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 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 polices 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 host
- Every device
- Every subnet
- Every service
- 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 Treat Detection Accurately

Attacks can take many steps that seem safe on their own. MENDEI 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

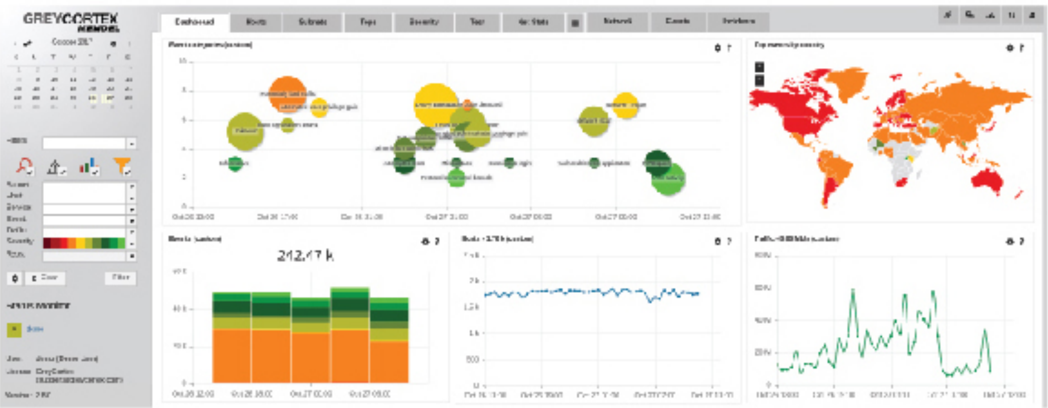
Network Audit

MENDEL Implements

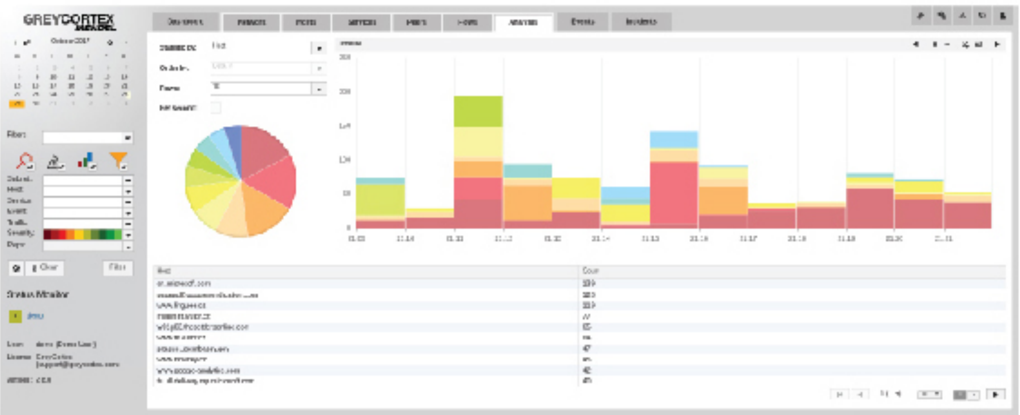
30 Minutes to Install

Automatically learns your network

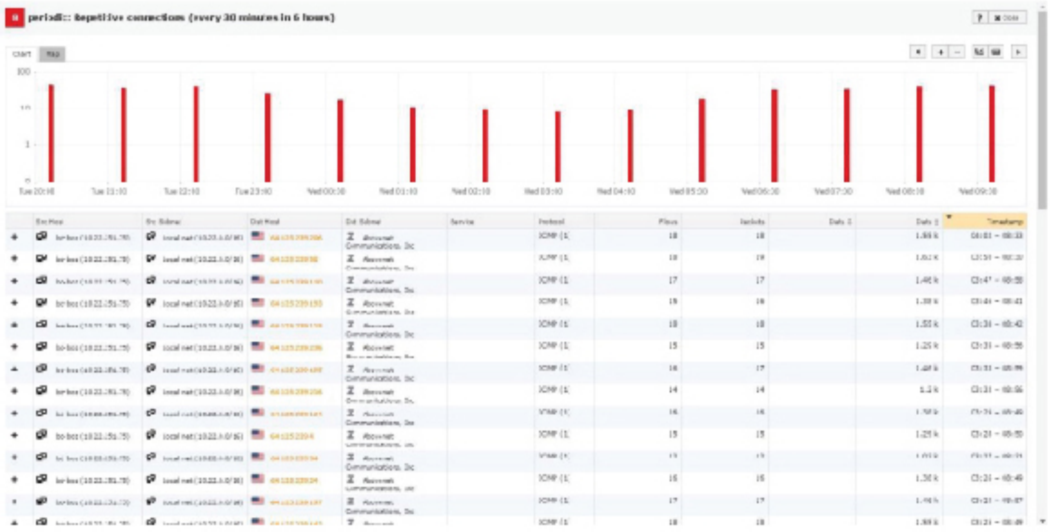
Assisted machine learning
~5 minutes/day



GREYCORTEX MENDEL is a network traffic analysis tool designed for the operational and security monitoring of computer network traffic. The solution consists of several detection modules that jointly supervise operational and security events in the monitored network. It includes several methods

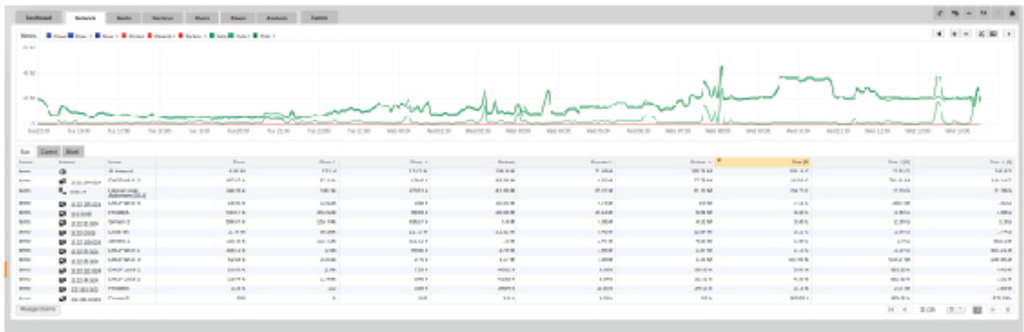


Analysis – Provides statistical visualization of selected parameters according to the user selection. Visualized data is based on non-computed views. Generating views can be computationally advanced, and thus time consuming.



periodic: Repetitive connections (every 30 minutes in 6 hours)

The full details of each event are displayed in the "Lightbox" component. At the top is a chart that has the same properties as the chart in the Events tab, and can be used as a time filter.



Use the Network Tab to track individual data streams. The tab shows basic overviews of the entire network, subnets, access to individual services, and sub-network streams. The data is always visualized in the graph and table. Visible parameters can be changed for each view in the Manage Columns Manager.

Version 2 二版
www.version-2.com
Sales Hotline : (852) 2893 8860
Technical Support : (852) 2893 8186

GREYCORTEX