Human and Machine Threat Hunting

A list of prioritized leads to accelerate security team efforts

Security analytics give cyberhunters radical advantages in containing cyberthreats. Powered by dynamic machine learning, Interset distills billions of real-time events into a prioritized list of high-risk entities. This, in turn, is sent back to the McAfee® product ecosystem to focus cyberhunting efforts on actionable, high-value threats. The combination of the Interset Security Analytics Platform with McAfee solutions delivers human-machine threat-hunting for a force-multiplying productivity gain in cybersecurity defense.

McAfee Compatible Solution

- Interset 5.4+ with McAfee Enterprise Security Manager
- Interset 5.4+ with DXL
- Interset 5.4+ with McAfee ePO

The Business Problem

In modern cyberwarfare, we do not know where the next attack will come from or which form it will take. Attack vectors are intentionally stealthy and multifaceted to avoid detection by traditional security tools, which are rigid by nature. Attackers take advantage of hard-coded rules and thresholds, which produce far too many alerts and false positives for human investigation. To truly assess the risk impact of a threat, it needs to be holistically evaluated through all relevant angles and data points. This is only possible with contextual Big Data analytics and machine learning.

McAfee and Interset Joint Solution

The focus of cybersecurity practices is now detection and not prevention. Yet detection is challenging due to stealthy and asymmetrical attack surfaces. To tip the scale of power towards the defender, McAfee and Interset work together 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, Interset's analytics bring an unprecendented level of productivity to security teams.

Security practioners can see at a glance the current risk posture of any entity, such as a user, file, machine, project, server, IP address, or printer. Interset 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 practioners 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 Interset Security Analytics Platform for in-depth investigation

Based on automatically measured risk postures, even those with scarce cyberhunting resources can initiate measured responses to a prioritized list of security leads. This human-machine approach to containing cyberthreats is profoundly advantageous to security teams.

About Interset

Interset is a pioneer in security analytics, machine learning, Big Data, and risk forensics to radically accelerate threat detection. Interset actively measures the unique digital risk footprint of different systems and users using mathematical models and machine learning. This distills billions of events into a list of prioritized security leads for efficient threat detection.

About McAfee ePolicy Orchestrator Software

McAfee ePO software is the industry-leading security and compliance management platform. With its single-agent and single-console architecture, McAfee ePO software provides intelligent protection that is automated and actionable, enabling organizations to reduce costs and improve threat protection and compliance.

About McAfee Enterprise Security Manager

McAfee Enterprise Security Manager—the foundation of the security information and event management (SIEM) solution family from McAfee—delivers the performance, actionable intelligence, and real-time situational awareness at the speed and scale required for security organizations to identify, understand, and respond to stealthy threats, while the embedded compliance framework simplifies compliance.

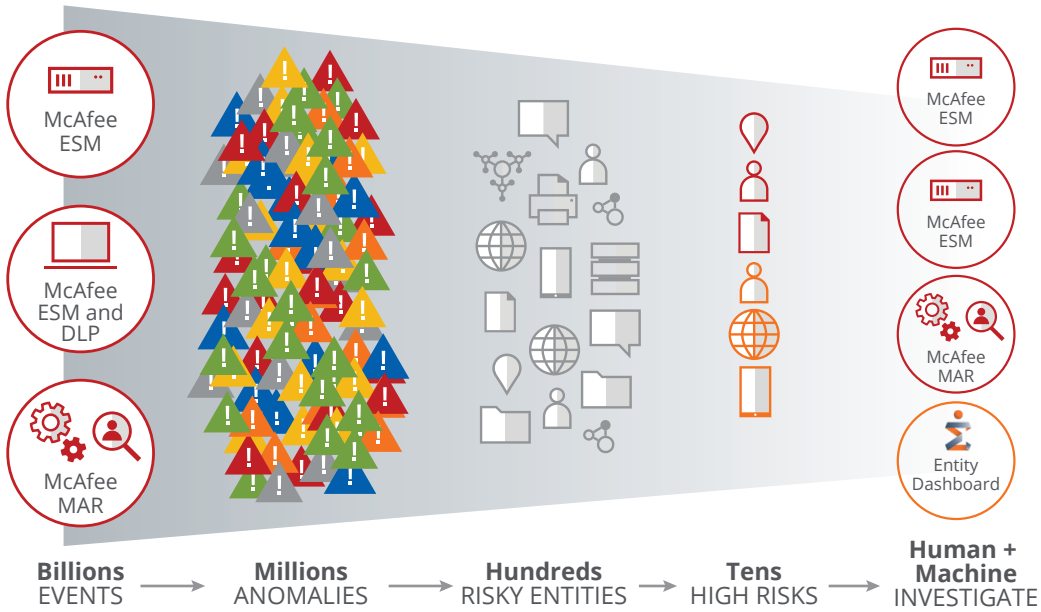

Figure 1. The Interset Security Analytics Platform in action.

About Data Exchange Layer

Bringing high-speed messaging to security systems, the Data Exchange Layer provides a universal fabric for exchanging data in real time. It leverages a one-to-many integration model so that each application can publish and subscribe to messages over a common communication system.

McAfee
Together is power.

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