Security.Desk

USB- UND ENDPOINT-SECURITY

Für weitere Informationen
besuchen Sie: **www.fair-computer.de**

Kostenübersicht

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

Schnittstellenüberwachung und -management 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 interaktiven 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	**Schwarze Liste Dateitypen**	**Schwarze Liste Software**
Freigabe von Speichermedien und mobilen Geräten an den Clients, beispielsweise über die USB ID	Kopierverbot für bestimmte Dateitypen von bzw. auf mobile Speicher, z.B. exe-Files	Sperren von bestimmten Softwareanwendungen auf den Clients

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.

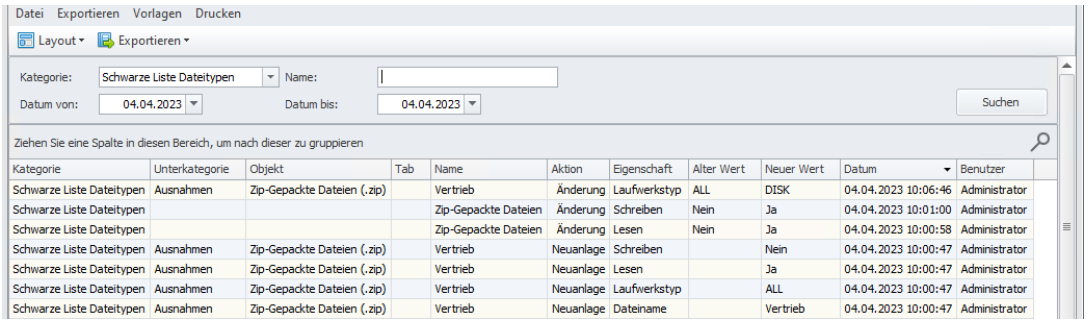
Durch einen **neuen Parameter** in den Optionen legen Sie auf Wunsch bei eingeschalteter “Bad USB”-Kontrolle nun zusätzlich fest, ob neu erkannte USB-Geräte am Client automatisch akzeptiert werden sollen, und zwar wahlweise:

- 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.

Historie für Änderungen an den Security Rechten

Security.Desk zeichnet sämtliche Änderungen an den Security Rechten auf, einschließlich Änderungen an den Rechten von Jeder, Benutzern, Gruppen und OUs. Die Änderungen werden in einem Historien-Bericht erfasst und können jederzeit angezeigt und gefiltert werden. Darüber hinaus protokolliert das System Änderungen an den Non-Storage und Bad USB Einstellungen, Terminalserver Einstellungen, Temporär-Freigaben sowie den Weißen und Schwarzen Listen. Bei jeder Änderung werden der Benutzer und der Zeitpunkt vermerkt, um die Revisionssicherheit zu gewährleisten.



Kategorie	Unterkategorie	Objekt	Tab	Name	Aktion	Eigenschaft	Alter Wert	Neuer Wert	Datum	Benutzer
Schwarze Liste Dateitypen	Ausnahmen	Zip-Gepackte Dateien (.zip)		Vertrieb	Änderung	Laufwerkstyp	ALL	DISK	04.04.2023 10:06:46	Administrator
Schwarze Liste Dateitypen				Zip-Gepackte Dateien	Änderung	Schreiben	Nein	Ja	04.04.2023 10:01:00	Administrator
Schwarze Liste Dateitypen				Zip-Gepackte Dateien	Änderung	Lesen	Nein	Ja	04.04.2023 10:00:58	Administrator
Schwarze Liste Dateitypen	Ausnahmen	Zip-Gepackte Dateien (.zip)		Vertrieb	Neuanlage	Schreiben		Nein	04.04.2023 10:00:47	Administrator
Schwarze Liste Dateitypen	Ausnahmen	Zip-Gepackte Dateien (.zip)		Vertrieb	Neuanlage	Lesen		Ja	04.04.2023 10:00:47	Administrator
Schwarze Liste Dateitypen	Ausnahmen	Zip-Gepackte Dateien (.zip)		Vertrieb	Neuanlage	Laufwerkstyp		ALL	04.04.2023 10:00:47	Administrator
Schwarze Liste Dateitypen	Ausnahmen	Zip-Gepackte Dateien (.zip)		Vertrieb	Neuanlage	Dateiname		Vertrieb	04.04.2023 10:00:47	Administrator

