



Managed CompuSec®

Software Sicherheit für Desktop PC's und Notebooks.
Optional mit Fingerprint Authentifizierung.



Managed CompuSec® ist die Sicherheits-Suite zum Schutz von Desktop PC's und Notebooks. Optional mit Fingerprint Authentifizierung. Sie bietet Zugriffskontrolle, Single Sign On, Festplattenverschlüsselung, CD Verschlüsselung, Dateiverschlüsselung, Netzwerkverschlüsselung, Containerverschlüsselung und VoIP Verschlüsselung.

Managed CompuSec® repräsentiert höchste Sicherheitsstandards und ist kombiniert mit einer flexiblen, für den Nutzer transparenten Funktionsweise. Einzelnutzer, kleine Nutzergruppen sowie auch große Unternehmen nutzen Managed CompuSec®. Managed CompuSec® kombiniert eine Reihe von oft benötigten Sicherheitsfunktionen, die der Nutzer je nach Bedarf bei der Installation oder bei der Personalisierung wählen kann. Große Organisationen und Unternehmen erhalten zudem alle Funktionen für eine effiziente Installation und Nutzung von Managed CompuSec®, wie z.B. die bedienerlose Installation, automatisierten Rollout, die Unterstützung von Festplattenimages, die zentrale Softwareverteilung, zahlreiche Servicefunktionen und das zentrale Nutzermanagement.

Pre-Boot-Authentifizierung

Bei jedem Start des Rechners wird der Benutzer zur Eingabe der Benutzer-ID und seines Passwortes aufgefordert. Erst danach startet das Betriebssystem. Dieser Prozess garantiert höhere Sicherheit als der Login-Prozess des Betriebssystems. Eine zusätzliche Funktion in Managed CompuSec® ermöglicht die Nutzung des UPEK TouchStip Fingerprint Sensors als Teil des Authentifizierungsprozesses. Der Nutzer authentifiziert sich per Fingerprint oder Passwort oder Fingerprint und Passwort. Managed CompuSec® stellt sowohl in der Pre-Boot-Phase als auch nach dem erfolgreichen Login zahlreiche nützliche Hilfefunktionen zur Verfügung u.a. bei Verlust des Passwortes.



Passwortverwaltung

Der Kunde kann die Passwort-Strategie seinen Bedürfnissen anpassen. Variabel sind die Passwortlebensdauer nach Tagen und/oder Logins, der Passwortwechsel zu jeder Zeit, die Passwortlänge und weitere Einstellungen. In den Fällen wo ein Passwort vergessen wurde, bietet ein Challenge/Response Verfahren in Verbindung mit der GlobalAdmin Station eine einfache und sichere Möglichkeit, um dem Benutzer ein neues Passwort zuzuteilen.

Single Sign On

Managed CompuSec® verschlüsselt und speichert das System-Anmeldepasswort zusammen mit der Benutzer-ID und dem Domain-Namen für das automatische Logon am Betriebssystem. Dies ersetzt die traditionelle Anmeldeprozedur des Benutzers am Betriebssystem. Zusätzlich kann der Benutzer den Rechner über die Tastatur oder einen Bildschirmschoner vor unbefugtem Zugriff sperren.



Festplattenverschlüsselung

Die Festplattenverschlüsselung von Managed CompuSec® nutzt den schnellen AES Algorithmus. Die Verschlüsselung erfolgt für alle Sektoren der Festplatten und schließt das Betriebssystem mit ein. Die Initialverschlüsselung kann direkt nach dem Login des Benutzers bei Managed CompuSec® oder nach dem Login unter dem Betriebssystem (Hintergrundverschlüsselung) ausgeführt werden. Die Hintergrundverschlüsselung ermöglicht es dem Benutzer, den Verschlüsselungsprozess zu unterbrechen und den Computer jederzeit herunterzufahren oder den Hibernation-Modus zu nutzen. Sehr wichtig für Nutzer von mobilen Systemen ist die Unterstützung des Hibernation Modus des Windows Betriebssystems. In diesem Modus werden die Inhalte des Arbeitsspeichers (RAM) als verschlüsselte Hibernation-Datei auf die Festplatte geschrieben, bevor der Computer herunterfährt. Beim Neustart werden nach der Pre-Boot-Authentifizierung des Benutzers die RAM-Inhalte wieder von der verschlüsselten Hibernation-Datei geladen und der Benutzer kann seine Arbeit fortsetzen.

