# Sec-Gate Plus

Eliminate threats by malware



USB Quick-Scan          USB to Secure USB          USB to Network-Share          Network to Network

# Preventing malware through the Sec-Gate Plus - the best solution for your company

Once commissioned, the Sec-Gate Plus can access all contents of USB storage media and check for threats, or control the data traffic between network segments and protect them.

Through the use of 8 to 20 different antivirus products working in parallel, the best possible security check will be carried out.

**USB Quick-Scan**

**USB to Secure USB**

**USB to Network-Share**

**Network to Network**

## The right solution pays off

Protect your network. Through a secure verification of removable media or by safeguarded automation components in segmented production networks.

### Use cases
- Secure management of mobile data storage devices (USB flash drives)
- Secure management of partition data transfer

### Software
- Sec-Gate Plus System (Datenschleuse Plus) including 8 Antivirus-Engines
- Antivirus Engines (a.o. Bitdefender, ClamAV) Standard Windows- and Web-Client
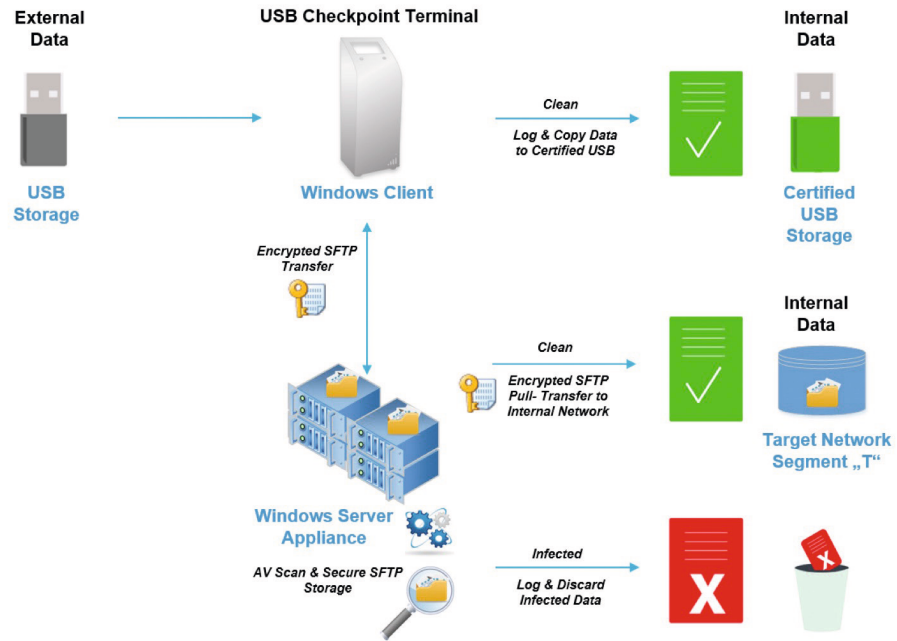
# Secure management of mobile data carriers

The Sec-Gate Plus helps you to control external data drives in three ways.
These include the USB Quick Scan, the scan from the USB to the certified USB stick and secure transfer from USB stick to network share.



The USB stick is checked for malware. If it is checked and classified as free of malware, the content is transferred to a stick certified by the company or made available directly on the Sec-Gate-Server for further internal processing.

