Attivo Networks and Palo Alto Networks

Firewall Integration that Automatically Blocks and Quarantines Infected End-points

Highlights

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

A modern day adaptive security approach requires a blend of prevention and detection solutions. Prevention and detection solutions will protect an organization by blocking and quarantining against known and unknown threats. With the increase in zero day, stolen credential, insider, and phishing attacks, threat actors will find a way to bypass even the most sophisticated security prevention systems.

The Challenge

The manual sharing of information between detection and prevention systems can cause delays in isolating an attacker from infecting other systems or blocking data from exfiltrating a company. This situation can be compounded when an attacker chooses to launch an attack during non-business hours or in organizations with limited IT resources.

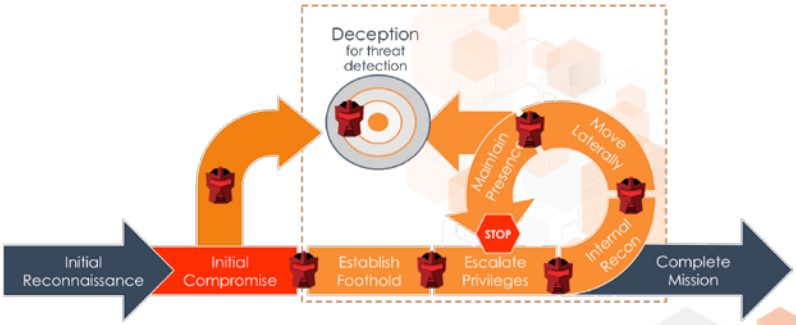
The Joint Solution

Detection provides the next line of defense for BOTs and APTs that have made their way inside the network and are seeking out ways to escalate privileges and launch an attack. Using technology such as deception, which is not reliant on signatures or known attack patterns, provides the visibility needed to promptly detect these threats inside the network and the ability to analyze and identify them in order to pass back the forensic attack information required to stop an attacker in their tracks.

Attivo Networks ThreatDefend Deception and Response Platform

A comprehensive security solution must include inside-the-network threat detection as a next layer of defense in today's security infrastructure. The ThreatDefend™ Deception Platform brings a new complementary layer of security by accelerating breach discovery and providing an additional line of defense designed to make it difficult for attackers to reach or compromise valuable assets.

The ThreatDefend Deception Platform is an elegant way to trap the BOTs and APTs that bypass perimeter and endpoint security. Additionally, the platform provides the full Techniques Tactics and Procedures (TTP) with associated forensics (IOC, STIX, CSV & PCAPs) for fast remediation. API access to this data enables it to publish to existing network security infrastructure.



Joint Solution Brief

© 2017 Attivo Networks. All rights reserved.

About Attivo Networks

Attivo Networks® provides the 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 Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, Palo Alto Networks' game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.

Attivo NETWORKS

paloalto NETWORKS

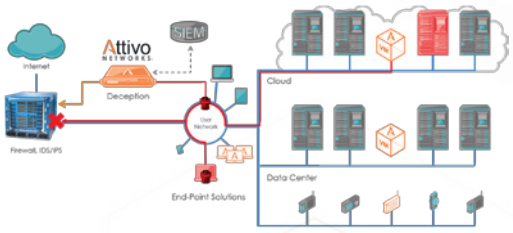
Joint Solution Brief

Attivo Networks ThreatDefend Deception Platform and Palo Alto Networks Next-Generation Firewall

The ThreatDefend Platform seamlessly integrates with the Palo Alto Next-Generation Firewall to provide the needed intelligence to block the infected nodes from gaining Internet access and exfiltrating valuable company data. Once the ThreatDefend platform identifies an infected node, its IP address is sent to the Next-Generation Firewall through its API for policy enforcement; quarantining the device, stopping any communication with the Command and Control (CNC) and preventing any data exfiltration.

The ThreatDefend platform will provide a full coverage attack surface to engage the attack during its discovery and lateral infection phase (as the BOT/APT probes and scans the network looking for high-value targets) or during a targeted attack. The BOTsink decoys are real operating systems based on Windows XP, 7, 8, 10, 2008, 2012 Servers, CentOS, and Ubuntu. In addition, the BOTsink decoys host various applications and protocols including Apache, SNMP, SMTP, File Shares, MySQL, etc. The BOTsink solution supports "golden image" customization to match an organization's network or datacenter environment, and allow customers to import their virtual machines to deploy as a decoy.

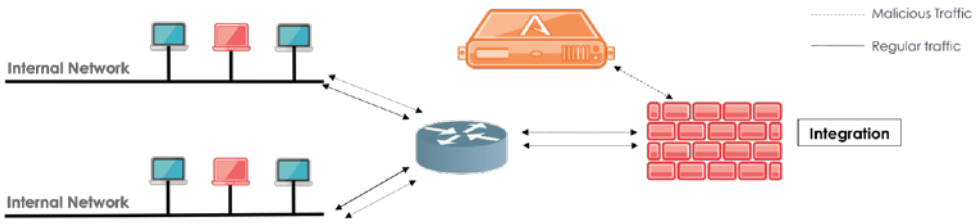
The integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, eliminating the opportunity for an attacker to exfiltrate valuable company assets and information.



Summary

The integration of prevention and detection solutions provides organizations with real-time detection of attackers and a critical time advantage, which can be used to block an attacker from exfiltrating data or causing other harm. With the automated delivery of attack information, organizations are empowered to promptly and efficiently quarantine and remediate infected systems as part of their incident response program.

The value of this integration is quite high. In 2015 alone, over one billion of records were stolen with personal impact to individuals and in many cases damage to the company's reputation and balance sheet. Today's security posture requires organizations to take an assumed breach stance and that they need to be prepared for intrusions that will occur.



© 2017 Attivo Networks. All rights reserved.
Attivo Networks, ThreatDefend, and ThreatPath are registered trademarks of Attivo Networks, Inc. All other trademarks are of their respective companies.