cryptware
secure your way

Vorteil von Secure Disk DesInfect:

- Erkennung von Schädlingen, die sich bei aktivem Windows verstecken oder wieder aktivieren
- Zeitgesteuerter Start einer Virensuche (Full-Scan) über Wake-on-LAN oder Aktivierung über die Management-Konsole
- Zentrales Management (welches End-gerät, welche OUs, welche virtuellen OUs)
- Erhöhung der Sicherheit durch die Verwendung einer zweiten Scan-Engine
- PreBoot basierter Virus-Scan von BitLocker-verschlüsselten Festplatten
- Zentraler Einblick auf die Scan-Ergebnisse

Funktionen von Secure Disk DesInfect:

- Scannen von BitLocker-verschlüsselten Festplatten bei inaktivem Windows
- Definierbarer Start des Linux-basierten PreBoot-Betriebssystems von der Festplatte
- Zentrale Administration der Policy
- Zentrales Dashboard der Scan-Ergebnisse
- Zentrale Auswahl der Rechner, die gescannt werden sollen
- Direkter Start des Scan-Vorganges für definierte Rechner
- Unterstützung verschiedener Antivirus-Anbieter (Scan-Engine) möglich
- Policy für gefundene Viren (verschieben in Quarantäne, Report only, ...)

CryptoPro
Secure Disk DesInfect
Antivirus-Notfall-System für BitLocker-verschlüsselte Endgeräte

Cyberattacken auf Industrieanlagen, Würmer, Trojaner, Malware, Code Red, Nimda usw. sind ein großes Problem!

Einige Schädlinge können Schäden in Milliardenhöhe verursachen. Viren werden immer raffinierter und intelligenter. Ihre Entwicklung geschieht im professionellen Umfeld; finanzielle Mittel und qualifiziertes Personal stehen ausreichend zur Verfügung. Ein Ziel des Schädlings ist, neben seiner eigentlichen Aufgabe, für die er entwickelt wurde, vom Virenscanner unentdeckt zu bleiben oder sich erneut zu aktivieren, wenn er scheinbar „entfernt“ wurde.

Die meisten Antivirus-Hersteller bieten ihren Kunden einen bootfähigen Notfall-USB-Stick an, der es erlaubt, Schädlinge zu entfernen, auch wenn der Rechner nicht mehr lauffähig ist oder sich der Schädling im laufenden Windows-Betriebssystem nicht entfernen lässt. Hierzu wird über das externe Medium (CD oder USB-Stick) der lokale Rechner mit einem Linux-basierenden Betriebssystem gebootet und der Virenscanner gestartet. Dank integrierter Updatefunktion ist der Virenscanner, bevor er seinen Scan-Vorgang beginnt, auf dem aktuellen Stand der Virensignaturen.

Diese Methode, infizierte Rechner oder Daten zu retten, ist oftmals der letzte Rettungsanker! Außerdem ist diese Methode die Einzige, Viren zu entfernen, die sich selbst wiederherstellen, da sie sich in geloggten, nicht löschbaren Dateien befinden oder sich als Systemdienst eingetragen haben. Die Stealth-Viren (Tarnkappen-Viren) versuchen, ihre Entdeckung systematisch zu verhindern. So können sie sich z.B. vor einem

Virenscan selbst aus der Datei entfernen und infizieren diese Datei nach der Überprüfung erneut. Das gleiche gilt für Rootkits; Programme die sich im System verstecken und dem Virenscanner das Bild eines nicht infizierten Rechners vorspiegeln.
Da die Anwendung der „Rescue-CD" von einem lokalen Booten des Rechners über ein externes Medium ausgeht, ist dies zwar für einzelne Rechner eine brauchbare Lösung, nicht jedoch für eine großflächige Überprüfung im Enterprise-Umfeld mit BitLocker-verschlüsselten Festplatten.

