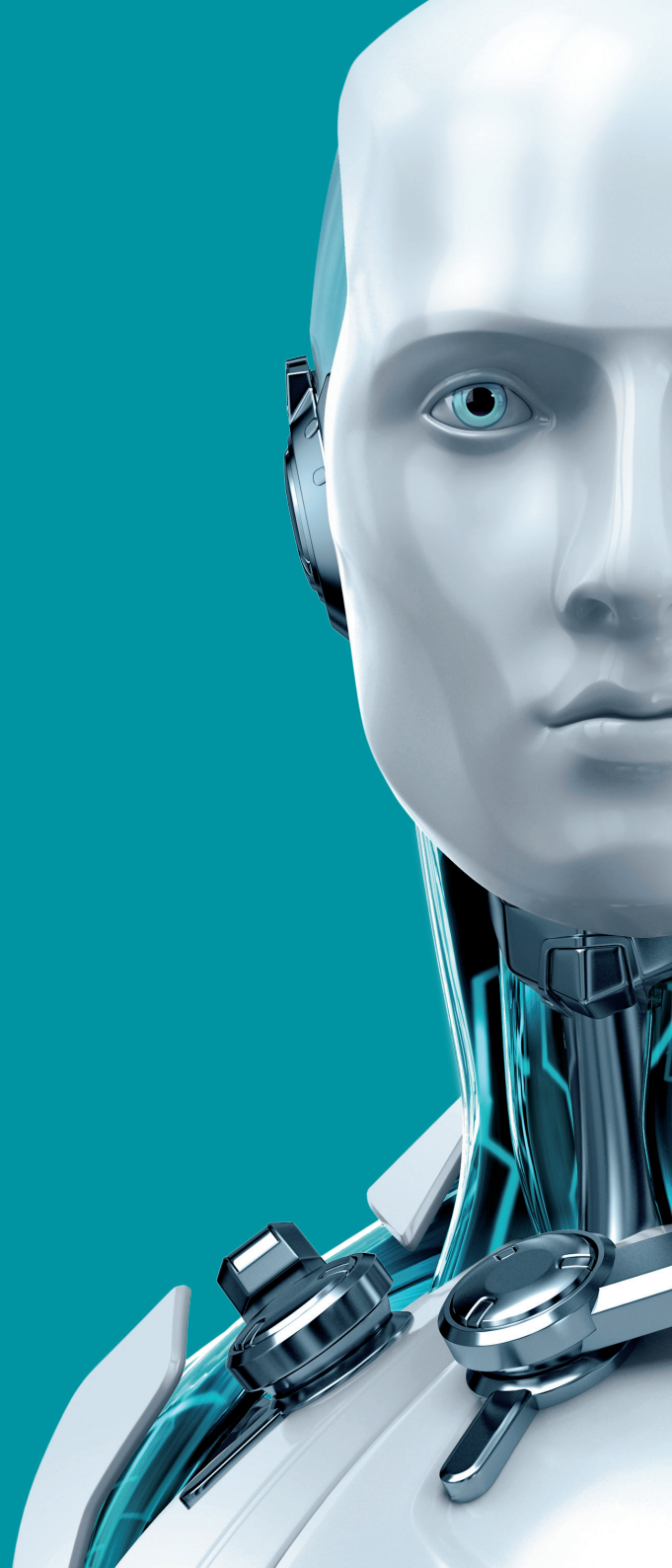
GREYCORTEX MENDEL

# Network Traffic Analysis

## Product Overview

BUSINESS

ESET TECHNOLOGY ALLIANCE



GREYCORTEX MENDEL

**Network Traffic Analysis with GREYCORTEX MENDEL**

GREYCORTEX MENDEL is an advanced network traffic analysis, performance monitoring, threat detection, and deep network visibility solution for enterprise, government, and critical infrastructure. MENDEL uses state-of-the-art artificial intelligence, machine learning, and big data analysis to make organizations' IT infrastructure secure and reliable.

MENDEL is not another network behavior monitoring tool. It uses a combination of threat analysis, machine learning, artificial intelligence, packet inspection, event correlation, and other tools to identify suspicious activity within a network. This allows security teams to find threats with greater certainty and take action more quickly than with traditional network security solutions.

## Identify Threats Before Damage Happens

Many other providers focus on known methods of attack or pieces of malicious code. Using advanced artificial intelligence methods, MENDEL goes beyond known threats to detect and identify symptoms of malicious behavior at the atomic level. Threats are identified in their early stages, decreasing incident response time, preventing further damage, and reducing overall risk.

MENDEL also adds integrated signature-based detection and known threat intelligence; increasing its detection capabilities, while reducing the false-positive rate.

**8 – 16 hours**
Time an adversary needs to break into a network

**8 months**
Average time an APT goes unnoticed on a victim's network

**98 days**
Average time to detect an APT attack

**71%**
Of organizations do not detect a breach themselves

## Automatic Adaptation

MENDEL's unique Network Behavior Analysis engine (NBA) uses advanced mathematical analysis in machine learning to generate and adapt detection rules from past traffic. It integrates inputs from its other detection engines and includes specialized algorithms which, among other functions, distinguish between machine and human behavior. MENDEL's NBA engine is the only solution on the market which offers this ability.

