WHITE PAPER

McAfee
Together is power.

User and Entity Behavior Analytics for McAfee Enterprise Security Manager

Detecting and responding to anomalous behavior

Table of Contents

User and Entity Behavior Analytics for McAfee Enterprise Security Manager

Detecting and responding to anomalous behavior

User and entity behavior analytics (UEBA) applies a variety of advanced technologies to track and flag suspicious or malicious behavior. Analytics initially centered on user activities but quickly expanded to include unusual behavior by other networked assets such as sensors, databases, and hosts. The discussion in the market around UEBA has increased recently for several reasons:

- Companies are worried about risky user behavior—accidental or deliberate—that may lead to data exfiltration or compliance violations.
- Credential theft is a common reason for attacker success, permitting remote access, privilege escalation, and lateral movement while the attacker is disguised as a legitimate user. Unusual user activity can be a clue to this situation.
- High-performance security operational systems, such as security information and event management (SIEM), have teamed with newer technologies, such as UEBA, to add additional context to continuous, real-time (or near real-time) detection, monitoring, analysis, and enforcement.
- Some vendors are positioning standalone UEBA solutions as sufficient for monitoring and understanding user behavior, creating confusion and uncertainty around which solutions to invest in both budget and team resources.

As with many areas of security operations, the UEBA space overlaps other infrastructure in its scope and contribution. While user directories and identity management can tell you and your tools about user and role usage, UEBA provides analytics that highlight patterns and unusual behavior, ideally before the theft, disruption, or compromise occurs. In most cases, UEBA offers dedicated analytics that complement the baselining and rule-based analytics capabilities that have been maturing within the SIEM space for several years, with different SIEM vendors offering varying levels of native and integrated support for UEBA applications.

UEBA can play multiple roles within the enterprise, providing added visibility to SIEM solutions for compliance and user monitoring; improving the speed, accuracy, and precision of security alerts; and enlightening security analysts and data breach

investigators. Today's most advanced security operations use the technologies together to maximize each tool's strengths. Core baselining, detection, and monitoring functions and high-speed correlations within the SIEM deliver on many basic UEBA use cases. By leveraging UEBA's specialized analytics and merging the insights back into the SIEM, you achieve advanced detection bridged to efficient operations. The more sophisticated your organization's security operations, the more you will want to adapt and extend analytics to integrate UEBA insights into your threat hunting, risk escalation, and investigation processes.

This document provides an overview of core UEBA capabilities available in the McAfee® Enterprise Security Manager solution and introduces the many partners whose products are tightly integrated and certified with McAfee Enterprise Security Manager. The goal of these native capabilities and key partner integrations is to help each enterprise make the best decision on adopting this important toolset.

UEBA with Standalone McAfee Enterprise Security Manager

The benefit of monitoring user activity and behavior is being able to increase security operations accuracy while shortening investigation timelines. For many years, understanding user activity and behavior—insights gained from SIEM baselining and anomaly detection—has helped McAfee Enterprise Security Manager users identify threats hidden among vast amounts of data. Rather than focusing exclusively on users or entities, McAfee Enterprise Security Manager uses a combination of anomaly detection and customized rules, along with other intelligent and advanced correlation models. These analytics use baselines to establish what is "normal," then factor in outlier behavior as part of ongoing monitoring and alerting. User activities are treated as part of a larger calculation of security and risk that helps operations recognize and prioritize incidents.

For example, McAfee Enterprise Security Manager has been designed to interpret several mainstream situations where user and entity visibility have a significant impact, such as:

- When anomalous user account activities, such as creation, lockouts, sharing, abuses, or exploitation, point to a more serious breach.
- When data exfiltration activities indicate something is not "normal," such as a user sending sensitive information outside the network.
- When unusual activities, such as a late-night user logins sourced from an unusual location and followed by a system misuse, deserve further investigation.

McAfee Enterprise Security Manager offers access to such UEBA use cases though downloadable content packs that deliver preconfigured views, rules, alarms, and watchlists.

McAfee Enterprise Security Manager includes several methods of correlation—from traditional rule-based (example: five login failures within 10 minutes = brute force attempt) to more complex standard deviations (example: service account usage increases 20% above normal baseline). Moving beyond simple rules enables more precision in identifying meaningful patterns and events, with deviation techniques that detect events earlier in the attack to enable proactive disruption and prevent data loss. Furthermore, McAfee Enterprise Security Manager can automatically combine these two techniques with complementary methods of correlation.

