FAIR COMPUTER SYSTEMS GMBH

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

USB & ENDPOINT SECURITY

Security.Desk

SOFTWARE made in Germany

Kostenübersicht

Preisinformation:	Ab 8,00 € pro Client / einmalig
Gratis testen:	ja
Einsatz:	Installiert: Windows, Mac
Training:	Persönlich, live via Online-Präsentation, Webinare, Dokumentation
Kundenbetreuung:	Support während der Geschäftszeiten

Schnittstellen-überwachung mit Security.Desk

Die USB- und Endpoint-Security-Lösung Security.Desk hilft, externe Hardwareschnittstellen dauerhaft abzusichern, überwacht mobile Speicher und Internet-Protokolle und unterstützt dabei, Sicherheitslücken erfolgreich zu schließen.

Dabei geht sie 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 einem Wechseldatenträger bzw. auf einen Wechseldatenträger transferieren darf, und welche Dateitypen dafür nicht erlaubt sind (z.B. exe-Dateien). Sämtliche Dateibewegungen lassen sich dabei protokollieren. Der zentrale Kontrollstand der Managementkonsole ermöglicht es, sämtliche Rechte für die Nutzung mobiler Speicher und Schnittstellen vom Arbeitsplatz des Administrators aus zu setzen. Das zentrale Berichtswesen wird durch E-Mail-Alarme/ Benachrichtigungen unterstützt. Security.Desk lässt sich mit dem Active Directory koppeln, um Rechte auf Basis von OUs, Gruppen oder einzelnen Benutzerkonten 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 Security.Desk Sie dabei,...

- **unkontrollierten Datenabfluss zu verhindern,**
- **Dateibewegungen zu protokollieren,**
- **Dateien für Dritte unlesbar zu machen,**
- **die Ausführung unerwünschter Programme zu verhindern oder**
- **das Eindringen externer Gefahren unmöglich zu machen.**

Schützt

Schützt Daten und Netzwerke vor Datendiebstahl oder dem Einschleppen von Viren und Trojanern über Wechseldatenträger

Überwacht

Auch mobile Speicher an Thin Clients in Windows Terminal Server- oder CITRIX-Umgebungen lassen sich überwachen

Funktionsumfang im Überblick

Security.Desk

...überwacht sämtliche Hardware-Schnittstellen und Internet-Protokolle am Endgerät!

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

Dabei erkennt Security.Desk automatisch, wenn z.B. ein Flash-Speicher über USB an einen PC angeschlossen oder eine CD oder SD-Speicherkarte eingelegt wird. Sie geben vor, was dann zu tun ist: Wird der Datentransfer blockiert oder darf der Nutzer Dateien nur ansehen? Dabei lassen sich alle Dateibewegungen protokollieren.

...erstellt Dateiprotokolle und umfassende Reportings!

- 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

...kommt mit einem interaktivem 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

...erlaubt eine 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 Verbot

...sorgt für 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

...ver- und entschlüsselt Daten!

- 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

Weiße 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

Neuheiten

Schutz vor Bad USB

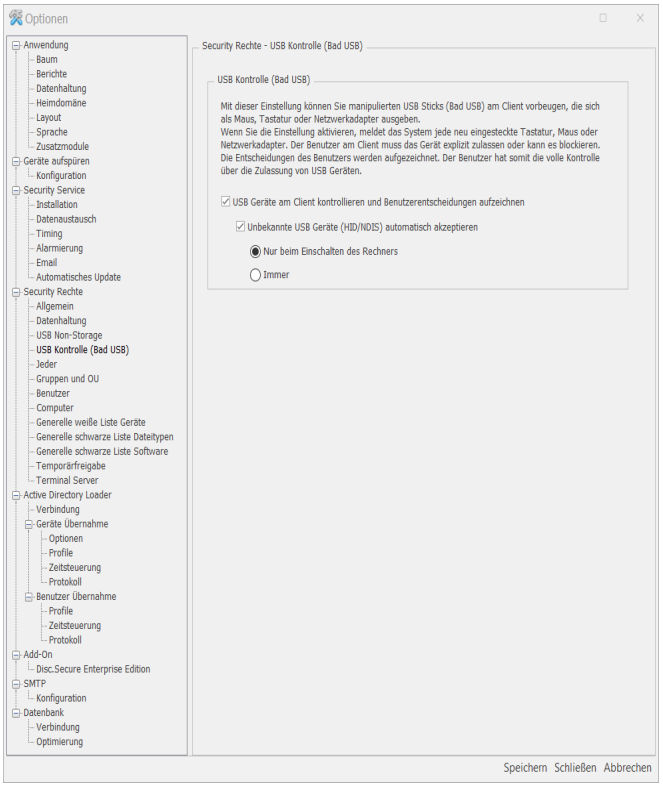
Flexibel reagieren auf neu erkannte USB-Geräte

Bad USBs 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 mit Security.Dek direkt vom User blockiert werden.

