

Siemens S7

EtherNet/IP

OPC UA

IEC 61850

PROFINET

Modbus

BACnet

IEC 60870-5-104

DNP3

Monitor and protect your IT and OT networks with a single solution

EUROPEAN VENDOR

Visibility into IT and OT assets

One unified inventory, each device identified by type, vendor, and hardware and software version, and rated by a risk score you can track over time.

Zero operational impact

Non-intrusive monitoring that reads your network traffic based on flows and packets without touching your devices or adding load.

Threat detection before disruption

Detection of known cyber attacks, unauthorized changes and unusual activity across your IT and OT networks, before they impact operations.

Support for NIS2 and IEC 62443

Continuous monitoring, audit trails and reporting that support your compliance with NIS2, IEC 62443 and related national regulations.

On-premise and air-gapped deployment

Full deployment inside your own infrastructure, from single sites to distributed networks, including fully air-gapped environments.

**GREYCORTEX Mendel
secures**



**ENERGY DISTRIBUTION
& GENERATION**



WATER & OTHER UTILITIES



MANUFACTURING & PROCESSING



PHARMACEUTICAL MANUFACTURING



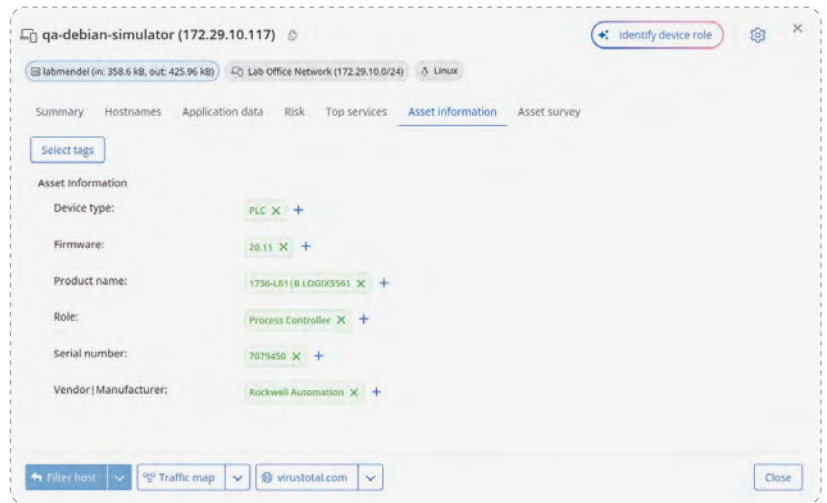
BUILDING MANAGEMENT

One view across IT and OT

Asset inventory

every device, its details, and its known vulnerabilities

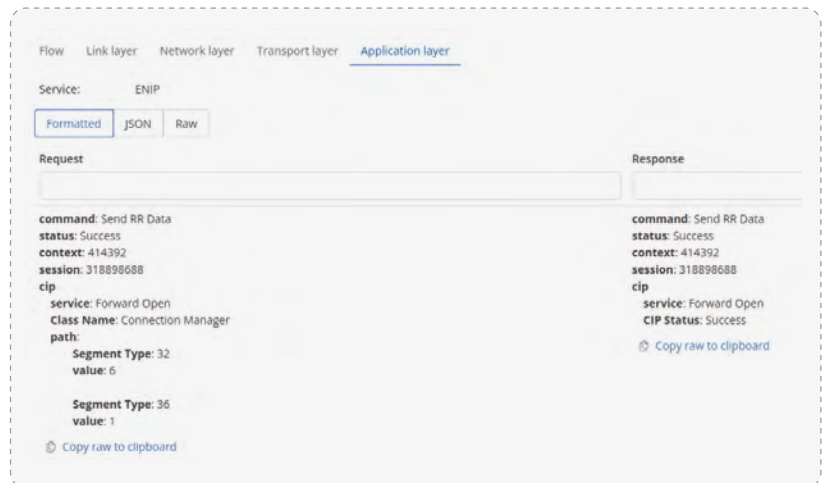
- Discovery of asset information from network traffic: vendor, hardware and software version, operating system, and network information.
- Mapping of known vulnerabilities (CVEs) to discovered devices.
- Detection of new devices, services, and subnets.
- Inactive and lost device detection: a device that stops communicating is reported as inactive first, so it can be investigated before it is removed.
- Automatic and manual tagging of devices by type and role.