Historie

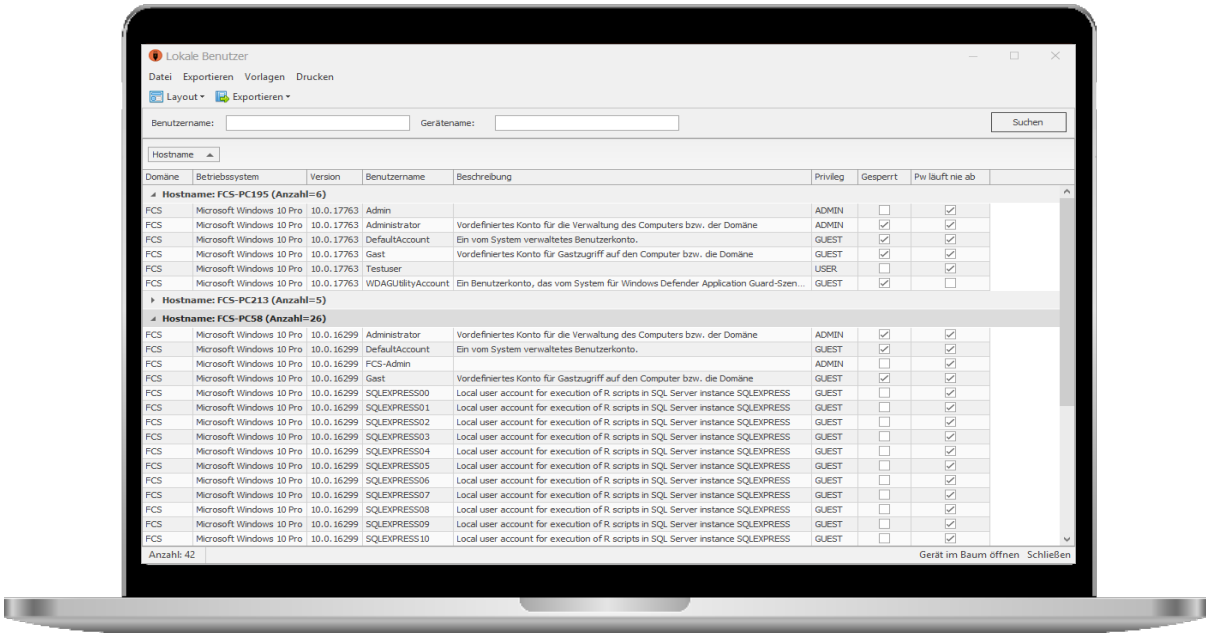
Die Änderungen werden im System in den Historien vorgehalten und können jederzeit angezeigt und rekonstruiert werden, wenn entsprechende Rechte dafür eingerichtet sind. Die Protokollierung der Änderungen (die Historie) kann einzeln pro Kategorie in den Einstellungen ein- und ausgeschaltet werden.

Ebenfalls kann pro Kategorie eingestellt werden, wie lange die historischen Daten im System vorgehalten werden sollen.

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.

Praxisbeispiel mit Security.Desk: Gezielte Freigabe einer Wartungs-EXE-Datei

Ein Produktionsunternehmen setzt fortschrittliche Maschinen ein, die regelmäßige Software-Updates benötigen. Diese Updates werden über eine spezielle EXE-Datei durchgeführt, die auf einem USB-Stick geliefert wird. Aus Sicherheitsgründen ist es im Unternehmen generell untersagt, EXE-Dateien von USB-Sticks auszuführen. Um die Maschinen dennoch aktuell zu halten, ohne die Netzwerksicherheit zu gefährden, wird Security.Desk eingesetzt.

Identifikation des spezifischen USB-Sticks: Der für die Updates vorgesehene USB-Stick wird in Security.Desk über seine Seriennummer erkannt. Dies gewährleistet, dass ausschließlich dieser Stick für die Update-Prozesse verwendet wird.
Zielgerichtete Berechtigung für bestimmte EXE-Dateien: In Security.Desk wurde im Vorfeld eine Regel definiert, die es nur erlaubt, eine spezifische EXE-Datei für die Maschinenaktualisierung von diesem Stick auszuführen. Andere EXE-Dateien, die sich möglicherweise auf dem Stick befinden, bleiben gesperrt.
Ausführung der Wartungs-EXE: Wartungspersonal, das für die Aktualisierung der Maschinensoftware zuständig ist, erhält die Berechtigung, die identifizierte EXE-Datei von dem autorisierten Stick auszuführen. Sobald der Stick angeschlossen und die spezifische EXE-Datei gestartet wird, prüft Security.Desk, ob alle Kriterien erfüllt sind, und erlaubt die Ausführung.
Überwachung und Protokollierung: Jede Ausführung der spezifischen Wartungs-EXE wird von Security.Desk protokolliert, um Compliance zu gewährleisten und eine lückenlose Nachverfolgbarkeit zu sichern.