Durch einen **neuen Parameter** in den Optionen legen Sie auf Wunsch bei eingeschalteter "Bad USB"-Kontrolle nun zusätzlich fest, ob neu erkannte USB-Geräte am Client automatisch akzeptiert werden sollen, und zwar wahlweise:

- nur nach Neustart des Rechners
- immer.

Security.Desk stellt sicher, dass die neu erkannten USB-Geräte in jedem Fall weiterhin protokolliert und zentral gemeldet werden.
Der neue Parameter ist z.B. dann sinnvoll, wenn im laufenden Betrieb **defekte USB-Tastaturen** an ausgeschalteten PCs öfters gegen neue Tastaturen getauscht werden müssen.



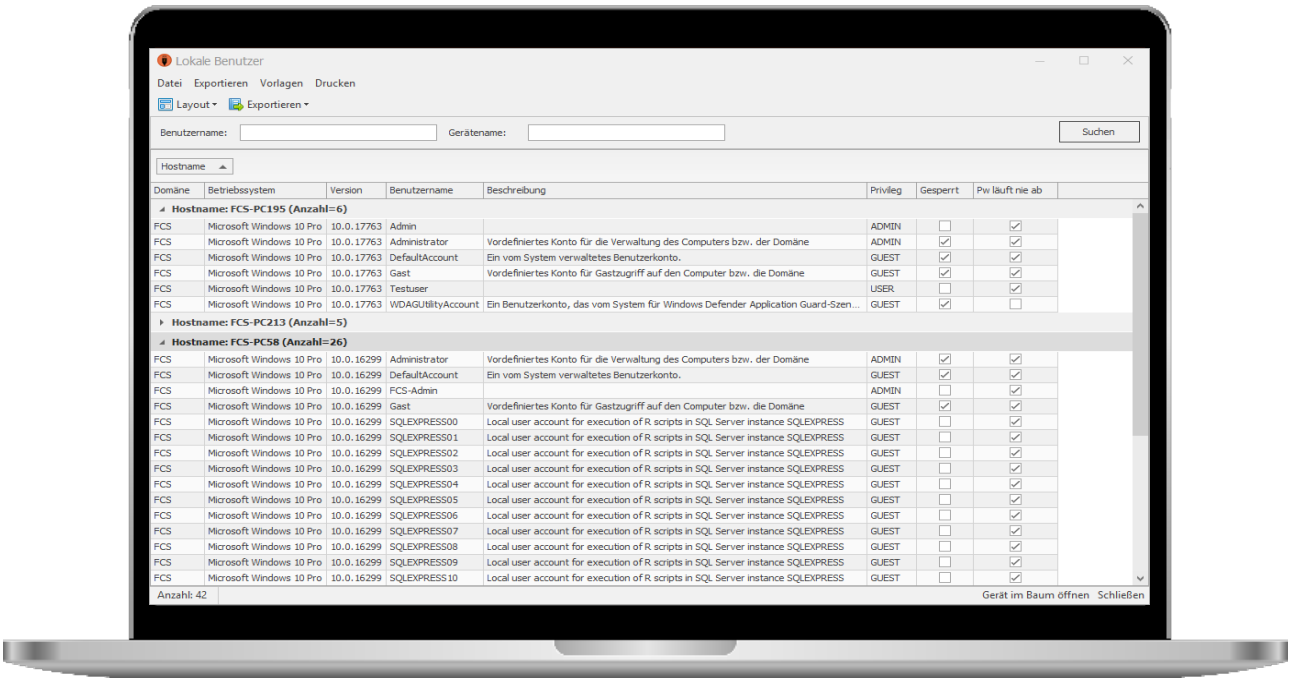
Einstellung Security Rechte: Bad USB

Lokale Benutzer und Administratoren

Auslesen der auf den Clients eingerichteten lokalen Benutzer und lokalen Administratoren

Die lokalen Benutzer inklusive Privileg sowie die Mitglieder der lokalen Administrator-Gruppe werden von jedem Client ausgelesen, importiert, im Manager pro Client angezeigt und in Berichten zusammengefasst.

