McAfee Advanced Correlation Engine

Detect threats based on what you value

Today's subtle threats defy standard rules-based threat detection. Deploy the McAfee® Advanced Correlation Engine solution with McAfee Enterprise Security Manager to identify and score threat events in real time using both rule- and risk-based logic. You tell the McAfee Advanced Correlation Engine solution what you value—users or groups, applications, specific servers, or subnets—and it will alert you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.

Key Advantages

- Simplifies startup: no rule updates, signature tuning, or other headaches
- Alerts if threats target your priority users, assets, applications, and activities
- Scores accurately through simultaneous rule-based and rule-less correlation
- Lets you check new attacks and vulnerabilities against your history to detect past events
- Adds specialized correlation and processing resources to McAfee Enterprise Security Manager
- Available in both appliance and virtual deployments

The McAfee Advanced Correlation Engine solution supplements McAfee Enterprise Security Manager event correlation with two dedicated correlation engines and purpose-built performance:

- A risk detection engine that generates a risk score using rule-less risk score correlation
- A threat detection engine that detects threats using traditional rule-based event correlation

The stand-alone McAfee Advanced Correlation Engine solution provides the processing power required to support this rich event correlation across your entire enterprise. Its data engine scales to accommodate even the largest networks.

Real-Time and Historical Threat Detection

The McAfee Advanced Correlation Engine solution can be deployed in either real time or historical modes. In real-time mode, the McAfee Advanced Correlation Engine solution analyzes events as they are collected for immediate threat and risk detection.

- Rule-based correlation of real-time event data for detection of threats as they occur
- Rule-less correlation of real-time event data for detection of threats as they develop

In historical mode, any data collected can be "replayed" through both correlation engines, for recursive threat and risk detection. When zero-day attacks are discovered, the McAfee Advanced Correlation Engine solution can look back to determine whether or not your organization was exposed to that attack in the past, for sub zero-day threat detection.

Dedicate Performance Where It Is Needed

Because the McAfee Advanced Correlation Engine solution is a self-contained appliance or virtual offering, there's absolutely no performance impact on McAfee Enterprise Security Manager in terms of event collection and event management. You can fully employ all the capabilities of the McAfee Advanced Correlation Engine applications without compromise, while maximizing your McAfee Enterprise Security Manager utility.

Rule-Based Event Correlation

Rule-based correlation uses traditional correlation logic to analyze collected information in real time. All logs, events, and network flows are correlated together—along with contextual information such as identity, roles, vulnerabilities, and more—to detect patterns indicative of a larger threat. While network-wide, rule-based correlation is already supported directly on all McAfee Enterprise Security Manager solutions, the McAfee Advanced Correlation Engine solution provides a dedicated processing resource to correlate even larger volumes of data, either supplementing existing correlation efforts or offloading them completely.

Risk Score Correlation Without Rules

While rule-based correlation is a necessary and valuable feature of any traditional security information and event management (SIEM), these systems can only detect known threat patterns, requiring constant signature tuning and updates to be effective. The answer is to supplement traditional event correlation with "rule-less" correlation technology. In rule-less correlation systems, detection signatures are replaced with a simple, one-time configuration: simply tell the McAfee Advanced

Correlation Engine solution what is important to your business. It could be a particular service or application, a group of users, or specific types of data.

Real-Time Tracking and Alerting

The McAfee Advanced Correlation Engine solution then starts to track all activity related to those items, building a dynamic risk score that rises or falls based on real-time activity. When a risk score exceeds a certain threshold, an event is generated within the McAfee Advanced Correlation Engine solution. This event can be used to alert a security analyst to growing threat conditions, or it can be used by the traditional rule-based correlation engine as a condition of a larger incident. The McAfee Advanced Correlation Engine solution keeps a complete audit trail of risk scores to allow full analysis and investigations of threat conditions over time.

Use Cases

Modeling enterprise risk

The McAfee Advanced Correlation Engine solution offers a platform to effectively model your enterprise risk. Access to highly classified documents by employees with high-level clearance may constitute risk to a defense organization while leak of celebrity patient records diagnosed with a critical illness may constitute risk to a hospital. The McAfee Advanced Correlation Engine solution provides impeccable modeling of your organizations risks by scoring attributes that matter—developing a baseline and sending notifications when normal thresholds are exceeded.

Proactive risk assessments against critical data

As the McAfee Advanced Correlation Engine solution monitors real-time data, both correlation engines can be used simultaneously to detect risks and threats before they occur. Risk scores can be used within traditional correlation logic. For example, a traditional rule-based threat detection signature might be "a malware event occurring after a brute-force login event." Normally, when this signature triggers, an event has already taken place. Instead, with the McAfee Advanced Correlation Engine solution, you can now incorporate a risk factor such as a 20 percent increase in risk score following a brute-force login event. When this event is noted, the McAfee Advanced Correlation Engine solution can provide a proactive alert of an impending incident, allowing intervention before the damage is done.

Recursive threat assessment

It is not uncommon to identify a threat or to uncover a breach, only to wonder whether it has been there all along. By deploying the McAfee Advanced Correlation Engine solution in historical mode, any historical data set within it can be replayed through the traditional and rule-less correlation engines.

By determining when a newly discovered threat first materialized, it is much more likely that the root cause of that condition can be identified.

Operational Modes

Real-time correlation mode

- Rule-based correlation of real-time event data for detection of threats as they occur
- Rule-less correlation of real-time event data for detection of threats as they develop

Historical correlation mode

- Rule-based correlation of historical event data for recursive threat detection
- Rule-less correlation of historical event data for recursive threat assessment

Correlation Capability

- Simultaneous rule-based and rule-less correlation
- Correlate data from any supported data source
- Correlate data across distributed networks and collectors
- Includes hundreds of predefined event correlation rules
- Includes configuration editor for rule-less correlation
- Includes easy to use GUI event correlation rule editor for customizing rules or creating new rules

For more information, visit mcafee.com/advancedcorrelationengine.

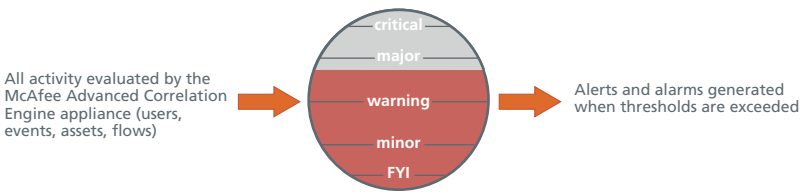

Figure 1. Risk-based correlation helps you detect looming threats against priority assets.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

41606ds_adv-corr-engine_1112_fnl_KG