Mit Security.Desk profitieren Sie von effektiver Netzwerksicherheit, die nicht auf Kosten der Flexibilität geht. Die Lösung bietet eine granulare Rechteverwaltung, die Ihnen erlaubt, individuell anzupassen, wer Zugriff auf was hat. So können Sie beruhigt sein, denn Security.Desk schützt Ihr Unternehmensnetzwerk intelligent und flexibel.

Was macht Security.Desk so besonders?

Warum sich mit weniger zufriedengeben? Security.Desk definiert Netzwerkschutz neu – mit individuell anpassbaren Zugriffsrechten, die Ihnen die Kontrolle zurückgeben.

Granulare Rechtevergabe – Komplexität war gestern

Mit Security.Desk haben Sie die Macht, präzise zu definieren, wer in Ihrem Netzwerk welche Aktionen ausführen darf. Es spielt keine Rolle, ob es um einzelne Benutzer, ganze Abteilungen, bestimmte Geräte oder sogar spezielle Dateitypen geht – die Möglichkeiten sind nahezu grenzenlos. Diese granulare Kontrolle ermöglicht eine Feinabstimmung der Berechtigungen, die in herkömmlichen Sicherheitssystemen oft fehlt.

Überlegen in Flexibilität – Die smarte Antwort auf Sicherheits-bedürfnisse

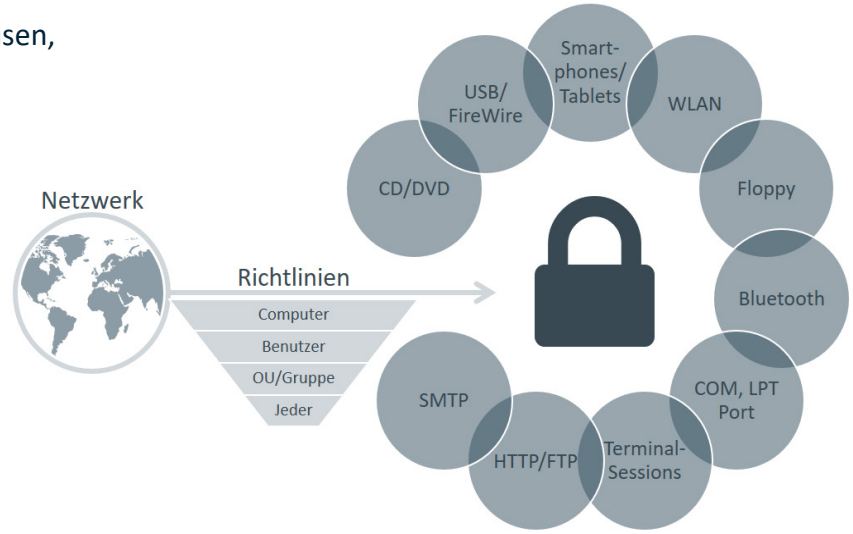
Während andere Sicherheitsprogramme nur ein starres Ja oder Nein kennen, erlaubt Security. Desk fein abgestufte Berechtigungen. So erhalten Ihre Mitarbeiter Zugang zu benötigten Daten und Geräten, ohne die Sicherheit zu gefährden.

Priorität, wo sie nötig ist – Ihre Regeln haben Vorrang

Die intelligente Software stellt sicher, dass Ihre wichtigsten Sicherheitsregeln immer an erster Stelle stehen. Und wenn es darauf ankommt, gelten die Ausnahmen, die Sie bestimmen.

Prävention statt Reaktion

Verhindern Sie Datendiebstahl, bevor er geschieht. Mit Security.Desk bestimmen Sie, welche Dateien bewegt werden dürfen und blockieren unerwünschte Software.
Kein Viren- oder Malware-Einschleusen,
kein unbefugter Datentransfer.



