2 solutions
intelligent growth

SecureG

Data Security Redefined

SecureG Cybersecurity

SecureG is a comprehensive security solution designed to meet the high security requirements of industrial environments. It provides a secure platform for data transfer and verification, protecting critical infrastructure and ensuring uninterrupted production processes.

SecureG Use Cases

Securely scan and manage external drives

Ensure secure data transfer between different network segments

Provide a security gateway to protect against cyber threats

SecureG Components

SecureG Kiosk Terminal App

Kiosk Touchscreen .NET WPF Application to run the 4 usecases:
1. QUICK SCAN, 2. USB-2-USB copy 3. USB-2-SHARE copy
4. DOWNLOAD-2-USB

SecureG Desktop Client App

File Explorer like interface to access SecureG solution. Lightweight .Net WPF app, distribution & update via ClickOnce – no admin rights required

SecureG Web App

SecureG web app offering all desktop app functionalities without a dedicated client

SecureG Automation Service Syncovery

3rd party app with SecureG integration for all kinds of interfaces to other protocols and services for all automation and integration requirements

SecureG Backend Server

Core SecureG service with logic, RabbitMQ, Mongo DB and integrated Rebex SFTP Server
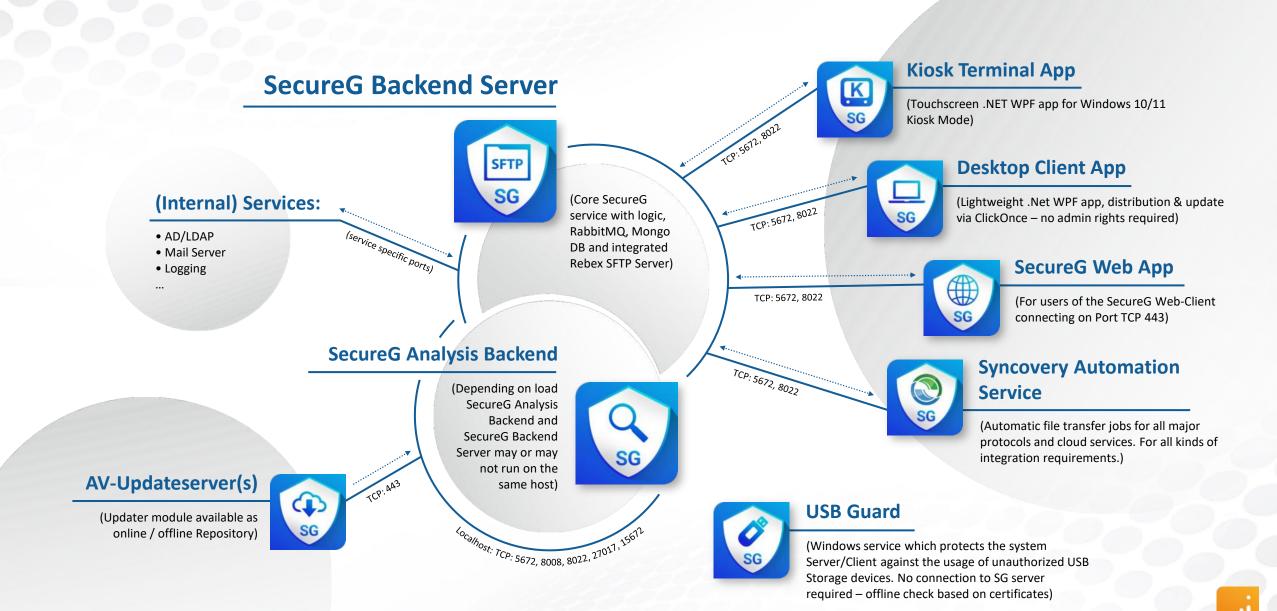
SecureG Analysis Backend

