ATTIVO NETWORKS THREATDEFEND® PLATFORM INTEGRATION WITH CISCO SYSTEMS PROTECTS THE NETWORK

INTRODUCTION

Attivo Networks® has partnered with Cisco Systems to provide advanced real-time inside-the-network threat detection, attack analysis, and improved automated incident response to block and quarantine infected endpoints.

THE CHALLENGE

Network, system, and data compromises are occurring at an unrelenting pace, and organizations across all industries are seeking innovative solutions to protect themselves. Security professionals understand that they have detection gaps inside their networks and face mounting concerns about their ability to quickly detect and stop attackers before they can cause too much damage.

Whether the attacker finds their way in through stolen credentials reuse, zero-day exploitation, ransomware attacks, or start as an insider, they will establish a foothold and move laterally throughout the network until they complete their mission. Once attackers evade the existing prevention mechanisms, they can easily move around the network undetected by the security solutions in place. Organizations need a new approach to security to quickly detect and shut down these attacks, one that focuses on the threats that are inside the network and does not rely on typical measures such as looking for known signatures or matching attack patterns. This new method to detect attacks deceives threats into revealing themselves and, once they engaged, can capture valuable attack forensics for security teams to use to block the attacker quickly from continuing or completing their mission.

HIGHLIGHTS

- Real-time Threat Detection
- Automated Quarantine and Blocking
- Expedited Incident Response
- Cross-platform Information Sharing
IN-NETWORK THREAT DETECTION

Organizations are actively turning to deception technology as the preferred security control for early and accurate detection of in-network threats. Some are first-time adopters, drawn to the accuracy and efficiency of the solution, while others are migrating off homegrown honeypot technology for additional accuracy and operational efficiency. Deception technology works by turning the network into a web of sensors with a maze of misdirection that tricks an attacker into engaging and revealing their presence. With the solution in the network, attackers only need to make one small engagement mistake to reveal their presence. By being present at both the network and endpoint layers, the solution blankets the network with lures and traps designed to attract and engage an attacker during reconnaissance, lateral movement, while harvesting credentials, or when seeking to compromise Active Directory. It also addresses alert and log fatigue by only generating engagement-based alerts substantiated with threat and adversary intelligence.

Advanced distributed deception platforms also save time and energy by providing automated analysis of each attack. It captures the attacker’s Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs) and provides valuable, actionable, company-centric intelligence of the attack to improve incident response and network defense postures.

THE ATTIVO THREATDEFEND AND CISCO JOINT SOLUTION

The ThreatDefend platform, recognized as the industry’s most comprehensive deception solution, includes the Attivo BOTsink® deception servers for decoys, ThreatOps® incident response orchestration playbooks, and the Informer dashboard for adversary intelligence; and the Endpoint Detection Net suite, composed of the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, and ADSecure for Active Directory defense. ThreatDirect virtual forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) adds enterprise-wide deception fabric management. Together, these solutions create a comprehensive early detection and continuous threat management defense against information security threats. The BOTsink server and the EDN solution are the components that integrate with the Cisco solutions.

The Attivo Networks BOTsink server improves security in enterprise networks as well as private and public data centers by identifying in-network threats and infected devices in real-time. The Attivo BOTsink solution creates a decoy engagement environment that lures attackers into interacting with decoys before they can infiltrate company production servers. The BOTsink solution creates mirror-matching decoys based on the production environment, including Cisco IOS decoys, to attract and engage attackers so it can collect forensic information about the infected endpoint, attacker IP address, and the methods and tools that an attacker is using. Frictionless in its deployment, the BOTsink solution easily scales to detect threats in the enterprise network either on-premises, in cloud environments, or at remote locations. The BOTsink server decoys detect lateral movement, network discovery, and many other targeted attack activities.
The EDN suite includes deceptive credentials, mapped network shares, ransomware mitigations, and Active Directory deceptions that lead attackers to the BOTsink server decoys for engagement. The decoys capture all of the attacker’s activities at the network, memory, and disk levels, including Indicators of Compromise (IOC) and full Tactics, Techniques, and Procedures (TTPs) of the attack. Security teams can install the EDN solution at endpoints from within the BOTsink server’s user interface or through existing software delivery mechanisms for a smooth, frictionless deployment. When an attacker attempts to use these credentials, the BOTsink server raises a high-fidelity alert, enabling the security operations team to take quick incident response actions.

The ThreatDirect solution, available as a virtual machine or a container application, allows organizations to scale their deception deployment to remote and branch offices, cloud environments, and distributed and micro-segmented networks without the need for a local appliance. Because of its modular nature, the solution can run on almost any virtual environment, including the Cisco Catalyst 9000 series devices that can host container applications natively. This feature gives organizations deployment flexibility in how they scale to remote locations.

The integration of the Attivo ThreatDefend platform with multiple Cisco solutions gives organizations real-time detection of cyberattacks and detailed forensics to proactively prioritize and address critical issues for prompt response, information sharing, and remediation.
THREATDEFEND PLATFORM INTEGRATION WITH CISCO ISE

The Cisco Identity Services Engine (ISE) is a solution to streamline security policy management and reduce operating costs. With Cisco ISE, organizations can see users and devices controlling access across wired, wireless, and VPN connections to the corporate network. Cisco ISE allows organizations to provide highly secure network access to users and devices. It provides visibility into network activities, such as connected users and systems, installed or running applications, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities, with integrated solutions from Cisco technology partners to identify, contain, and remediate threats faster.