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

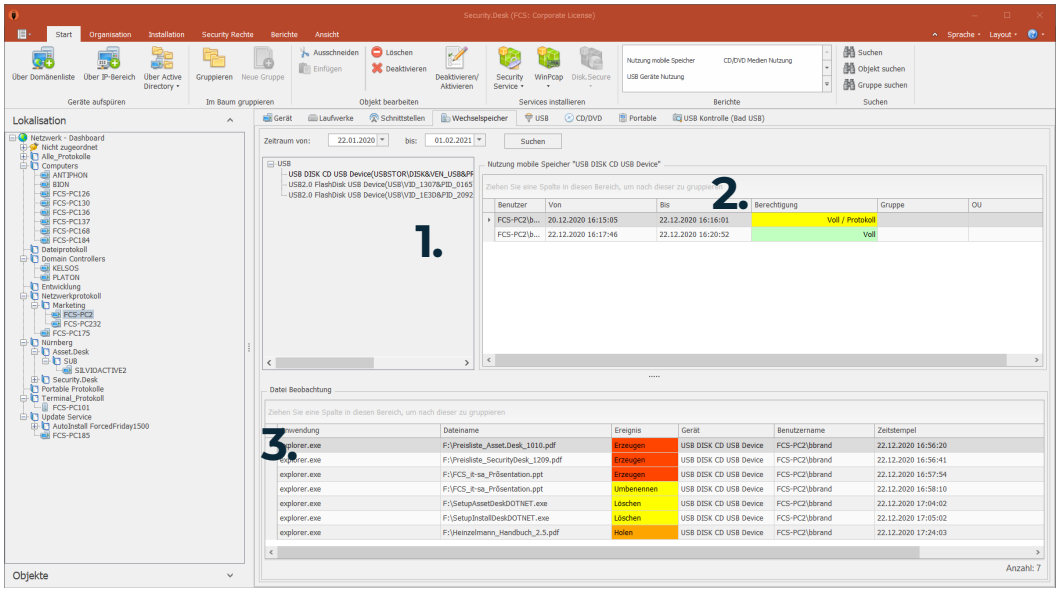
Großes Unternehmen? Komplexes Netzwerk?

Security.Desk Enterprise Edition: Active Directory Loader

Mit der Security.Desk Enterprise Edition lassen sich Clients, OUs und Gruppen aus dem Active Directory importieren und Clients diesen automatisch zuordnen.
Security.Desk wird mit der Enterprise Edition 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 jetzt auch das schnellere Auffinden bestimmter Gruppen und OUs im Active Directory. Die Zugriffsregeln über Schnittstellen auf PCs und / oder Thin Clients in komplexen Unternehmensstrukturen lassen sich so wesentlich effektiver zentral und dezentral verwalten.