Damit erhalten administrative Benutzer von Security.Desk wertvolle Informationen, um die Einrichtung von lokalen Benutzern und Administratoren an den Clients zu kontrollieren und zu konsolidieren.



Einstellung: Lokale Administratoren

Trusted Platform Module (TPM)

Erkennen, ob TPM-Chip vorhanden ist und Scan des Herstellers, Spezifikation und Version des Chips

Das Trusted Platform Module (TPM) ist ein Chip auf der Hauptplatine, der den Rechner um grundlegende Sicherheitsfunktionen erweitert. Security.Desk erkennt, ob ein TPM-Chip vorhanden ist und scannt sodann Hersteller, Spezifikation und Version des Chips.

- Die TPM-Daten werden am jeweiligen Gerät sowie im Bericht zur Hauptplatine angezeigt.
- Der Bericht zeigt auch an, wenn kein TPM-Chip implementiert ist.

Zusatzmodule

Active Directory Loader

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

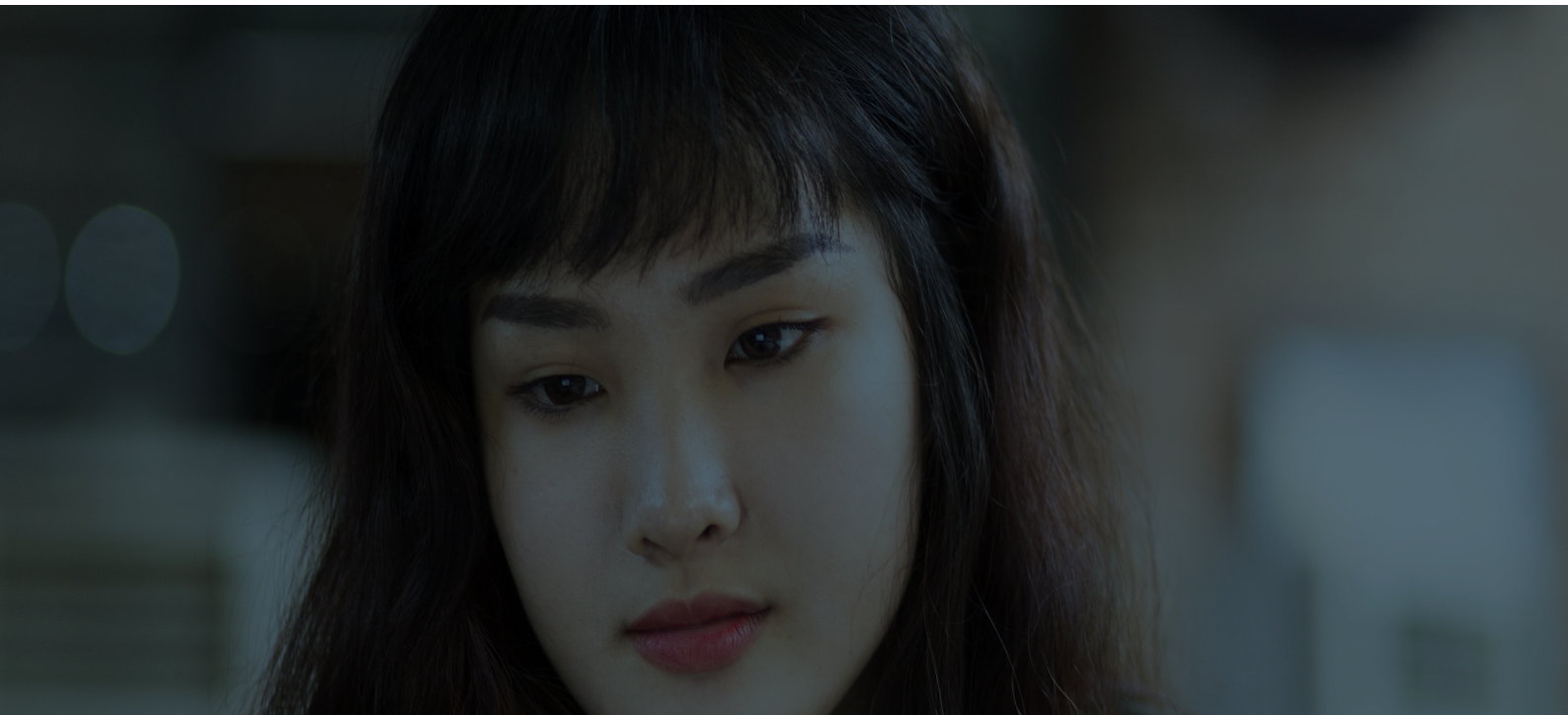
Zudem lassen sich unterschiedliche Profile für die Übernahme aus dem Active Directory (AD) definieren. Die Übernahme von Clients aus dem AD nach Security.Desk wird damit deutlich komfortabler und leichter. Eine Zeitsteuerung ermöglicht den periodischen Abgleich von AD und Security.Desk und übernimmt 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" macht 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 möglich.

