ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATION WITH FIREEYE HX®

Attivo Networks® has partnered with FireEye to provide advanced, real-time, in-network threat detection and improve automated incident response to stop active attacks. With the joint solution, customers can review high-fidelity alerts based on suspicious activity and gain the intelligence needed to hunt for other compromised systems. Organizations can reduce the time and resources required to detect threats, analyze attacks, and remediate infected endpoints, ultimately decreasing the organization’s risk of breaches and data loss.

HIGHLIGHTS
- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- End-point Deception Credentials Distribution

THE CHALLENGE

Cyber attackers have repeatedly proven that they can and will infiltrate even the most security-savvy organizations. Whether the attacker gets in using stolen credentials, a zero-day exploit, an email-based attack, or via insider access, they will establish a foothold and move laterally throughout the network until they reach their intended targets. Attackers have also proven that they can evade internal security solutions and traverse the network undetected once inside.

Quickly detecting and shutting down attackers that are already inside the network requires a new approach that expands upon conventional techniques, such as known signatures or attack pattern matching. This new method of detection uses deception and concealment technology to trick attackers into revealing themselves. Defenders can engage with threats to capture valuable attack forensics that the organization can use to promptly identify the attacker’s TTPs to delay them from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND FIREEYE HX JOINT SOLUTION

Integrating the Attivo ThreatDefend® Deception Platform with FireEye HX is simple. In minutes, organizations have an integrated adaptive security platform that provides effective, real-time detection of cyber attackers that can automatically block and isolate infected systems to contain the attack and stop data exfiltration. The integrated solution provides a real-time, non-disruptive way of detecting active in-network threats and blocking attackers from exfiltrating valuable company assets and information.

Automating threat identification has become critically important as lateral movement speeds increase for both live attackers and malware. Combining the Attivo Networks BOTSink® Engagement Server and the FireEye HX provides automated, real-time remediation, detection, and identification capabilities that outperform systems that rely on manual intervention.
ATTIVO NETWORKS THREATDEFEND PLATFORM

The Attivo Networks solution, recognized as the industry’s most comprehensive platform, provides network, endpoint, and data deception across an organization. The system has proven highly effective in detecting threats from all vectors, including reconnaissance, stolen credentials, Man-in-the-Middle attacks, Active Directory compromise, ransomware, and insider threats.

The Attivo Networks ThreatDefend® Platform provides early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a comprehensive fabric that blankets the network with deceptive decoys, credentials, shares, bait, and other misdirections that derail adversaries early in the attack lifecycle. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform’s components include the BOTsink deception server, the Endpoint Detection Net Suite, and ADSecure for Active Directory protection.

SUMMARY

The Attivo Networks ThreatDefend Platform plays a critical role in enabling an active defense with in-network threat detection and native integrations to dramatically accelerate incident response.

The ThreatDefend solution can identify compromised endpoints and automatically send validated alerts directly to FireEye HX. In turn, FireEye HX policies can automatically isolate and remediate infected systems and reduce the attacker’s ability to spread undetected. The time saved in automated isolation and remediation is critical in preventing lateral movement and data exfiltration. Automation gives the advantage back to the security team and will help contain the attacker before they can exfiltrate data or cause mass damage.

The need for this integration is urgent. In recent years, attackers have stolen billions of sensitive records with a detrimental impact to individuals and enterprises. The resulting damage to the companies’ reputations and balance sheets has reached into the billions of dollars. By implementing solutions that detect in-network threats early, automatically isolate them, and deliver the ability to hunt for additional threats, organizations can mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in cyber deception and attack lateral movement detection, delivers a superior defense for revealing and preventing insider and external unauthorized threat activity. The Attivo ThreatDefend® Deception Platform provides scalable protection, detection, and data concealment solutions for endpoints, Active Directory, and network devices. Comprehensive coverage is available for user networks, data centers, clouds, remote worksites, and specialized attack surfaces. It streamlines incident with forensics, automates attack analysis, and includes third-party native integrations.

ABOUT FIREEYE

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber-attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

www.attivonetworks.com

www.fireeye.com