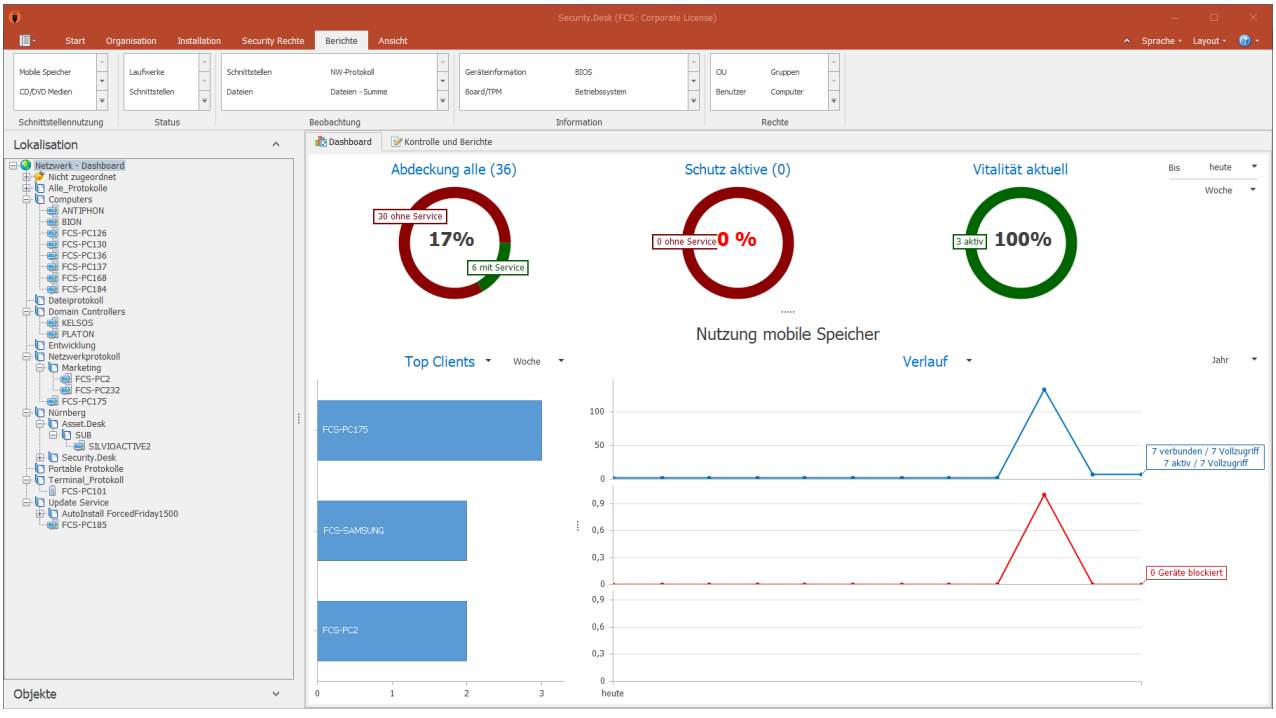
Screenshots

Security.Desk



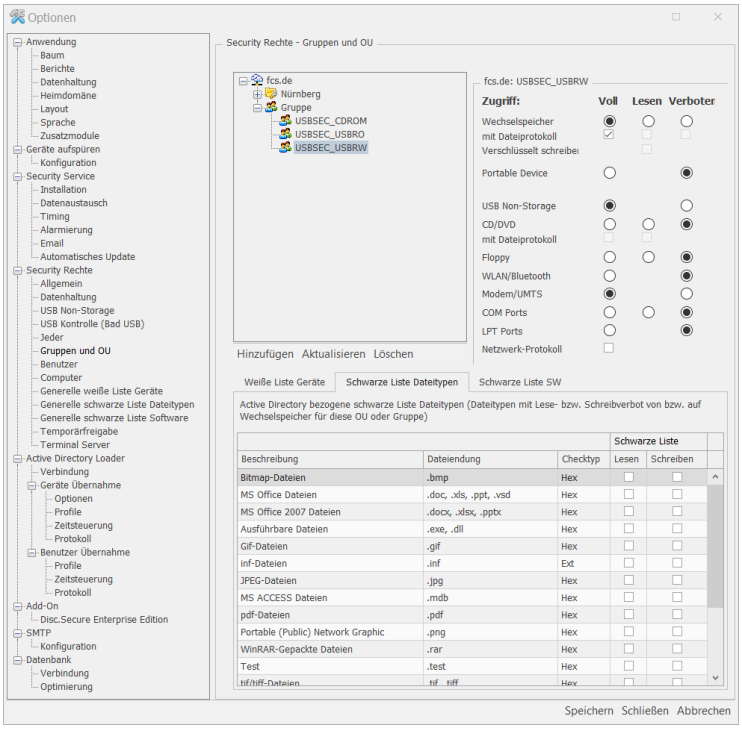
Ansicht “FCS-PC2” in der Managementkonsole