Backend services to analyse the data provided to SecureG (Choose different OnPrem AV Solutions (Kaspersky, Avira, ClamAV, Bitdefender,…), CDR (Glasswall), Virustotal, Sandboxing…)
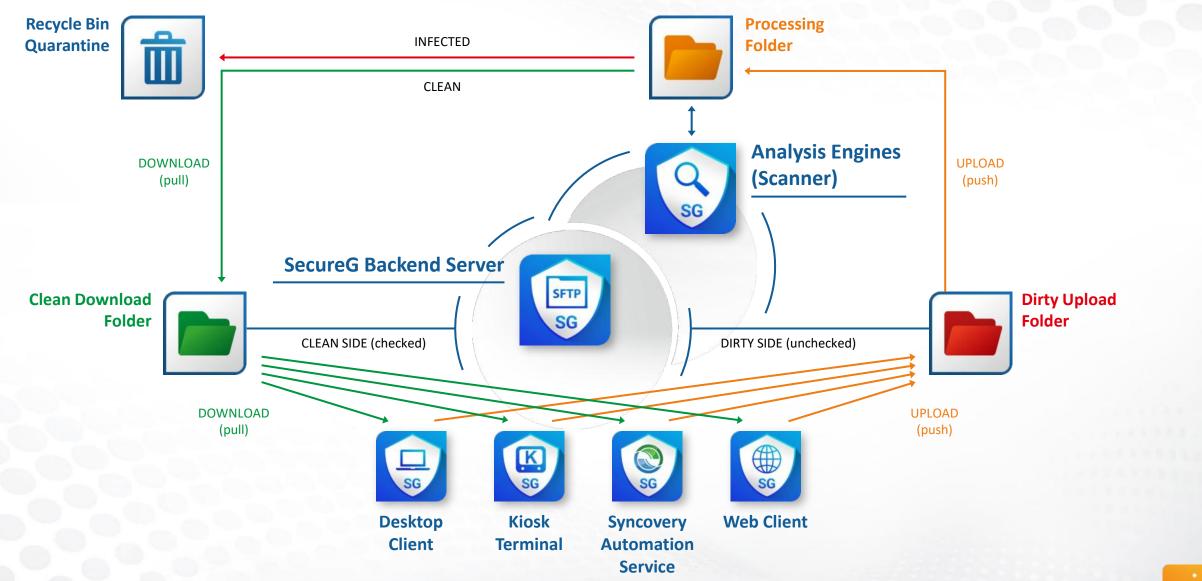
SecureG USB Guard

Client Windows Service to protect local USB ports against usage of unauthorized storage devices (e.g. USB pen drive). If a USB storage device has been scanned by the SecureG system and was marked as clean it may be used on the client machine.
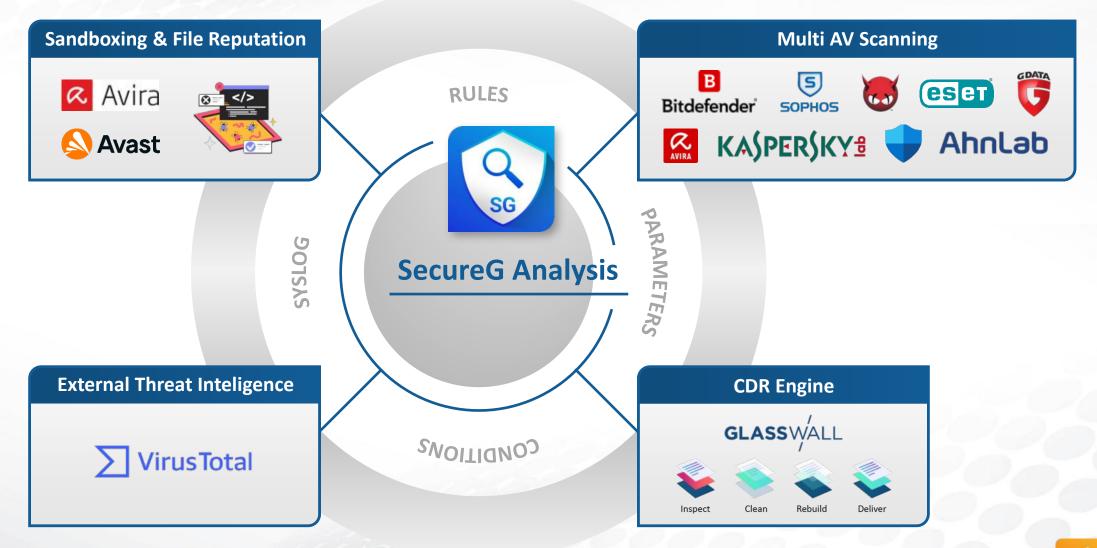
SecureG Technical Architecture

