

- Mobile Speicher blockieren
- USB-Sticks, Speicher, Kameras usw.
- Dateitransfer protokollieren
- HTTP und FTP überwachen
- Weiße und Schwarze Listen
- Berechtigungen und Freigaben
- Terminal Services und CITRIX-Umgebungen
- Active Directory-Integration

# USB- und ENDPOINT SECURITY

## Security.Desk

Schützt Ihre Daten und Ihr Netzwerk  
vor multiplen Gefahren.

Die USB- und Endpoint-Security-Lösung Security.Desk regelt und überwacht die Nutzung mobiler Speicher, Smartphones, Digitalkameras etc. an Ihren PCs und verhindert unbefugte Benutzung, Einschleusung von Malware und Datenklau über Hardware-Schnittstellen und das Internet. Dabei geht die Software weit über die Möglichkeiten von Add-Ons gängiger Virenschutzlösungen oder Bordmittel der Hersteller hinaus.



## Funktionsüberblick

- Active Directory-Integration
- Rechtevergabe: erlauben, nur lesen, verbieten – getrennt nach HW-Schnittstelle – pro User, Gruppe, OU & Gerät
- Protokoll der Dateibewegungen von und auf Wechseldatenträger
- Blockierung des Lesens oder Schreibens bestimmter Dateitypen von oder auf Wechselspeicher
- Erkennung von verbotenen „embedded files“ in Office-Dateien
- Überwachung der Dateibewegungen lokaler Laufwerke an Thin Clients
- Übersichtlicher zentraler Kontrollstand für Compliance Management, Dienstverteilung und Reporting
- Freie Ergänzung zu überwachender USB-Gerätetypen
- „Weiße Liste“ für spezielle Geräte (nach ID) oder Gerätetypen
- Verbot von Softwareanwendungen über die „Schwarze Liste“
- Temporäre Freischaltung von Offline-Rechnern über Zugriffscode
- Alarmierung via E-Mail oder Tray Icon
- Security-Dienst ist nicht beendbar
- Integration mit Store O`Crypt (AES 256 hardwareverschlüsselter USB Stick von FCS)
- Flash Reminder – Erinnerung beim Abmelden von Ihrem PC, falls sich am Rechner noch angeschlossene Wechseldatenträger befinden
- Schutz vor BadUSB (Speichersticks mit manipulierter Firmware) durch die Kontrolle von Eingabegeräten (Maus und Tastatur) sowie Netzwerkadaptern
- Pro Client werden die BIOS-Information sowie die Daten der logischen Laufwerke inklusive Kapazität (gesamt / belegt / frei) ausgelesen und angezeigt
- Die Daten der logischen Laufwerke der Clients werden zusammen mit dem „BitLocker“-Status ausgelesen
- Security.Desk zeigt die vollständigen Daten zum Betriebssystem der Clients an (Version, Release, Build-Nr., Service Pack etc.)
- Sie erkennen an der BIOS-Information in Security.Desk pro Gerät oder über einen Bericht, ob an diesen Clients „UEFI Secure Boot“ aktiviert ist oder nicht
- Windows Update-Optionen und Status je Rechner sowie Info zum Windows Update Server



## Schnittstellenüberwachung mit Security.Desk

**Die USB- und Endpoint-Security-Lösung Security.Desk regelt und überwacht die Nutzung mobiler Speicher, Smartphones, Digitalkameras etc. an Ihren PCs und verhindert unbefugte Benutzung, Einschleusung von Malware und Datenklau über Hardware-Schnittstellen und das Internet.**

Dabei geht die Software weit über die Möglichkeiten von Add-Ons gängiger Virenschutzlösungen oder Bordmittel der Hersteller hinaus. So können Sie z.B. genau definieren, welcher Benutzerkreis welche Dateien von und auf Wechseldatenträger(n) transferieren darf bzw. welche Dateitypen dafür nicht erlaubt sind (z.B. exe-Dateien). Sämtliche Dateibewegungen lassen sich auch protokollieren.

Der zentrale Kontrollstand der Managementkonsole ermöglicht es, sämtliche Rechte für die Nutzung mobiler Speicher und Schnittstellen vom Administratorarbeitsplatz aus zu setzen sowie Warnmeldungen oder Berichte auszuwerten.

Security.Desk lässt sich mit dem **Active Directory** koppeln, um die Rechte auf Basis von OUs, Gruppen oder einzelner Benutzern zu vergeben.