Multiple Correlations Pinpoint Events in Near Real Time

Speed is critical in security monitoring and triage and different types of correlations can be performed in different parts of the McAfee Enterprise Security Manager's architecture to quickly and efficiently collect, parse, normalize, enrich, aggregate, and process the data streams. Specifically, McAfee Event Receiver's initial real-time, rule-based correlation of events surfaces matches for further, expedited analysis. McAfee Advanced Correlation Engine (McAfee ACE), an optional dedicated physical or virtual correlation appliance, can perform advanced rule-based events correlations, as well as incorporating flows and deviations into the correlations. These deviation options help set accurate thresholds, with options for "percent from average" and "fixed value from average" rather than just a standard deviation.

In addition, McAfee ACE adds two specialized correlations: risk correlation to prioritize events based on asset value and threat severity and historical correlation to detect previous related events. Correlation rules and variables are provided as part of default content, and all rules are customizable. Unlike the simple if/then rules that permeate security controls, advanced correlations can nest components, use and/or logic, consult watchlists for current concerns, and include detailed filters for highly refined matching and alerts.

McAfee Enterprise Security Manager User Behavior Use Cases

Tracking user activity and being able to detect and understand anomalous behavior is an effective way to identify several types of security breaches. This section illustrates six use cases where McAfee Enterprise Security Manager's user behavior analysis is essential to understanding potential security breaches.

Account exploitation

A common attack method is to "guess" login credentials. The attacker usually automates a process to send login requests using a long list of common and inferred usernames and passwords within a short time period. It's a rapid-fire process, sometimes sending hundreds or thousands of requests per second.

In this example, a brute force login attempt was detected, followed by a successful login from the same source IP address. Below we can see a series of suspicious activities resulting in an alert. We are also able to profile the user affected along with his business department.

Possible Resolution*

- Immediately block access to the account and system.
- Notify the authorized user of whom to contact to restore their credentials and reset their password.
- Review the maximum number of allowed failed login attempts in your security policy.
- Start an investigation about the characteristics of the attack to be able to prevent similar ones in the future and develop new policies based on the attack profile.

Figure 1. Looking at our dashboard, we can see many correlated events related to user behavior.

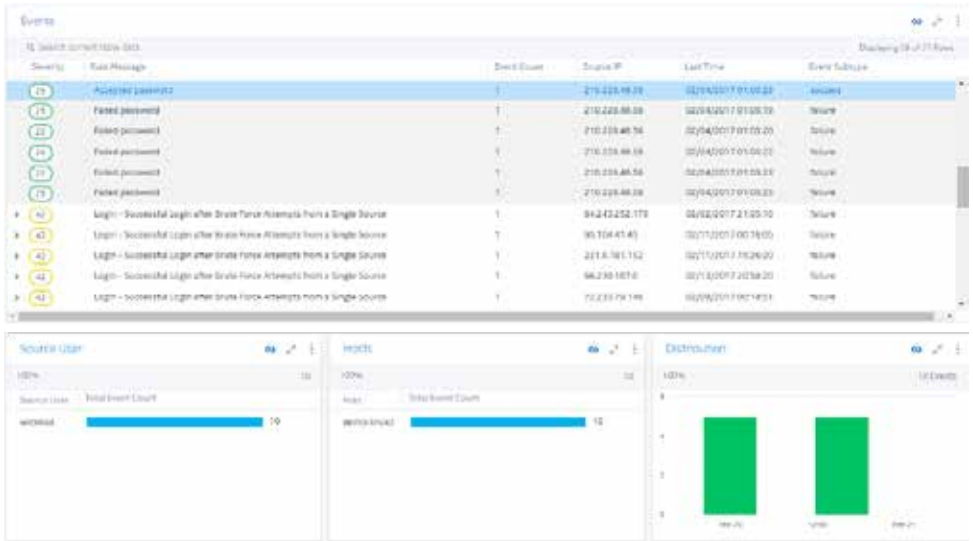

Figure 2. Drilling down into the event above, we can see the series of suspicious activities that resulted in the alert and can profile the affected user.

Potential malicious activity followed by data exfiltration

When a host is compromised, there will often be an increase in unusual behavior indicators, such as visits to random sites, extra traffic, and random protocols in use by a machine. These deviations from "normal" behavior can reflect such baselines as a volume change in outgoing data, which may indicate that confidential data is being leaked to an external source. A deviation in destination IP addresses and protocols may indicate that the host is infected and is now communicating with the attacker. In any case, these suspicious behaviors are indicative of potential threats and key indicators to drive investigations.

