McAfee
Together is power.

The Threat Inside Can't Hide

Surface and prioritize threats that matter

Inconsistent or unusual behavior, while potentially indicative of a threat, can be difficult to both uncover and accurately identify as a risk. McAfee® Behavioral Analytics uses big data security analytics and unsupervised machine learning to surface unusual and highly risky behavior often invisible to other security solutions. It processes and correlates vast amounts of data from multiple sources, creating a baseline of "normal" activity and a risk score for every monitored entity—from users to machines. McAfee Behavioral Analytics then monitors change, correlates activity, and surfaces suspicious behavior to security analysts for further investigation and action.

The Business Problem

Imagine you have a user from Los Angeles in accounting who suddenly VPNs in from China. That can happen in global companies, right? However, after a period of time (it could be three minutes or three weeks), she accesses three file repositories that she's never touched before. Technically, she has permission to do so, but no one else on her team has engaged with these resources in the last two months. Two days later, she downloads 2 GB of data and copies it to a USB thumb drive.

This user's account has been compromised. Someone is using it to exfiltrate data—your valuable corporate data.

How hard would it be for your organization to spot this? Would you catch any of these activities in the flood of alerts that you likely have today? Would you have paid attention to them? How long would it take to figure out the link between these discrete activities?

With McAfee Behavioral Analytics you can accurately identify this unusual behavior and take action.

McAfee Behavioral Analytics

Part of a solution category often referred to as user and entity behavior analytics (UEBA), McAfee Behavioral Analytics helps transform data and security events into a handful of prioritized leads upon which security teams can focus their efforts.

McAfee Behavioral Analytics first ingests data from multiple sources—from security information and event management (SIEM) solutions to data repositories in order to measure the unique digital footprint of each entity. Using unsupervised machine learning and advanced mathematical models, it dynamically learns what is normal and what is anomalous, considering the unique context of each entity's behavior, along with the behavior of similar entities or peer groups. No human can match the rate at which a computational system can process and correlate such vast amounts of data from so many sources.

Security practitioners can see at a glance prioritized risk scores of any entity, such as a user, file, machine, project, server, IP address, or printer. Using the McAfee Behavioral Analytics risk dashboard, analysts can drill down to learn why an entity's characteristics, usage patterns, and behaviors are deemed high risk. Prioritized risk scores are also shared with SIEM solutions and other SOC tools for further investigation. Analysts will understand what the greatest threat is and know where to start. McAfee Behavioral Analytics brings an unprecedented level of productivity to security teams. What used to take days or months, can now take only minutes.

Use Cases

- **Account compromise:** Unauthorized account usage by anyone other than the account holder—for example, an outsider who has spear-phished an executive in order to obtain and use those credentials to further infiltrate an organization
- **Insider threat (fraud):** The use of insider privileged access credentials for illegal personal use or personal profit—for example, a financial trader who uses employee discounted rates to resell services and pocket the difference
- **Data theft:** Unauthorized transfer of data from a computer—for example, a user transfers large amounts of sensitive data from a share that none of his or her peers are accessing

Better Together

Successful overall incident management requires broad visibility and access to data from throughout an organization's entire ecosystem. It also requires products to act as a cohesive system so all solutions can make better decisions, analysts and machines can take fast action, and analysts can work more efficiently and effectively. Our solutions are designed to work together to form a cohesive system. With products that not only work well together but also with other vendors' products, McAfee can help you maintain a safer environment with truly integrated security.

McAfee Behavioral Analytics integrates with numerous solutions across the McAfee portfolio along with other vendors' SIEM solutions and SOC tools. Within the McAfee portfolio, McAfee Behavioral Analytics risk information can be leveraged:

- Inside of McAfee Enterprise Security Manager SIEM for further investigation and action
- Inside of McAfee® ePolicy Orchestrator® (McAfee ePO™) software to set tags on the impacted entities
  - Through McAfee Active Response, managed by McAfee ePO software, remediation actions
- Inside a McAfee or third-party security solution that subscribes to Data Exchange Layer (DXL) updates

McAfee Enterprise Security Manager

McAfee Behavioral Analytics and McAfee Enterprise Security Manager are highly complementary. McAfee Behavioral Analytics finds unusual behavior over time and augments the extensive capabilities of McAfee Enterprise Security Manager, such as broad-based log collection and analysis, real-time alerting, compliance, file integrity monitoring, and reporting. SIEM logs and alerts are fed to McAfee Behavioral Analytics, where advanced analytics are applied. In turn, prioritized risk scores from McAfee Behavioral Analytics are shared with McAfee Enterprise Security Manager, where dashboards are updated and policy-based action can initiate remediation commands to other solutions.

McAfee ePolicy Orchestrator (McAfee ePO) Software

A single management console for multiple security solutions from McAfee Endpoint Security to third-party products, McAfee ePO software provides a unified view and streamlines security workflows for proven efficiencies. With prioritized risk scores from McAfee Behavioral Analytics, the McAfee ePO management platform can take immediate policy-based action to set tags on impacted entities across the enterprise.

McAfee Active Response

McAfee Active Response provides endpoint detection and response capabilities. Armed with a prioritized list of risky entities, McAfee Active Response enables the analyst to immediately react and remediate those systems that McAfee Behavioral Analytics has identified as exhibiting anomalous behavior.

Other Security Solution Integrated Through Data Exchange Layer (DXL)

DXL is a fast, bi-directional communications fabric that enables information sharing between any connected security technology. Additional McAfee or third-party security solutions that subscribe to DXL updates can also subscribe to McAfee Behavioral Analytics updates, incorporating risk scores into policy-based action or dashboards.

McAfee
Together is power.

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