Security.Desk ist führend bei der **granularen Absicherung** der Clients im Netzwerk gegen unerlaubte und unkontrollierte Verwendung von mobilen Speichern (USB-Sticks, Speicherkarten, Smartphones, Kameras etc.) und Datentransfers.

**Zudem unterstützt Sie Security.Desk dabei, indem die Lösung:**

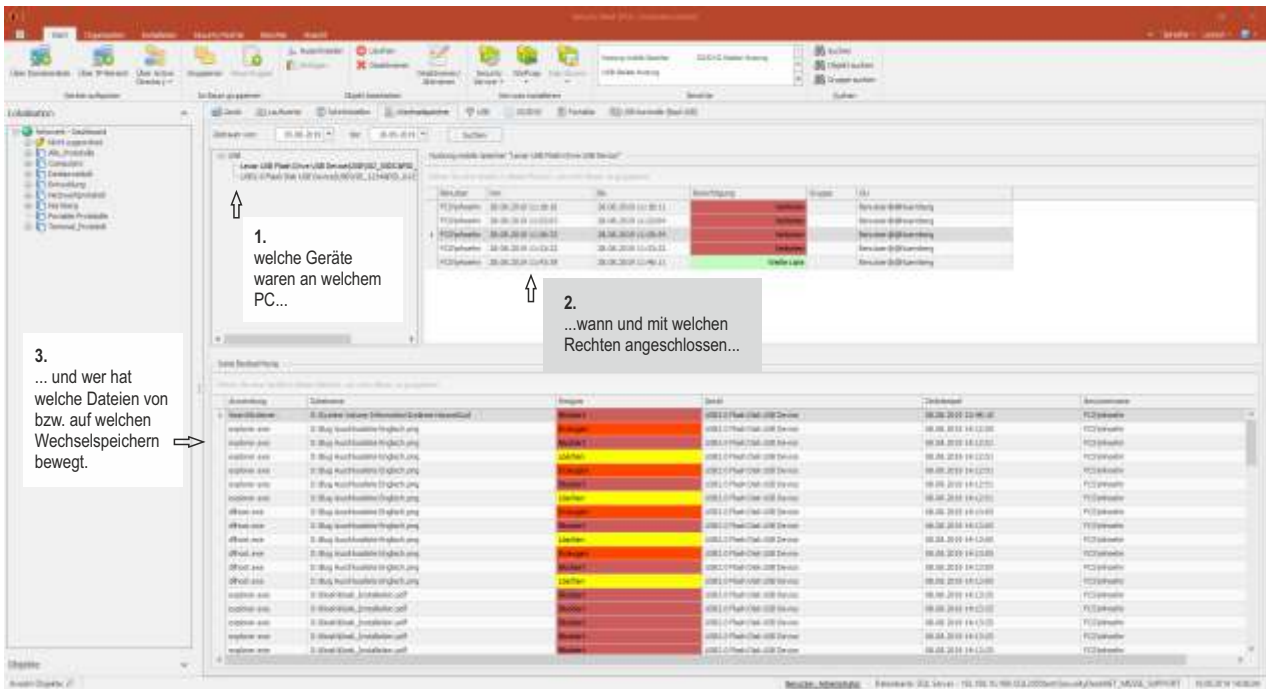
- **unkontrollierten Datenabfluss verhindert,**
- **Dateibewegungen protokolliert,**
- **Dateien für Dritte unlesbar macht,**
- **die Ausführung unerwünschter Programme verhindert oder**
- **das Eindringen externer Gefahren nicht möglich macht.**



- Schützt Daten und Netzwerke vor Datendiebstahl oder dem Einschleppen von Viren und Trojanern über Wechseldatenträger
- Auch mobile Speicher an Thin Clients in Windows Terminal Server- oder CITRIX-Umgebungen lassen sich überwachen

Überwacht werden sämtliche Hardware-Schnittstellen und Internet-Protokolle am Endgerät, u.a.:

- Wechselspeicher (USB, Speicherkarten etc.)
- CD/DVD
- Smartphones/Tablets
- Digitalkameras
- WLAN
- Bluetooth
- HTTP/FTP
- LPT und COM Ports
- SMTP
- Terminal Sessions