An unusual increase will be determined by the threshold that is set by the administrator. In this case, McAfee Enterprise Security Manager will trigger on events that are greater than two standard deviations from the baseline.

Possible Resolution*

- Users may wish to create an alarm to alert an incident response team when the correlation rule matches certain conditions.
- The host should be investigated for possible infection or compromise.

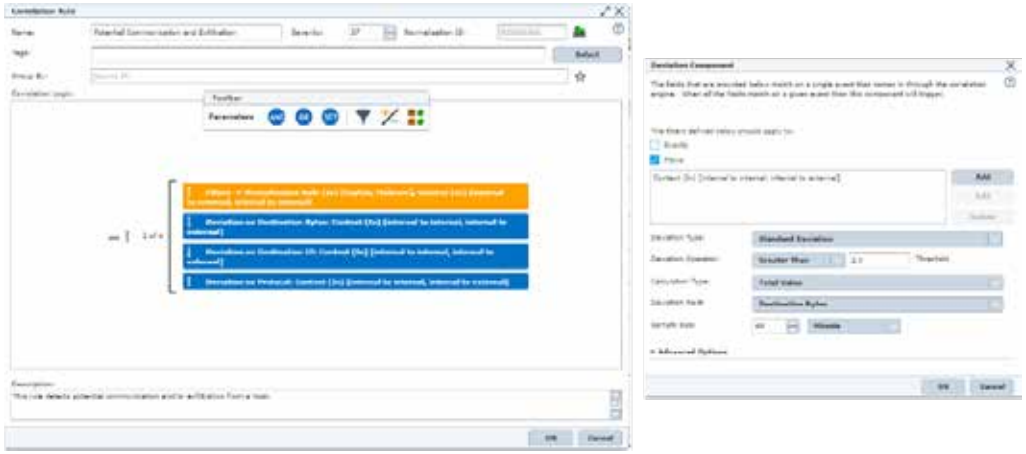

Figure 3. Here we can see the correlation rule that was triggered, as well as how to customize the deviation threshold to reflect learned behaviors.

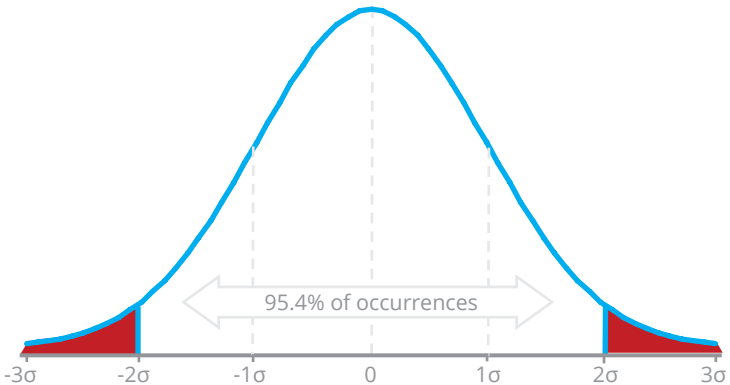

Figure 4. A threshold has been set to alert on events that fall outside of two standard deviations from the mean, or 4.6% of all occurrences.

Abnormal system use after unusual user login

Suspicious behavior could be any number of things that are not necessarily serious on their own, but when seen together form a pattern indicating a potential threat. It is not easy to predict every step a possible attacker may take. It is more helpful to understand what normal behavior is and treat anything abnormal with suspicion. In this case, an alert was triggered right after a successful user login event was performed from a suspicious location and time. Both events originated from the same source IP. This could indicate that an attacker has found a way to penetrate your security, putting your network, intellectual property, and customer information at risk.

Possible Resolution*

- First, investigate the source IP.
- If it is communicating from outside your local network, you may wish to block the address at your perimeter. If it is internal, carefully investigate to see if the host has been compromised and consider blocking access to the target.
- In either case, investigate what the suspicious activity is and isolate the host if necessary.
- If you consider it harmful, update your security policy accordingly.

Figure 5. Here is the correlation rule described in the scenario above.

