Menlo Security

MENLO SECURITY INSIGHTS FOR NEXT-GEN SECURE WEB GATEWAY

VALUABLE INSIGHTS AND CONTEXT INTO WEB BROWSING BEHAVIOR

Protecting the enterprise from today's cybersecurity threats requires deep insights and context into existing threats and vulnerabilities as well as user web and email behavior. Security analysts and threat detection and response teams need to know exactly what users were doing at the moment an attack occurs. However, visibility into user behavior is tough to come by if it exists at all.

The answer? Gain better visibility into users' web and email behavior with Menlo Insights to better inform threat and vulnerability detection and post-event analysis.

Cybersecurity Threats Growing in Sophistication & Volume

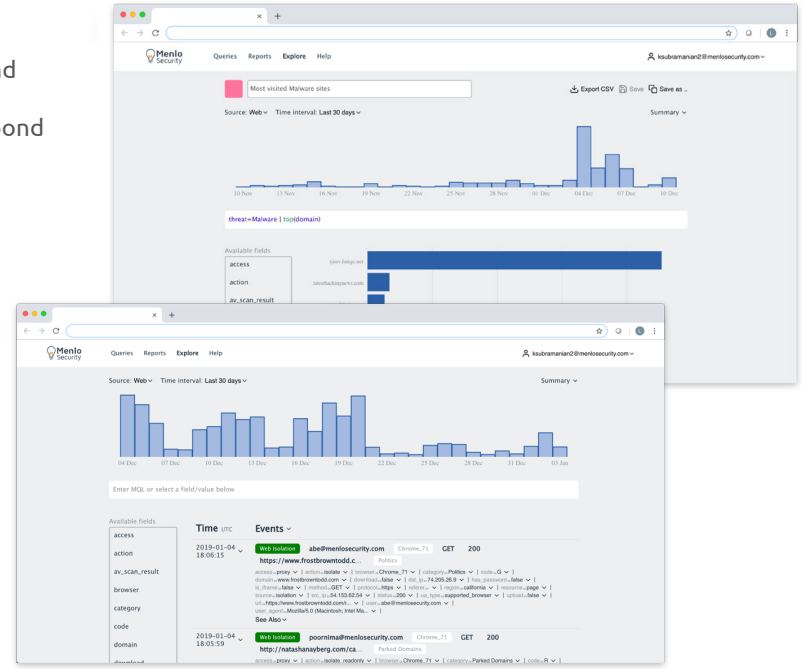
Today's enterprise security teams are understaffed and under-resourced to adequately take on today's increasingly sophisticated threats. Security teams often lack the context they need to identify and quickly remediate a breach--allowing even minor attacks to do major damage.

Unfortunately, logs and traditional Security Information and Event Management (SIEM) solutions don't provide proper context into what the user was doing just prior to an event, making it difficult to diagnose the threat. Clearly, a new approach is needed.

Menlo Security Insights

Menlo Security platform offers dedicated monitoring and forensic capabilities into users web browsing and email activity, allowing security teams to quickly identify, respond and mitigate risks.

Rather than rely on traditional general-purpose log management platforms or SIEM solutions, security and forensics teams are able to use the Menlo Security data management and reporting platform to deliver deep insights into both user activity and protection delivered to customers. A part of the Menlo Security Isolation Platform (MSIP), Menlo Insights was designed to interpret logs from the MISP and provide ready-to-use actionable data and reports.



KEY USE CASES

What You Can Accomplish with Menlo Security Insights

1. Monitor and report on the effectiveness of the NG-SWG in terms of threats mitigated and web activity
2. Identify risky users and websites and take appropriate remediation actions:
   - a. Limit or block access to sites through policies
   - b. Render websites and log-in sites in read-only mode
3. Export event logs to a SIEM for broader correlation with events collected from other enterprise security tools
4. Maintain compliance by ensuring data is retained for regulated periods of time
5. Export data to business intelligence and visualization tools for long-term historical and trend analysis
6. Identify outdated and vulnerable browsers, risky endpoint environments, unpatched laptops and unauthorized content

Menlo Security Insights Key Features and Benefits

Rich, Detailed, Easy to Read Reports

Detailed and granular logs of user web transaction and email activity

- Clearly understand the risks to your organization, so you can take steps to mitigate vulnerabilities

Explore and filter data

- Visual charts
- Export in CSV format
- Easy to read, analyze and share raw data
- Integration with existing solutions

Flexible queries

- Includes 60+ pre-defined commonly-used queries
- Rich query language enables custom queries using MQL
- Custom queries
- Gain the insights you need to keep your organization safe

Event logs

- Query event logs
- Display threats detected by existing AV tools
  - VirusTotal, SophosAV, Sophos Sandbox, Reversing Labs
- Display threats found in URLs that contain risky, badly-formed or phishing references
- Better understand user behavior and how it contributes to risk

Rich Reporting

- Schedule daily, weekly or monthly
- Automatically email to recipients
- Includes pre-defined commonly-used reports including:
  - Security Reports
  - Productivity Reports
  - Isolation Reports
  - User & Group Reports
- Create custom reports by selecting multiple queries
- Keep stakeholders informed on a regular basis

Flexible data retention periods

- 30, 60, 90 or 180 days
- Keep up to date on dynamic compliance requirements

About Menlo Security

Menlo Security protects organizations from cyberattacks by eliminating the threat of malware from the web, documents and email.

Menlo Security's cloud-based and on-premise Isolation platform scales to provide comprehensive web, email and document protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience.

Menlo Security is trusted by major global businesses, governments and verticals, including Fortune 500 companies and financial services institutions, and backed by leading venture capital firms and banks.

Menlo Security is headquartered in Palo Alto, California.

To learn more, visit **menlosecurity.com** or contact **sales@menlosecurity.com**