Datenschleuse Plus

Bedrohungen durch Schadsoftware beseitigen

USB Schnellprüfung

USB auf gesicherten USB

USB auf Netzwerkfreigabe

Zwischen Netzwerksegmenten

Einführung

Ihr Wächter beim Eintritt von Daten in ein Netzwerk und als Dienst zwischen segmentierten Netzwerken. Als Kiosk-Terminal, Server-Rack, Workstation oder Notebook.

Abwehr von Schadsoftware durch die Datenschleuse Plus - die beste Lösung für Ihr Unternehmen

Einmal in Betrieb genommen kann die Datenschleuse Plus alle Inhalte von USB-Speichermedien auf Bedrohungen überprüfen, bzw. den Datenverkehr zwischen Netzwerksegementen überwachen und schützen.

Durch den Einsatz von 8 bis 20 verschiedenen, parallel arbeitenden Antivirus-Produkten wird eine bestmögliche Sicherheitsüberprüfung vorgenommen.

USB Schnellprüfung

USB auf gesicherten USB

USB auf Netzwerkfreigabe

Zwischen Netzwerksegmenten

Anwendungsfälle

Die Datenschleuse Plus erleichtert den Arbeitsalltag sowie die Arbeit mit Beratern und externen Mitarbeitern enorm: Sie ist ein Sicherheitskonzept.

Die richtige Lösung zahlt sich aus

Schützen Sie Ihr Netzwerk. Durch eine sichere Verifizierung von Wechseldatenträgern oder mithilfe des Schutzes Ihrer Automatisierungskomponenten in segmentierten Produktionsnetzen.

Anwendungsfälle

- Sicheres Management von mobilen Datenträgern (USB Sticks)
- Sicheres Management von Datenverkehr zwischen Netzwerksegmenten

Software

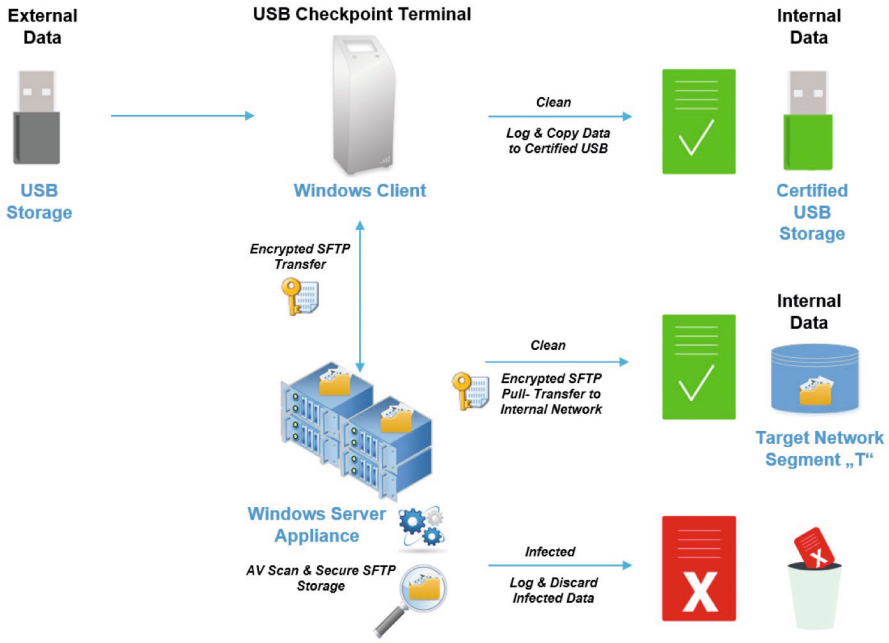
- Datenschleuse Plus inklusive 8 Virenscannern
- Virenscanner (u.a. Bitdefender, ClamAV) Standard Windows- und Web-Client

Kiosk für externe Datenträger

Die Datenschleuse Plus bietet internen und externen Besuchern die Möglichkeit, Datenträger und deren Inhalt vor dem Einbringen in das Netzwerk zu scannen (Multi-Simultan) und einen sicheren Prozess in Ihrer Organisation zu unterstützen.

Sicheres Management mobiler Datenträger

Die Datenschleuse Plus hilft Ihnen auf drei Wegen externe Datenträger zu beherrschen. Dazu gehören die USB-Schnellprüfung, der Scan vom USB zum zertifizierten USB-Stick und die sichere Übertragung vom USB-Stick zur Netzwerkfreigabe.



