SOLUTION BRIEF

SIEM Performance, Scalability, and Time Savings on a Scale Never Before Seen for SIEM

Addresses long-standing security operations challenges

The hurdles of managing a security infrastructure include a lengthy implementation period, a data volume greater than the events-per-second (EPS) ingestion rate, and mounting costs and resources required to maintain the environment. Implementing a security infrastructure using McAfee® Enterprise Security Manager Cloud technology can be done quickly, offers increased ingestion rate capabilities, and can yield huge cost efficiencies compared to on-premises or other public cloud solutions.

McAfee Solution

- McAfee Enterprise Security Manager version 11.2.x and above

Connect With Us

The Business Problem

Today's security information and event management (SIEM) solutions need to be able to identify and defend against attacks within an ever-increasing volume of events, sophistication of threats, and cloud infrastructures. These attacks come from constantly evolving threats hiding behind normal enterprise activity. Most common barriers to a traditional on-premises SIEM include lack of flexibility, complex and time-consuming hardware maintenance, performance limitations, and scalability issues. For these reasons, organizations are choosing to adopt cloud-based solutions. When deciding to utilize the cloud, customers must also determine whether to manage their own instance in the cloud or use a Software-as-a-Service (SaaS) solution.

McAfee Enterprise Security Manager Cloud

McAfee has taken our existing McAfee® Enterprise Security Manager SIEM product and transformed it into a cloud-based SIEM solution called McAfee Enterprise Security Manager Cloud (www.mcafee.com/esm). McAfee Enterprise Security Manager Cloud is not a SaaS-native solution, but it provides much of the value of SaaS applications, such as processing data faster and managing security systems more efficiently. With McAfee Enterprise Security Manager Cloud, customers can build a security operations center that can ingest data or search and scale correlation rules at speeds never before seen on large volumes of data sources. Plus, McAfee Enterprise Security Manager Cloud delivers increased convenience compared to other cloud SIEMs by providing a single, frictionless application that is easy to access and simple to use.

To bring real value to customers, we have focused on removing the barriers to customer success in security operations by providing:

- **Automatic installation and maintenance:** Customers never need to install or update McAfee Enterprise Security Manager Cloud. The system is ready to ingest data from day one.
- **Continuous Improvement:** McAfee handles all updates to McAfee Enterprise Security Manager Cloud. Customers are freed from the burden of software updates and upgrades.
- **Consistent performance:** McAfee Enterprise Security Manager Cloud delivers a consistent high-performance SIEM platform. The performance a customer experiences on day one will be the performance they still have as their security operations requirements grow.
- **Scalability:** We take away the dependence on a customer's data center and instead increase capacity and compute power with a few clicks of the mouse within conveniently packaged templates.

Challenges

- Managing security infrastructure with an ever-increasing volume of security events from mounting numbers of data sources
- Cyberattacks increasing in volume and sophistication
- More mission-critical workloads and sensitive data residing in the cloud

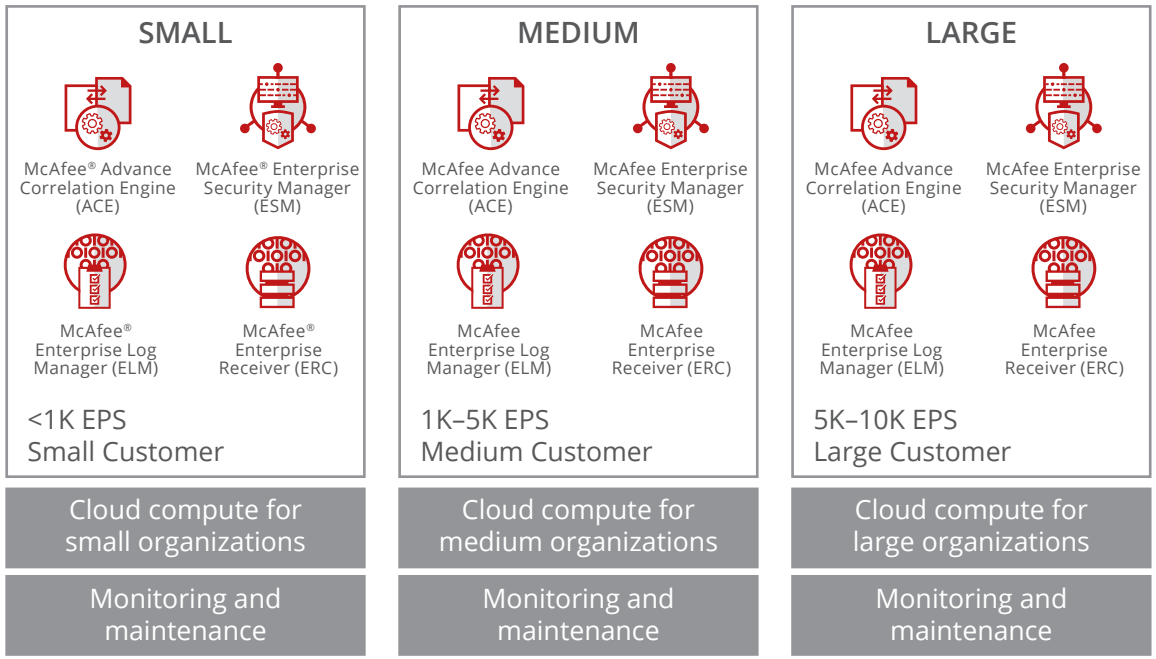
McAfee Solution

- Record-breaking events/second ingest performance
- Real-time visibility
- Advanced threat intelligence

Results

- Huge cost savings compared to on-premises or other public cloud solutions
- Record-breaking performance, regardless of initial topology: up to 500,000 events/second across 600,000 data sources
- Decreased time of implementation—just three days on OCI compared to 35 to 40 days on premises
- Flexible architecture

McAfee Enterprise Security Manager Cloud Templates



Once implemented, McAfee Enterprise Security Manager Cloud provides the information and context needed for fast, risk-based decisions, making it practical to support organization's current and future security and compliance goals.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager is a SIEM solution that delivers actionable intelligence and integrations to prioritize, investigate, and respond to threats.

Learn More

For more information, contact your McAfee representative or channel partner, or visit www.mcafee.com/esm.

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