



edge.SHIELDOR

Technical data sheet

Protect your industrial machines from outside and inside attacks

The edge.SHIELDOR prevents uncontrolled information exchange of industrial machines. By using only required services as well as segmenting and monitoring these services, the network of manufacturing plants (OT network) is separated from the higher-level IT network.

The entire network topology is concealed, so that if a sub-network is compromised, it is not possible to access the gateway. Additional protection is provided by the functionality to convert outdated and unsecure protocols into secure protocols (according to current knowledge). As a result, all units to be protected in the OT network can be operated without interruption and security is guaranteed throughout by the edge.SHIELDOR.

The product supports common administrative services and their supporting protocols. Additionally, you can use the customizable configuration interface: web services, machine status, logging and user authentication can be accessed from outside with access authorization.

► Firewall and gateway

- Easy set-up and operation via central management interface
- IP configuration of the control computer
- Secure web-based configuration via HTTPS encryption
- Positive and negative filtering rules (IP-, port-, time-controlled)
- Host- and network-based Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) - identification and blocking of unwanted communication attempts
- Defense against DoS attacks
- Operating mode: No routing
- Operating mode: Standard router
- Operating mode: NAT router
- Integration via a single intranet IP
- Static NAT for 1:1 mapping of intranet IPs to hosts

► Supported protocols

- IPv4 / IPv6, TCP/UDP/ICMP/SCTP
- IEEE 802.1X Ethernet Authentication
- VLAN (IEEE 802.1Q)
- DHCP server, DHCP client
- DNS server
- Transfer to Azure/IoT Hub, AWS/IoT Core and others

Further protocols upon request.



edge.SHIELDOR

Technical data sheet

▶ Secure access and operation

- Own user management
- Token-based authentication
- LDAP-integration of a company-wide LDAP
- Two-factor authentication
- Server: Secure VPN dial-in to segregated network with Windows, Linux, MacOS, Android, IOS clients
- Firewall access control of VPN clients (IP-, port-, and time-controlled)
- VPN remote access from external network participants such as manufacturers and service providers
- Encryption: SSL / TLS v1.3 (company certificates importable)
- Two-factor authentication: certificate authentication
- All service / management services deactivatable
- All services configurable through REST API (OpenAPI definition)
- Seamless update, otherwise automatic update in service window
- Interaction via / collaboration of multiple product instances
- Simplified configuration and analysis through machine learning

▶ Supported ports

- HTTP/S server (port 80, 443)
- FTP server (port 21)
- SMB server (port 139, 445)
- SMTP server (port 25, 587)
- LDAP server (port 389, 636)
- FTP(S) server (port 21, 30000-30009)
- User-defined port forwarding from the OT network (optional: additional encryption)
- User-defined port forwarding from the IT network

▶ Logging of Information

- Logging of transfer types, services, authentications, user actions, configuration changes, firewall, IP forwarding
- Forwarding to central company logging system
- Automated analysis of log data and informing of users

▶ Backup, recovery, and data protection

- 120 hours of data retention
- Automatic backup and restore to external system

▶ Transfer variants

File transfer / synchronization

- Filtering by positive and negative lists (file names, file types, SHA512 checksums)
- Virus scan incl. defense against viruses, ransomware, botnet, and spyware
- Supported operating systems: Windows 10 or later (IT network only), Windows 7, Windows XP, Windows NT (protocol: SMB NTLM v1)

Remote transfer

- Protocols: RDP, VNC, SSH, Telnet

Process data transfer

- Protocols: OPC-UA server/client,
- Modbus/TCP, S7 protocol (RFC 1006)

▶ Support Plan

Basis Support and Premium Support available upon request.

You would like to know more about the edge.SHIELDOR?

Contact our expert team directly at sales@cbb.de

TRIOVEGA GmbH
Isaac-Newton-Straße 8
23562 Lübeck, Germany
T: +49 451 39771 0
E: info@triovega.com