PARTNER BRIEF

ATTIVO NETWORKS® THREATDEFEND® PLATFORM INTEGRATES WITH PALO ALTO NETWORKS TO AUTOMATICALLY BLOCK AND QUARANTINE INFECTED ENDPOINTS

A modern-day adaptive security approach requires a blend of prevention and detection solutions. Together, these solutions will protect an organization by blocking and quarantining known and unknown threats. Threat actors have proven that they can find ways to bypass even the most sophisticated security prevention systems. Attivo Networks has integrated with Palo Alto Networks to provide advanced real-time inside-the-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints.

HIGHLIGHTS

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

THE CHALLENGE

Manual sharing information between detection and prevention systems can cause delays in isolating an attacker or blocking data exfiltration. This situation can result in increased complications when an attack happens during non-business hours or in organizations with limited IT resources. Such constraints and challenges hamper an organization's ability to respond quickly and effectively to attacks as they occur and propagate inside the network. An organization that can't effectively respond to fast-moving threats will experience difficulty preventing a compromise from becoming a full-scale breach.

THE ATTIVO THREATDEFEND AND PALO ALTO NETWORKS JOINT SOLUTION

With the joint solution, customers can detect and defend against advanced threats by automating a Palo Alto Networks initiated quarantine from the Attivo ThreatDefend Platform based on suspicious activity and the severity of the attack. The combination of Palo Alto Networks with the Attivo solution 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.

The ThreatDefend platform uses deception and concealment technologies to hide and restrict access to sensitive or critical data while misdirecting attackers to decoys for detection and engagement to collect adversary intelligence. These capabilities provide an organization with the means to quickly identify an attacker and pass the information onto an active defense to stop them in their tracks.

The Attivo ThreatDefend platform seamlessly integrates with Palo Alto Networks next-generation firewalls to provide the needed intelligence to block infected nodes from gaining Internet access and exfiltrating valuable company data. Once the platform identifies an infected node, it sends the IP address to the Palo Alto Networks next-generation firewalls through APIs to enforce policies. The firewalls then quarantine the devices, stopping any communication with Command and Control (C2), and preventing any data exfiltration.

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.

ATTIVO NETWORKS THREATDEFEND PLATFORM

The ThreatDefend Platform creates an active defense against attackers using its many modular components. The Attivo BOTsink® deception servers provide decoys, the Informer dashboard for displaying gathered threat intelligence, as well as the ThreatOps® incident response orchestration playbooks.

The Endpoint Detection Net suite includes the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The ThreatDirect deception forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

SUMMARY

The Attivo ThreatDefend Platform alongside Palo Alto Networks empowers organizations with an active defense platform that provides real-time attack detection and critical time advantage, which organizations can use to prevent an attacker from exfiltrating data or causing other harm. With the automated attack information delivery, organizations can promptly and efficiently quarantine and remediate infected systems as part of their incident response program.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and attack detection across endpoints, Active Directory (AD), clouds, and networks. Concealment technology hides critical AD objects, data, and credentials, while misdirection and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership.

www.attivonetworks.com

ABOUT PALO ALTO NETWORKS

The Palo Alto Networks® Security Operating Platform prevents successful cyberattacks through intelligent automation. Our platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection, and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners deliver consistent security across clouds, networks, and mobile devices, natively providing the right capabilities at the right place across all stages of an attack lifecycle.

www.paloalonetworks.com