ZeroFOX, the Social Risk Management Company, is pioneering security technology that enables organizations to detect and prevent social media-based cyberthreats, including targeting malware, phishing, social engineering, and other attacks. ZeroFOX is a McAfee® Security Innovation Alliance partner that integrates social media attack intelligence into McAfee Enterprise Security Manager. ZeroFOX’s solution detects and prevents social media-based threats. Social media has become an unprecedented, unchecked attack vector. By integrating intelligence from the ZeroFOX Attack Detection System (ADS) into the McAfee Enterprise Security Manager SIEM solution, security teams can combat a critical security blind spot and enhance their security posture with proactive intelligence.
Social Media: The New Battleground for Cybersecurity

Social media has become the most prolific mode of communication in human history. Nearly 75% of internet-connected people are active on social media, totaling more than two billion accounts between Facebook, Twitter, and LinkedIn alone. It is powerfully democratizing—an ideal vehicle for organizations to market, sell, recruit, and engage. But democratization comes at a cost. Each social media account—be it the account of a brand, employee, CEO, or customer—is an equally vulnerable and exploitable endpoint for cyberattacks. These accounts exist outside an organization’s security framework, rendering traditional security measures inadequate. Moreover, social media-based attacks are inexpensive and extremely effective, making them increasingly popular among cybercriminals. As social media continues to grow, cybersecurity must grow with it.

ZeroFOX Attack Detection System (ADS) and McAfee Enterprise Security Manager

The ZeroFOX Attack Detection System analyzes links, content, and profiles on social media to produce real-time alerts on targeted attacks affecting an organization’s social media footprint. ADS also produces a global threat intelligence feed that analyzes malicious activity on social media worldwide.

ZeroFOX’s threat intelligence syslog is integrated with, parsed, and displayed on McAfee Enterprise Security Manager. McAfee Enterprise Security Manager users can visualize and manage attack data, as well as global social media threat intelligence, via their SIEM. The intelligence is correlated with existing event data to provide a robust new layer of analysis. This attack intelligence is critical in effectively providing a proactive defense-in-depth security posture, detecting and correlating threats in real time, and contextualizing an attack after it has occurred.

Before an attack

Because ZeroFOX identifies threats external to an organization’s network, intelligence gathered by McAfee Enterprise Security Manager can be used proactively. The McAfee security analysis engine detects malicious links across the social media landscape, providing a critical early-warning system for developing or trending attacks, regardless of whether an organization is being targeted. Social media attack intelligence gives security teams the ability to prevent attacks before they impact the organization itself.

During an attack

ZeroFOX’s intelligence enhances the ability of an SIEM to correlate and alert on an attack in progress. ZeroFOX provides a critical baseline of cyberattacks in the broader social media landscape. The first instance of an event can be correlated with external attack intelligence. Moreover, this intelligence can be correlated with the existing McAfee watch list of URLs. SIEM systems integrated with ZeroFOX are more efficient, alerting on attacks after the first compromising event.

After an attack

ZeroFOX attack intelligence can provide insights into the origin and nature of an attack after it has occurred. Tracing an attack to a prior event on social media gives
organizations critical context regarding the origin of an attack and how to better combat such threats in the future.

**ZeroFOX Security Analysis Engine**

ZeroFOX’s patented Security Analysis Engine (SAE) is the heart of ADS. The SAE analyzes links, content, and profiles using patented algorithms to provide a comprehensive analysis of social media-based threats. The SAE has three components:

- The Link Analyzer determines the malicious nature of links on social networks, assessing URLs for an ever-expanding list of threat attributes. Once a link is deemed malicious, it is further categorized as phishing or malware and assigned a risk score (from one to 100).

- The Profile Analyzer detects suspicious profile activity using a system of interoperating algorithms to find impersonators and prevent social engineering campaigns before they strike.

- The Content Analyzer detects inappropriate content affiliated with an organization’s social objects, including vulgarity, slurs, and threatening terms. Moreover, our pattern-matching capabilities uncover sensitive information with predictable string characteristics, such as Social Security numbers, addresses, bank accounts, Bitcoin wallet addresses, or other personally identifiable information.

**About ZeroFOX**

ZeroFOX, the Social Risk Management Company, provides pioneering security technology that enables organizations to detect and prevent social media-based cyberthreats, including targeted malware, phishing, social engineering, impersonations, and other fraudulent or malicious activity. At its core, ZeroFOX is an Attack Detection System (ADS) that monitors an organization’s social media entities and alerts on incoming attacks. Our proprietary Security Analysis Engine (SAE) analyzes threat intelligence and visualizes alerts through ZeroFOX Enterprise, a centralized, cloud-based platform, empowering users to take action on alerts and incoming threats. As the first solution to combat social media risk exposure, ZeroFOX enhances an organization’s security posture, while reducing incident response and crisis communications costs.

**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.