

**Kennen Sie Jemand dem der Computer gestohlen wurde, oder abhanden gekommen ist?**

*Secuware – schützt Ihre Daten, egal wo sie gespeichert sind: ob Laptop, PC, USB Stick, Netzwerkfolder, Personal Digital Assistant, Floppy, Smartphone, DVD oder CD.*

## Unsere Aufgabe

*Mit Secuware haben Sie ein starkes Instrument um das wichtigste Gut Ihrer Firma zu schützen – ihr geistiges Eigentum.*

Die meisten Firmen haben heutzutage einen wasserdichten Schutz um gefährliche Daten am Eindringen in ihrer Firma zu verhindern. Antivirus software, firewalls und SPAM-Filter geben Sicherheit gegen unerwünschte und zerstörerische Dateien. Aber wie schützt man wertvolles geistiges Eigentum ohne einen freien Fluss –sowohl innerhalb wie außerhalb Ihrer Firewall – zwischen Angestellte, Partner im Outsourcing, Kunden und Lieferanten im Laufe des normalen Geschäftsbetriebes zu verhindern? Wie verwaltet man die Firmendaten die anderen zur Verfügung stehen – zum Ansehen, Verarbeiten , Manipulieren, sogar zum Mitnehmen außerhalb der Firmen Infrastruktur?

## SECUWARE

### Eine mobile DATENVERLUST Lösung

- 1 Was wir tun
- 2 Wie es funktioniert
- 3 Seelenruhige Sicherheit
- 4 Vorteile der Security Admin

(Sicherheitsverwaltung)

---

Wissen Sie wer Ihre Daten gerade benutzt?

---

Secuware ist aufgrund seiner langjährigen Anwender Erfahrung- mehr als jeder Konkurrent - und ein weltweites Netz von über 500 Kunden als hochqualifizierter Partner in der Lage die sehr kritischen Datenschutzprobleme heute zu lösen. Unser marktführendes True-Enterprise System für mobiler Datenschutz und die gesicherte Virtualisierungs-Management-Lösung helfen Firmen und Behörden auf dem Weltmarkt überall ihre empfindlichen Daten aktiv zu schützen , kontrollieren und zu speichern – ob innerhalb einer Arbeitsgruppe, zwischen Abteilungen und Dienststellen oder mit Partnern und Lieferanten einen halben Globus entfernt. Gleichzeitig helfen wir die Vertriebskosten zu senken und den sicheren Informationsfluss (Verteilungsprozess?) zu optimieren. Sie arbeiten nach den Vier Autorisierungsprinzipien, die sichern, dass NUR:

**Autorisierte Einzelpersonen**, die  
**Autorisierte Geräte** benutzen, haben auf  
**Autorisierte Information** Zugriff durch  
**Autorisierte Anwendungen**.

Secuware wurde 1998 vom Internet Sicherheitspionier Carlos Jiménez gegründet um den Bedarf empfindliche Daten innerhalb und außerhalb der Wirtschaftssphäre zu schützen anzusprechen. Heute liefert die Secuware Security Framework (SSF) Plattform eine einzigartige Möglichkeit um Informationen dynamisch zu schützen, kontrollieren und zu verwalten. SSF basiert auf das Konzept der Closed Circuits for Information und wurde ursprünglich von Grund auf nach militärischen Vorgaben entwickelt, um sicherzustellen, dass autorisierte Personen produktiv arbeiten und die Information gemeinsam benutzen können, diese gleichzeitig aber vor Diebstahl und Mißbrauch geschützt ist. Mit diesem Design erlaubtes unsere flexible Struktur ihre Daten zu Schützen ohne Ihren bisherigen Workflow zu ändern.