Verschlüsselung von CD's/DVD's & Wechselmedien - CDCrypt

CD's/DVD's und Wechselmedien wie Memory Sticks und USB Laufwerke können mit Managed CompuSec verschlüsselt werden. Mit der zentralen Administration über GlobalAdmin ist es möglich die Verschlüsselung für alle oder einzelne Computer ein- oder auszuschalten. Der Nutzer kann das Recht erhalten, den Verschlüsselungsmodus zu verändern. Damit erhält das Unternehmen die Möglichkeit Sicherheitsrichtlinien umzusetzen, z.B. die ausschließliche Nutzung von verschlüsselten CD's/DVD's und Wechselmedien. Dies minimiert Datendiebstahl durch Insider und schützt beim Verlust von Daten. Die Verschlüsselung arbeitet transparent im Hintergrund.



Netzwerkverschlüsselung für sichere Kommunikation in Firmennetzwerken – IPCrypt Client

Managed CompuSec® bietet IP-Verschlüsselung für WAN- und LAN-Nutzer. Der IPCrypt Client ist eine bei der Installation auswählbare Funktion von CompuSec®. Der IPCrypt Client unterstützt IP Adresspools, Datenkompression, mehrere Einwahlpunkte und weitere Funktionen. Die IP Verschlüsselung von Managed CompuSec® benötigt einen Cryptor als VPN-Gateway im Netzwerk.



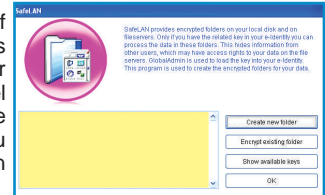
Dateiverschlüsselung - DataCrypt

Managed CompuSec® beinhaltet DataCrypt, welches den Nutzern ermöglicht, einzelne Dateien zu verschlüsseln. Mit DataCrypt können die Nutzer verschlüsselte Nachrichten per E-Mail, FTP etc. versenden. Die Daten werden verschlüsselt versendet oder mit einem anderen Medium transportiert. Zusätzlich ist es mit Managed CompuSec® möglich die Dateien auf sicherem Wege auszutauschen. DataCrypt nutzt dazu ein Public-Key Verfahren mit der Schlüsselgenerierung über elliptische Kurven. DataCrypt nutzt die neue "Sealing" Technologie, die alle Strukturen im Header der verschlüsselten Dateien versteckt. Sealing erlaubt den Schutz der verschlüsselten Dateien vor neugierigen Augen bei Ihrer Reise durch das Internet.



Verschlüsselung von Dateien und Verzeichnissen auf Servern - SafeLan

Datei- und Verzeichnisverschlüsselung mit Managed CompuSec® kann auf dem lokalen Rechner oder auf Netzlaufwerken durchgeführt werden. Diese Funktion stellt sicher, dass alle Dateien, die in das Verzeichnis zur Verschlüsselung geschrieben, verschoben oder kopiert werden, automatisch und absolut transparent für den Benutzer verschlüsselt werden. Dies gewährleistet, dass nur Nutzer, die einen autorisierten Zugangsschlüssel besitzen, Zugang zu diesem Verzeichnis haben und somit Dateien entschlüsseln, d.h. lesen können. Diese Funktion wird verwendet um Benutzerrennung auf Unternehmensservern auf kryptografischem Wege zu realisieren. Sicher ist, dass selbst der Server-Administrator die Inhalte der verschlüsselten Dateien nicht lesen kann.



