RELEASE 5.0 | AUGUST 2026

GREYCORTEX Mendel 5.0

MAIN FEATURES

01 Traffic Flow Map

Using **host-centric visualization**, the traffic flow map enables fast **investigation of network communication** around a single internal host, helping analysts quickly understand which peers a host communicates with, in what direction, and at what scale.

The map starts from one internal host and **displays its most significant peers** within the selected time window. By default, peer selection and graph emphasis are based on flow count, but analysts can switch the metric to packets, data volume, retransmissions, and unreplied flows depending on the investigation context. **Analysts can expand the view** from any selected node and explore communication paths step by step.

Host and communication details are visible directly in the map. By hovering over a node, users can see IP-related details, while hovering over an edge shows communication details between the connected hosts. Clicking an edge opens an additional detailed communication window for closer inspection.

KEY CAPABILITIES

- A host-centric communication overview
- Automatic or user-defined entry host
- Incremental expansion from selected nodes
- Communication prioritized and highlighted by a selected metric
- Supported metrics: flows, packets, data, retransmissions, unreplied flows percentage, and absolute unreplied flows
- Default view based on flow count
- Directional edges and incomplete-flow distinction
- Node hover for IP details
- Edge hover for communication details
- Edge click-to-open detailed communication information
- Zoom, pan, and filter support

02 AI Assistant

By providing AI-assisted explanations for internal IP addresses, external IP addresses, and security events, the assistant helps analysts **interpret device roles, IP reputation**, and event context in structured, plain language. For security events, the assistant works at two levels: **Explain event** provides context for the event itself, while **Investigate this event** analyzes a specific communication in the context of a specific host and returns a structured assessment. Both actions are available for Network Behavior Analysis, IDS, Log Processing, and UnTE detections; they are not available for System Monitoring events.

Internal IP analysis identifies the likely device role using available host context, such as Layer 7 metadata, hostnames, tags, MAC addresses, and observed services. External IP analysis assesses reputation and classifies addresses as malicious, suspicious, reconnaissance-related, benign, likely benign, or unknown. Event explanations summarize what happened, why it matters, relevant MITRE ATT&CK context, as well as recommended operational follow-up actions, and include guidance on how to verify whether the alert is a false positive.

Investigate this event performs a deeper, host-specific analysis of a single communication. In addition to the explanation, it provides an assessment: a verdict, detection relevance and confidence, and an estimated false positive probability, each with the reasoning behind it. It separates observed facts from possible interpretations, states what the available data does not prove, lists recommended investigation steps in priority order, and — where appropriate — suggests a scoped exception limited to the specific signature, source, destination, and traffic direction.

Users can configure the AI output language independently from the UI language and the assistant supports English, Czech, German, and Polish. The feature can be globally enabled or disabled. It includes a first-use notice for external AI processing, and provides thumbs up/down feedback for quality tracking. These settings apply to the AI Assistant as a whole, regardless of which function generates the output.

KEY CAPABILITIES

- Internal IP device role identification
- External IP reputation assessment
- Security event explanation and recommended follow-up
- Two levels of event analysis: Explain event for context, Investigate this event for a host-specific assessment
- Available for Network Behavior Analysis, IDS, Log Processing, and UnTE detections; not available for System Monitoring events
- Guidance on verifying whether an alert is a false positive
- Event verdict with detection relevance, detection confidence, and environmental realism
- Estimated false positive probability with reasoning
- Clear separation of observed facts from possible interpretations
- Recommended investigation steps in priority order
- Scoped false positive exception suggestion limited to signature, source, destination, and traffic direction
- Operational recommendation for follow-up configuration or containment
- Use of host context, Layer 7 metadata, tags, MAC addresses, and service information
- Reputation categories for external IPs: malicious, suspicious, reconnaissance, benign, likely benign, and unknown
- Plain-language explanations of what happened and why it matters
- MITRE ATT&CK context explanations where applicable
- Highlighting of key technical indicators
- Multilingual AI output: English, Czech, German, and Polish
- AI language setting independent from UI language
- Global AI Assistant enable/disable setting
- First-use notice for external AI processing
- AI-generated output disclosure
- Thumbs up/down usefulness feedback

03 New Risk Score and Visualization

The **redesigned host-based risk scoring** model helps analysts identify the riskiest hosts faster. The new score replaces the previous calculation with a unified, normalized model based on host-related security events, with consistent risk visualization across the UI.

