирано на агенти, без агенти и смесено сканиране.

DeviceLock Discovery може да извършва сканирането ръчно или автоматично - чрез конфигуриране на график. Агентите на DeviceLock Discovery могат да бъдат инсталирани и деинсталирани дистанционно от целевите компютри чрез напълно автоматичен и прозрачен за крайните потребители процес.

Инфинити ООД
Официален представител на **DeviceLock®** за РБългария
Интерпред - СТЦ София 1040, бул."Драган Цанков"No:36
тел.: +359 2 489 02 59
+359 2 489 02 60
GSM: +359 884 166 118
е-поща: office@infinity.bg

infinity Endpoint Security

[www.infinity.bg