Verschlüsselte Sprachkommunikation - [ClosedTalk]

[ClosedTalk]® ist die CompuSec® Komponente für die verschlüsselte Sprachübertragung zwischen zwei CompuSec® Nutzern. [ClosedTalk]® verwendet die Soundkarte des PC's und spart dadurch externe Geräte. Die Sprachdaten werden kostengünstig und sicher über das Internet ausgetauscht. Anstatt mit der Telefonnummer erfolgt die Anwahl des Gesprächspartners mittels der persönlichen E-Mail Adresse. [ClosedTalk]® nutzt gesicherte Vermittlungsrechner im Internet zur Vermittlung der Gespräche. Die Verwendung ausgefeilter Sicherheitstechnik garantiert die Vertraulichkeit sowohl der Gesprächsinhalte als auch die der Verbindungsdaten.



Containerverschlüsselung - [DriveCrypt]

Die DriveCrypt Funktion von Managed CompuSec bietet eine einfache und sichere Möglichkeit der Datenspeicherung auf der Festplatte ohne diese komplett zu verschlüsseln. [DriveCrypt] erzeugt dazu einen Datencontainer auf der Festplatte verschlüsselt mit AES Algorithmus und 256Bit Schlüssellänge. Für den normalen Gebrauch wird der Datencontainer als separates Laufwerk verbunden und angezeigt. Alle Daten die in die in den Datencontainer geschrieben, verschoben oder kopiert werden, werden automatisch und absolut transparent für den Benutzer verschlüsselt.



Identitätsmanagement

Ein universelles Passwortmanagement unterstützt PC und Internet basierende Anwendungen. Die Identität des Anwenders wird bei der CompuSec® Anmeldung einmalig festgestellt und dann auf Wunsch automatisiert anderen Anwendungen mitgeteilt. Es werden zusätzlich zertifikatsbasierte Anmeldeprozesse an Microsoft Domain Controllern, Lotus Notes, Novell und anderen Netzwerken unterstützt.

Installation & Verwaltung

Managed CompuSec® kann nur mit zentraler Verwaltung – GlobalAdmin - installiert werden. Die GlobalAdmin Station verwaltet alle Rechner, Benutzerprofile, Rechte, Schlüssel und weitere Daten der Managed CompuSec Installationen und bietet Funktionen für zentrale, bedienerlose Installationen, automatische Software Rollouts und Software Updates, ein remotes Passwortrücksetzen und komplette Verwaltung der VPN-Funktionen. GlobalAdmin verwaltet den Zugriff mehrerer Benutzer auf einen Rechner bzw. den Zugriff eines Benutzers auf mehrere Rechner. Managed CompuSec® kann als integrierter Teil einer unternehmensweiten PKI-Struktur genutzt werden. Ein automatischer Abgleich mit der Microsoft Nutzerverwaltung und "Active Directory" ist für die Managed CompuSec® Verwaltung vorhanden.

Support

Der Abschluß eines Wartungs- und Servicevertrages ist empfehlenswert. Wir beraten Sie gerne zu den Supportangeboten für Ihr Unternehmen.

Systemanforderungen

- PC Notebook / Workstation oder Tablet PC mit Intel Architektur
- Windows 7, Windows Vista und Windows XP (64 & 32 Bit)
- Windows Server 2003, Windows Server Server 2008 und Windows Server Server 2008R2
- 40 MB freier Festplattenspeicherplatz
- Soundkarte für [ClosedTalk]®
- UPEK TouchStrip Fingerprint Sensor bei optionaler Nutzung.



CE-Infosys GmbH
 Am Kümmerling 45
 D-55294 Bodenheim
 Germany
 Tel.: +49 (0) 6135 / 77 0
 Fax: +49 (0) 6135 / 77 77
 de.sales@ce-infosys.com

CE-Infosys Pte Ltd
 12 Tanney Road
 #09-01/02 HB Centre 1
 Singapore 347722
 Tel.: +65 6899 9392
 Fax: +65 6899 9373
 sg.sales@ce-infosys.com

CompuSec und [ClosedTalk] sind registrierte Markenzeichen der CE-Infosys Pte Ltd in Singapur. UPEK und TouchStrip sind registrierte Markenzeichen der UPEK, Inc.

Händler: