PARTNER BRIEF

ATTIVO NETWORKS AND FORESCOUT TECHNOLOGIES

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH FORESCOUT®

Attivo Networks has partnered with Forescout Technologies, Inc. to provide advanced, real-time, in-network threat detection and improved automated incident response to block and quarantine infected endpoints. With the joint solution, customers can review alerts and the choice to make manual updates or create policies that automatically block endpoints based on suspicious activity. Customers can reduce the time and resources required to detect threats, analyze attacks, and remediate infected endpoints, ultimately reducing the organization's risk of breaches and data loss while increasing the Incident Response team's efficiency and effectiveness.

THE CHALLENGE

Cyberattackers have repeatedly proven that they can breach the networks of even the most security-savvy organizations. Whether the attacker finds their way in using stolen credentials, a zero-day exploit, a malware attack, or simply start as an insider, they will establish a foothold and then move laterally through the environment until they complete their mission.

Malicious actors have shown that once they bypass existing perimeter defenses, they can easily move around the network undetected by existing security solutions. Organizations need a new approach to security that can quickly detect and shut down these attacks, one that focuses on the threats that are inside the networks and does not rely on typical measures, such as known signatures or attack pattern matching. This new detection method uses deception to lure attackers into revealing themselves and, once engaged, capture valuable attack forensics. This live intelligence enables the organization to promptly block the attacker and keep them from continuing or completing their mission.

THE ATTIVO THREATDEFEND PLATFORM AND FORESCOUT JOINT SOLUTION

Integrating the Attivo ThreatDefend Deception Platform with Forescout is easy. In minutes, organizations can have an integrated adaptive security platform that provides effective prevention, real-time detection of cyberattackers, and automatically blocks and quarantines infected systems to effectively stop data exfiltration and contain the attack. The integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, removing the opportunity for an attacker to exfiltrate valuable company assets and information. Automating remediation is becoming critically important as malware moves more rapidly through an environment. The combination of the Attivo BOTsink® Engagement Server and Forescout provides real- time remediation capabilities that outperform systems that depend upon manual intervention.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions, and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credentials, Man-in-the-Middle, Active Directory, malware, and insider threats. The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink engagement servers, decoys, lures, and breadcrumbs, the ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM) which together create a comprehensive early detection and active defense against cyber threats.

SUMMARY

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

The Attivo ThreatDefend Platform can reveal infected hosts and send alerts directly to Forescout to identify compromised endpoints. Policies configured in Forescout can then automatically quarantine the endpoint, isolating it and preventing network access. The time saved in blocking malicious traffic on the network is critical to preventing

lateral movement and data exfiltration. A strategy that depends upon manual intervention may work for low severity alerts, but high-severity attacks rarely give security teams the luxury of time when they need to react. Automatically blocking and quarantining infected systems gives the advantage back to the security team and can help contain the attack before the damage escalates. The need for this integration is urgent. In a single year, over one billion sensitive records have been stolen with serious impact to individuals and enterprises and 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 and having the ability to automatically block and quarantine those threats, 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 FORESCOUT TECHNOLOGIES

Forescout Technologies is the leader in device visibility and control. Forescout's unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment.

www.forescout.com