# Data download

To eliminate the need to connect external data media to internal devices, data can also be transferred to portable media via the terminal. Authorized users can access their entire data inventory in the Sec-Gate Plus after authentication. Individual one-time codes can be generated for external users. Your visitor only needs to enter this code at the terminal and automatically receives the data linked to it on his or her selected data media.
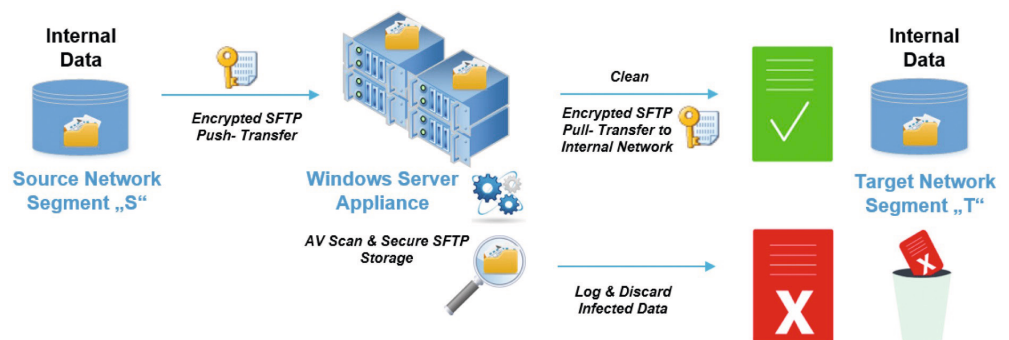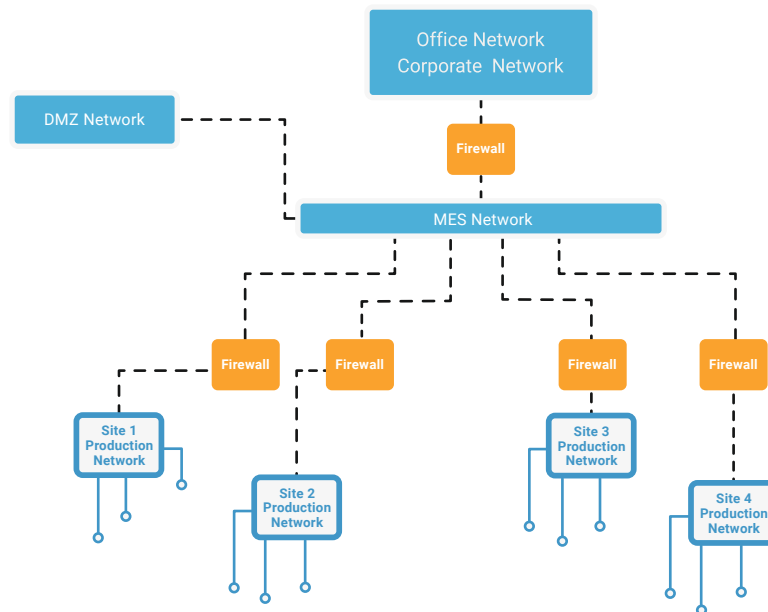
## Secure management of cross-partition data transfers

Network partitioning, such as Ethernet-based fieldbus systems, is the ubiquitous solution for the separation of networks in the industry 4.0. However, this results in increased risks that can be solved by the Sec-Gate Plus.



## The Sec-Gate Plus can do even more

Do you want to provide your visitors with company-specific information? The kiosk can be configured to display any accessible website in parallel if desired. You alone decide whether this content is static, dynamic, internal or external. Of course, the configuration can be adapted individually for each terminal in order to be optimally adapted to the respective location.

# Choose your perfect combination

Choose the right combination of hardware and software.
The following combinations can be used in your company:

## Software combinations

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

+ (optional)
- CVE Guard Module
- Data Sanitization Module

## Hardware combinations

| | Standalone Architecture | Client-Server-Architecture | |
|---|---|---|---|
| | | Client | Server |
| Terminal/Kiosk | ✖ | ✖ | ✖ |
| Server Rack 19" | — | — | ✖ |
| Workstation | ✖ | ✖ | ✖ |
| Notebook | ✖ | ✖ | ✖ |
| Use case 1: Mobile Data Storage | ✖ | ✖ | |
| Use case 2: Partition Data Transfer | — | ✖ | |

# Requirements

## Hardware and Software

The following configuration refers to the minimum requirement of the Sec-Gate Plus System. Depending on your specific needs (scanning processes, data volume, number of users), these requirements may vary.

**Client-Server Architecture (Client Frontend)**

- Any Client running Windows 10 / .net Framework 4

**Client-Server Architecture (Server Backend)**

- Virtual Machine
- Specs: 16GB RAM / 8 (v)CPUs / at least 200GB of free Storage
- Operating System: Windows 10 / Server 2012 R2 / Server 2016 / .net Framework 4

**Hardware requirements**

- Standalone Version: 1 physical CPU
- Client-Server: 1 physical CPU (Frontend) and 1 CPU (Backend)
  (physical or virtual machine)
- RAM (without System): 16 GB
- Free Hard Drive Space: 200 GB
- CPU: 8 cores

**Software requirements**

- Operating System: Windows 10 / Server 2012 R2 / Server 2016 / Server 2019 / .net Framework 4
- Bitness: 64-bit only
- Internet access for Antivirus Updates, Reporting, Logging, Service
  (via proxy or direct WAN gateway)

