GREYCORTEX Mendel Datasheet

NDR

Mendel, the network detection and response solution from GREYCORTEX, offers deep network visibility, advanced threat detection, and reliable response for enterprise, government, and critical infrastructures.

DATA SOURCES

- Network mirrored traffic (SPAN, TAP)
- NetFlow/IPFIX
- Network and application logs
- Recorded network traffic (PCAP)
- Kubernetes network traffic

DETAILED NETWORK VISIBILITY

- All subnets, hosts, services, and flows with detailed information
- Metadata provides rich information on network behaviour for forensic investigation, regulatory compliance, etc.
- Tunneled traffic
- Decrypts encrypted traffic with a decryption key
- Automatic identification of critical devices in the network like Active Directory, Email server, etc.
- Months of stored historical data are indexed and quickly accessible
- Powerful search across collected data using user-friendly filtering

ROBUST DETECTION

Based on machine learning processes, and mathematical models, with the elimination of false positives.

PREDICTION ANALYSIS

- Volumetric anomalies
- DDoS attacks

Use of advanced AI algorithms and machine learning techniques to anticipate and identify potential security threats before they manifest into full-fledged attacks.

DISCOVERY ANALYSIS

- New devices, services, and communication vectors
- New administration access

Process of systematically exploring and mapping the network environment to identify assets, vulnerabilities, and potential points of compromise.

RULE-BASED ANALYSIS

- Detection of known malware and exploits
- Security policies violations

Method of identifying and evaluating security threats based on predefined rules or criteria to detect and respond in real-time.

REPETITIVE ANALYSIS

- Command and control attacks
- Brute force attacks

Identifying and analyzing repetitive patterns or behaviors within network traffic to uncover potential security threats or anomalies.

FLOW ANALYSIS

- Scans
- Brute force attacks
- Enumerations

Examination and interpretation of network traffic flows to gain insights into communication patterns, behavior, and potential security threats.

PERFORMANCE ANALYSIS

- Network performance issues: high response time, slow round trip time

Evaluating and optimizing operational efficiency, reliability, and scalability of security systems and network infrastructure by continuous monitoring of the performance metrics.

LOG ANALYSIS

- New firmware, new users
- Changes in registry and configuration

Collecting, parsing and analyzing log data generated by various network devices, systems and applications to identify security incidents, anomalies and operational issues.

RESPONSE

- Centralized platform for tracking, documenting, and reporting security incidents.
- Plugin system for universal way of interaction with Firewalls, NACs, etc.
- Extensive data export capabilities to share everything with other security tools.

KEY CAPABILITIES

Network Behavior Analysis

Flow-based analysis of network traffic with unsupervised machine learning and several detection techniques (see above).

Detection capabilities:

- Malware activity – propagation, downloading, spamming, etc.
- Attacker activity – scanning, brute-forcing, exploitation, etc.
- C&C activity – RAT, APT, AVT, bots, worms, rootkits, etc., and exfiltration

Deep Packet Inspection

- Monitors any interaction with, or inside the internal network
- Allows to inspect traffic up to 100Gbits/sec
- Detection signatures for malware, policy violations, attacks, and other activity
- Malicious file detection by hashing
- Communication with blacklisted hosts
- Possibility to add user-created signatures with easy-to-write syntax in the rule wizard

Network Inventory

- Merged Visibility and Detection layer into one clear view.
- Network infrastructure with added value of subnet and host detailed information flavored with calculated risk and security view.
- Data represented as a sortable table or scalable graphical interpretation

Performance Monitoring

Flow-based analysis of network and application performance (NPM, APM):

- Application awareness
- Monitoring current and average bandwidth
- Monitoring performance metrics such as application response times, round-trip time, user-experience time
- Rule-based detection (e.g. SLA)
- Automatic anomaly-based detection

Historical Metadata and Forensics

Mendel's proprietary Advanced Security Network Metrics (ASNM) protocol is security and performance-focused for advanced description of network traffic.

Capabilities include:

- Bi-directional flow recording (single flow contains both request and response)
- Metadata of application protocols for FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP/S, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, SSL/TLS, Kerberos, etc.
- Data can be stored for months or years (depending on storage capacity)

Device Taxonomy

- Extended classification of devices and their roles.
- Dynamic visibility by tracking new activities or changes caused by devices communicating in the network.
- Manual or automated way of tagging hosts or subnets by user-defined rules with easy-to-understand syntax wizard.

