Attivo Networks Deception Platform Integration with ForeScout CounterACT®

Highlights

- Real-time Threat Detection
- Attack Analysis and Forensics
- Automated Quarantine and Blocking
- Expedite Incident Response
- End-point Deception Credentials Distribution

Attivo Networks has partnered with ForeScout Technologies, Inc. to provide real-time attack detection and to improve incident response and remediation through automation to block and quarantine infected endpoints. With this joint solution, customers are provided the choice to review alerts and make manual updates or alternatively to create policies to automatically block endpoints based on suspicious activity. Customers will benefit from the reduction of time and resources required to detect threats, analyze attacks, and to remediate infected endpoints, ultimately reducing the organization's risk of breaches and data loss.

The Challenge

Cyber attackers have repeatedly proven that they can and will get inside the networks of even the most security-savvy organizations. Whether the attacker finds their way in through the use of stolen credentials, zero-day exploitation, a ransomware attack or simply start as an insider, they will establish a foothold and will move laterally throughout the network until they can complete their mission.

Once attackers bypass the existing security prevention mechanisms they can easily move around the network undetected by existing security solutions. To quickly detect and shut down these attacks, a new approach to security is needed. This approach focuses on the threats that are inside the networks and does not use typical measures such as looking for known signatures or attack pattern matching. This new method to detect attacks uses deception to deceive attackers into revealing themselves and once engaged, can capture valuable attack forensics that can be used to promptly block the attacker from continuing or completing their mission.

Changing the Game

A modern day adaptive defense requires a blend of prevention and detection solutions. The Attivo Deception Platform is a highly efficient detection solution that uses deception and decoy techniques to entice engagement with WWW Robots (BOTs) and Advanced Persistent Threats (APTs) that are inside networks and are seeking ways to escalate privileges and launch their attack. The Attivo Deception Platform is designed to catch all threat types that have bypassed even the most sophisticated prevention systems. Using deceptive credentials, lures, and deceptive systems deployed throughout the network, the Attivo BOTsink solution will detect and identify the attacker and will generate detailed attack forensic information. Through integration
with ForeScout CounterACT, the BOTsink will automatically provide the attack information required to block and quarantine the infected endpoint to stop any exfiltration of data or lateral movement of the attacker, which would be used to infect additional systems.

Joint Solution Brief

"Two thirds of respondents said most cyber threat information is not timely enough by the time it's shared"

Ponemon Second Annual Study on Exchanging

Cyber Threat Intelligence: There Has to Be a Better Way

Attivo NETWORKS

ForeScout

Joint Solution Brief

The Joint Solution

The integration of CounterACT with the Attivo Deception Platform is very simple to set up and in minutes, organizations can have an integrated adaptive security platform that provides effective prevention, real-time detection of cyber attackers, and the ability to automatically block and quarantine infected systems so that data is not exfiltrated or additional endpoints infected.

Attivo Networks Deception Platform

A critical part of an adaptive defense security system, the Attivo Networks Deception Platform provides the inside-the-network threat detection as an additional line of defense designed to make it difficult for attackers to reach or compromise valuable assets.

The deception platform will detect threats from all threat vectors including targeted, stolen credentials, ransomware, phishing, and insider attacks. Detection can start at the point of initial reconnaissance or scanning of the network through to detecting the lateral movement of an attacker as they look to escalate privileges and move laterally. With early detection, attack attempts to breach the network are detected and provide organizations the notice and time to deflect and stop the attack.

The Attivo Deception Platform is comprised of two core products.

1. The BOTsink® Engagement Server provides a complete attack surface to engage the attacker during the discovery and lateral infection phase of an attack which provides the deception decoys, lures, analysis engine, and threat reporting. The engagement server is designed to replicate the production environment and lure attackers into engaging before they discover the targeted production assets. The solution runs real operating systems and services can be completely customized to match the environment—whether it be a typical corporate networked server or endpoint—through to mimicking ICS- SCADA and medical devices. Additionally, the platform provides the full Techniques Tactics and Procedures (TTP) with associated forensics (IOC, STIX, CSV & PCAP) for fast remediation.
2. The Attivo End-point Deception Suite adds in additional lures to deceive and trap attackers. The suite includes the lures designed to look like employee credentials, target drives for ransomware attacks, and other deceptive bait.

Attivo Networks BOTsink and ForeScout CounterACT Integration

The integrated solution provides a real-time, non-disruptive way of detecting and blocking BOTs and APTs inside the network, closing the opportunity for an attacker to exfiltrate valuable company assets and information. Automation of remediation is becoming critically important as malware lateral movement speeds increase. The combination of the BOTSink Engagement Server and CounterACT provides real-time remediation capabilities that outperform systems that depend upon manual intervention.