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 begünstigt 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/HTTPS, 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 gezielter und sehen, wer Ihrem Unternehmen potenziellen Schaden zufügt!

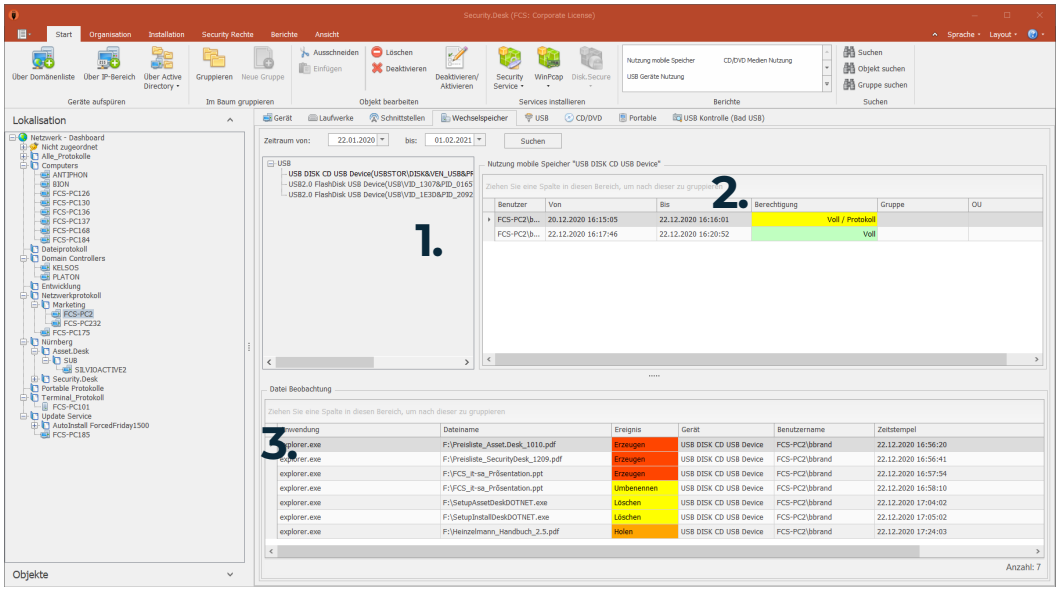
Security.Desk Enterprise Edition

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.