Protocol visibility

detailed insight into your industrial protocols

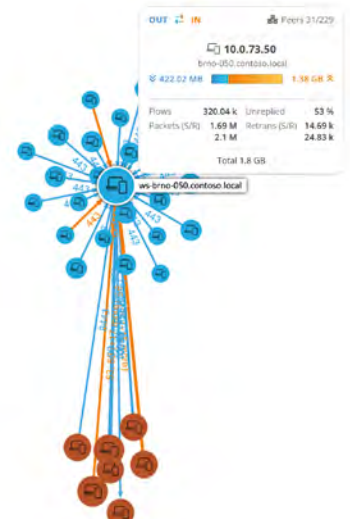
- Support for the most used protocols from various vendors, including Siemens, ABB, Honeywell, Emerson, Schneider, and GE.
- Deep analysis and extraction of protocol-specific metadata for supported ICS and SCADA protocols, including BACnet, CC-Link, CoAP, DLMS/COSEM, DNP3, EtherNet/IP, EtherCAT, Ether-S-Bus, GE-SRTP, IEC 60870-5-104, IEC 61850 (GOOSE, SV, MMS), Modbus, MQTT, OMRON FINS, OPC UA, PROFINET (IO DCE/RPC, DCP, Realtime PN-IO), MELSEC-E4, Siemens S7, SNMP, HART-IP, M-Bus, DICOM, HL7 and 30+ office protocols.



Network visibility

every connection between your IT, OT, and the outside world

- Full visibility into both IP and Ethernet traffic.
- Visualization of the network, its dependencies, assets, and communication, filtered by subnet, protocol, vendor, and flow direction, for any time period.
- Network-wide view of which devices communicate with each other and with the outside, filterable to internal or external traffic.
- Visibility into remote and third-party access, including VPN and vendor connections.
- Traffic Flow Map showing a device's most significant peers and the direction and volume of each connection, expandable step by step.



Threat detection

known attacks, anomalies, and unauthorized activity

- Detection of known attacks, malware, and vulnerability exploits (CVEs).
- Detection of unauthorized control commands, using OT-specific detection signatures.
- Command-and-control communication, scans, brute-force attacks, and data exfiltration.
- Previously hidden, targeted, and zero-day attacks, found through network behavior analysis and machine learning.
- Detection mapped to MITRE ATT&CK, showing the attack stage and progress.

Investigation & threat hunting

explained by AI, prioritized by risk, and searchable history

- A single risk score per internal device, calculated from its security events, how unusual its behavior is, and how recent activity is.
- Score history and trend per device.
- AI explanations of what a device is, whether an external IP is dangerous, and what a security event means — with MITRE ATT&CK context and recommended next steps.
- AI assessment of a single suspicious communication, giving a verdict, a false-positive probability, and investigation steps in priority order.
- Threat hunting across indexed, searchable metadata.

AI Assistant: Explain **EARLY ACCESS**

Event Summary:

Signature ID: 900005006

Name: Blacklist: Spamhaus DROP blacklist

MITRE ATT&CK: Information/Blacklist

Description: This event is generated when there is a communication with a host present in low reputation databases. This host is then blacklisted and tagged as untrusted. An IP address earns a negative reputation when a suspicious activity, like spam or viruses originating from that address is detected and reported to blacklist sources.

1. What this event means

This alert indicates that traffic was observed involving an IP address listed on the Spamhaus DROP (Don't Route Or Peer) blacklist. DROP-listed IPs are typically associated with serious abuse (spam, malware, botnets, or other malicious activity) and are recommended to be completely blocked at the network edge.

The rule logic (`!prep:src,spamhaus_drop,>10;`) shows that the **source IP** has a high-risk reputation score in the Spamhaus DROP list, above the defined threshold.

