FireEye Threat Analytics Platform (TAP)™ and ZeroFox

Detect and Defend Against Social Network Exploitation & Social Media-based Cyber Attacks

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- Combines ZeroFox's industry-leading social media monitoring and analysis engines with FireEye's unequaled threat intelligence.
- Employs an automated discovery engine that continuously maps and monitors the organization's unique social fabric.
- Analyzes organization-specific data for both technical and behavioral indicators using ZeroFox's patented Security Analysis Engine.
- Increases security response effectiveness by an average of 83% using ZeroFox's unique social profile and content takedown capability.
- Joins the security data generated by ZeroFox with critical insights into the technical details of the threat, the social context, and additional security analysis.
- Delivers ZeroFox data to FireEye Threat Analytics Platform (TAP) that then applies threat intelligence, expert rules, and advanced security data analytics to noisy event data streams, enabling security teams to prioritize and optimize their response efforts.
- Provides high-level risk visibility and drill-down reporting via the ZeroFox custom-built dashboard.

OVERVIEW

Organizations invest immense resources into social media, which is quickly becoming the primary communication method for both individuals and businesses. But intertwined in the snaps, pins and tweets of social media applications are a multitude of information security and business risks, spanning targeted phishing, social engineering, account takeover, piracy, fraud, and more. Social networking has now become a major avenue to compromise corporate and government networks. As social media continues to increase in business communications, security teams must understand and address the risks posed by social media, the largest unsecured IT network on earth.

THE CHALLENGE

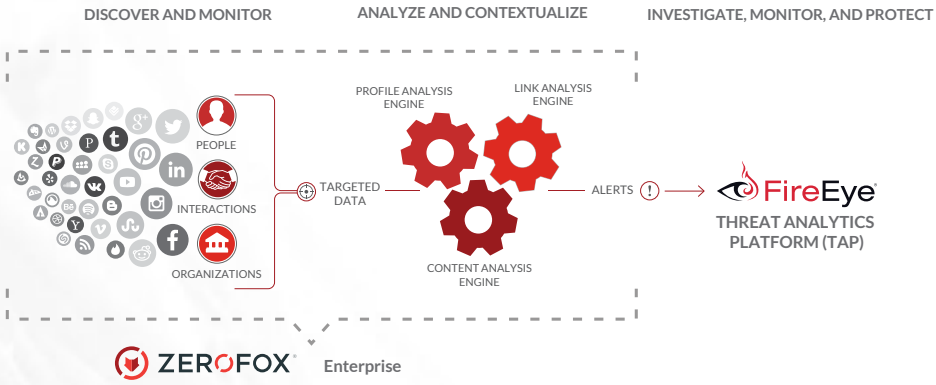
Social networking has introduced a global communication revolution, forever changing the way humans interact. However, it has also forever changed the cyber kill chain — giving attackers access to our customer organizations' vulnerable human targets, all of whom have never been more trusting. Leveraging tactics perfected through years of email phishing as well as new concepts of operation specific to social networking, adversaries have drastically reduced their costs and increased their rate of compromise. The front lines for cyber defense now start in the social world.

The challenge for network security staffs is to mitigate the tactics used by the cyber attackers, such as:

- Exploiting employees where traditional security platforms can't follow.
- Building fraudulent or impersonating profiles on social media.
- Phishing by leveraging the openness, scale, and trusted nature of social media.
- Using social media to coordinate attacks and to recruit followers.

THE INTEGRATED SOLUTION

The integration of FireEye Threat Analytics Platform (TAP) and ZeroFox Enterprise social media security platform gives customers unprecedented visibility into the largely unseen and unprotected social media attack vector without making changes to their existing security environment. ZeroFox Enterprise puts the power of advanced social data monitoring, security analysis, and threat detection at the fingertips of the security team. By supercharging the FireEye Threat Analytics Platform (TAP) with ZeroFox's organization-specific social media alerts and intelligence, customers can defend attacks targeting their people and their systems through one of the fastest growing cyber attack vectors. This defense enables customers to take the fight to cyber security adversaries.



FIREEYE PRODUCT AND VERSION
FireEye Threat Analytics Platform (TAP)

ZEROFOX PRODUCT AND VERSION
ZeroFox Enterprise

HOW THE JOINT SOLUTION WORKS TOGETHER

ZeroFox Enterprise continuously monitors social media for threat actors and malicious activity targeting employees, customers, or business operations. Serving as an early-warning system for targeted attacks, ZeroFox Enterprise identifies social engineering, phishing threat data, fraud and tactics, techniques, and procedures of the adversary.

ZeroFox performs analysis on the targeted data using people analysis, link analysis, and content analysis engines. The resulting alerts forward to FireEye Threat Analytics Platform (TAP). Utilizing information from the ZeroFox alerts, the analyst can use TAP to initiate an investigation to determine the potential impact and scope.

FireEye Threat Analytics Platform (TAP) identifies threats and accelerates response by layering real-time FireEye threat intelligence over enterprise event streams. This layering provides prioritized visibility into an organization's full threat landscape. Additionally, FireEye Threat Analytics Platform (TAP) manages incidents to improve efficiencies in assigning, tracking, and resolving events with on-demand portal access.

THE VALUE OF THIS PARTNERSHIP

FireEye and its Mandiant Services team are at the forefront of identifying the sources of today's advanced threats, targeting social media as a threat source that has exploded as one of the most dangerous sources of cyber attacks. The integration of FireEye Threat Analytics Platform (TAP) and ZeroFox allow both companies to bolster the customers' security posture that addresses unique threats from social media. ZeroFox monitors customers' social media footprints for malicious activity and then integrates finished intelligence into the FireEye Threat Analytics Platform (TAP) where is can be analyzed and acted upon. Together these solutions provide social protection for organizations operating in a modern online business environment.

This ZeroFox and FireEye partnership provides comprehensive, tailored protection from social threats without forcing organizations to adopt a new security infrastructure. More than anything, FireEye's participation with ZeroFox to solve social media security problems is validation that this is an enormous new risk to organizations that must be addressed before more breaches hit the headlines.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

ABOUT ZEROFOX

ZeroFox protects organizations from the risks introduced by social communication and collaboration platforms. It protects users where they are most vulnerable by continuously monitoring social platforms for cyber attacks, sensitive information loss, social engineering campaigns, account compromise, and fraud. Leveraging cutting edge technology and proven security practices, ZeroFox provides both targeted protection and global insights into the world of social media threats.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**