Traffic Recording and Replay

- On-demand or rule-based packet capture based on source and destination IP, MAC, protocol, port, etc.
- Ability to replay PCAPs recorded by Mendel itself or to upload captured traffic from other tools for further analysis.

OT Capabilities

- Detection, parsing and alerting with rich metadata for industrial protocols for BACnet, CC-link, COAP, DLMS/COSEM, DNP3, ENIP, EtherCAT, GE-STRP, IEC-104, IEC61850 (GOOSE, SV, MMS), MODBUS, MQTT, OMRON FINS, OPC UA, Profinet IO DCE/RPC, PROFINET-DCP, PROFINET Realtime (PN-IO), Siemens S7, SNMP, DICOM, HL7, Ether-S-Bus
- OT specific detection signatures by GREYCORTEX
- OT application metrics
- Asset discovery with context characteristics and roles
- Purdue and MITRE ATT@CK data presentation overlays

INPUTS

A comprehensive approach to ingest data from many different sources to ensure network data analysis and security, including various layers of the OSI model, utilisation of threat intelligence feeds, network and user awareness features for effective policy enforcement and threat mitigation.

Network Data

- Mirrored traffic (TAP, SPAN, RSPAN, ERSPAN or other type of mirrored data port)
- Link layer support
- Network layer support including IPv6 protocols
- Decapsulation tunneled traffic
- Transport layer support
- Application layer support
- Flow monitoring protocols (NetFlow family, IPFIX, sFLOW, JFlow, NetStream, and VPC Flow Logs)
- Other Mendel appliances (sensor or collector)

Threat Intelligence

- Detection rule-set by Proofpoint Emerging Threats and GREYCORTEX in-house research
- Other threat intel databases of IPs, domain reputations, and malicious file
- Possibility to integrate your own TI feeds (including national MISP platforms)
- MITRE ATT&CK Enterprise and ICS frameworks

Network Awareness

- Definition of policies by segments/subnets that share the same patterns of network behavior e.g. management, sales, servers, WiFi, VoIP, printers, DMZ, etc.
- IP to domain name (using DNS records)

User Awareness

- IP to host/user name (AD, LDAP, CISCO ISE, and any provided logs with such information within the monitored network from various services)

OUTPUTS

The system provides a comprehensive set of outputs and integrations for efficient network monitoring and security management and ensures efficient monitoring, analysis, and response to network security incidents.

Graphical User Interface

- Web user interface (Firefox, Chrome, Opera, Edge)
- Main interactive dashboard based on GREYCORTEX's and MITRE ATT&CK®'s frameworks
- Easily customizable dashboards with preprocessed data analysis
- Managerial and security dashboards for a simple overview
- Fast and rich filtering capabilities
- IDS rule wizard
- Two design themes (light and dark)
- Context help and wide user documentation

Reporting and Alerting

- Conditional reporting (alarms)
- Rich customizable output format with custom links to the GUI
- Human-readable formats: email (HTML), and PDF

Integration

- SIEM – batch or real time reporting based on CEF, LEEF, Syslog or API
- SOAR – generic integration based on event export and API with content pack for Palo Alto XSOAR
- XDR – generic or vendor-specific integration with EDR platforms based on API
- IPFIX – Export of flows in IPFIX format
- IDENTITY – Active Directory, Cisco ISE, and common external logs for user identity
- FIREWALL/NAC – MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint, etc.
- OUTPUT – Customizable data outputs
- API – Generic RESTful API to integrate with other infrastructure
- BACKUP – data and configuration throughout SMB, HCP, AWS S3 or locally mounted USB storage

DEPLOYMENT

Deployment scalability and high availability varies according to specific conditions and combinations in the infrastructure. Interoperability with identity services to properly manage users and its permissions, including compatibility with SSO/MFA.

Sensor

- Up to 100Gbps monitored throughput
- Up to 20× monitoring interfaces per HW appliance with any combination of 1GbE, 10GbE, 25GbE or with HW accelerated FPGA cards up to 8× 25/10GbE or 4×100/40GbE
- Support for virtual or Cloud appliances up to 10Gbps
- Optionally small-factor HW microsensor with up to 3× 1GbE monitoring ports

Collector

- Up to 100 sensors per single collector (based on overall processed throughput)
- Up to 150,000 monitored nodes per collector
- Data retention is limited only by the size of the available (designed) data storage
- Virtual appliances (including Cloud) with up to 20 connected sensors
- Multi-partition storage with fast disk support (NVMe, SSD, SAS)
- Online and offline capability to upgrade itself or connected sensors

