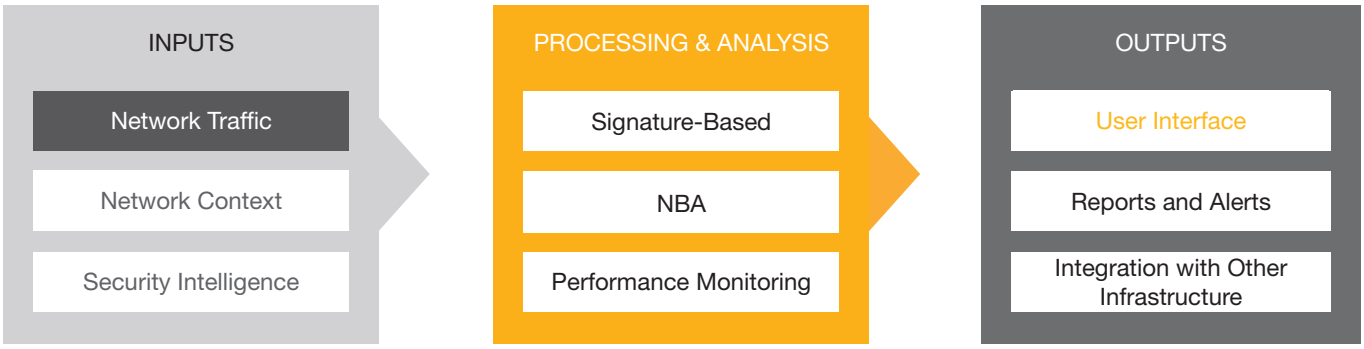
GREYCORTEX MENDEL

PRODUCT DATA SHEET

GREYCORTEX MENDEL is an advanced network traffic analysis, performance monitoring, threat detection, and deep network visibility solution for enterprise, government, and critical infrastructure. MENDEL employs artificial intelligence and machine learning to analyze and monitor network traffic, so new and unknown attacks both from inside and outside an organization are detected; including data leaks, operational anomalies, and other advanced threats invisible to other technologies. MENDEL deploys in minutes and fills the gaps left by traditional security tools, decreasing the time and resources necessary to make network operations secure and reliable.



Detection Methods

MENDEL continuously monitors network traffic and employs a number of advanced methods to detect malicious, anomalous, and outlier behavior:

Prediction Analysis	Based on previously-learned network behavior for all subnets, hosts, and services on each host, GREYCORTEX MENDEL predicts expected communication behavior. Events not in line with learned behavior patterns are reported as anomalous. Examples of anomalies include: data transfer, number of communication partners, number of communicating ports, number of flows, duration of communication, time of communication, etc.
Discovery Analysis	MENDEL maintains an up-to-date list of active services and hosts. If a new host (for example a BYOD) or a service appears in the monitored network segment, a discovery event is reported. The same method is used when services or hosts stop communicating, change their MAC addresses, or when a DNS name changes. This method also reports communication between permitted and denied services based on preset policies.
Flow Analysis	Detection of known and unwanted behavioral patterns in a network, like port scans, brute force attacks, tunneled communication, blind communication, etc.
Repetitive Analysis	This method distinguishes between human behavioral patterns; which are not predictable, and machine-based behavioral patterns which can be predicted. This capability is based on long-term data processing of stored data, which enables MENDEL to detect communication by infected hosts which have been attacked by RATs, C&C malware, APTs, etc. This approach brings the added advantage of the ability to detect malware communication through various protocols including HTTP/S, DNS, or ICMP.
Performance Analysis	Network performance monitoring and application performance monitoring modules analyze data transmission efficiency and SLA breaches for various protocols including HTTP/S, MSSQL, or SIP.
Rule-Based Analysis	Incidents are reported based on user-defined rules like data transfer volume, data transfer time, average response time, communication frequency, thresholds on subnets, hosts, services, allowed or denied communication vectors (firewall audit), etc.
Signature-Based Analysis	Incidents are reported based on detection of common or predictable threats, malware, and attacks in several categories like C&C, P2P, Malware, Trojans, Chat, Web, Anomalies, Scan, Policy, etc.