2. Typical risk and impact

- Potential connection to known malicious or heavily abused infrastructure.
- Risk of:
 - Malware delivery or command-and-control (C2) communication
 - Spam or phishing campaigns
 - Scanning, brute-force, or other preparatory attacks
- If the blacklisted IP is **internal** (NATed or misclassified), it may indicate a compromised host in your environment.

3. How to verify if this is a false positive

1. Confirm the blacklisting status

- Identify the source IP from the event in your SIEM/NDP logs.
- Check it directly against Spamhaus:
 - Use Spamhaus lookup tools (e.g., web lookup for DROP/EDROP).
 - Verify that the IP is currently listed and not an outdated entry.

2. Determine if the IP is internal or external

- If it is an **internal IP** (RFC1918 or your assigned ranges):
 - Check if your IP reputation feed is misconfigured (e.g., applying to internal ranges).
 - Investigate the internal host for compromise (see section 4).
- If it is an **external IP**:
 - Check whether this IP belongs to a legitimate partner, vendor, or customer.
 - Contact the owner only if you have an established relationship and business need.

3. Review the context of the connection

- Direction: Was the connection **outbound** (internal → internet) or **inbound** (internet → internal)?
- Ports and protocols: HTTP/HTTPS, SMTP, SSH, RDP, custom ports, etc.
- Volume and pattern: Single connection vs. repeated/automated attempts.
- Associated alerts: Any malware, C2, or intrusion alerts involving the same IP or host.

4. Check for business justification

- Verify with application owners or system owners if there is any legitimate reason to communicate with this IP or its network.
- If there is no clear business need, treat the event as suspicious by default.

4. Immediate operational actions

1. Block or restrict traffic

- At perimeter firewalls, IPS, or routers, block traffic to/from the specific IP or its broader netblock if aligned with your policy.
- Ensure your edge devices are already enforcing Spamhaus DROP recommendations where appropriate.

2. Investigate the internal host involved

- Identify the internal source/destination host (depending on direction) using:
 - Firewall logs
 - NetFlow/sFlow
 - DHCP logs (`/bin/main IP ==> hostname/user`)

This analysis is produced by an AI system. Decisions should not be based solely on this output without appropriate validation.

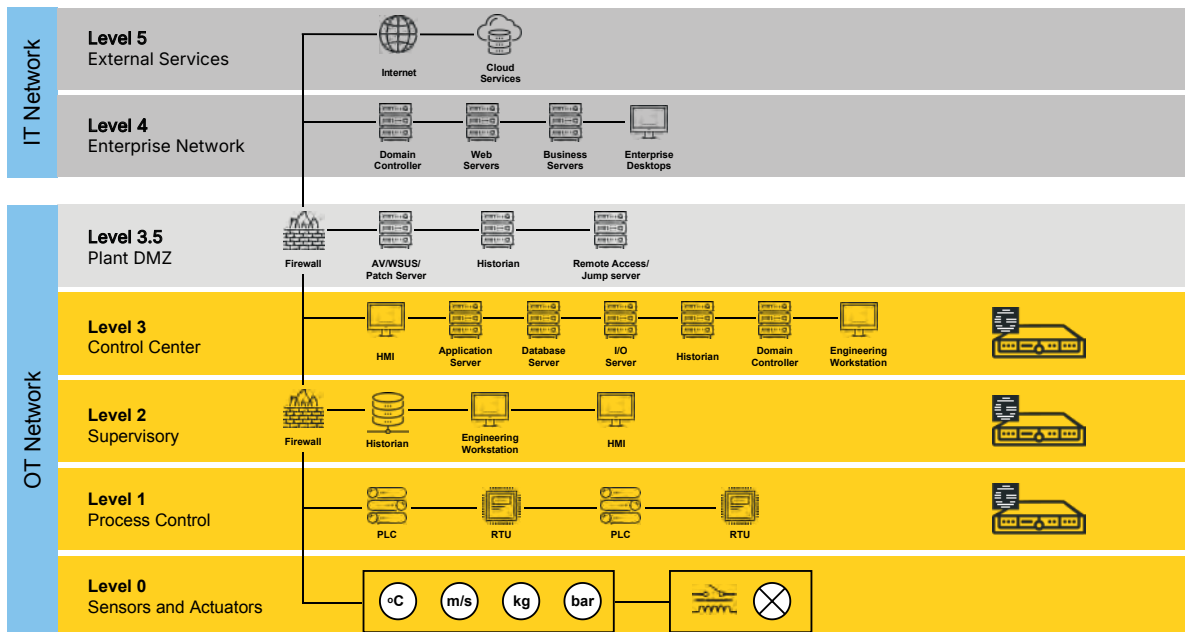
Is this information helpful?  