Der USB-Stick wird auf Schadsoftware untersucht. Sollte er überprüft und als frei von Schadsoftware klassifiziert werden, wird der Inhalt auf einen vom Unternehmen zertifizierten Stick übertragen oder direkt auf dem Datenschleuse-Server zur internen Weiterverarbeitung bereitgestellt.

Mitnahme von Daten

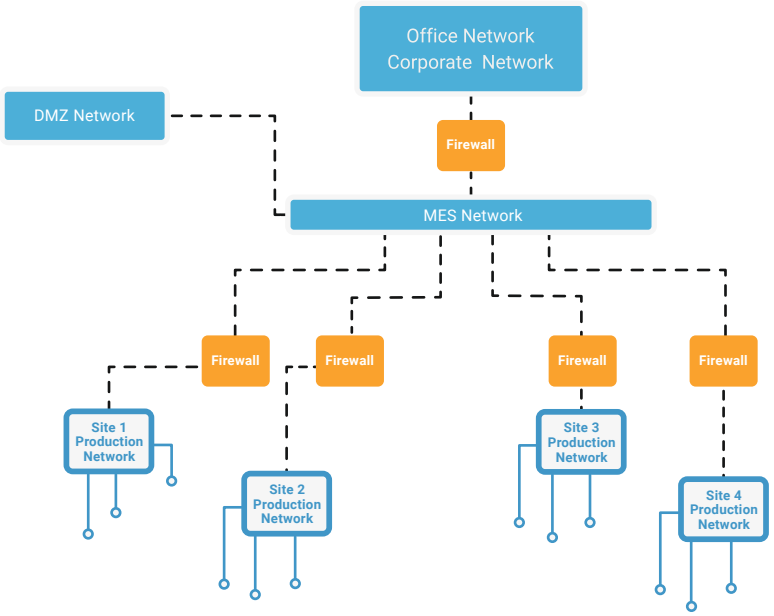
Um den Anschluss von externen Datenträgern an interne Geräte überflüssig zu machen, können über den Terminal auch Daten auf portable Medien übertragen werden. Autorisierte Benutzer können nach Authentifizierung auf ihren gesamten Datenbestand in der Datenschleuse Plus zugreifen. Für externe Benutzer können individuelle Einmal-Codes generiert werden. Diesen Code braucht Ihr Besucher dann lediglich am Terminal einzugeben und erhält automatisch die damit verknüpften Daten auf seinen gewählten Datenträger.

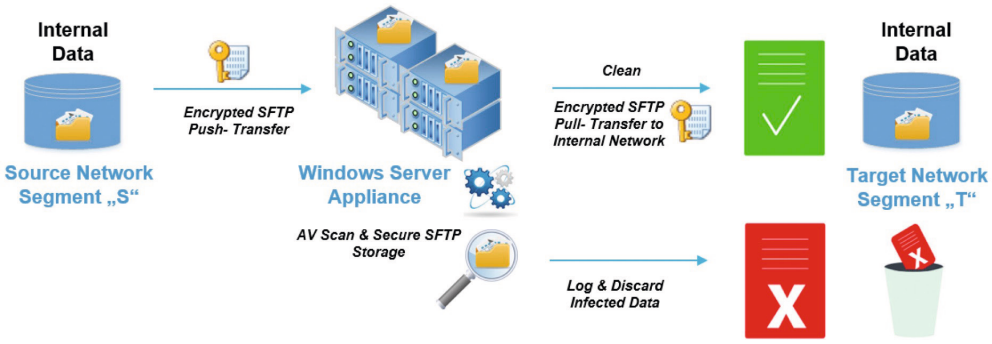
Datentransfer zwischen Netzwerksegmenten

Die Datenschleuse Plus kann auch als Rack-Variante zwischen Ihren Netzwerken als Sicherheits-Gateway eingesetzt werden. Beim Transfer zwischen Netzwerken werden Daten in der Datenschleuse Plus gescannt und, falls keine Schadsoftware erkannt wird, im gewünschten Zielordner abgelegt.

Sicheres Management von partitionsübergreifenden Datentransfers

Zur Trennung von Netzen sind in der Industrie 4.0 verschiedene Netzwerkpartitionen allgegenwärtig, z. B. ethernet-basierte Feldbussysteme. Allerdings ergeben sich damit auch erhöhte Risiken, die durch die Datenschleuse Plus gelöst werden können.





Die Datenschleuse Plus kann noch mehr

Wollen Sie Ihren Besuchern unternehmensspezifische Informationen zur Verfügung stellen? Der Kiosk lässt sich so konfigurieren, dass er auf Wunsch parallel auch eine beliebige erreichbare Webseite anzeigen kann. Ob es sich dabei um statische, dynamische, interne oder externe Inhalte handelt entscheiden ganz alleine Sie. Selbstverständlich kann die Konfiguration individuell für jeden Terminal angepasst werden, um optimal auf den jeweiligen Standort abgestimmt zu sein.