# Architecture of the Sec-Gate Plus

This scenario illustrates the architecture of the Sec-Gate Plus. The user communicates between several perimeter networks in a company using various components of the Sec-Gate Plus.
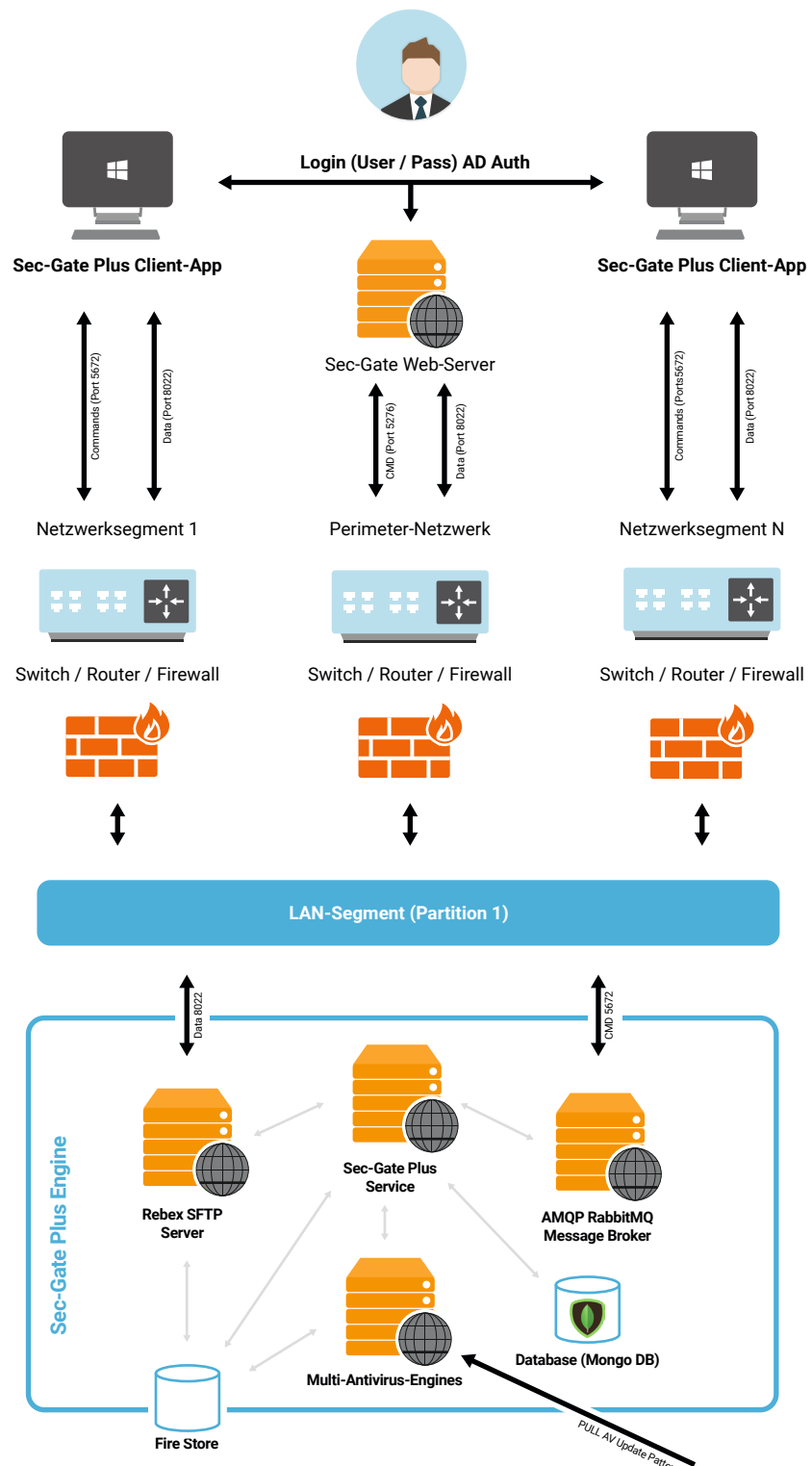
# Operation & Maintenance

## Running operations of the Sec-Gate Plus can be completely taken over

The exact services are provided via an associated "Service Level Agreement" (SLA). They are defined and oriented to the requirements of your company.

## The following options exist for online access to the Sec-Gate Plus

- **File server access recommended**
  (additional service required to provide update files)
- **Gateway access without proxy**
- **Proxy access**

---

# Customization

And last but not least, the Sec-Gate Plus can be customized in your company's corporate design if desired.

- **Customer branding of kiosk case** (for an additional charge)
- **Customer branding of graphical user interface** (Logo included)
- **Customization of Pass/Deny rules** (included)
- **Roles- & Rights Management Active Directory based**
- **Customization of workflows** (Time & Material basis)

# Sec-Gate Plus

A central component for your
individual security concept.

**USB Checkpoint**