Compliance & audit support

for NIS2, IEC 62443, and your auditors

- Verification of network segmentation, with alerts when a device reaches the internet or crosses between segments where it should not.
- Continuous monitoring and audit trails supporting NIS2 and IEC 62443 requirements.
- Event and metadata retention over months or years, meeting audit requirements.
- A record of how each device was classified over time, including when and why its classification changed, for audit evidence.
- Detection and classification of AI services in network traffic.
- Human-readable exports (email, PDF).
- Data export in CSV and IPFIX.

Mendel deployment across the Purdue model



Inputs

Network traffic, telemetry and logs

- Mirrored traffic (TAP, SPAN, RSPAN, ERSPAN, or other mirrored traffic, including from firewalls)
- NetFlow, IPFIX, sFlow, JFlow, NetStream, and VPC Flow Logs
- Decapsulation of tunneled traffic
- L2 to L7 of the IP protocol, both IPv4 and IPv6
- Ethernet traffic
- Recorded traffic (PCAP)
- Device and application logs

Complete metadata of ICS protocols

- BACnet, CC-Link, CoAP, DLMS/COSEM, DNP3, EtherNet/IP, EtherCAT, Ether-S-Bus, GE-SRTP, IEC 60870-5-104, IEC 61850 (GOOSE, SV, MMS), Modbus, MQTT, OMRON FINS, OPC UA, PROFINET (IO DCE/RPC, DCP, Realtime PN-IO), MELSEC-E4, Siemens S7, SNMP, HART-IP, M-Bus, DCOM, HL7 and 30+ office protocols
- Other and custom protocols can be added on request

Assets discovery and network context

- Passive asset discovery from network traffic
- Integration with identity services, NACs, and user directories via logs or RESTful API

Outputs

Reporting and alerting

- Conditional reporting and alarms
- Customizable output format
- Incident management
- Human-readable reports

Integration

- SIEM integration via Syslog, CEF, LEEF, and API
- SOAR and XDR integration via API
- IPFIX flow export with filtering
- Identity: Active Directory, Microsoft Entra ID, Cisco ISE, and external logs
- Firewalls and NACs
- RESTful API

Scalability

Hardware or virtual

- Rack and DIN rail appliances from multiple vendors, including Dell and HPE
- Virtual and cloud appliances (VMware, KVM, Hyper-V, AWS, Google Cloud, Microsoft Azure and others)
- Optional microsensor with up to 3× 1GbE monitoring ports

Sensor

- Up to 100 Gbps monitored throughput
- Up to 20 monitoring interfaces (1/10/25GbE, or FPGA cards up to 8× 25/10GbE or 4× 100/40GbE)
- Virtual and cloud up to 10 Gbps

Collector

- Up to 100 sensors per collector
- Up to 250,000 monitored hosts per collector
- Data retention limited only by available storage

All-in-One

- Single appliance containing sensor and collector
- Up to 50 Gbps monitored throughput
- Up to 20 connected sensors
- Up to 80,000 monitored hosts

PROTECT YOUR INFRASTRUCTURE

GREYCORTX Mendel gives you full visibility and threat detection across your IT and OT networks, in one European solution.

Enhance your cybersecurity with GREYCORTX Mendel today.

Contact our sales representatives at info@greycortex.com.