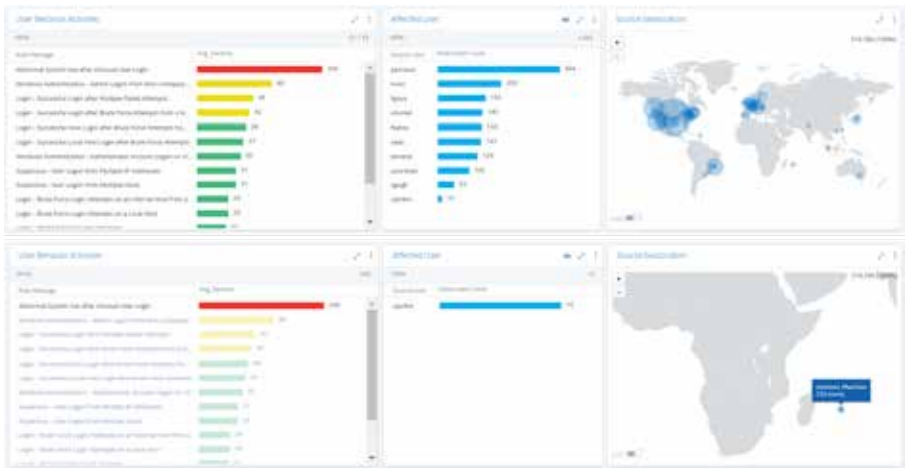

Figure 6. By clicking on the event alert on our dashboard, we can drill down and identify the affected user and the source geolocation, providing immediate insight into the who and where for this suspicious activity.

User traffic to a business application deviates from average

In this case, an abnormal increase in traffic sent to a business application from the same user could indicate a potential threat or improper usage. In both instances, the security operations team should be able to quickly identify this activity.

McAfee Enterprise Security Manager profiles and correlates this abnormal traffic to highlight the user involved, as well as the application affected. Additionally, the solution can also reveal the exact moment when the behavior rule triggered.

Possible Resolution*

- If you are concerned that the user is violating company security policy, investigate further.
- Send an email to the executive involved to check whether it really was abnormal usage or not.

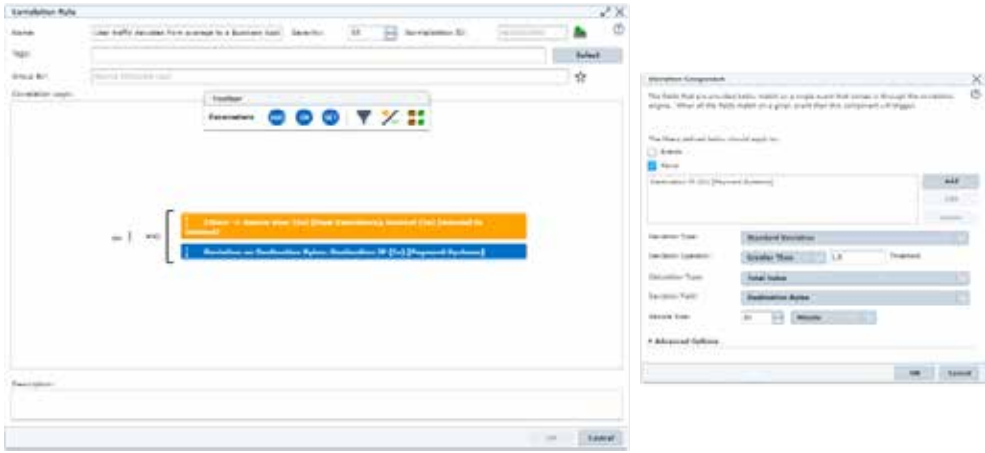

Figure 7. Here is the correlation rule described in the scenario above.

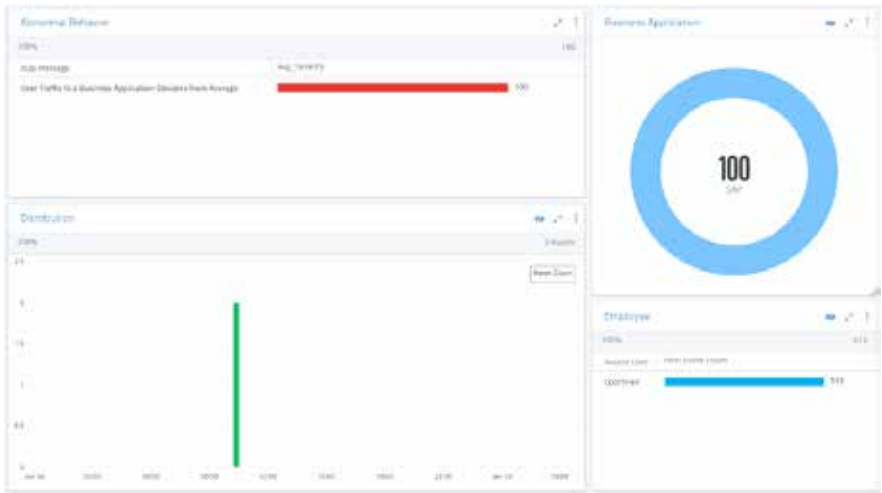

Figure 8. Drilling down, we can identify the user, time frame, and application involved.

