PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATION WITH FIREEYE® ENDPOINT SECURITY

Attivo Networks® has collaborated with FireEye® to provide an accelerated, automated incident response to stop active attacks and aid in triage. With the joint solution, customers can reduce the time and resources required to respond quickly to an infected endpoint and automatically initiate collection of the available forensic information to aid in analysis and investigations, ultimately decreasing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine
- Expedited Incident Response
- Automatic Forensic Collection

THE CHALLENGE

Cyber attackers have proven that they can infiltrate the networks cyber infrastructure of even the most security-savvy organizations. Whether attackers break in using stolen credentials, zero-day exploits, malicious email, or insider access, they will establish a foothold and move laterally through the network until they reach their intended target. Attackers have also proven that, once inside, they can often evade internal security solutions and traverse the network undetected.

Quickly detecting and shutting down attackers that are already inside the network requires a new security approach that expands upon conventional techniques, such as known signatures or attack pattern matching. Deception delivers this new approach, tricking attackers into revealing themselves and providing high fidelity alerts to quickly and efficiently disrupt the attack. It can also capture valuable attack forensics and threat intelligence that organizations can use to bolster their defenses against future attacks.

THE ATTIVO THREATDEFEND PLATFORM AND FIREEYE ENDPOINT SECURITY JOINT SOLUTION

Integrating the Attivo ThreatDefend® Deception Platform with FireEye Endpoint Security is simple. In minutes, organizations can have an integrated adaptive security platform that provides effective, real-time detection of cyberattackers that can automatically block and isolate infected systems. The integrated solution provides an efficient, non-disruptive way of detecting and blocking active threats inside the network to quickly contain the attack and stop it from progressing.

The ThreatDefend platform provides deception-based detection and visibility to in-network attack activity. With the high-fidelity and low false-positive alerts the platform offers, organizations can accelerate their investigations and safely automate response actions to critical alerts. The FireEye Endpoint Security solution can block the attacking system and begin forensic collection immediately, thus reducing response times and streamlining investigations.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Considered the industry's most comprehensive deception platform, the Attivo Networks solution provides network, endpoint, application, and data deception across the entire network of an organization. The system has proven highly effective in detecting attack activity that other security solutions overlook, including network reconnaissance, credential theft/reuse, man-in-the-middle attacks, Active Directory reconnaissance/compromise, ransomware, and insider threats.

The ThreatDefend Deception Platform is a modular solution comprised of the Attivo BOTsink engagement servers that forms the foundation of the deception environment, the ThreatDirect® endpoint deception solution for deception in remote sites, the ThreatStrike® endpoint deception suite, the ThreatPath® solution for attack path visibility, the ThreatOps® solution that provides repeatable incident response playbooks, and the Attivo Central Manager (ACM) for enterprise-wide management of the deception environment. Together, these components create a comprehensive deception platform to detect and respond to in-network attackers.

FIREEYE ENDPOINT SECURITY

To protect against cyber threats and reduce risk, security teams need comprehensive endpoint defense for both common and advanced cyberattacks.

FireEye Endpoint Security brings front-line intelligence and experience to the endpoint, using multiple combined protection engines to block malware and exploits. Endpoint Security detects advanced attacks that bypass protection and enables response with tools and techniques developed by the world's leading frontline responders.

SUMMARY

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

The ThreatDefend solution can identify compromised endpoints and automatically send validated alerts directly to FireEye Endpoint Security. In turn, FireEye Endpoint Security policies can automatically isolate infected systems and initiate forensic collection to reduce the attacker's ability to spread undetected. The time saved in automated isolation is critical to preventing lateral movement, while automatically triggering forensic collection accelerates the investigation. Automation gives the advantage back to the security team and helps contain the attacker before they can cause extensive damage.

The need for this integration is urgent. In a single year, attackers have stolen over one billion sensitive records with a detrimental impact on 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 initiating forensics to speed up the investigation, organizations can mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

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 cyberattacks.

www.fireeye.com | integrate@fireeye.com