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



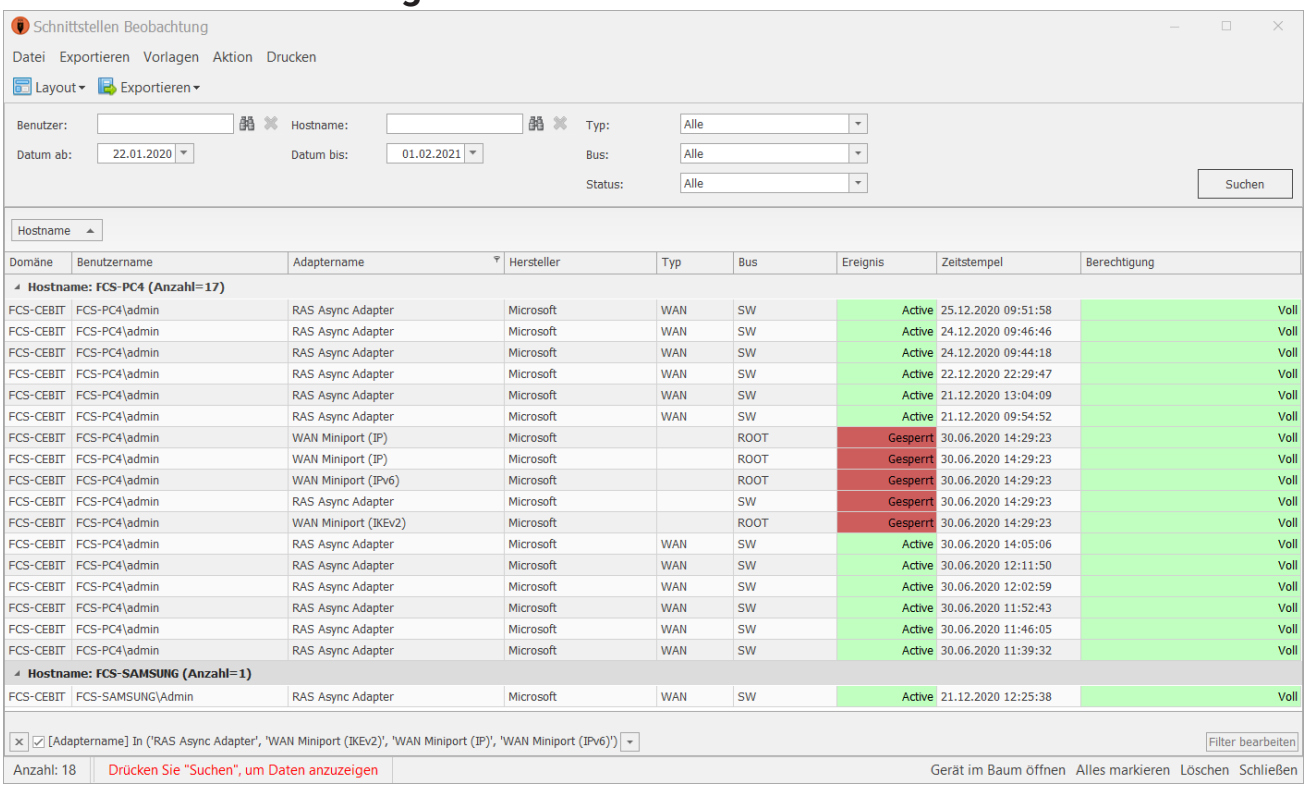
Dashboard

Volle Information

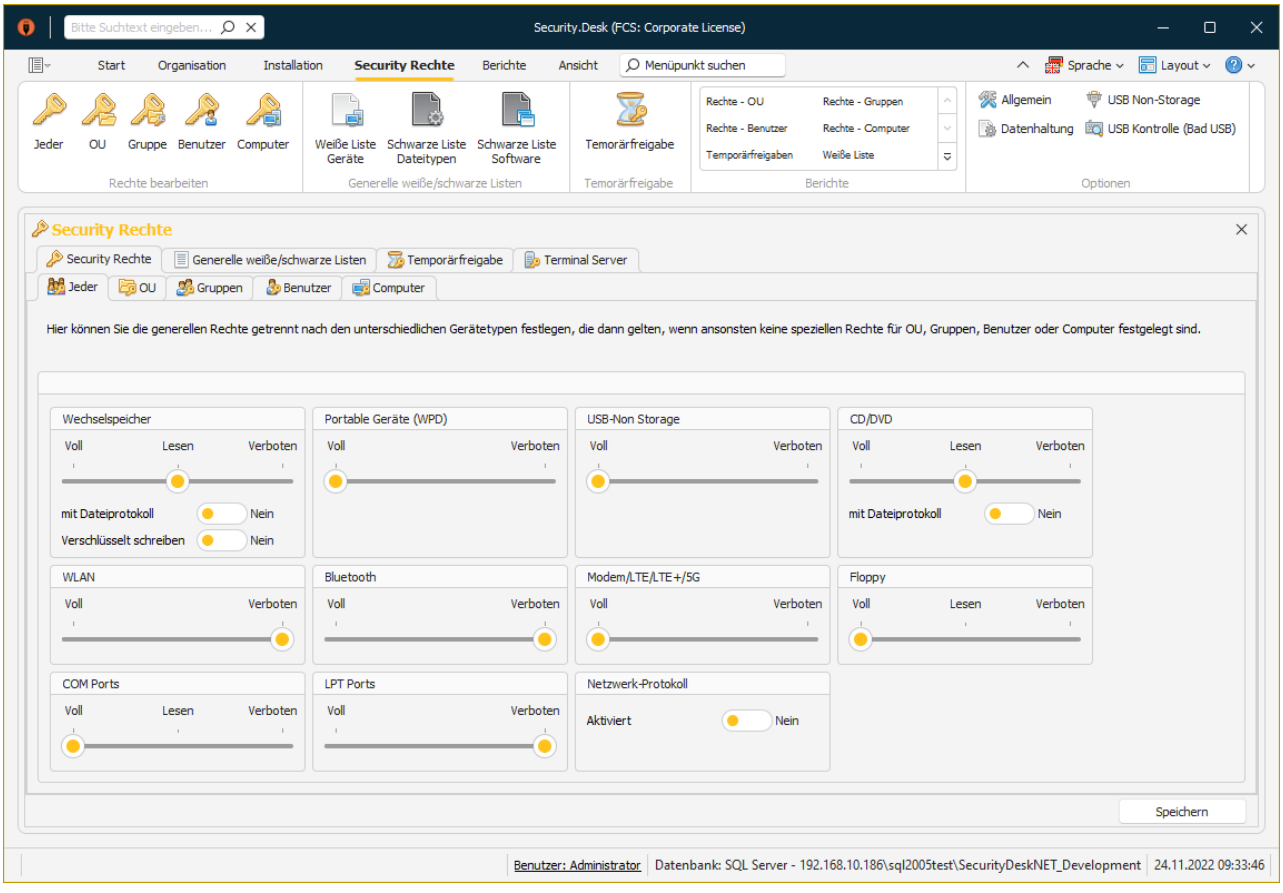


Einstellungsdialog

Schnittstellen aktiv managen



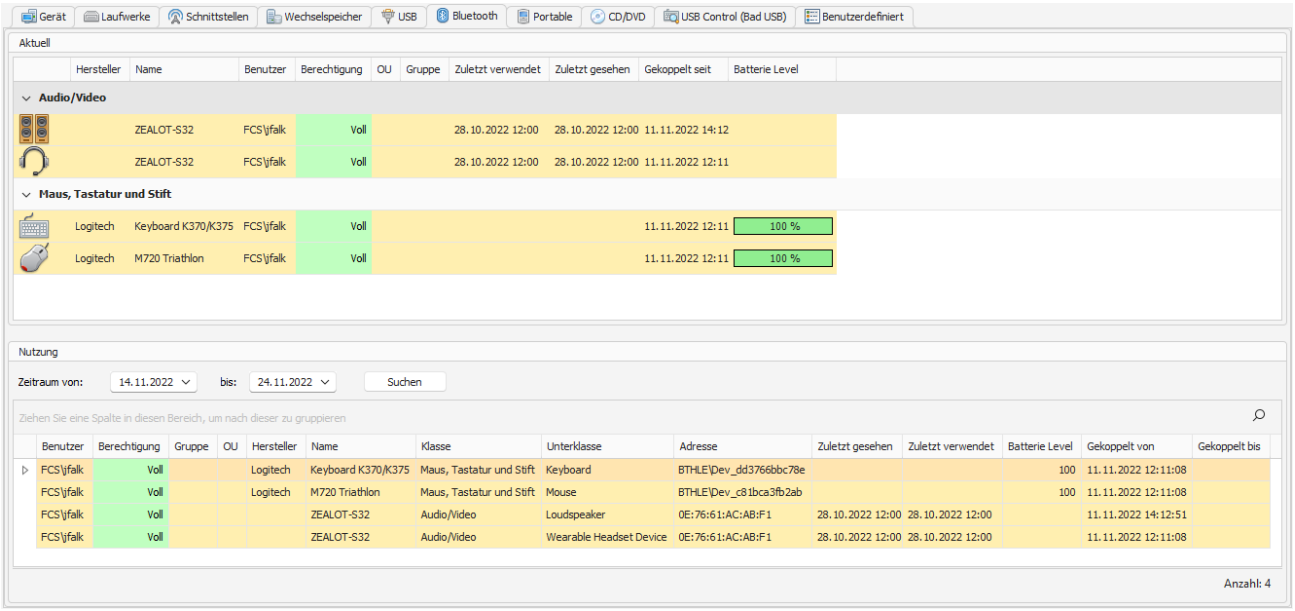
Beispiel für einen interaktiven Bericht



Security Rechte

Bluetooth Batterie Level

Bei HID-Bluetooth-Geräten wird beim Koppeln ein Batteriestatus an den Manager gesendet, so dass Sie zentral sehen können, wo im Unternehmen eine Batterie in einer Bluetooth-Maus oder einer Bluetooth-Tastatur ausgetauscht werden muss.



Batterie Level

Modernes Design und intuitive Bedienung der Rechte

Security.Desk bietet verschiedene Windows 11 Layouts an, die das gesamte Layout an das moderne Design anpassen. Auch stehen spezielle FCS Layouts in den Farben „Orange Sky“, „Blue Ocean“ und „Green Mint“ zur Verfügung.

Für die Bedienung der Security Rechte steht eine benutzerfreundliche Oberfläche zur Verfügung. Die Rechte auf Ebene Benutzer, OU, Gruppe und Computer können übersichtlich und intuitiv in interaktiven Listen gesetzt werden, was eine einfache und zielgenaue Anpassung ermöglicht.

Dr. Falk´s 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.