Same ID used in different locations at the same time

Simultaneous remote logins can have an innocent explanation. An employee could be on a business trip and accessing the internal network while traveling. However, another possibility is that an attacker has gained access to an existing employee account. In either case, the event warrants further investigation.

This rule detects multiple user logon events from the same username originating from multiple locations within a specified period of time.

Possible Resolution*

- Verify that the user is an authorized employee on approved business travel.
- You may wish to create special rules for employees who travel often.
- Monitor the host for any suspicious behaviors that may indicate a breach of security.

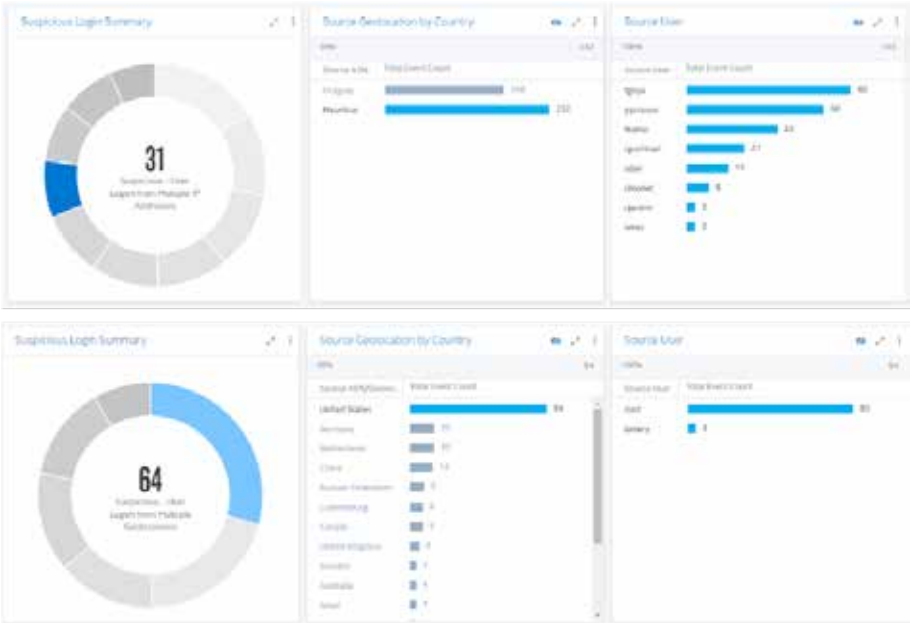

Figure 9. In the top row, we can see where suspicious user logins from multiple IP addresses have occurred, along with the users involved. In the bottom row, we can see the same for suspicious user logins from multiple locations, providing insight into the users and locations impacted.

Recurrent bad behaviors

The detection of recurrent bad behavior by employees is a critical capability—by tracking the frequency of these situations, the security team will be able to identify the most difficult challenges inside the company, focus its security measures, and discuss effective actions and policies. McAfee Enterprise Security Manager provides this visibility with the required security information context. The dashboard below, as an example, puts together the most problematic users and details their activities. It appends all users caught to a specific watchlist.

Possible Resolution*

- Make sure these issues have been discussed and addressed properly through an effective incident management and response plan.
- Recurrent users must be observed carefully as they are responsible for most security problems.