## More Sensitive Detection

MENDEL's Advanced Security Network Metrics protocol allows it to monitor over 70 features of each individual network flow. This advanced level of analysis makes MENDEL more effective at detecting malicious behaviour and other threats than solutions on the market today.

MENDEL's advanced data mining techniques ensure that it can process many more data flow features than solutions based on NetFlow protocols, in real time. Furthermore, MENDEL can scale up to 10Gbps in a single sensor and collector configuration, and up to 40Gbps per collector.

**Mendel Detects Hidden Threats**

- Malware on mobile or embedded devices
- Data leaks with DNS, SSH, HTTP(S), etc.
- Tunneled traffic
- Protocol anomalies
- Masquerade attacks
- Spam detection
- Preparation for data theft and exfiltration
- Automated data harvesting
- Data theft
- Phishing attacks

## Better Performance Monitoring

MENDEL provides detailed insight into application performance both from the user and network point of view. Its agentless design offers the ability to monitor each and every transaction, across multiple types of applications. These transactions are displayed in a broad range of visualizations with full sorting and filtering capabilities, giving teams detailed data to safeguard and optimize business critical processes as well as enabling easy and quick root cause analysis; all in real time. This means organizations see not only improvement in network security, effciency, and visibility, but appreciable ROI as well.

## Ease of Use Without Slowing Your Network

MENDEL isn't just advanced tools, methods, and capabilities. It deploys quickly, saves administrative time, and collects data without slowing network speed. IT managers love MENDEL because:

- Installing and configuring basic settings in MENDEL takes 30 minutes. MENDEL learns the network and the IDS engine begins reporting results immediately. Actionable data is available after seven days, and a complete learning cycle for the NBA engine is finished in 28 days.
- MENDEL makes reporting and understanding identified threats easy, with filtering and sorting, customizable reports, and an intuitive web interface to save time.
- MENDEL monitors and visualizes, rather than interrupts, network traffic while it records information on each data flow. This means users can easily identify each flow in real time and find out who uses certain services, network nodes, and bandwidth. It assess application and network performance, and conducts root-cause analysis, without creating a drag on network response time.

**Network Behavior Analysis Meets Machine Learning**

MENDEL's NBA engine employs advanced mathematical analysis in machine learning, supervised and unsupervised classification methods, clustering, and outlier analysis:

- Models of normal behavior in the network, all subnetworks, hosts, services, and individual data flows
- Bayesian Analysis of transformed features
- Probabilistic mixture models (Gaussian expectation-maximization (EM) algorithm)
- Various ad hoc reasoning techniques

## About GREYCORTEX

GREYCORTEX uses advanced artificial intelligence, machine learning, and data mining methods to help organizations make their IT operations secure and reliable. MENDEL, GREYCORTEX's network traffic analysis solution, helps corporations, governments, and the critical infrastructure sector protect their futures by detecting cyber threats to sensitive data, networks, trade secrets, and reputations, which other network security products miss.

GREYCORTEX has named its software "MENDEL," in honor of Gregor Johan MENDEL, the father of modern genetics, who made his discoveries in the city of Brno, South Moravia, Czech Republic, where GREYCORTEX is based.



ESET TECHNOLOGY ALLIANCE

ESET Technology Alliance aims to better protect businesses with a range of complementary IT security solutions. We provide customers with a better option when staying protected in the ever-changing security environment by combining our proven and trusted technology with other best-of-breed products.

# Technical Information

| | |
|---|---|
| **Architecture** | MENDEL's enterprise architecture consists of sensors and collectors. Sensors are used to detect known threats and deliver network traffic data for the NBA engine at the collector. Collectors are used to transform these metrics into information. MENDEL sensors can support up to 10Gbps, and collectors can handle up to 40Gbps. Large deployments across many locations are designed with a collector that can support 10 or more sensors (both physical and virtual). |
| **Inputs** | Network data streams from mirrored traffic (SPAN or TAP), and IP reputations like known botnets, spam sources, TOR nodes, proxies, and more. |
| **Outputs** | Web GUI and downloadable .pcap files, customizable reports in .pdf and .doc (delivered via email), exports to SIEM in CEF and IDEA. |
| **Implementation** | GREYCORTEX MENDEL can be implemented as a hardware appliance or, with some limitations, as a virtual device. Other possibilities include MENDEL in a SECaaS environment, security operations center models, or as a one-off security audit of a client's network. |
| **Deployment** | **Single Deployment:** MENDEL can be deployed as a single network sensor and collector in a single appliance.<br>**Distributed Deployment:** MENDEL can be deployed with several collectors and sensors sharing knowledge about network traffic and threats (for monitoring geographically distant locations and/or processing high traffic volumes). |