It can often seem that attackers have all the advantages. To tip the scale of power towards the defender, McAfee® Behavioral Analytics and Atos work together to narrow down billions of real-time security events to a handful of actionable leads. By distilling billions of events into a prioritized list of high-risk entities, security analytics gives Atos cyberhunters new tools in containing cyberthreats. As a service provider, Atos is able to combine McAfee advanced threat lifecycle and analytics into a dynamic and effective threat mitigation system.
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.

One example of where security analytics gives cyberhunters radical advantages in containing cyberthreats is Atos managed security service, which combines McAfee Advanced Threat Lifecycle and McAfee Enterprise Security Manager with McAfee Behavioral Analytics to distill billions of real-time events and scores them in terms of their risk. This data is sent back to the McAfee product ecosystem so that Atos cyberhunting is focused on the highest priority threats.

The combination of McAfee Behavioral Analytics with McAfee solutions delivers human-machine threat-hunting for a force-multiplying productivity gain in cybersecurity defense.

The rest of this document provides an overview of core UEBA capabilities available in the McAfee Enterprise Security Manager solution and also discusses how Atos and McAfee Behavioral Analytics in particular work with McAfee ESM.

**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 dynamically create unique baselines to establish what is “normal,” and 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 dynamic risk assessment of risky entities through downloadable content packs that deliver preconfigured views, self-learning AI risk detection, meaningful alarms, and watch lists.

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 for a unique entity). 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 analyze 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. Beyond this, behavioral analytics dynamically measures and generates unique thresholds with machine learning and AI. This gives the defenders an advantage with automated threat detection at a scale that is impossible to achieve with existing rules and thresholds based systems.

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 watch lists 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 uniquely 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. To the right 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 flagged by behavioral analytics. Then McAfee Enterprise Security Manager can trigger on events with more accuracy and speed. A threshold can also be preset 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.

To further investigate the unusual system behavior, the administrator can immediately click on the event alert on the dashboard to directly drill down to the relevant details, relieving hours of effort to manually piece together the relevant pieces of information needed.

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 to the left.

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 on the right, as an example, puts together the most problematic users and details their activities. It appends all users caught to a specific watch list.

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.](image-url)
Better Together: McAfee and Atos

Customers may find that today’s complex and diverse threats, and the new IoT and Big Data challenges, need specialized advanced analytics to help minimize the likelihood of breaches. To tip the scale of power toward the defender, McAfee Behavioral Analytics works to narrow down billions of real-time security events to a handful of actionable leads where security teams can focus their efforts.

These security leads provide clear views of measured risk generated through dynamic machine learning and advanced mathematical models. No human can match the rate at which a computational system can process and correlate vast amounts of data from multiple sources. In this way, behavioral analytics bring an unprecedented level of productivity to security teams.

Following this model, Atos security practitioners can see at a glance the current risk posture of any entity, such as a user, file, machine, project, server, IP address, or printer. The McAfee Behavioral Analytics platform measures the unique digital footprint of each entity. It dynamically learns what is normal and what is anomalous, considering the unique context of each entity’s behavior.

Using the risk dashboard, security practitioners can then drill down into why an entity’s characteristics, usage patterns, and behaviors are deemed high risk. What used to take days or months, now takes only minutes.

For the first time, a security team can have a measured response to a measured threat. Those measured responses can be leveraged:

- Inside of McAfee Enterprise Security Manager SIEM for prioritization and investigation
- Inside of McAfee® ePolicy Orchestrator® (McAfee ePO™) software to set active and passive tags on the relative entities
- Through McAfee Active Response reactions for remediation
- Inside of the McAfee Security Analytics platform for in-depth investigation

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.

As a service provider, Atos is able to use Data Exchange Layer (DXL) to integrate the entire McAfee TDL infrastructure with McAfee Behavioral Analytics. By doing this, Atos is able to not only detect threats rapidly, but also (via DXL’s automation and orchestration) to remediate threats faster than ever before.

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