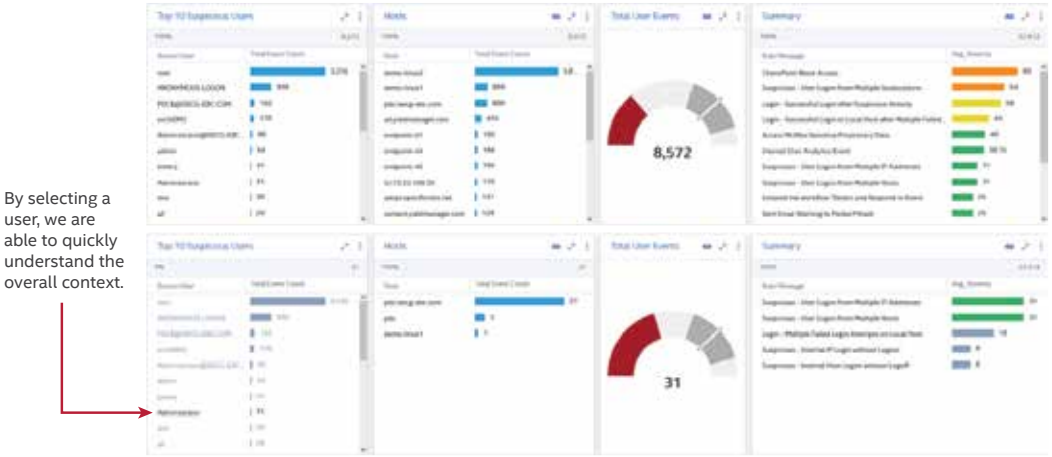

Figure 10. This dashboard shows the top suspicious users in our organization and a summary of what they have been up to.

Better Together: Third-Party UEBA and McAfee Enterprise Security Manager

Customers may find they need specialized analysis to tackle a specific use case, analysis that is available through a third-party UEBA vendor. In successful UEBA deployments, the advantage comes from combining the specialized capabilities of UEBA with the broad visibility of SIEM. Successful overall incident management requires visibility and access to data and trends from throughout the McAfee Enterprise Security Manager architecture, which includes endpoint system and application data, threat intelligence, and asset profiles.

Integrating UEBA with McAfee Enterprise Security Manager provides a central point from which actions can take place—such as managing wide-ranging investigations, automating repetitious tasks, and remediating breaches. Furthermore, McAfee Enterprise Security Manager offers dashboards, reporting, alerting, workflow support, and integration with countermeasures and ticketing systems. Once a business has deployed and customized these operational functions, it is more efficient and effective to enrich these processes with user and entity data, rather than create a parallel set of systems and tasks that offer limited and manual data integration and fail to leverage existing and more expansive solutions.

Given these complementary strengths, many companies find value in deploying a tightly integrated combination of the two technologies. Integrating UEBA with McAfee Enterprise Security Manager helps to prioritize alerts for prompt intercept and prioritized response. By combining fresh user data with other threat, contextual, and organizational parameters within McAfee Enterprise Security Manager, watchlists and rules can trigger policy changes, alerts, and escalations. These rapid response activities complement after-the-fact user data mining that is also helpful in forensic investigations that span beyond user and entity behavior for optimal incident resolution. The combination also leverages the SIEM's robust reporting engine. When UEBA solutions send information back to McAfee Enterprise Security Manager, it can visualize that data within a report, as well as synthesize the data inside existing operational reports, dashboards, and workflows.

McAfee Enterprise Security Manager Enables UEBA Options

The UEBA specialty has evolved quickly, starting with users and now encompassing entities. As the core of an open ecosystem, McAfee Enterprise Security Manager integrates with multiple UEBA products, providing proven integrations you can leverage instead of creating ad-hoc one-off connections. This helps simplify security investigations and remediation regardless of your organization's preferred processes.

While the exact features of the integration vary depending on the capabilities of the specific UEBA solution, we've evaluated and selected vendors that we and our customers have identified as providing the highest quality analytics in the market. McAfee partners with both established and emerging UEBA vendors. The complete list of current McAfee Enterprise Security Manager integrations is available on the McAfee Innovation Alliance page.

Security Innovation Alliance Partners have integrated, tested, and certified their security solutions to work with McAfee Enterprise Security Manager. We have collaborated with our partners to simplify the integration of these products in even the most complex customer environments. This provides a truly connected security ecosystem that optimizes the value of your existing investments, improves efficiency, maximizes protection, and reduces operational costs.

* Specific resolutions may vary based on your network conditions and security policy.

McAfee Enterprise Security Manager integrated UEBA partners include:

- Exabeam
- Fortscale
- Gurucul
- Interset
- Niara
- Securonix
- And more

Get Started

For more information on McAfee Enterprise Security Manager, visit **www.mcafee.com/siem**.

Explore current McAfee Innovation Alliance Partners: **www.mcafee.com/SIA**.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

McAfee™
Together is power.

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