## Überwachung sämtlicher Schnittstellen

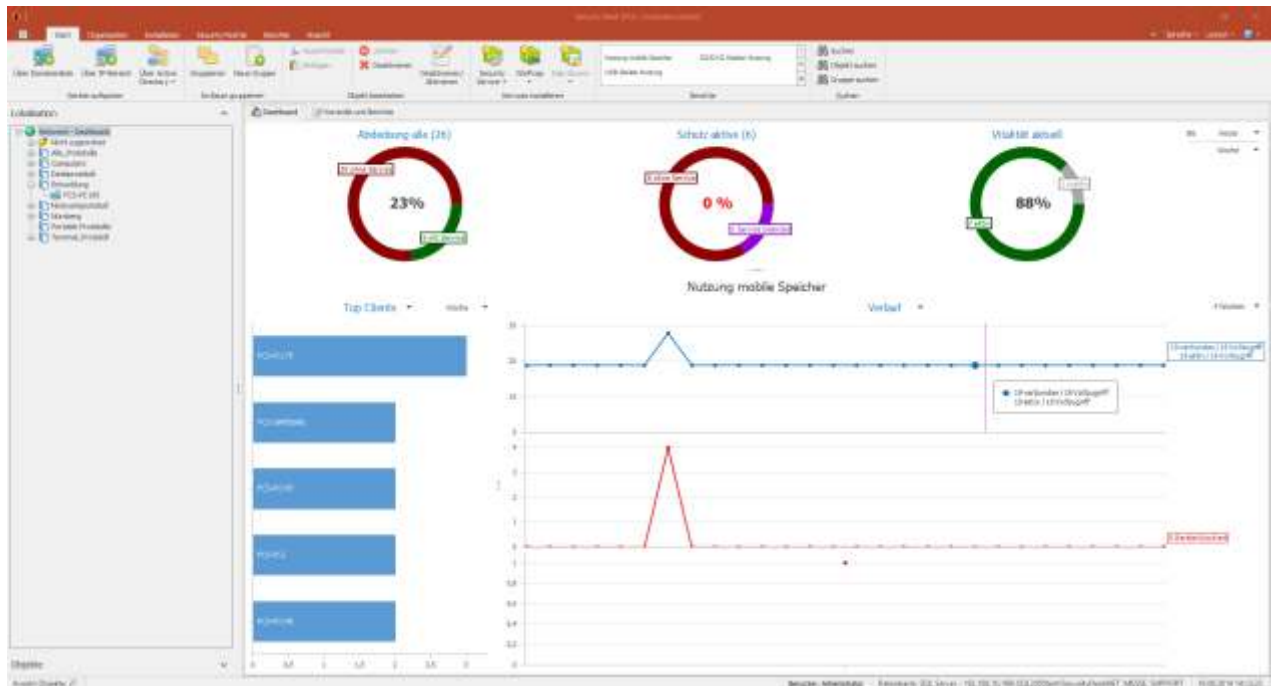
- Security.Desk kontrolliert den Einsatz von mobilen Speichern, Smartphones, Digitalkameras etc. an den PCs Ihres Netzwerkes
- Die Software überwacht sämtliche Hardware-Schnittstellen und Internet-Protokolle (z.B. http, ftp, ...) am Endgerät
- Es wird automatisch erkannt, wenn z.B. ein Flash-Speicher über USB oder über FireWire an einen PC angeschlossen oder eine CD oder SD-Speicherkarte eingelegt wird
- Sie geben vor, was dann zu tun ist: z.B., ob der Datentransfer komplett blockiert wird oder ob der Nutzer die enthaltenen Dateien nur ansehen darf. Dabei lassen sich alle Dateibewegungen protokollieren

## Dateiprotokolle und Reporting

- Dateiprotokolle helfen z.B. dabei zu verfolgen, welcher Mitarbeiter an einem PC Daten mit einem mobilen Speicher ausgetauscht und verwendet hat
- Diese Kontrolle kann bis auf die Ebene der erlaubten Dateien und Dateitypen heruntergebrochen werden
- Das Reporting gibt einen aktuellen Überblick über den Einsatz von z.B. externen Speichermedien pro User und Rechner im Netzwerk
- Zudem informiert es über die Aktionen Ihrer Benutzer an den Schnittstellen der Endgeräte per E-Mail

