aruba
a Hewlett Packard
Enterprise company

Attivo
N E T W O R K S®

ATTIVO NETWORKS® THREATDEFEND™ PLATFORM INTEGRATION WITH ARUBA CLEARPASS POLICY MANAGER

Attivo Networks® has partnered with Aruba, a Hewlett-Packard Enterprise company, to provide advanced real-time inside-the-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints. With the joint solution, customers can detect and defend against advanced threats by automating a ClearPass-initiated quarantine from the Attivo® ThreatDefend™ Deception and Response Platform based on suspicious activity and the severity of the attacks. Aruba ClearPass Policy Manager along with the Attivo® ThreatDefend Platform provides enhanced visibility and control, resulting in higher productivity and efficiencies in security management, ultimately reducing the organization's risk of breaches and data loss.

HIGHLIGHTS

- Real-time Threat Detection
- Attack TTP Analysis and Forensics
- Automated Quarantine and Blocking
- Expedited Incident Response
- Centralized Threat Intelligence

THE CHALLENGE

The attack vectors are constantly evolving and can range from tailor-made APTs to mass-produced malware to methods based on social engineering or spear phishing. Reliably defending the perimeter against such a wide variety of attacks has proven unachievable and has resulted in numerous companies disclosing that they have been breached. Additionally, the ubiquity of mobile and IoT devices connected to enterprise networks and applications requiring external admin controls pose a major challenge to IT professionals in maintaining network security, as points of

entry can open for attackers into some of the most security-savvy organizations. Once attackers bypass the existing security prevention mechanisms, they can establish a foothold and move laterally throughout the network until they can complete their mission.

THE ATTIVO THREATDEFEND AND ARUBA CLEARPASS JOINT SOLUTION

The integration of the Attivo ThreatDefend Platform with Aruba ClearPass empowers organizations with an integrated, active defense platform that provides effective endpoint control through policy and threat prevention, real-time detection of cyber attackers, and the ability to mitigate risks by instantly quarantining the infected endpoints. The Attivo solution brings a new approach of dynamic deception that deceives attackers into revealing themselves. Once engaged, the solution captures valuable attack forensics, which can be communicated to Aruba ClearPass to promptly block the attacker from continuing or completing their mission.

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 credential, Man-in-the-Middle, Active Directory, ransomware, and insider threats The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink® engagement servers, decoys, and deceptions, 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.
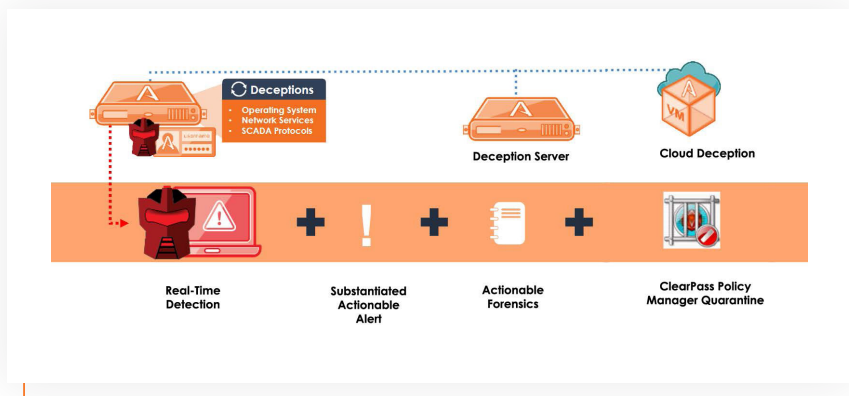
SUMMARY

The Attivo ThreatDefend Platform and the Aruba ClearPass Policy Manager empower organizations with an active defense platform that provide seamless visibility, effective threat containment, and the ability to instantly mitigate risks by auto-blocking infected endpoints through set policy enforcements with Aruba ClearPass. The time saved in blocking malicious traffic on the network is crucial to preventing lateral movement and data exfiltration. Automating blocking and quarantining gives the security team additional time that can be critical to containing the attack before mass damage can be done.

REAL-TIME IN-NETWORKS VISIBILITY AND THREAT DETECTION

ThreatDefend Platform for An Active Defense

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 ARUBA

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT and cybersecurity solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives.

www.arubanetworks.com