Kombinieren Sie

Um Ihnen die nötige Flexibilität zu ermöglichen, kann Ihre Lösung vollständig an Ihre Bedürfnisse angepasst werden. Die folgenden Engines können in jedes der genannten Datenschleuse-Plus-Pakete integriert werden.

Entscheiden Sie sich für Ihre perfekte Kombination

Wählen Sie die passende Kombination aus Hard- und Software.
Folgende Kombinationen können in Ihrem Unternehmen Anwendung finden:

Softwarekombinationen

Paket-Name	Multi-Scanning-Engines inklusive			
8 Engines	AhnLab ESET	Avira Quick Heal	Bitdefender K7 SECURITY	ClamAV VirIT
12 Engines	Cyren	IKARUS	Emisoft	TECHYON
16 Engines	NANO Pro	Kaspersky	VirusBlokAda	Zillya!
20 Engines	Anity	McAfee	COMODO	Sophos
Available Custom Engines	AegisLab HUORONG RocketCyber Trend Micro	ByteHero Lavasift Symantec Xvirus	CrowdStrike Windows Systeak WEBROOT	Filseclab NETGATE Trend Micro

\+ (optional)

- CVE Guard Module
- Data Sanitization Module

Hardwarekombinationen

	Einzelgerät Architektur	Client-Server-Architektur	
		Client	Server
Terminal/Kiosk	✕	✕	✕
Server Rack 19“	—	—	✕
Workstation	✕	✕	✕
Notebook	✕	✕	✕
Anwendungsfall 1: Verarbeitung mobiler Datenträger	✕	✕	
Anwendungsfall 2: Datenverkehr zwischen Netzwerksegmenten	—	✕	

Voraussetzungen

Hardware und Software

Die folgende Konfiguration bezieht sich auf die Minimalanforderung des Datenschleuse Plus-Systems. In Abhängigkeit Ihrer Anforderungen (Scan-Vorgänge, Datenvolumen, Anzahl der Anwender) können diese Vorraussetzungen variieren.

Client-Server Architektur (Client Frontend)

- Jeder Client mit Windows 10 / .net Framework 4

Client-Server Architektur (Server Backend)

- Virtuelle Maschine
- Spezifikation: 16GB RAM / 8 (v)CPUs / mindestens 200GB freier Speicherplatz
- Betriebssystem: Windows 10 / Server 2012 R2 / Server 2016 / .net Framework 4

Hardware Anforderungen

- Einzelgerät: 1 physische CPU
- Client-Server: 1 physische CPU (Frontend) und 1 CPU (Backend) (physische oder virtuelle Maschine)
- RAM (ohne System): 16 GB
- Freier Festplattenspeicher: 200 GB
- CPU: 8 Kerne