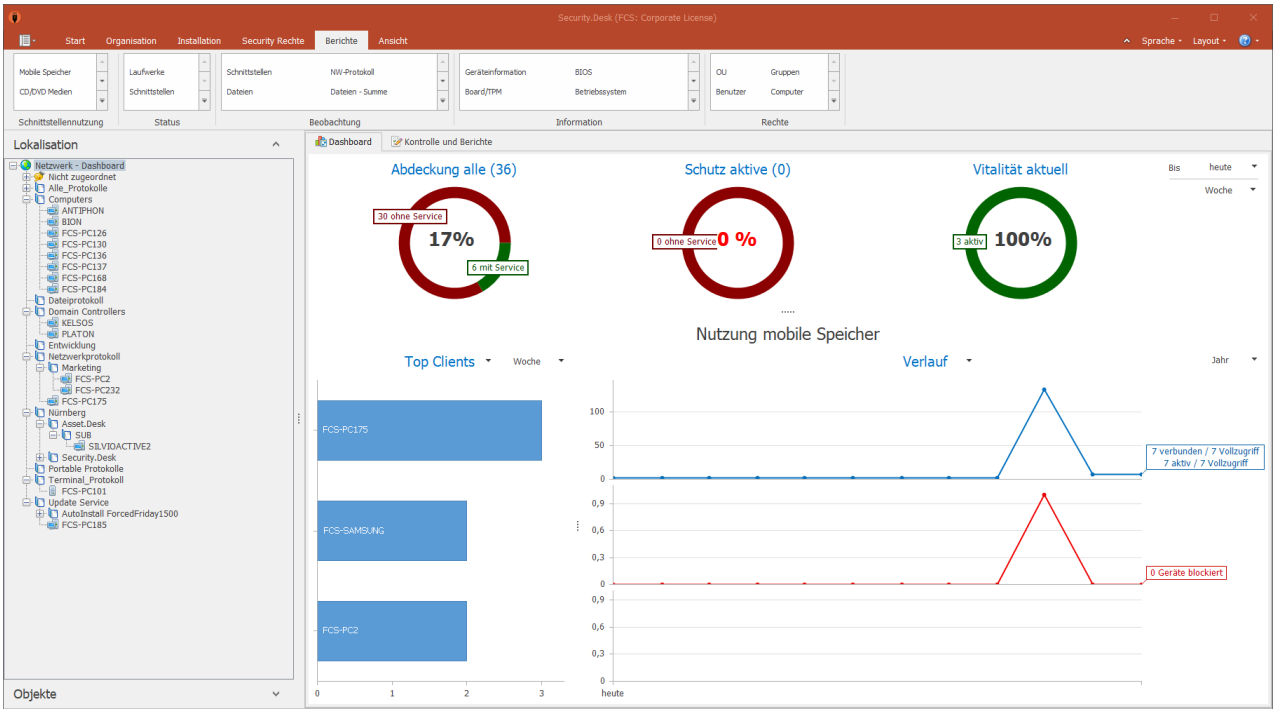
Unterschiedliche Profile für die Übernahme von OUs und Gruppen aus dem Active Directory lassen sich einfach und komfortabel definieren. Eine Zeitsteuerung gewährleistet einen periodischen Abgleich des Active Directorys mit Security.Desk. Neue Clients werden so automatisch zum passenden Profil (z.B. einem 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



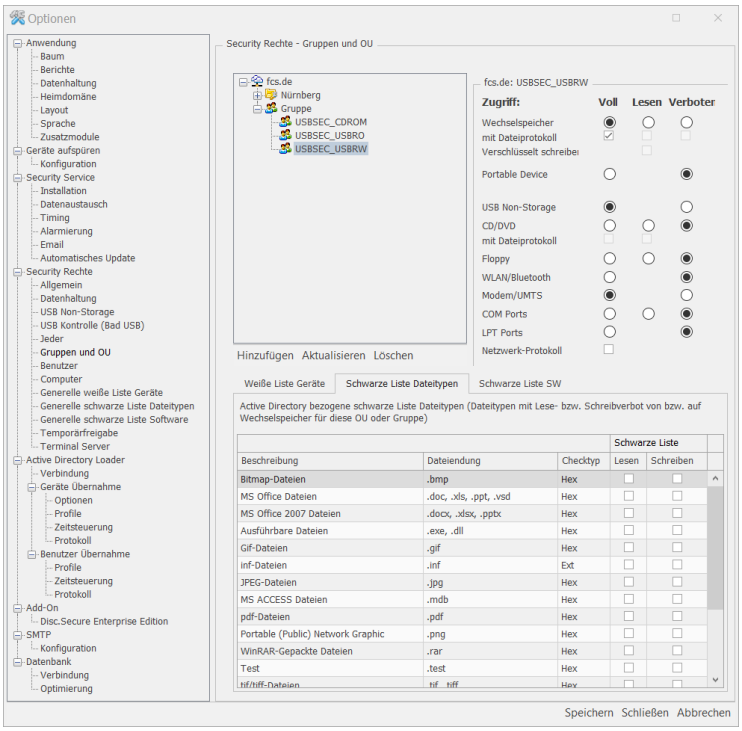
Ansicht "FCS-PC2" in der Managementkonsole

1. Welche Geräte waren an welchem PC ...
2. ... wann und mit welchen Rechten angeschlossen ...
3. ... und wer hat welche Dateien geöffnet oder von bzw. auf welchen Wechselspeicher bewegt?