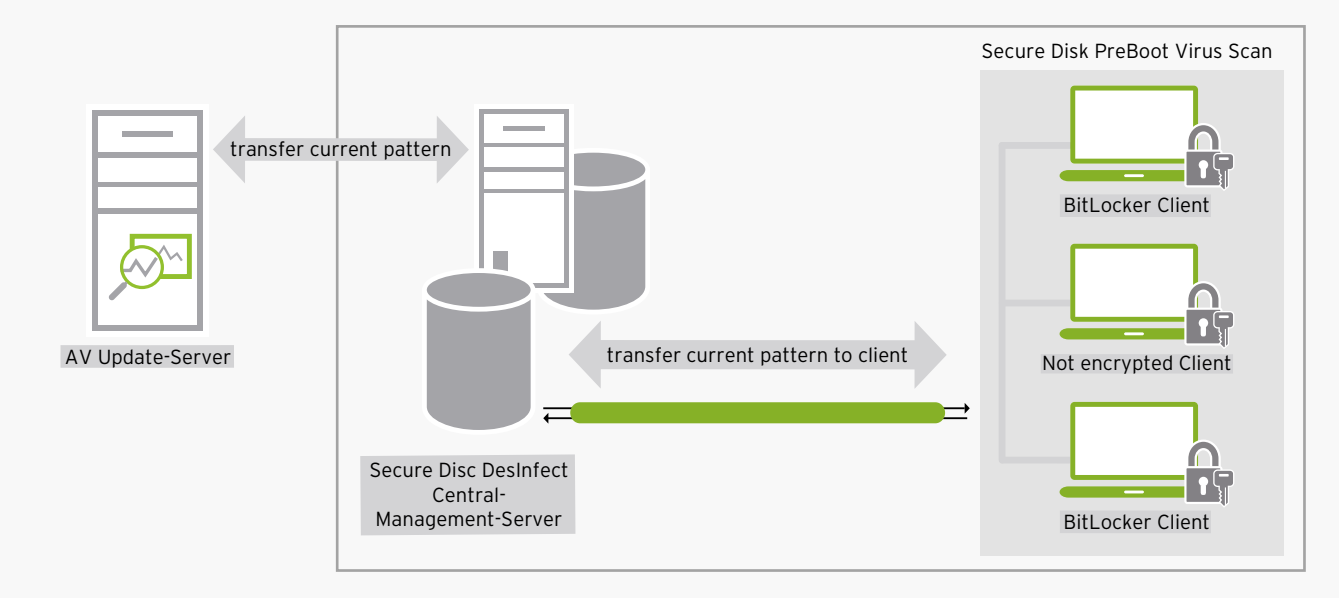
Der Wunsch nach einer zentral administrierbaren Lösung liegt auf der Hand, um den nachfolgenden Fragestellungen gerecht zu werden:

- Wie sieht das Notfall-Szenario aus, wenn 5.000 oder 50.000 oder > 100.000 Rechner infiziert sind?
- Ist es logistisch und technisch möglich, alle Rechner in allen Lokationen und Landesorganisationen lokal zu booten und zu scannen?
- Können einzelne Lokationen ausgewählt werden, um zu einem bestimmen Zeitpunkt überprüft zu werden.
- Ist der Scan-Vorgang möglich, wenn die Festplatte mit BitLocker verschlüsselt ist?

CryptWare präsentiert nun eine neue Technologie unter dem Namen „Secure Disk DesInfect" und hat die Methode der „Notfall CD" in ein zentral gemanagtes Boot-System integriert, welches auf der lokalen Festplatte des Endgerätes installiert wird und in der Lage ist, BitLocker-verschlüsselte Festplatten zu scannen.

Secure Disk DesInfect wird über eine zentrale Managementkonsole konfiguriert und administriert. Hierbei wird das Linux-basierte Bootsystem auf der Festplatte gestartet und nimmt zunächst über einen geschützten Kanal Kontakt mit dem Management-Server auf, um sich dort die aktuellen Virensignaturen abzuholen.

CryptWare setzt bei der integrierten Scan-Engine auf etablierte Antiviren-Hersteller des Marktes. Die in Secure Disk DesInfect integrierte BitLocker-Protektor-Technologie erlaubt nun den Zugriff auf das BitLocker Schlüsselmaterial und der Virenscanner kann die BitLocker-verschlüsselte Festplatte scannen.



cryptware
secure your way

CryptWare IT Security GmbH
Frankfurter Str. 2
65549 Limburg

Phone: +49 (0) 6431 977790 - 0
Fax: +49 (0) 6431 977790 - 22
info@cryptware.eu

www.cryptware.eu