Dr. Falk´s 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

Security.Desk

Vorteile im Überblick

- Active Directory-Integration
- Rechtevergabe: erlauben, nur lesen, verbieten – getrennt nach HW-Schnittstelle – pro User, Gruppe, OU oder 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 einen individuell erzeugten Zugriffscode
- Alarmierung via E-Mail oder Tray Icon
- Beenden des Security-Dienstes nicht möglich
- 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 Bad USB (Speichersticks mit manipulierter Firmware) durch die Kontrolle von Eingabegeräten (Maus und Tastatur) sowie Netzwerkadaptern
- Auslesen und Anzeigen der BIOS-Information sowie der Daten der logischen Laufwerke inklusive Kapazität (gesamt / belegt / frei) pro Client
- Auslesen der Daten der logischen Laufwerke der Clients zusammen mit dem „BitLocker“-Status
- Ausgabe der vollständigen Daten zum Betriebssystem der Clients (Version, Release, Build-Nr., Service Pack etc.) durch Security.Desk
- „UEFI Secure Boot“ Aktivierung erkennbar an der BIOS-Information in Security.Desk pro Gerät oder über einen Bericht
- Windows Update-Optionen und Status je Rechner sowie Info zum Windows Update Server

“Bei FCS steht der Kunde im Mittelpunkt.