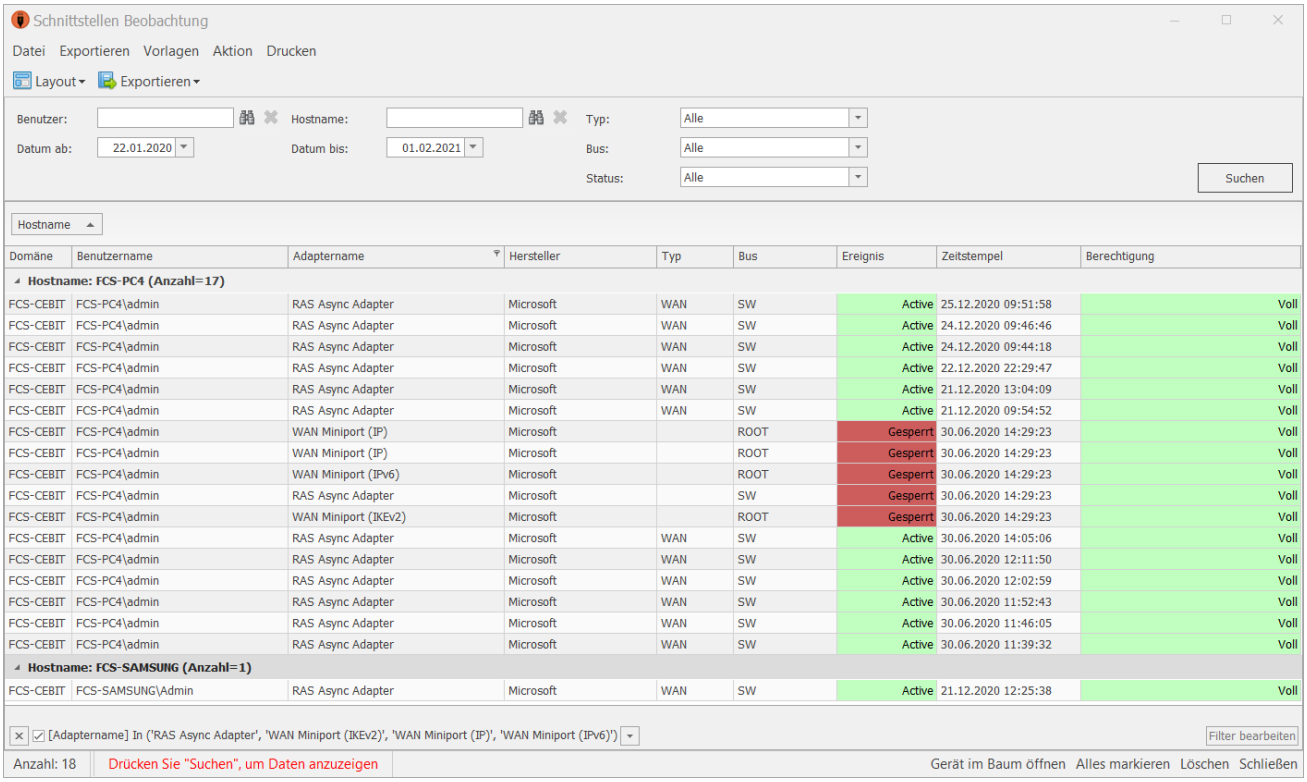
Dashboard

Volle Information



Einstellungsdialog

Schnittstellen aktiv managen



Beispiel für einen interaktiven Bericht

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
- Verhindern des Einschleußen von Malware durch optionalen Schreibschutz

