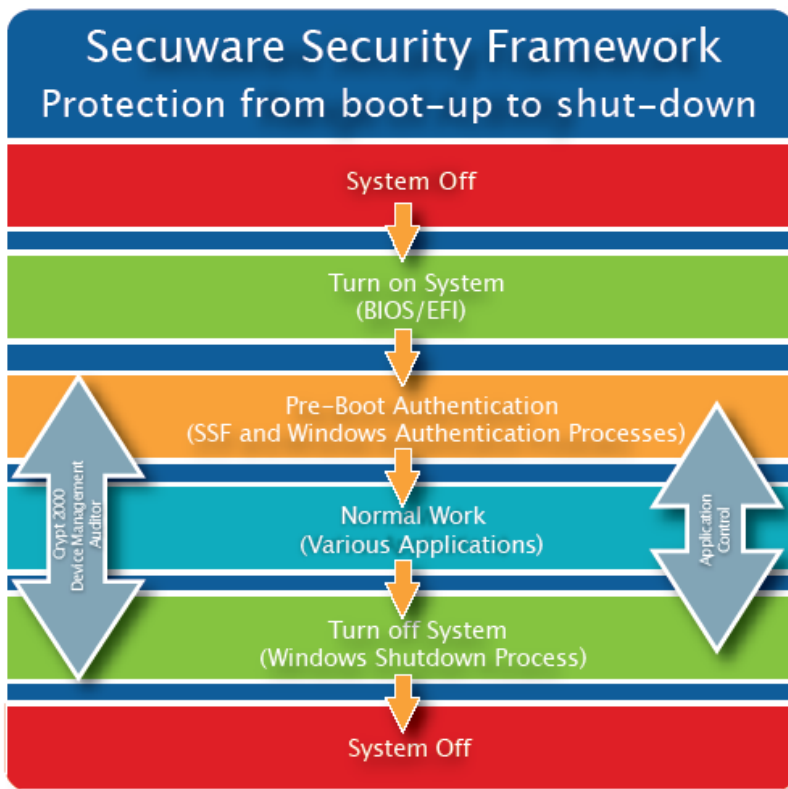


Secuware™ Crypt 4000

Secuware Security Crypt4000 macht es Besitzern sehr einfach ihre Daten gegen unerlaubten Zugriff durch Verschlüsselung zu schützen. Crypt4000 stellt sicher das nahezu alle externen und internen Geräte die gleiche perfekte Verschlüsselung und Pre Boot Authentication erhalten, wie sie sonst nur dem zentral verwalteten Systemen zur Verfügung steht.

Crypt4000 wurde für PC's mit Windows Betriebssystem optimiert. Mit hoher Performance und geringem Einfluss auf alle I/O Operationen ist Crypt4000 zugeschnitten auf die neue Generation aller PC's Alle Anwendungen unter Windows laufen vollständig transparent mit dem verschlüsseltem Datenträger. Crypt4000 liefert eine vollständige Festplattenver-schlüsselung für alle Windows Versionen an Windows XP..



Crypt4000 wurde entwickelt für PC's und Notebooks mit installiertem Windows XP und neuer. Es ist einfach zu installieren und arbeitet als eine leicht zu administrierende sorgenfreie Festplattenverschlüsselung.

Crypt4000 schützt gegen internen und externen Missbrauch von Daten:

- Bei verlorenen oder gestohlenen Notebooks.
- Bei Notebookwechsel oder Entsorgung und Verkauf.
- Externe Geräte werden verschlüsselt.
- Bei Missbrauch von vertraulichen Daten durch Dritte.

Crypt4000 schützt Daten gegen unerwünschten Zugriff.

- Einfache Installation, einfache Konfiguration und hohe Optimierung schützt die Daten auf dem lokalen Datenträger.
- Durch Pre Boot Authentication höchstes zertifiziertes Sicherheitslevel für einen PC
- Schützt wirkungsvoll und wächst mit den Anforderungen.

Statistik: 16.000 verlorene Laptops pro Woche

(Fast) jeder verlorene Laptop ist eine kleine - oder mittlere - Datenpanne.

Etwa die Hälfte der Geräte enthielten vertrauliche Daten. in den 106 größten Flughäfen der USA, dabei knapp 5.000 in den Big 5. 3.400 verlorene Laptops pro Woche in den 7 größten Flughäfen Europas, dabei 300 in Frankfurt. Quelle: worldpress.com. 20.10.2009

Crypt4000 ist leicht zu Verwalten

- Hoch skalierbare Architektur in Verbindung mit einem lokalen Administrationsclient.
- Kein Server oder Policy-datenbank benötigt. Das senkt administrative Aufwände.
- Policies und Geräteschlüssel werden in der PBA im sicheren AES Container aufbewahrt.
- Symmetrische Schlüssel. vermeiden hohen PKI Aufwand.
- Separate Rollen für IT- und Security Administrator.



Crypt4000 besteht aus einem lokalen Verschlüsselungs- und Administrationsmodul.

Produkt Spezifikationen

Clients (PC's)

- Windows 7
- Windows Vista
- Windows XP

Installation

- Administratorzugang wird benötigt.
- MSI Installations-Datei.
- Verschlüsselt Festplatten ohne vorhandene Daten zu löschen.

Funktionen

- Pre Boot Authentication (PBA)
- Auto User Enrollment in der PBA
- Single Sign On mit Windows Benutzern
- Volle HD Verschlüsselung
- Smartcards und Token werden unterstützt.

- **Crypt4000** erzwingt sichere Anmeldung durch eine fest mit Windows verbundene Pre Boot Authentication. Bestehende Benutzernamen oder Anmeldekonto können problemlos weiterverwendet werden. Das System kann nicht durch bootbare Rettungs- CDs oder einfaches umhängen der Festplatte umgangen werden. Crypt4000 erzeugt eine sektorbasierte, vollständige Festplattenverschlüsselung. Dateien sind immer verschlüsselt und werden nur zur Ansicht oder zur Bearbeitung transparent entschlüsselt geöffnet oder geschrieben. Dateien auf einer solchen verschlüsselten Festplatte können nicht entschlüsselt werden, selbst wenn die Festplatte in einen anderen Computer eingebaut wird, sogar selbst wenn dieser eine weitere Installation von Crypt4000 enthält. Das Betriebssystem und alle temporären oder Speicherabbilddateien (pagefile.sys, Hibernation Datei) sind 100% verschlüsselt.
- **Lokale Administration.** Die Administrationskonsole kann vom Windows Administrator entkoppelt werden, um maximale Sicherheit zu gewährleisten. Die Konfiguration ist innerhalb der PBA in einem sicheren AES Container gespeichert. Verschieden Sicherheitskonfigurationen können verschiedenen Windowsbenutzern zugewiesen werden.
- **Wiederherstellung und Support.** Während der Installation muss der Benutzer eine PBA Sicherheitskopie (Snapshot) anlegen. Diese Kopie sollte auf einem externen Datenträger abgelegt werden. Die Technik der PBA Datensicherung wird von der Secuware genutzt, um dem Endbenutzer die Wiederherstellung und Supportdienste anzubieten. Support und Wiederherstellung ist ein Web basierter Service. Bitte besuchen Sie auch die Webseite www.secuware.de, um sich über diese Möglichkeiten zu informieren.