Risk is **calculated from host-related events**, subnet-relative uniqueness, and the recency of severe activity. Older signals reduce over time through historical fading, while recent and relevant problematic behavior increases risk. The score is stored over time, allowing analysts to **review trends and understand how host risks develop**.

Risk Score is separate from event severity and uses a dedicated visual indicator with a numeric score and risk tiers. Risk information appears in dashboards, Hosts by Risk, Host Dialog, and the Host page, including trends, related events, and related context.

KEY CAPABILITIES

- New normalized host-based Risk Score
- Event-based risk calculation
- Consideration of subnet-relative uniqueness and recent severe activity
- Historical fading of older risk signals
- Dedicated visual indicator distinct from event severity
- Risk tiers from No Risk to Critical Risk
- Risk history and trend visualization

RISK SCORE RANGE

Score	Tier
1–19	No Risk
20–49	Low Risk
50–69	Medium Risk
70–89	High Risk
90–99	Critical Risk

- Hosts by Risk table and dashboards such as Main, Overview, Risks, etc.
- Risk details in Host Dialog and Host page
- Filtering by score range or risk tier

04 Host Dialog Redesign

The **Host Dialog has been redesigned** to provide users a clearer, more investigation-oriented view of internal and external hosts. The Summary page now presents host identity, subnet, sensor, hostname, MAC address, discovery time, risk, tags, and related context in a cleaner structure.

For internal hosts, the dialog includes the new Risk Score presentation and improved tag representation, including time-based context. For external hosts, the layout focuses on IP identity, hostname, reputation, network ownership, and relevant investigation actions.

Common actions have also been reorganized. Analysts can use improved Filter host options for IP, subnet, and hostname with set, OR, and NOT logic. The sensor selector now supports search and displays observed traffic volume, helping analysts understand which sensor detected the host and how much traffic it observed.

KEY CAPABILITIES

- Redesigned Host Dialog for internal and external hosts
- Reorganized Summary page with clearer host context
- New Risk Score presentation for internal hosts
- Improved tag representation with time-based context
- Searchable sensor selector with traffic volume information
- Reorganized action buttons
- Improved Filter host options for IP, subnet, and hostname
- Support for set, OR, and NOT filter logic
- Updated visual design

05 Tag History and Time Reference

Tag handling has been redesigned to support historical tracking of tag assignments. Tags are no longer only treated as a current host attribute — Mendel now stores when tags were applied, updated, or removed, including their source where available.

Analysts can review tag history for hosts and identities, filter using tags valid within a selected time interval, and distinguish tag sources such as user actions, detection logic, UnTE rules, network capture module rule matches, or external imports.

Backend tag handling has also been unified and refactored to improve reliability, API usage, and long-term maintainability.

KEY CAPABILITIES

- Historical tag assignment tracking
- Apply, update, and removal time for tags
- Tag source visibility
- Tag history for hosts and identities
- Time-based tag filtering
- Unified tag persistence model
- Improved API and backend handling
- Better support for auditing, troubleshooting, and reporting

06 Inactive and Lost Host Detection

Inactive Host Detection introduces a new intermediate host lifecycle state that reports when a host stops communicating, giving analysts time to investigate before it is permanently removed.

When a host remains inactive for the configured inactivity period, the system generates an **Inactive Host** event while preserving all host information. If the host does not reappear before the configured Lost Host lease expires, the existing **Lost Host** policy generates a Lost Host event and permanently removes the host and its associated information.

Temporary communication loss is now separate from permanent host removal, providing earlier visibility into disappearing hosts while preserving automatic host lifecycle cleanup.