Traffic Processing and Analysis

Network Behavior Analysis	Flow and packet-based network traffic analysis as well as machine learning, intelligent false positive elimination, and several detection principles (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. – Data exfiltration
Deep Packet Inspection	On-demand and packet capture-based; covering source and destination IP, MAC, subnet, protocol, time, port, IP family (IPv4, IPv6)
Signature-Based Detection	Signature-based intrusion detection engine: – Internal network monitoring – Multithreaded processing – Several signature sources – Detection of known malware, attacks, and other activity – Rule profiling
Performance Monitoring	Flow and packet-based analysis of network and application performance (NPM, APM): – Application awareness – Monitoring current and average bandwidth, response times, transit times, delay, jitter, ports in use, connection peers, etc. – Rule-based detection (e.g. SLA) – Automatic anomaly-based detection
Historical Metadata	GREYCORTEX MENDEL's Advanced Security Network Metrics (ASNM) protocol is a security and performance-focused protocol which provides much richer analysis than NetFlow. Capabilities include: – Bi-directional flow recording and deduplication (no record of network flow represents requests, as well as responses) – Consistent (longer communications are not split into 1 or 5 minute intervals) – Application protocol metadata for HTTP, SSL, TLS, SMB, SMB2, SMTP, FTP, SSH, DNS, XMPP, SIP, ICQ, SSH, MySQL, MS SQL, etc. – Customizable ASNM content recording according to customer needs – Complete ASNM records may consist of 900+ parameters – Data can be stored for several months to several years (depending on storage capacity)

Main Benefits

Effective & Efficient

- More sensitive and reliable
- Lowers demands and costs of operation and integration

Much More Than NetFlow

- More sensitive behavioral detection than NetFlow (and similar protocol)
- NetFlow/IPFIX records are enhanced by security parameters and performance analysis
- Packet-based detection that improves flow-based detection (both for security and performance monitoring)

Robust Detection

- Zero-day & advanced threats (APTs, etc.)
- Remote Access Trojans (RATs)
- Data leakage (misused DNS, SSH, HTTP/S, ICMP, etc.)
- Tunneled traffic (DNS, SSH, HTTP/S, ICMP, etc.)
- Protocol anomalies
- Time consuming port scans
- Dictionary & brute-force attacks
- Preparation for internal data theft and other internal issues like breaches of internal security rules
- Network misconfigurations
- DoS, DDoS
- Automatic data harvesting (e.g. eshop)

Detailed Network Visibility

- Detailed information on subnets, hosts, services, and flows
- Metadata provides sufficient information on network behavior for forensic investigation, regulatory compliance, etc.
- Months of historical data are indexed and quickly accessible

Risk Assessment

- Robust risk assessment capabilities

Reporting

- Widely customizable reports (including granular reporting, alarms, etc.)
- Intuitive web GUI
- Incident management

Outputs

Graphical User Interface	Web user interface (IE, Firefox, Chrome, Opera, Safari, Edge, etc.) – Java-based – Completely granular access – Easy customizable dashboards – Unlimited filtering & sorting
Reporting & Alerting	– Conditional reporting (alarms) – Incident management – Customizable output format – Human readable formats: email (html), pdf, docx, custom links to the GUI
Integration	– SIEM: Based on the CEF (Common Event Format) format or the IDEA reporting protocol – Integration with other infrastructure possible – Customizable output format

Inputs

Network Data	– Mirrored traffic (TAP, SPAN, or other types of mirror data ports) – IP layer support: L2 to L4 layer of TCP/IP, incl. IPv6 protocols – Flow-based protocols (NetFlow family, IPFIX)
Security Intelligence	– Various sources of IDS signatures (e.g. Emerging Threats) – Other databases (IP reputation, domain reputation, GEO IP, WHOIS, etc.)
Network Awareness	– Definition of functional network segments/subnets (that share the same patterns of network behavior e.g. management, sales, servers, WiFi, VoIP, printers, DMZ, etc.) – IP to host name (using DNS records)
User Awareness	– IP to domain user (using domain controller event logs, LDAP)

Product Models	Capabilities						Premium Services	
	Network Visibility	NBA	IDS	APM	Packet Capture	SIEM Connector	External Monitoring	Threat Intelligence
MENDEL Analyst	✓	✓	✓	✓	✓	✓	o	o
MENDEL SaaS	✓	✓	✓	✓	✓	✓	✓	o

✓ standard o optional

Appliances		Network Throughput Gbps							
		0.1	0.5	1	2	4	10	20	40
HW	All-in-One (Sensor + Collector)		✓	✓	✓	✓	✓		
	Collector				✓	✓	✓	✓	✓
	Sensor	✓	✓	✓	✓	✓	✓		
VA	All-in-One (Sensor + Collector)		✓	✓	✓	*	*		
	Collector			✓	✓	✓	✓		
	Sensor	✓	✓	✓	✓	*	*		

* Virtual environment monitoring only

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 389, info@greycortex.com, www.greycortex.com

GREYCORTEX