McAfee
Together is power.

# McAfee Enterprise Log Search

## Hunt faster by searching billions of events at high speeds

Security teams need tools to move with greater speed in environments that increasingly generate too many alerts. Analysts on these teams need access to richer context and have the ability to quickly pinpoint relevant event details concerning an incident. McAfee® Enterprise Log Search accelerates threat hunting with ultra-fast search of raw, uncompressed event data. An Elasticsearch™-powered backend optimizes query performance, delivering immediate access to raw logs. Enhanced search functionality enables queries with both natural language inputs of simple keywords and more sophisticated regular expression patterns for targeted retrieval of data.

### Optimized Log Management

McAfee Enterprise Log Search is built on Elasticsearch, a technology that utilizes an inverted index to store data. The inverted index catalogues data in a structure that facilitates efficient retrieval of search terms. Since Elasticsearch is designed for high-performance ingestion and indexing, McAfee Enterprise Log Search makes raw data available for search at high speeds after it is captured and catalogued.

McAfee Enterprise Log Search is a component of the McAfee® Enterprise Security Manager, a security information and event management (SIEM) solution. Another complementary component is the McAfee® Enterprise Log Manager, which is designed to be the storage of record by hashing (MD5) inbound raw logs for forensic integrity and compressing those raw logs for storage efficiency. When combined, these two components provide purpose-built storage solutions that can be used simultaneously to maximize fast search (via McAfee Enterprise Log Search) and log retention for compliance (via McAfee Enterprise Log Manager), freeing customers from having to compromise on choosing one capability over the other.

With McAfee Enterprise Log Search, retention policies can be customized to store uncompressed data for different durations in years (365 days), quarters (90 days), or months (30 days). Users can identify which data sources to associate with McAfee Enterprise Log Search and add up to six individual retention policies.

### Key Advantages

- Optimized log management for both log retention and fast search
- Elasticsearch-powered backend supports high-speed ingestion, indexing, and query performance
- Natural language search
- Pivot from parsed data views to raw logs quickly and easily
- Fully integrated with McAfee Enterprise Security Manager
- Flexible deployment options include physical and virtual appliances (mix-and-match ready)

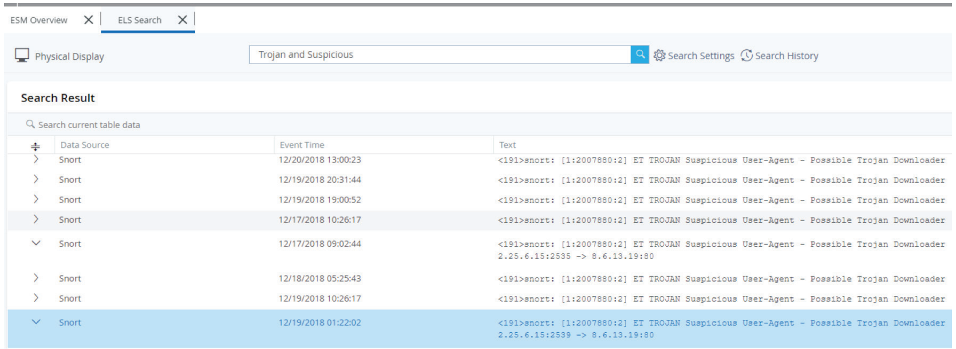
Connect With Us

## Enhanced Search Functionality

The search function within McAfee Enterprise Log Search is like that of popular search engines, allowing for natural language inputs. Search results can be retrieved from simple text or keywords. In addition, searches can be performed with more sophisticated patterns that include Boolean logic, wildcards, and regular expression (RegEx). To further narrow search results, users can apply filters by data source and date. The date filter allows users to select from time periods of when the log events were generated, such as in the last hour, current day, previous year, or custom-defined ranges.

## Integrated with McAfee Enterprise Security Manager

Tight Integration with McAfee Enterprise Security Manager allows analysts to move from parsed data to raw data with a single click. When an event is generated within McAfee Enterprise Security Manager, the parsed event files are linked directly to the source log file and specific raw log record. Analysts who want additional visibility to that record or portions of it can simply select the log in question to prompt a raw log search. There's no extra step, application, or interface to launch in order to dig deeper with raw log search.



Trojan and Suspicious

| Data Source | Event Time | Text |
|---|---|---|
| Snort | 12/20/2018 13:00:23 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader |
| Snort | 12/19/2018 20:31:44 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader |
| Snort | 12/19/2018 19:00:52 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader |
| Snort | 12/17/2018 10:26:17 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader |
| Snort | 12/17/2018 09:02:44 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader 2.25.6.15:2535 -> 8.6.13.19:80 |
| Snort | 12/18/2018 05:25:43 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader |
| Snort | 12/19/2018 10:26:17 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader |
| Snort | 12/19/2018 01:22:02 | <191>snort: [1:2007880:2] ET TROJAN Suspicious User-Agent - Possible Trojan Downloader 2.25.6.15:2539 -> 8.6.13.19:80 |

Figure 1. Search keywords using Boolean logic to uncover events that contain a Trojan and are suspicious.

## Flexible Deployment and Pricing

Flexible delivery options include physical and virtual appliances. Appliances are rated and sold by their ability to ingest a certain event-per-second (EPS) capacity rather than a price per data source, price per EPS, or price by data volume indexed. Virtual machines (VMs) are licensed with the same philosophy and sold by the number of CPU cores needed to support a given EPS. This allows customers to add additional cores as needed without replacing hardware.

## Collect and Rapidly Search the Data You Need

When deploying McAfee Enterprise Log Search, there are six types of logs that are commonly used for threat hunting. These logs can provide specific insights and context to security incidents.

| Log Type | Data Commonly Available |
|---|---|
| DNS Logs | ▪ Queried domain name<br>▪ Source IP address of the DNS query<br>▪ Success or failure of DNS queries<br>▪ Resolved IP address if the query was successful<br>▪ TTL value of response<br>▪ DNS server used |
| Proxy Logs | ▪ Domain/IP address being connected to<br>▪ Bytes transferred<br>▪ Timestamp of the connection<br>▪ URI being used<br>▪ Referrer<br>▪ User-agent string |

| Log Type | Data Commonly Available |
|---|---|
| SMTP Logs | ▪ Email sender domain<br>▪ Email subject<br>▪ Sender IP address |
| Window Logs | ▪ Windows security log events<br>▪ Windows application log events<br>▪ Windows system log events<br>▪ Windows Code Integrity log events |
| DHCP Logs | ▪ Source MAC address<br>▪ IP address granted<br>▪ Lease period<br>▪ Timestamp of request and lease grant |
| VPN Logs | ▪ Source IP address<br>▪ Authenticating identity<br>▪ Timestamp of VPN connection establishment<br>▪ Type of connection: resumption or new<br>▪ Failed authentication attempts—if any—and corresponding identities |

## Learn More

For more information, visit **mcafee.com/siem**

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com