Ein transparentes und faires Preismodell ist uns enorm wichtig!”

Maximilian Höhn
Support und Vertrieb bei FCS

HÄUFIGE FRAGEN

FAQs

Security.Desk ist eine preisgünstige Lösung, die für alle Branchen einsetzbar ist. Sie bietet eine effiziente und kosteneffektive Möglichkeit zur Sicherheitsverwaltung und ist in den Sprachen Deutsch und Englisch verfügbar. Mit einem Preis pro Client, geringem Beratungsaufwand und schneller Einsatzmöglichkeit, ist Security.Desk die ideale Wahl für Unternehmen und öffentliche Verwaltungen jeder Größe, die eine günstige, modulare und leistungsstarke Softwarelösung benötigen.

TESTEN

Sie haben die Möglichkeit, den Security.Desk unverbindlich und risikofrei zu testen. Unsere Experten unterstützen Sie gerne dabei, den Testzugang einzurichten und beantworten Ihre Fragen während des Testzeitraums.

PRÄSENTATIONEN

In unserer “Online-Demo” interagieren Sie persönlich mit einem FCS-Experten, der Ihnen die Funktionen und Möglichkeiten vom Security.Desk persönlich zeigt. Während des Termins können Sie Ihre Anforderungen direkt abgleichen und wichtige Fragen stellen.

WEBINARE & VERANSTALTUNGEN

In unseren Webinaren, EventDays und Messen treten Sie persönlich in Interaktion mit unseren Experten und gewinnen Einblicke, Expertise und Mehrwert.
Sie können Fragen stellen, sich vernetzen, von anderen Kunden lernen und sich über neue Features, Funktionen, Best Practices, Tipps und Tricks informieren. Erleben Sie z.B. unsere monatlichen Webinare bequem online.

FAIR COMPUTER SYSTEMS GmbH

TOP 100
top100.de
Top-Innovator 2021

IT-, Asset- und Service-Management Software für Ihre Digitalstrategie

Unser Ziel ist es, Komplexes einfach zu machen. Wir haben unseren Funktionsumfang modular aufgebaut und entwickeln unsere Software kontinuierlich weiter, um sicherzustellen, dass sie nahtlos in jede IT-Landschaft integriert werden kann.

Sie möchten den Security.Desk kostenlos testen?
Kein Problem!

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

FAIR COMPUTER SYSTEMS

Wir sind ein eigentümergeführtes, deutsches Softwareunternehmen, das sich auf die Realisierung innovativer betrieblicher Software spezialisiert hat. Unsere Software-Anwendungen erhalten regelmäßig Auszeichnungen und sind in vielen Bereichen zertifiziert. Besonders stolz sind wir darauf, dass FCS mit dem renommierten TOP 100-Siegel als eines der innovationsstärksten deutschen Mittelstandsunternehmen ausgezeichnet worden ist.

IT Management Solutions

Im Bereich “IT Management Solutions” entwickeln wir herausragende Standard-Software-Lösungen. Unsere Palette umfasst IT-Inventarisierung, IT-Asset- und Lifecycle-Management, Enterprise-Asset-Management, Lizenz- und Vertragsmanagement, Softwareverteilung, USB- und Endpoint Security sowie umfassendes IT-Service-Management und Helpdesk-Lösungen, die durch uns selbst europaweit vertrieben und supportet werden. Zu unseren Kunden zählen namhafte Unternehmen des Mittelstands aus allen Branchen, öffentliche Verwaltungen, Behörden und Organisationen. Wir unterstützen unsere Kunden bei der Entwicklung und Umsetzung ihrer digitalen Strategie im Bereich IT- und Asset-Management mit unseren Produkten und unserem Know-How. Mehr als 600 Kunden vertrauen auf die Software-Lösungen von FCS und setzen auf eine enge Zusammenarbeit mit uns.

FCS Drive

In unserem Geschäftsbereich “FCS Drive” entwickeln wir mit modernsten Technologien webbasierte Anwendungen, Data Warehouses, Web Services und mobile Apps für die Automobilwirtschaft. Zu unserem Kundenkreis gehören internationale Automobilhersteller, große Autohandelsgruppen und Importeure, wie Stellantis, die PSA Gruppe, Opel/Vauxhall, Ford, die AVAG Holding und die Emil Frey Gruppe.

ZUFRIEDENE KUNDEN SIND DIE BESTE REFERENZ!

Scannen Sie mich!

Adresse
FCS Fair Computer Systems GmbH
Ostendstraße 132
90482 Nürnberg

E-Mail
info@fair-computer.de

Telefon
+49 (0) 911 810881 0

CO_2 NEUTRAL