SSF erweitert die Sicherheit von Windows Netzwerke durch Zusammenfügen verschiedener Technologien zu einer einzigartigen Kombination: Pre-Boot Authentifizierung (PBA) garantiert, dass nur autorisierte Nutzer Zugang zu einem autorisiertem Computer haben; zugleich verknüpft sich PBA mit Full Disk Verschlüsselung um Daten vor Diebstahl zu sichern; Device Controll erweitert diese Sicherheit – egal wo der User diese Information gespeichert hat oder trägt(z.B. USB Sticks); Anwendungs Controll schützt gegen Entführung und bietet zero-day Malwareschutz für die Computer Plattform; und durch Management der Enterprise-klasse lässt sich die Gesamtlösung skalieren und

hebt es zu einem grundsatzstützendes Fundament. (? Fragen Sie mich nochmal...) Wir nennen diese Weitsicht ein 360°- Vorgehen weil es nicht nur unseren Kunden ermöglicht, sich ihre Closed Circuits zu erstellen, es ist die umfassendste Komplettlösung erhältlich, um Datenlecks (Datenverlust) zu verhindern und ein stabiles Arbeitsumfeld zu schaffen.

Wenn es um SSF geht, dann kann keine andere Firma an die patentierte Technologie, Schlüsselösungen, erstklassigen Kundenstamm und Anwendungserfahrungen von Secuware heran.

## ***Schützt Daten, PCs und mobile Speichergeräte gegen Kompromittierung durch unbefugten Zugriff oder Diebstahl***

### ***Wie es Funktioniert***

360° (rundum) Sicherheit: Closed Circuits of Information (geschlossene Informationskreise)

**„Autorisierte Einzelpersonen, die Autorisierte Geräte benutzen, haben auf Autorisierte Information Zugriff durch Autorisierte Anwendungen.“**

Der Kunde (Sicherheitsadministrator, Chef der Sicherheitsabteilung (CSO –Chief Security Officer) oder Chef der Informationsabteilung) benutzt SSF um individuelle Profile für jeden Nutzer und jeden Computer zu erstellen. (Die Profile zu erstellen und zu unterhalten ist easy – kann aus Microsoft Active Directory her gemacht werden ohne Einbindung von einer Verwaltung durch Dritte.

Jeder Nutzer kann einer oder mehrerer Gruppen angehören – z.B. Finanz oder HR – und kann alle Informationen innerhalb jeder Gruppe teilen und ausschöpfen.

Hinter den Kulissen bewirkt SSF sämtliche Verschlüsselung, Schlüsselverwaltung, usw. um sicherzustellen, dass nur die User in den richtigen Gruppen Zugang zu den Informationen haben – ob sich diese auf einem USB Stick oder auf der Festplatte oder im Netzwerk befinden.

Weil jeder Computer sein eigenes Profil hat, ist es leicht einzurichten, dass dieser von vielen User genutzt werden kann, oder dass Einzelne Zugang auf mehrere verschiedene Computer haben.

