

Das Sicherheits-Betriebssystem

Secuware Security Framework (SSF) erhöht die Sicherheit des Windows Netzwerks, indem ein Informationsnetz gebildet wird, in dem nur autorisierte Personen Zugang zu vertraulichen Daten haben. SSF kontrolliert Programme und Anwendungen, um den Verlust von Informationen zu verhindern und liefert somit eine äußerst stabile Computerumgebung.

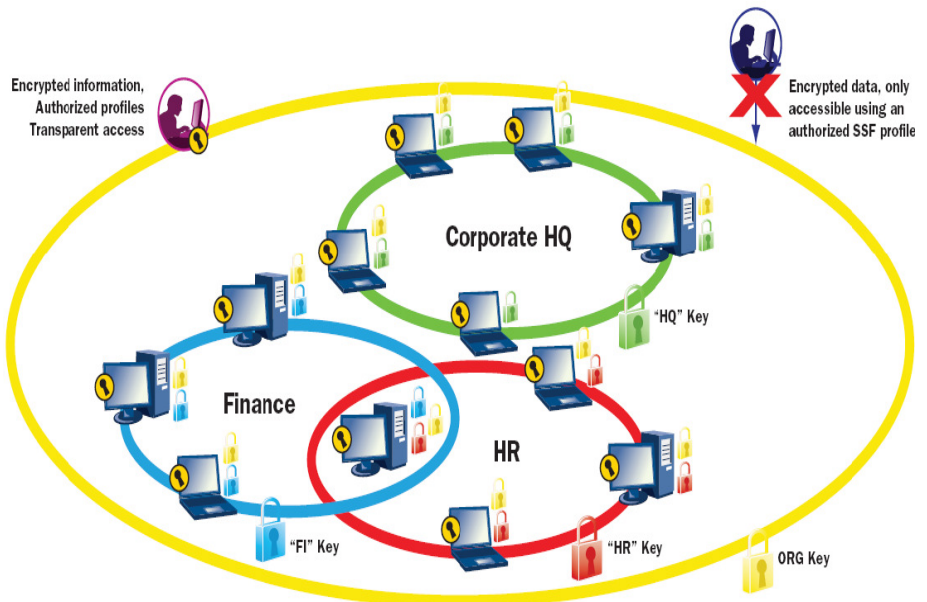
SSF bringt den Unternehmen nach der Installation die Kontrolle über ihr Netzwerk zurück:

- Ein Sicherheitsbetriebssystem für Zugangskontrolle und Verschlüsselung
- Flexible Architektur, die sich veränderten Verhaltensweisen, Bedrohungen und Systementwicklungen anpasst.
- SSF bildet innerhalb von Unternehmen geschlossene Informationssicherheitszonen, bis über die Grenzen des Unternehmens hinweg.
- Bildet eine sichere Umgebungen zum Schutz vor Datendiebstahl und Blockieren von Malware
- Ermöglicht einfaches Erstellen und Überwachen von Regeln durch enge Integration mit Windows und dem Active Directory
- Sorgt für erhöhte interne Sicherheit durch getrennte IT und Informations-Sicherheitskontrollen

„Piraterie ist ein sehr großes Problem. Wir benötigen einen Datenschutz für unsere Videoabteilung, da diese mit sehr empfindlichen kommerziellen Informationen arbeiten. Seitdem wir Secuware installiert haben, können wir unseren Kunden eine wasserdichte Garantie geben, dass es keine Informationsverluste gibt.“

“- Luis Valente, regionaler Administrator für Infrastruktur und Sicherheit, Warner Bros Mexiko

Closed-Circuit of Information



Secuware Security Framework ist für Windows entwickelt worden und übernimmt dabei die Eigenschaften von Windows, bei gleichzeitiger Bereitstellung höherer Sicherheitslevel. SSF erreicht dies durch ein „Sicherheitsgitter-Konzept“, das das ganze Unternehmen und dessen Netzwerke und Systeme umfasst und verbindet. Nicht autorisierte Angriffe, egal ob durch eingehende Malware oder Datendiebstahl, werden sofort gefunden und die betroffenen Systeme isoliert. Die Quelle kann sofort lokalisiert werden.

SSF liefert dauerhaft verfügbare, mehrdimensionale Sicherheit:

Sicherheit ab dem Start

Systeme werden ab dem Boot Prozess geschützt. Der Schutz kann nicht durch Low Level Tools umgangen werden

Closed-Circuit of Information

Benutzer bekommen nur den Zugang, den sie für ihre Aufgabe benötigen. Informationen werden innerhalb einer definierten Gruppe geschützt.