## Interaktives Dashboard

- Das Dashboard zeigt den aktuellen Status der Endpoint Security im Netzwerk
- Es ermöglicht detaillierte Analysemöglichkeiten
- Kuchen- und Balkendiagramme informieren über den Schutz-Status der Clients
- Umfasst diverse Verläufe über die Nutzung mobiler Speicher und über Dateibewegungen
- Intuitive Drilldown-Optionen
- Darüber hinaus verfügt es über vorgefilterte Standardberichte



Interaktives Dashboard

## Granulare Rechtevergabe

- Rechtevergabe: auf User-, Gruppen- oder Computerebene; so können jedem einzelnen Computer, Benutzer, jeder Gruppe oder OU pro Schnittstellentyp unterschiedliche Rechte zugewiesen werden
- Rechtehierarchie: lässt Ausnahmen von Richtlinien auf mehreren Ebenen zu
- Individuelle Restriktionsmöglichkeiten: Schnittstellen können in jeder Hierarchiestufe mit folgenden Rechten belegt werden: alles erlaubt, nur lesen, nicht schreiben, alles verboten
- Weitere individuelle Konfigurationsmöglichkeiten: Erlaubt z.B. die Nutzung einzelner Geräte (nach ID) oder Gerätetypen trotz Verbots

## Temporäre Freigaben

- Mit Security.Desk können auch mobilen Usern am Notebook via Code-Fernfreischaltung zeitlich begrenzte Benutzerrechte für die Schnittstellen erteilt werden, auch wenn die Notebooks vom Netzwerk getrennt sind

## Dateiverschlüsselung

- Dateien können im AES-Verfahren verschlüsselt werden
- Bequem können eine oder mehrere Dateien über das Kontextmenü des Windows Explorers mit FCS CryptMe! ver- oder entschlüsselt werden

## Schutz vor BadUSB

- BadUSBs melden sich heimlich als Maus, Tastatur oder Netzwerkkarte am Computer an und erlauben dann eine Fernsteuerung bzw. externe Nutzung der befallenen Systeme
- Sollte es sich um einen manipulierten USB Stick handeln, der sich z.B. als Tastatur oder Maus ausgibt, dann kann dieser direkt vom User blockiert werden

## Weißer Liste Geräte

Freigabe von Speichermedien und mobilen Geräten an den Clients, beispielsweise über die USB-ID

## Schwarze Liste Dateitypen

Kopierverbot für bestimmte Dateitypen von bzw. auf mobile Speicher, z.B. exe-Files

## Schwarze Liste Software

Sperren von bestimmten Softwareanwendungen auf den Clients

## Zusatzmodule

### Active Directory Loader

Der Active Directory Loader ermöglicht die einfache und schnelle Übernahme von Clients aus dem Active Directory nach Security.Desk.

Es lassen sich – wie in Asset.Desk – unterschiedliche Profile für die Übernahme aus dem Active Directory (AD) definieren. Die Übernahme von Clients aus dem AD nach Security.Desk wird damit deutlich komfortabler und leichter. Eine Zeitsteuerung ermöglicht den periodischen Abgleich von AD und Security.Desk und übernimmt neue Clients zum passenden Profil automatisch nach Security.Desk. Aus der OU-Struktur im AD werden vom System optional Gruppen im Baum des Managers angelegt.

### Terminal Server

Der Baustein „Terminal Server“ ermöglicht die Überwachung von Dateibewegungen lokaler Laufwerke an Thin Clients in Remote Sessions im Betrieb mit Windows Terminal Server, Windows Server 2016 RDS, Citrix MetaFrame oder Citrix XenApp.

Security.Desk informiert Sie durch das Terminal-Server-Modul auch immer bestens über Dateitransfers bei den Arbeitsstationen Ihrer Serverfarmen. Dadurch können Sie entsprechend handeln, wenn z.B. Dateien auf USB Wechselspeicher an Thin Clients kopiert werden oder von dort ins interne Netz gelangen. Das Modul ermöglicht ebenfalls die Überwachung oder das Verbot von Netzlaufwerken, wenn diese über Laufwerksbuchstaben verbunden und in den Einstellungen vorgegeben (angehakt) sind.

Die sogenannten „Redirected Drives“ lassen sich generell oder auf Benutzerebene erlauben, sperren oder auf „Nur Lesen“ setzen. So kann z.B. ein Kopieren auf lokale Laufwerke von Thin Clients verboten werden. Die Schwarze Liste für Dateitypen (im Austausch mit lokalen Laufwerken) ist bei Thin Clients ebenfalls aktivierbar.