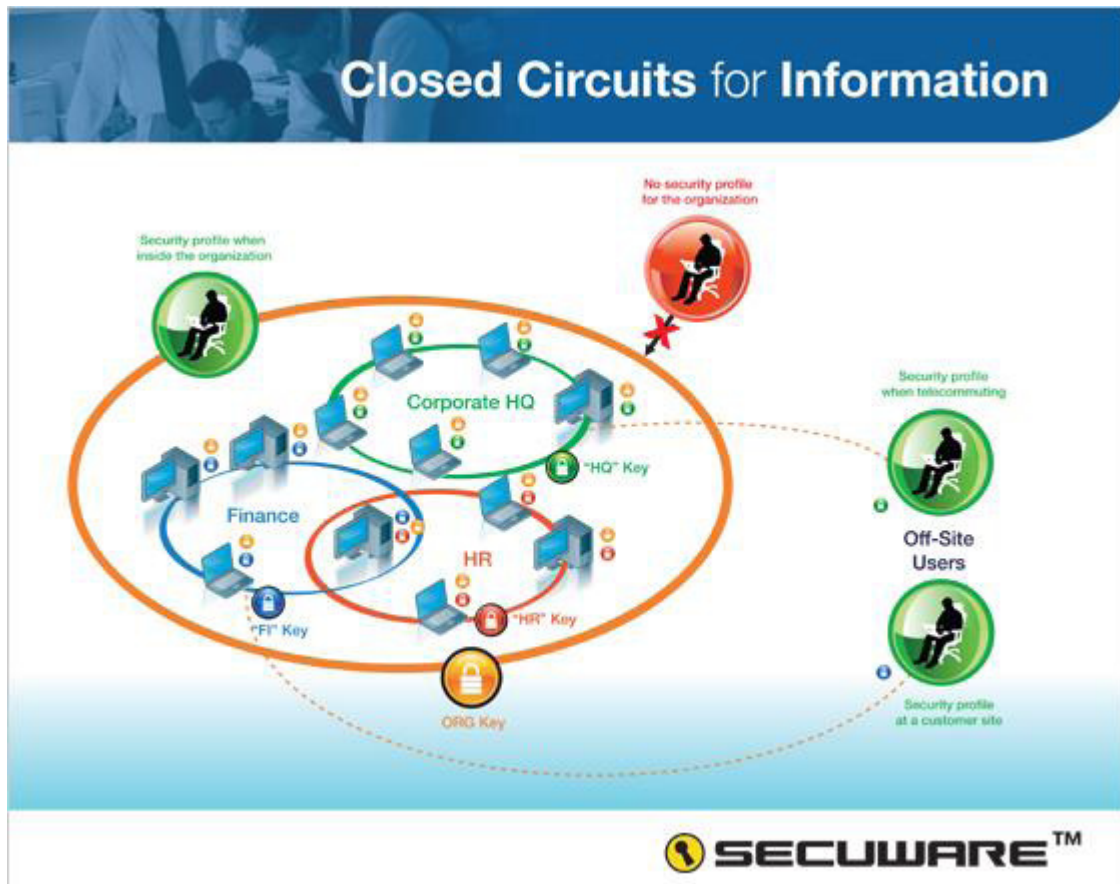
Zudem erweitert die Möglichkeit Informationen mit anderen sicher zu teilen die mobile Archivierung, so dass wiederum nur diejenigen, die autorisiert sind, auch diese Daten sehen können.

So, zum Beispiel, wie aus dem Diagramm zu sehen, hat Firma X es so eingerichtet, dass sollte J. Grün User von der Firmen Hauptstelle einen USB Stick den A. Blau User aus der Finanzabteilung im Flur verloren hat finden, er diesen wohl an sein PC anschließen könnte, ihm aber sämtliche Daten darauf versperrt bleiben. Wichtiger noch, dieser USB Stick ist physikalisch gesichert, so dass, sollte A. von der Finanzabteilung seinen USB Stick mit den Quartalsergebnissen auf der Straße verloren haben, ihn keiner lesen oder entziffern oder seine AES 256-bit Verschlüsselung knacken könnte.



[www.secuware.com](http://www.secuware.com)

Letztendlich hat J. ganz andere Anwendungen die ihm zur Verfügung stehen als A., eingerichtet nach den wirtschaftlichen und Sicherheitsbedürfnissen der Firma. SSF bietet außerdem Anwender-Kontrolle damit J's Zugang zu Anwendungen und Geräten/Ports auf seinen Standort – ob am Flughafen oder innerhalb der gesicherten Firmen LAN- angepasst wird.



## Es ist Zeit Ihre Information zu schützen

### Beruhigende Sicherheit

*Wenn Sicherheit zählt...*



	<b>Felsenfeste Sicherheit</b>	
Feature	Funktion	Vorteil
Sicherheitsprofile ./ Group policy Objekteinbindung	In anderen Lösungen, haben IT Angestellte Zugang zum GPO, auch zu denen die die Sicherheit betreffen. Mit SSF hat NUR das Sicherheitsteam Zugang zu den Sicherheitsprofilen.	Verbessert die Sicherheit indem der Bereich ausschließlich dem Sicherheitsteam unterliegt.
Aufgabenbasierende Verwaltung	Wie oben erwähnt, ist die Systemverwaltung getrennt von der Sicherheitsverwaltung	Die Trennung der Befugnisse und Aufgaben fördert sowohl Administration wie auch Sicherheit: Die Sicherheitsverwaltung kontrolliert die Sicherheitsprofile, die Systemverwaltung kontrolliert alle anderen IT- und Netzwerkbereiche.
IT Administrator und Sicherheitsadministrator haben keinen Zugang zu den eigentlichen Sicherheitsschlüssel	Verschlüsselungsschlüssel sind auch verschlüsselt auf allen Systemen und sind niemandem zugänglich.	Schließt eine weitere kompromittierbare aber menschliche Versuchung aus.
Sämtliche gekoppelte Speicher – interne Festplatten, CD/Rs, DVDs, USB Sticks und Laufwerke – sind physikalisch verschlüsselt	Viele andere Produkte benutzen logische Verschlüsselung, die viel einfacher zu knacken ist.	Höhere Sicherheit für alle gespeicherten Medien die außerhalb des Schutzes des Firmennetzwerkes und Standortes mitgenommen werden.