Software Anforderungen

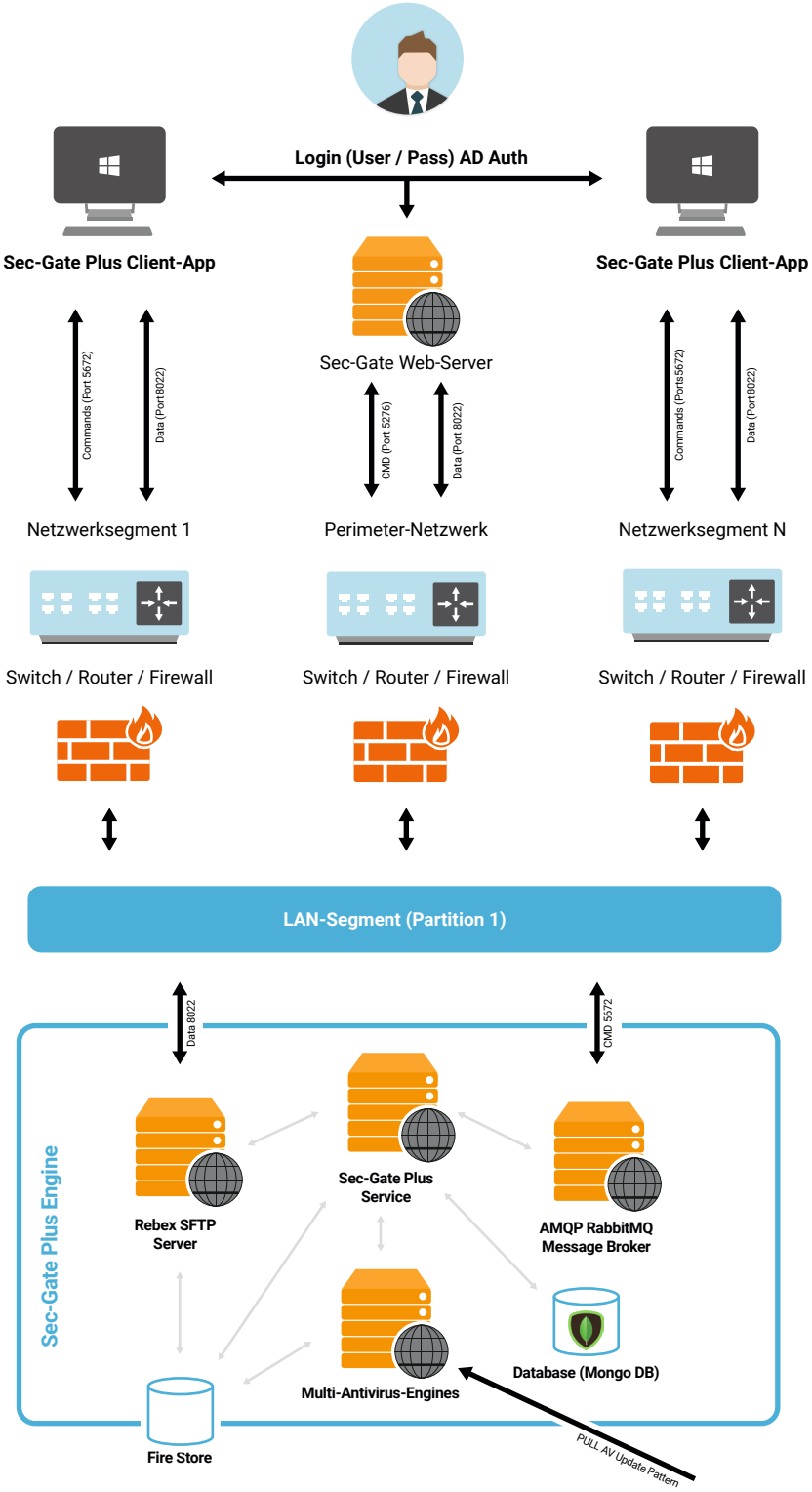
- Betriebssystem: Windows 10 / Server 2012 R2 / Server 2016 / Server 2019 / .net Framework 4
- Architektur: 64 Bit
- Internetzugriff für Updates der Virenscanner, Berichte, Logging, Service (direkt oder per Proxy)

Systemarchitektur

So kann die Datenschleuse Plus-Architektur in Ihrem Unternehmen aussehen.

Architektur der Datenschleuse Plus

Dieses Szenario illustriert die Architektur der Datenschleuse Plus. Der User kommuniziert mithilfe verschiedener Komponenten der Datenschleuse Plus zwischen mehreren Perimeter-Netzwerken in einem Unternehmen.



Betrieb & Wartung

Der Betrieb der Datenschleuse Plus kann vollständig übernommen werden

Die genauen Serviceleistungen werden über ein zugehöriges „Service-Level-Agreement“ (SLA) definiert und orientieren sich an den Anforderungen Ihres Unternehmens.

Für den Online-Zugang der Datenschleuse Plus existieren folgende Möglichkeiten

- **File-Server-Zugang empfohlen**
  (weiterer Service zur Bereitstellung der Update-Dateien erforderlich)
- **Gateway-Zugang ohne Proxy**
- **Proxy-Zugang**

Kundenspezifische Anpassung

Und nicht zuletzt kann die Datenschleuse Plus auf Wunsch im Corporate Design Ihres Unternehmens individualisiert werden.

- **Kunden-Branding des Kiosk-Gehäuses** (gegen Aufpreis)
- **Kunden-Branding der grafischen Benutzeroberfläche** (Logo inklusive)
- **Kundenspezifische Anpassung der Scanregeln** (inklusive)
- **Rollen- & Rechteverwaltung Active Directory-basiert**
- **Kundenspezifische Anpassung von Arbeitsabläufen** (nach Aufwand)

Datenschleuse Plus

Ein zentraler Baustein für Ihr
individuelles Sicherheitskonzept

i2 solutions
intelligent growth

Pfarrer-Gau-Str. 13
52223 Stolberg

+49 2402 10 29 94 0
info@i2solutions.de

www.i2solutions.de
www.sec-gate.de