Physikalische Sicherheit gegen nicht autorisierten Zugriff

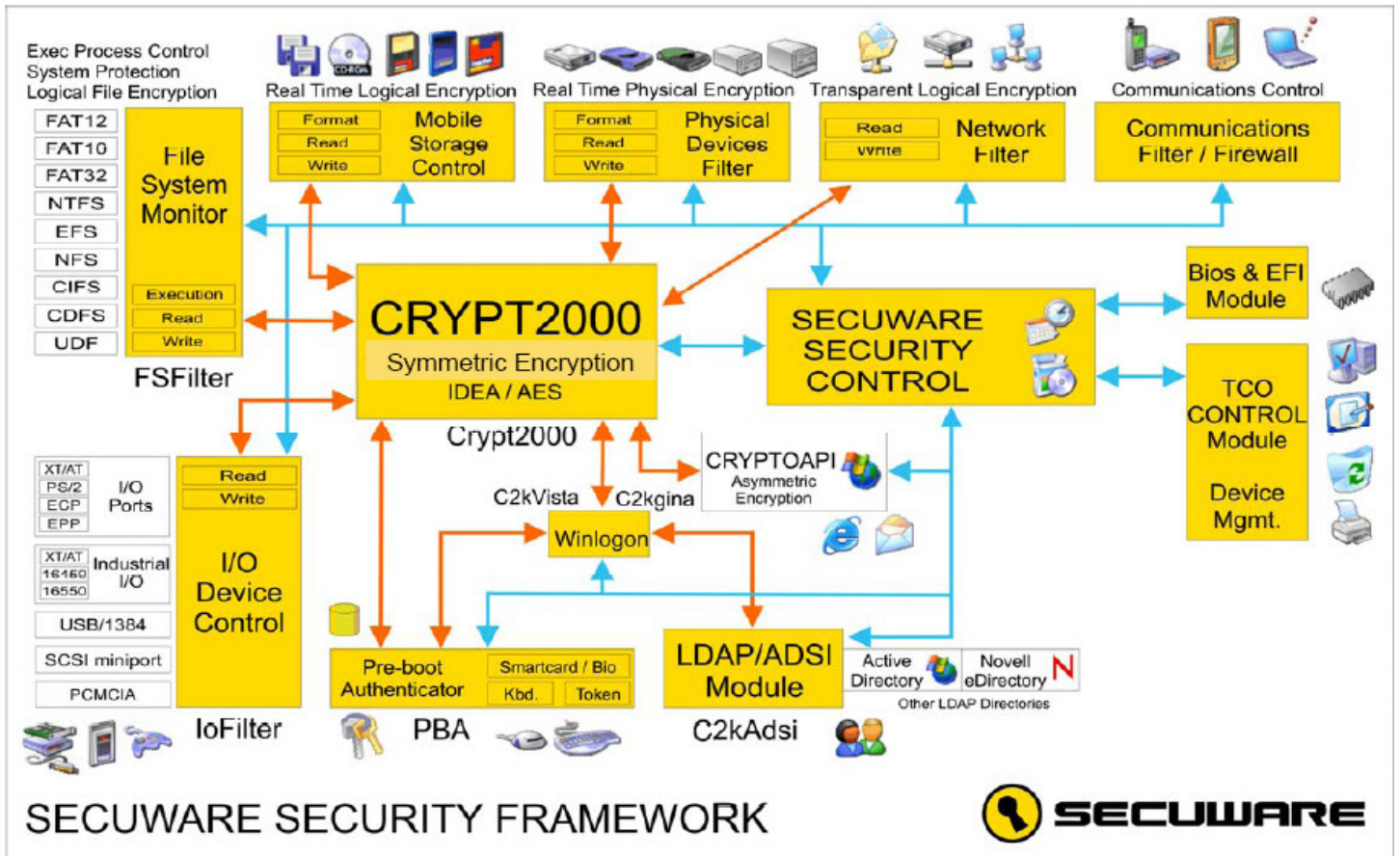
Sicherheit für jede Peripherie: Festplatten, USB, CD, DVD. Autorisierte Benutzer erhalten einen transparenten Zugriff.

Logische Sicherheit für Daten im Netzwerk

Daten bleiben passwortgeschützt, egal, wo sie gespeichert werden. Kodierte Daten sind dem Administrator oder Malware nicht zugänglich.

Erhöhte Stabilität für Soft- und Hardware

SSF ermöglicht die Autorisierung von Software. SSF ermöglicht die Autorisierung von Geräten.



Der modulare Rahmen von SSF liefert multidimensionale Sicherheit in einer Komplettlösung, die sich wechselnden Bedrohungen, Veränderungen und neuen Systemanforderungen über die Zeit hinaus anpasst.

Crypt2000 ist das Herz von SSF. Entwickelt, um sichere, vertrauliche Informationen, wie z.B. im spanischen Nationalen Amt für Abwehr, zu verschlüsseln. Crypt 2000 besitzt zwei Schlüsselfunktionen. Zuerst stellt es vor dem Booten des Betriebssystems eine PreBoot -Zugangskontrolle bereit.

Zweitens verschlüsselt es alle neuen Informationen auf dem Computer, sowie alle abgespeicherten Informationen, die auf ein anderes Gerät kopiert werden könnten. Crypt2000 stellt sicher, dass der Computer, alle Daten und Anwendungen, die auf diesem Computer gespeichert sind, nur von autorisierten Personen verwendet werden können.

Crypt2000 verschlüsselt alle Daten auf Festplatte, angeschlossenen Geräten, sowie Netzwerkordnern.

Alle Komponenten von Crypt2000 sind zentral verwaltbar durch einfache Integration in das Microsoft Active Directory.

Das **Devicemodul** kontrolliert alle Geräte, die sich an das Netzwerk anschließen. Seine Aufgabe ist es, nicht-autorisierten Hardware Geräten, wie z.B. CD- oder DVD-Brenner, USB Driver und/oder entfernbare Medien, den Zugang zum Unternehmensnetzwerk zu verwehren. Weiter verhindert SSF das Eindringen von Malware und Datendiebstahl.

Die **SSF Management Konsole** liefert eine einfache Schnittstelle, die direkt in an das Microsoft Active Directory angeschlossen werden kann. Microsoft Technologien stehen hier zur Verteilung und Verwaltung der Benutzer- und Computerprofile zur Verfügung..

Über Secuware

Gegründet 1998, ist Secuware eines der führenden Unternehmen in Europa für Unternehmenssicherheit. Die Firma ist von einem spezialisierten Anbieter stabiler Sicherheitslösungen für das spanische Verteidigungsministerium zu einem weltweiten Anbieter von Sicherheitsinfrastrukturen mit mehr als 800.000 Benutzern gewachsen.