Off-line Sicherheitsprofil	SSF funktioniert weiter, auch wenn das System auf Firmen LAN arbeitet.	Bewahrt die Sicherheit wenn der User nicht ans Firmennetz angeschlossen ist.
Option der flexiblen Verschlüsselung für tragbare Medien	Passt die Firmensicherheitsfunktion den Wirtschafts- und Sicherheitsbedürfnissen der Firma an.	Erlaubt es der Firma Entscheidungen zu treffen, die die Produktivität gegenüber den Sicherheitsbedürfnissen abwägt.
Granulare Gerätekontrolle/Erlaubnis Einstellungen	Siehe oben	Siehe oben
Mehrere Sicherheitsschichten	SSF ist eine multi-dimensionale Sicherheitslösung, was bedeutet, dass SSF Sicherheitsprofile bei User, Computer, Anwendungen und externe Geräte durchsetzt.	Erlaubt es den Firmen eine Sicherheitsrichtlinie aus strategischen Gesichtspunkten zu entwickeln und durchzusetzen.
Schutz gegen Datenverlust	Sämtliche SSF ist darauf abgestimmt einen Datenverlust zu verhindern.	Beugt Peinlichkeiten vor und schützt vor Kosten verursacht durch den Verlust vertraulicher Daten
Einfache Anwendung	Für Administrator und User	„Einfache in der Anwendung“ bietet deshalb bessere Sicherheit, weil eine komplizierte, schwierig-anzuwendende Lösung nicht korrekt bedient wird.

## Hat Ihre Firma USB-Sorgen?

### USB Sticks sind eine echte Sicherheitsgefahr für Firmen ohne Datenschutz oder Geräte-Management!

80% der Angestellten nehmen Akten von der Arbeit mit um sie zuhause zu benutzen und die meisten bevorzugen USB Sticks über Laptops um Daten abzuspeichern einfach weil sie leichter, günstiger, handlicher und viel bequemer sind. 33% speichern ihre Arbeit auf USB Sticks – gegenüber 14% die noch einen Laptop benutzen. Firmen werden viel zu spät darauf aufmerksam, meist ist es zu spät!!!

C4K ist leistungsfähiger im Schutz von kritischen Daten und transparenter für seine Anwender als jedes andere Produkt auf dem Markt heute. Ursprünglich für das Verteidigungsministerium (von ?) entwickelt, bietet es tatsächlich einen Schutz der höchsten Ansprüche für Ihre kritischen Firmendaten.

### Robuste Endpunktschutz gegen Informationsverlust

**Secuware SSF** ist der umfassendste, sicherste und in der Anwendung, der einfachste Endpunktschutz gegen Datenverlust auf dem Markt heute - es bietet Kontrolle über jeden Endpunkt und jedes Gerät, über jeden Interface.

Mit Secuware Lösungen können Sie nach Bedarf aufstocken. Fangen Sie mit Pre Boot Autorisierung, Zugangskontrolle, physikalische und logische Verschlüsselung der C4K an. Nehmen Sie dann Geräteverwaltung um die Nutzung und Mißbrauch von USB Sticks und anderen tragbaren Medien zu kontrollieren dazu und Sie sind schon auf halbem Weg zu einer vollen Secuware Security Framework (SSF). Wenn Sie später so weit sind, können nun noch das Anwendungsintegritätsmodul und das Auditverlaufmodul hinzunehmen. Jedes Element wird durch eine einzelne Zentralkonsole gesteuert und ist direkt in die Netzwerkverzeichnisstruktur eingebunden um die Ausführung der Richtlinien zu erleichtern.