Set up time: Typically only takes a few minutes.

1. Start by configuring the BOTSink Engagement Server to treat the CounterACT system as a Syslog server.
2. Set high and medium severity events to be automatically sent to CounterACT.

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

Attivo NETWORKS®

ForeScout®

Joint Solution Brief

3. Install Attivo plugin in for CounterACT Enterprise Manager Console
4. This immediate response to attack detection can mean the difference between remediation of a single infected endpoint and a catastrophic event where entire network segments are affected. Some recent ransomware has been seen to replicate in less than a minute. Can your enterprise afford to wait to take action?

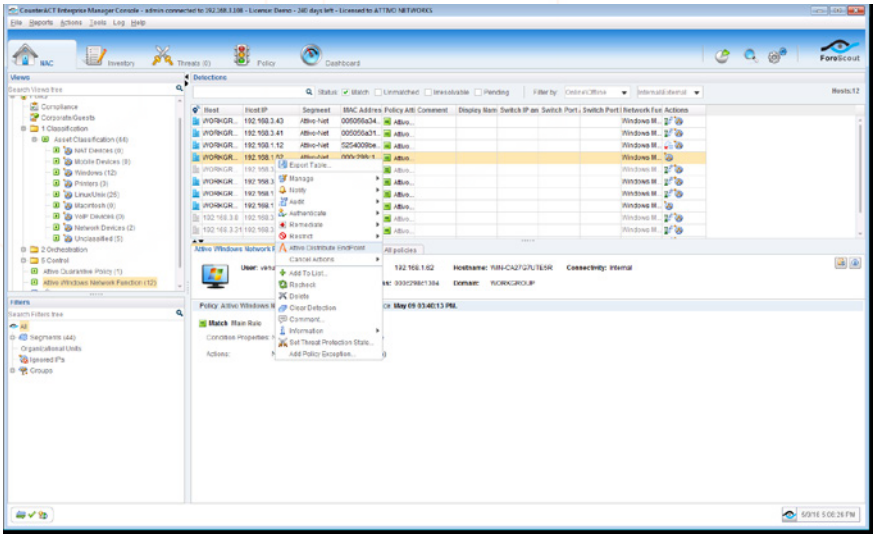
Attivo Networks End-Point Deception Suite Deployment using ForeScout CounterACT

CounterACT plays an important role in simplifying the large-scale deployment of the End-Point Deception Suite. To deploy the End-point Deception Suite using CounterACT, an administrator simply creates a policy in CounterACT to install and define criteria in that policy to automatically install deceptive lures on your endpoints.

For example, a policy can require deceptive lures to be installed on corporate Windows endpoints. Similarly, you can also define policies in CounterACT to uninstall deceptive lures. In addition, it is possible to enable automatic installation of deceptive lures by configuring a policy in CounterACT on a newly detected endpoint in the NAC tab of CounterACT.

Once the IRES credentials are installed, configure CounterACT as follows:

1. Select NAC → All Hosts in the CounterACT console, and right-click on the required endpoint.
2. Select Attivo Distribute EndPoint to install deceptive lures on the selected endpoint.



About ForeScout Technologies

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of January 2016, more than 2,000 customers in over 60 countries improve their network security and compliance posture with ForeScout solutions.

Attivo NETWORKS

ForeScout

Joint Solution Brief

Summary

Automation of remediation that allows for blocking of on-going attacks through the integration of preventative and detection solutions can dramatically shorten the time to resolve breaches. This is best accomplished by combining the technologies of intrusion prevention, Network Access Control (NAC) and deception systems. Attivo Networks deception technology allows for the identification of reconnaissance activities that are often the first step in a sophisticated breach strategy. Configuring CounterACT to integrate with BOTSink Engagement Server is simple and effective.

By identifying the source of breach attempts, the BOTSink Engagement Server can be configured to send alerts of compromised endpoints directly to CounterACT. Policies configured in CounterACT can then automatically quarantine the endpoint by 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. High-severity attacks may not afford security teams the benefit of time to react to these alerts. Automation of blocking and quarantining gives back the advantage to the security team and will help contain the attack before mass damage or exfiltration can be done.

The need for this integration is urgent. In 2015 alone, over one billion sensitive records were stolen with detrimental impact to individuals and enterprises. The resulting damage to the company's reputations and balance sheets has reached into the billions of dollars.