

# GREYCORTEX MENDEL

## All-Seeing Network Security

**MENDEL** uses advanced artificial intelligence, machine learning, and data analysis to find threats, identify vulnerabilities, and give your IT team full network visibility, all while saving time.

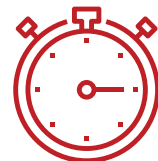
### Advanced Attacks Are Common and Hard to Find



**8 Attacks**  
enter enterprise  
networks per year



**40%**  
of cyber threats are  
undetected



**49 Days**  
to detect breaches with  
current tools alone

### Existing Security Tools Are Vulnerable

#### Unknown Threats

Advanced unknown threats like malware, RATs, and ransomware; if not detected in time they lead to:

- Loss of sensitive data
- Attacks on organizations
- Business damage
- Loss of reputation



#### Lack of Visibility

Lack of network visibility makes it hard to identify suspect devices and bad actors, as well as:

- Critical delays
- Mystery devices
- Lost time
- Wasted money



#### Employee Negligence

Employees and contractors violate policies intentionally or unintentionally. This creates:

- Leakage of sensitive data
- Attacks on other organizations
- Compliance issues
- GDPR violations



# Business Risk Is **REAL**

## Network Traffic Analysis Prevents Breaches

Network Traffic Analysis (NTA) combines **artificial intelligence**, **machine learning**, and other tools to detect suspicious or anomalous network events. **MENDEL uses NTA** to monitor the network perimeter, and also traffic within the network for complete coverage.

**MENDEL detects threats** across the entire network, including BYOD/IoT devices, and even advanced unknown attacks **that other solutions miss**.

**65%**  
Customers  
Lose Trust



### Powerful Detection at Exceptional Speed

Advanced unknown threats, including malware, ransomware, RATs, and Zero-day attacks detected in 1 min - 6 hours, not 49 days

**23%**  
Business  
Opportunity Loss



### Detailed Network Visibility

- Even on SCADA networks
- Every subnet
- Every host
- Every service
- Every device
- Every application
- Even BYOD/IoT

**5%**  
Drop in  
Stock Price



### Effective Response

- Block communication at the firewall from within MENDEL
- Manage incidents between analysts
- Conduct root cause analysis and forensics
- Easier incident management

# MENDEL Includes



## Machine Learning Drives Detection

MENDEL's advanced artificial intelligence and machine learning detects threats more effectively than other solutions:

- Differentiate between human and machine communication
- Detect anomalous behavior
- Find hidden threats

## Stop Attacks in Their Tracks

MENDEL goes the extra mile to cut off attacks when detected.

- Integrates with your existing firewall
- Simple interface allows general or specific blocking
- When minutes matter, configuration and blocking happen in seconds



## Full Visibility, including BYOD/IOT

MENDEL identifies traffic into and out of the network, as well as communications between devices within the network:

- Works equally well on BYOD/IOT
- Visualizes individual devices and applications, not just layers
- Quickly filter every communication

## Context Visibility for Faster Resolution

Detecting an attack effectively is only part of the network security puzzle. MENDEL adds additional context data for faster event resolution.

- Integrated GEOIP and Blacklists
- Decrypt SSL/TLS traffic with imported private key
- Integrate MENDEL with Active Directory to identify users in your network



## Correlate Threat Detection Accurately

Attacks can take many steps that seem safe on their own. MENDEL brings these events together to show the true nature of attacks.

- Threats can't hide in heavy data volumes
- Identify events in multiple offices from one central location
- Resolve issues in under two minutes

## Effective Alone, or as an Added Data Source

Different security infrastructures demand different configurations. MENDEL compliments your existing tools to fill gaps.

- SIEM-like results at half the cost, and a tenth of the time for small and medium enterprises
- Export data to SIEM systems for larger security teams
- Incident management permits more advanced resolution

# MENDEL Secures



SMB & Enterprise



Government



SCADA/ICS



Infrastructure

## MENDEL Deploys

Locally (virtual or physical)

Security as a Service

Security Operations Center

Network Audit



## MENDEL Implements

30 Minutes to Install

Automatically learns your network

Assisted machine learning  
~5 minutes/day



## Experience MENDEL

**FREE 30-day** Proof of Concept (POC)

Identify serious issues in your network – from attacks to performance problems.

### Problems Exist Even in “Clean” Networks:

20% of network devices pose threat to greater network from virus/malware/RATs

Zero-Day attacks

Mobile malware

Vulnerable IoT devices

Ineffective network matrix

Unpatched applications

Performance anomalies/issues

Unauthorized data access

Preparations for data exfiltration

Compliance problems (future GDPR issues)