# *Schützt Ihre Daten, persönliche Rechen- und mobile Speichergeräte gegen Kompromittierung durch unbefugten Zugriff oder Entwendung*

**Die Leistungsfähigkeit durch die Zentralverwaltung bietet Organisationen eine betriebliche Effizienz und sichert niedrigste Betriebskosten**  
**- Die Regierung CISO**

## Vorteile für den Sicherheitsadministrator

Von Tomas Lara & Jürgen Saamen

	Anwendung	
Datenschutz	Geschäftsrisiko	Wert der SSF
		(SSF bietet: )
Sicheres Outsourcing	Zusammenarbeit und Informationssharing sind wichtig für den Erfolg eines Geschäfts. Wenn aber geistiges Eigentum an die Konkurrenz gelangt, können Umsatzverluste, Verlust von Marktanteile, Wertverlust sowie verminderter Markenwert die Folge sein.	<ul style="list-style-type: none"> <li>• Sichert wertvolle Dateien und Daten in Dokumenten innerhalb der RFPs.</li> <li>• Sichert gemeinsame Nutzung von Produktspezifikationen und Designinformationen mit OEM Partner</li> <li>• Verhindert eine Weitergabe sensibler Daten an Konkurrenten der auf die gleichen Partner weltweit angewiesen ist.</li> <li>• Gewährleistet und belegt Einhaltung des ITAR</li> <li>• Sichert Kundendaten</li> </ul>
Einhaltung von Richtlinien	Traditionelle Sicherheitsvorkehrungen reichen heute nicht mehr aus um unerwünschte oder unbeabsichtigte Zugriffe auf vertrauliche Inhalte wie externe Kommunikationen mit Partnern, Vorstandskommunikationen, Informationen aus dem Personalwesen oder Geheimplaten zu verhindern.	<ul style="list-style-type: none"> <li>• Ununterbrochenen Schutz um sicherzustellen, dass Informationen während ihrer ganzen Lebensdauer geschützt sind, ohne Rücksicht auf den Aufbewahrungsort.</li> <li>• Dynamische Richtlinienkontrollen erlauben dem Inhaltseigner seine Informationsrichtlinien dynamisch zu ändern und abgelaufene Dokumente aufzurufen, auch nachdem deren Inhalt bereits verteilt wurde.</li> <li>• Detaillierte Auditnachverfolgung spürt ununterbrochen den Informationszugang während der Lebensdauer des Inhaltes und liefert den Nachweis der Einhaltung der Richtlinien</li> <li>• Integration innerhalb existierende Anwendungen und Sicherheits-Infrastruktur erhält den existierenden Workflow und vermindert die indirekten Kosten.</li> </ul>
Einhaltung von Vorschriften	Neue Datenschutzgesetze und Einhaltungsrichtlinien gewährleisten eine durchsichtige Revision und Haftung für die Verteilung empfindlicher Daten, stellen aber große Belastungen für Finanzinstitutionen, Gesundheitsanbieter und andere dar. Diese Vorschriften nicht einzuhalten kann zu zivilrechtlichen und strafrechtlichen Konsequenzen und Schadensersatzansprüchen führen.	<ul style="list-style-type: none"> <li>• Durchgehende Verschlüsselung schützt Daten, Dokumente und HTML Inhalt, egal wo diese entstehen, verteilt oder gemeinsam genutzt werden.</li> <li>• Dynamische Richtlinienkontrolle sichert die Einhaltung von Informationsklassifizierungsrichtlinien</li> <li>• Für Einzelfalluntersuchungen bieten detaillierte Revisionsspuren den Nachweis der Einhaltung (der Richtlinien) und unterstützen die Bildung einer Nachweiskette.</li> </ul>



**Extending Enterprise Windows Security  
and Beyond**

**Secuware Deutschland GmbH**  
 Eifelstraße 9  
 53119 Bonn  
**Telefon:**  
 0228 962979 0  
**E-mail:**  
 sales@secuware.de