Vorteile im Überblick

1. Active Directory-Integration
2. Rechtevergabe: erlauben, nur lesen, verbieten – getrennt nach HW-Schnittstelle – pro User, Gruppe, OU oder Gerät
3. Protokoll der Dateibewegungen von und auf Wechseldatenträger
4. Blockierung des Lesens oder Schreibens bestimmter Dateitypen von oder auf Wechselspeicher
5. Erkennung von verbotenen „embedded files“ in Office-Dateien
6. Überwachung der Dateibewegungen lokaler Laufwerke an Thin Clients
7. Übersichtlicher zentraler Kontrollstand für Compliance Management, Dienstverteilung und Reporting
8. Freie Ergänzung zu überwachender USB-Gerätetypen
9. „Weiße Liste“ für spezielle Geräte (nach ID) oder Gerätetypen
10. Verbot von Softwareanwendungen über die „Schwarze Liste“
11. Temporäre Freischaltung von Offline-Rechnern über einen individuell erzeugten Zugriffscode
12. Alarmierung via E-Mail oder Tray Icon
13. Beenden des Security-Dienstes nicht möglich
14. Integration mit Store O´Crypt (AES 256 hardwareverschlüsselter USB-Stick von FCS)
15. Flash Reminder – Erinnerung beim Abmelden von Ihrem PC, falls sich am Rechner noch angeschlossene Wechseldatenträger befinden
16. Schutz vor Bad USB (Speichersticks mit manipulierter Firmware) durch die Kontrolle von Eingabegeräten (Maus und Tastatur) sowie Netzwerkadaptern
17. Auslesen und Anzeigen der BIOS-Information sowie der Daten der logischen Laufwerke inklusive Kapazität (gesamt / belegt / frei) pro Client
18. Auslesen der Daten der logischen Laufwerke der Clients zusammen mit dem „BitLocker“-Status
19. Ausgabe der vollständigen Daten zum Betriebssystem der Clients (Version, Release, Build-Nr., Service Pack etc.) durch Security.Desk
20. „UEFI Secure Boot“ Aktivierung erkennbar an der BIOS-Information in Security.Desk pro Gerät oder über einen Bericht
21. Windows Update-Optionen und Status je Rechner sowie Info zum Windows Update Server

IT Management Solutions

FAIR COMPUTER SYSTEMS

IT- und Asset-Management Software für Ihre Digitalstrategie

Unser Ziel ist es, Komplexes einfach zu machen. Daher ist der Funktionsumfang unserer Lösungen modular aufgebaut. Unsere Software wird kontinuierlich weiterentwickelt und kann leicht in nahezu jede IT-Landschaft integriert werden.

Sie möchten Security.Desk kostenlos testen? Kein Problem!

20 Tage kostenlos testen unter:
https://www.fair-computer.de/download_testversionen/

Wir sind ein eigentümergeführtes, deutsches System- und Beratungshaus.
Seit 1999 realisieren wir innovative High-End-Software.

In unserem Geschäftsbereich „IT Management Solutions“ entwickeln wir Standard-Software für IT-Inventarisierung, IT-Asset Management, Enterprise Asset Management, Lizenzmanagement, Softwareverteilung, Endpoint Security und ITSM Software / Helpdesk, die wir europaweit vertreiben. Zu unseren Kunden zählen namhafte Unternehmen des Mittelstands aus unterschiedlichen Branchen, die selber in ihren Märkten als führend gelten. Wir unterstützen unsere Kunden bei der Entwicklung und Umsetzung ihrer Strategie im Bereich IT- und Asset Management mit unseren Produkten und unserem Know-How. Über 600 Kunden vertrauen mittlerweile auf die Software-Lösungen von FCS.

In unserem Geschäftsbereich „FCS Drive“ entwickeln wir europäische Webportale, Data Warehouses und betriebliche Anwendungen für die Automobilwirtschaft.

Ebenso ist die Entwicklung mobiler Lösungen ein Schwerpunkt unserer Arbeiten. Wir bauen und betreiben Lösungen zur Unterstützung von Sales und After Sales, wie z. B. Angebotswerkzeuge, Service Assistent, Reporting Tools, Vehicle Health Check, Vermietlösungen. Daneben bieten wir unsere Expertise im Automobilhandel in zahlreichen Beratungsprojekten. Große internationale Automobilhersteller gehören zu unserem Kundenkreis, wie General Motors, Opel und Ford.

Die technologische und innovative Kompetenz von FCS wird u. a. dokumentiert durch die Auszeichnung “Microsoft Gold Certified Partner” oder dem “TOP 100-Siegel 2021”. Unsere Software für das Lizenzmanagement (SAM) wurde von der KPMG zertifiziert.

Unsere Geschäftspartner schätzen unsere Expertise und unsere Unternehmenskultur. Nürnberg ist seit der Gründung von FCS der Hauptsitz des Unternehmens. Die Niederlassung in Eltville besteht seit Anfang 2010.

FAIR COMPUTER SYSTEMS GMBH

Ostendstraße 132
90482 Nürnberg

Tel.: +49 (0) 911 810 881 0
Fax: +49 (0) 911 810 881 11

info@fair-computer.de
www.fair-computer.de

2021