Werden neben Thin Clients auch herkömmliche Windows-Clients in Remote Sessions betrieben, so können dort die zu überwachenden Laufwerke (A-Z) global vorgegeben werden.

### Netzwerkprotokoll

Mit seinem optionalen Zusatzbaustein „Netzwerkprotokoll“ bietet Security.Desk ein Dateiprotokoll für die gängigen Internet-Protokolle wie HTTP, SMTP und FTP. Egal, ob die Dateien z.B. per Internet Browser hochgeladen oder per Outlook verschickt werden – das Modul „Netzwerkprotokoll“ zeichnet sämtliche Dateibewegungen über das Internet auf, die mit beliebigen Anwendungen ausgeführt werden.



Dabei rekonstruiert das Modul sämtliche Parameter aus dem „Netzwerk-Traffic“ des Endgeräts, so dass u.a.

- der Protokoll-Typ (HTTP, SMTP und FTP)
- der Dateiname
- der ausführende Benutzer
- der ausführende Rechner, Quell- und Zieladresse sowie
- Datum und Uhrzeit

mit aufgezeichnet werden. Das Netzwerkprotokoll ist für sämtliche Adapter eines Endgeräts aktiv, also Ethernet, WLAN und Bluetooth. Durch die Kombination dieses Moduls mit Security.Desk machen Sie Ihr Netzwerk noch sicherer – denn Sie überwachen den Dateiaustausch noch besser und sehen, wer Ihrem Unternehmen potenziellen Schaden zufügt!

## Security.Desk Enterprise Edition



**OUs und Gruppen importieren, Clients automatisch zuordnen, Zugriffsrechte nach Units vergeben und mit Single Sign On anmelden.**

**Mit der Enterprise Edition wird Security.Desk direkt an das Active Directory angebunden.**

Unterschiedliche Profile für die Übernahme von OUs und Gruppen aus dem Active Directory lassen sich einfach und komfortabel definieren. Eine Zeitsteuerung ermöglicht einen periodischen Abgleich des Active Directorys mit Security.Desk. Neue Clients werden so automatisch zum passenden Profil (z.B. einem Standort oder einer Abteilung) zugeordnet. Aus der OU-Struktur im Active Directory werden vom System optional Gruppen im Baum des Managers angelegt.

Die Kopplung mit dem Active Directory ermöglicht das Single Sign On für Security.Desk-Admins und erleichtert neben der Rechtevergabe auf AD-Basis auch das schnellere Auffinden bestimmter Gruppen und OUs im Active Directory. Die Regeln für individualisierte Zugriffe auf externe Medien, die über Hardwareschnittstellen an PCs und Thin Clients angeschlossen sind, lassen sich so wesentlich effektiver verwalten.

## Security.Desk & Store O'Crypt

FCS bietet noch mehr Sicherheit mit einem eigenen USB-Stick an, der Ihre Daten „on board“ verschlüsselt und den Zugriff nur durch Eingabe eines sicheren Passworts erlaubt. Store O'Crypt kann ideal mit Security.Desk verbunden und mit nur einem Klick unternehmensweit freigegeben werden.

### Die Highlights des Store O'Crypts

- Automatische Verschlüsselung aller Daten mit AES-256 durch den on-board Prozessor
- Sofortige Verwendung an jedem PC – ohne zusätzliche Software
- Zugriff auf verschlüsselte Daten durch Eingabe des sicheren Passworts
- Bis zu drei Benutzerrollen (Administrator, Benutzer, Gast)
- Limitierte Anzahl von fehlerhaften Anmeldeversuchen
- Epoxidharzverguss zum Schutz gegen unerlaubten Zugriff auf verwendete Bauteile und zum Schutz gegen das Eindringen von Wasser
- Investitionssicherheit durch Stick-Update über das Internet
- Optionaler Schreibschutz verhindert das Einschleusen von Malware





**FCS Fair Computer Systems GmbH**  
Nürnberg

Telefon .....0911 / 810881 - 0

Fax.....0911 / 810881 - 11

E-Mail .....[info@fair-computer.de](mailto:info@fair-computer.de)

Internet .....[www.fair-computer.de](http://www.fair-computer.de)

Facebook.....[www.facebook.com/FairComputerSystems](https://www.facebook.com/FairComputerSystems)