KEY CAPABILITIES

- New Inactive Host Detection
- Configurable inactivity detection period
- Early notification when a host becomes inactive
- Existing Lost Host policy for permanent host removal
- Configurable Lost Host lease time
- Automatic cleanup after extended inactivity
- Clear separation of inactive and lost host states
- Allowed/Not allowed Lost Host policy behavior
- Improved UI explanation of host lifecycle

IMPORTANT TECHNICAL CHANGES

Platform Upgrades and Modernization

Mendel now runs on an upgraded operating system platform with a newer kernel and refreshed core components, improving overall security, stability, and long-term maintainability.

- Upgraded operating system platform
- Newer Linux kernel based on CentOS Stream 9
- Security updates and vulnerability fixes
- Improved system stability and reliability
- Modern platform foundation for future enhancements

IDS Engine Upgrade

The IDS engine has been upgraded to the latest generation, improving detection performance, expanding protocol coverage, and providing a modern foundation for future enhancements.

- Upgraded IDS engine
- Improved detection performance
- Expanded protocol support: LDAP, mDNS, SIP/SDP, ENIP, FTP
- Enhanced rule engine capabilities (VLAN support)
- Improved maintainability and long-term platform support

Status Monitor Improvements

The Status Monitor subsystem has been significantly improved to provide more reliable service monitoring and more consistent reporting of system status.

- More reliable service status monitoring
- More consistent outage detection and reporting
- Improved system stability
- Easier diagnostics and troubleshooting
- Reduced technical debt
- Modern foundation for future platform improvements

Improved Administrative Access

Administrative privileges are now managed through the Admin role, reducing reliance on the default administrator account and improving overall security.

- Admin role for administrative tasks
- Reduced dependency on the default administrator account
- Mandatory password change after deployment
- Improved security during customer handover
- Better role-based access management

AI Service Detection

Mendel now detects and classifies AI services in network traffic, providing greater visibility into the use of AI applications across monitored environments.

- Detection of AI-related network traffic
- Classification of AI services in network flows
- Improved visibility into AI application usage
- Support for organizational security policies
- Extensible framework for emerging AI services

Improved OS Detection

Operating system fingerprinting has been refined to improve device identification accuracy and host classification reliability.

- More accurate Windows version detection
- Improved Android device identification
- Reduced false positives
- More reliable host classification
- Enhanced operating system fingerprinting

Entra ID Identity Correlation

Mendel now correlates Microsoft Entra ID login and logout events with monitored hosts, providing additional identity context for security investigations.

- Automatic correlation of Entra ID logins and logouts
- User-to-device association
- Improved investigation context
- Better identity visibility across the network
- Enhanced audit capabilities

NetFlow Interface Visibility

NetFlow records can now include the logical input and output interface names reported by network devices, providing additional context for traffic analysis.

- Logical input and output interface names stored with flows
- Interface metadata available during analysis
- Improved traffic visibility
- Production validated with KB devices
- Enhanced NetFlow investigations

S3-Compatible Backup Storage

Backup storage now supports **S3-compatible object storage**, providing greater flexibility beyond Amazon S3 deployments.

- Support for S3-compatible object storage
- Compatibility with standard S3 API implementations
- Greater deployment flexibility
- Support for on-premises object storage
- Simplified backup configuration

ADDITIONAL IMPROVEMENTS

Miscellaneous enhancements to everyday operation, platform usability, and overall user experience.

- New UnTE Layer 7 tags
- Plugin compatibility information
- Updated profile naming
- User interface and usability improvements
- Various stability and performance enhancements

OFFICIAL GREYCORTEX MENDEL PRODUCT SUPPORT

With the release of version 5.0.0, **full-service support is provided for versions 5.0.x and 4.6.x**, plus **basic support for version 4.5.x.**

Versions 4.4.x and older are no longer supported.

End-users with valid support and maintenance or an active software subscription are highly advised to upgrade to a supported version.