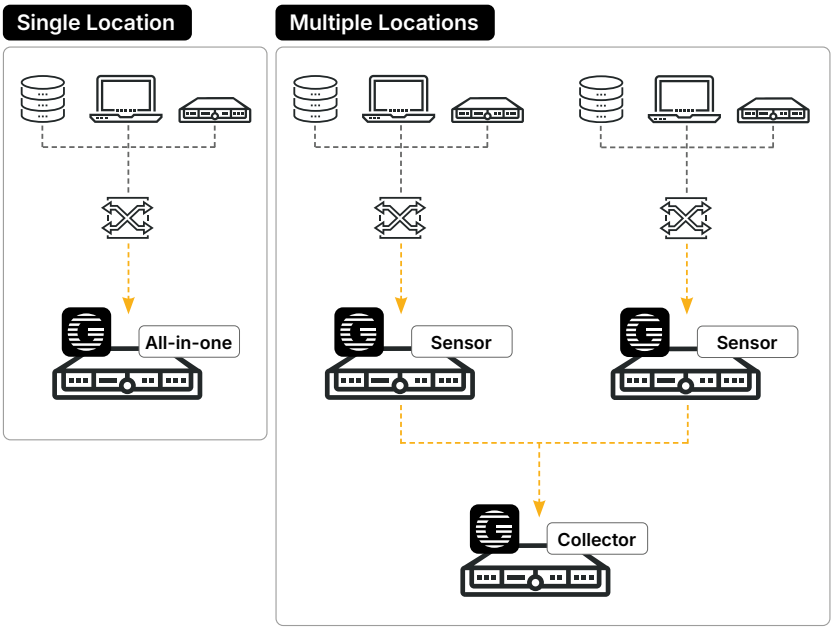
All-in-One

- Single appliance containing sensor and collector at once
- Up to 50Gbps monitored throughput
- Up to 20× monitoring interfaces per HW appliance with any combination of 1GbE, 10GbE, 25GbE or with HW accelerated FPGA cards up to 8× 25/10GbE or 4×100/40GbE
- Up to 20 connected additional sensors per single All-in-One appliance
- Up to 50,000 monitored nodes per All-in-One appliance
- Multi-partition storage with fast disk support (NVMe, SSD, SAS)
- Online and offline capability to upgrade itself or connected sensors

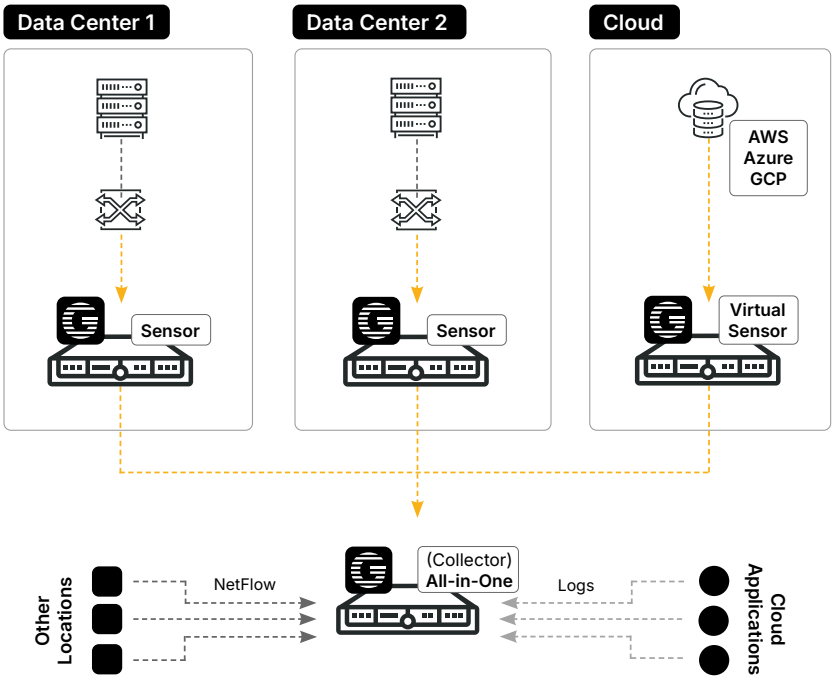
Central Event Management

- Clustering of up to 20 collectors together
- One-site event overview of the whole infrastructure

Deployment



Hybrid Cloud Deployment



Experience GREYCORTEX Mendel

Proof of Concept (PoC)
Try GREYCORTEX Mendel for yourself. We can even offer a monthly network security audit.

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com

www.greycortex.com