SecureG Backend Server

(Internal) Services:

- AD/LDAP
- Mail Server
- Logging
- …

(service specific ports)

(Core SecureG service with logic, RabbitMQ, Mongo DB and integrated Rebex SFTP Server)

Kiosk Terminal App

(Touchscreen .NET WPF app for Windows 10/11 Kiosk Mode)

TCP: 5672, 8022

Desktop Client App

(Lightweight .Net WPF app, distribution & update via ClickOnce – no admin rights required)

TCP: 5672, 8022

SecureG Web App

(For users of the SecureG Web-Client connecting on Port TCP 443)

TCP: 5672, 8022

SecureG Analysis Backend

(Depending on load SecureG Analysis Backend and SecureG Backend Server may or may not run on the same host)

Syncovery Automation Service

(Automatic file transfer jobs for all major protocols and cloud services. For all kinds of integration requirements.)

TCP: 5672, 8022

AV-Updateserver(s)

(Updater module available as online / offline Repository)

TCP: 443

Localhost: TCP: 5672, 8008, 8022, 27017, 15672

USB Guard

(Windows service which protects the system Server/Client against the usage of unauthorized USB Storage devices. No connection to SG server required – offline check based on certificates)

SecureG Workflow

SecureG Analysis Backend - Zero-Trust File Protection

Sandboxing & File Reputation

Multi AV Scanning

Bitdefender · SOPHOS · eset · GDATA · AVIRA · KASPERSKY lab · AhnLab

External Threat Inteligence

VirusTotal

CDR Engine

GLASSWALL

Inspect · Clean · Rebuild · Deliver

SecureG Analysis

RULES · PARAMETERS · CONDITIONS · SYSLOG

Hardware Options for the SecureG System

Standard Hardware
+ i2solutions Extensions

Large Kiosk (with 19" rack)

Mobile Client

Small Kiosk

Large Kiosk in
Corporate Design

Screenshot Kiosk App (Touchscreen)

Screenshot Windows Client App

Screenshot Windows Client App

Screenshot Web App

Screenshot Syncovery Automation

SecureG Offers the Following Security and Data Protection Benefits

Zero-Trust File Protection
Comprehensive threat protection through a combination of sandboxing, multi-AV scanning and CDR

Usability
Simple and intuitive user interfaces for kiosk terminals, desktop and web applications

Optimised Workflow
Seamless and efficient management of security processes through automated checks and centralised data management

Flexible and customized
Customisable, including custom hardware solutions and branding options

Sales & Support

Dr. Thomas Wiegand
Partner

E-Mail: t.wiegand@i2solutions.de

Phone: +49 (0)2402 102994-22
Mobile: +49 (0)170 4519082

Technical Information & Support
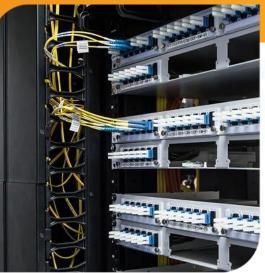
Stephan Schopen
Dipl.-Ing.(FH), MBA
Partner

E-Mail: s.schopen@i2solutions.de
Phone: +49 (0)2402 102994-24

i2 solutions
intelligent growth

i2solutions GmbH
IT Consulting Germany

CEO David Bergstein

Pfarrer-Gau-Str. 13
52223 Stolberg
Germany

SecurITy
made in Germany
Trust Seal
www.teletrust.de/itsmig

www.i2group.de

Member of **i2 group**