The ThreatDefend platform and Cisco ISE integrate to offer customers a collective defensive solution that provides detection of real-time threats, gathering of attack analysis, manual or automated blocking of attacks, and quarantining of endpoints based on suspicious activity. The combined solution also offers a centralized portal for easy blocking of infected endpoints. Together, the solution enables continuous threat management through early detection, analysis, and remediation capabilities.

A vital part of the ThreatDefend platform, the BOTsink solution includes distributed decoy systems based on real operating systems and services for the highest levels of authenticity. The server deploys the decoys across the network to lure the attacker into engaging. Once engaged, the attack continues to play out safely in the BOTsink server’s engagement environment, which in turn identifies the infected endpoints and attacker IP addresses. It also generates attack signatures to send on to the Cisco pxGrid platform automatically. The BOTsink server then initiates endpoint policies through the ThreatOps solution to enforce the automated blocking and quarantining of the devices. This function prevents the attacker from completing their mission and provides organizations with an efficient solution to detect and respond to active cyberattacks quickly.

CISCO ISE INTEGRATION TO AUTOMATICALLY QUARANTINE INFECTED END-POINTS

Attivo ThreatDefend platform with the Cisco ISE platform allows customers to shorten response time with detailed insight provided by actionable dashboards with advanced queries and reports.

ATTACK DETECTION AND BLOCKING

- BOTsink detects attacks and raise an alert
- BOTsink sends IP to Cisco ISE to block
- Cisco ISE blocks all traffic originating from Threat IP
THREATDEFEND PLATFORM INTEGRATION WITH CISCO ASA AND FTD

Cisco’s Adaptive Security Appliance (ASA) Software is the core operating system that powers the Cisco ASA family of security devices. It delivers enterprise-class firewall and VPN capabilities and integrates with Cisco Intrusion Prevention System (IPS), Cisco Cloud Web Security, Cisco Identity Services Engine (ISE), and Cisco TrustSec for comprehensive security solutions that meet continuously evolving security needs. Cisco’s Firepower Threat Defense (FTD) is a unified software image, which includes the Cisco ASA features and FirePOWER Services. This unified software is capable of offering the function of ASA and FirePOWER in one platform, both in terms of hardware and software features. The Firepower Management Console (FMC) administers FTD to provide simplified management and operations of Cisco Next-Generation firewalls. FMC consumes feeds from ISE through pxGrid and forwards the information to FTD.

QUARANTINING INFECTED ENDPOINT

Integration between the Attivo ThreatDefend platform and Cisco ASA or FTD is simple to set up and takes minutes to complete, like the Cisco ISE configuration. The process begins with the ThreatDefend Platform identifying an attacker that has evaded traditional prevention systems and has started to infect machines on the network. Once the attacker engages with the decoys, they analyze the attack and let it safely play out in an isolated environment.

Detailed attack forensics including signatures and attack patterns can be relayed from the Attivo ThreatDefend platform to the Cisco ASA or FTD device which allows organizations to automate blocking to prevent exfiltration of their valuable data.
THREATDEFEND PLATFORM INTEGRATION WITH CISCO PXGRID

The Cisco Platform Exchange Grid (pxGrid) fosters communication with multiple security products to share data and work together. This open, scalable, and IETF standards-driven platform helps automate security to get answers and contain threats faster. Cisco pxGrid uses one API for open automated data sharing and control to support an entire ecosystem of dissimilar IETF standards-track technologies work together through a single interface, allowing for rapid visibility and threat containment via Cisco ISE.

PXGRID INTEGRATIONS

Cisco pxGrid provides a common transport language between the various network and security systems in the IT environment. Eliminating the need for each system to rely on single-purpose APIs, they can all seamlessly integrate with pxGrid to share contextual information. Intersystem communications occur automatically and immediately with no manual intervention required. Cisco pxGrid enables multivendor, cross-platform network system collaboration among multiple parts of the IT infrastructure. This function allows for IT and security vendors to use pxGrid to share context with other Cisco platforms that use it, as well as with systems from any other pxGrid ecosystem partner.

Organizations benefit from the value of the Attivo ThreatDefend platform integration with Cisco pxGrid via the sharing of IOCs with other partner solutions and initiating Cisco ISE quarantines.
THREATDEFEND PLATFORM FEATURES FOR CISCO INTEGRATIONS

The ThreatDefend platform offers several features to enhance deception functionality with specific Cisco products. The BOTsink server can project Cisco IOS router and switch decoys, allowing organizations to plant IT infrastructure decoys in the network to mislead attackers. When the attacker engages with the router decoys, it captures all the commands they enter through the command-line interface, giving valuable intelligence about the attacker’s tactics, techniques, and procedures.

The EDN suite includes credentials, mapped shares, and ransomware bait. The deceptive credentials are username and password combinations stored on endpoints. They are indistinguishable from production credentials and lead attackers to the decoys on the network rather than production assets. When an attacker compromises the endpoint and steals the credentials, they will follow them to the decoys and engage. Since the BOTsink solution can project Cisco IOS decoys, the ThreatStrike credentials can appear as router credentials and stored where attackers can steal them.

REMOTE DEPLOYMENT WITH CISCO

- The ThreatDirect solution projects deception to remote branch offices. It acquires IP’s on one or more network segments and tunnels to centralized Attivo BOTsink server for engagement.

- Cisco Catalyst 9000 series switches run the Attivo ThreatDirect solution locally at the remote office.

The ThreatDirect solution is a virtual forwarder mechanism for scaling to remote or branch offices, micro-segmented networks, and cloud environments. Cisco Catalyst 9000 series switches can run the ThreatDirect container application to provide coverage on a per-VLAN basis. This feature allows for scaling the deception fabric to remote sites with the existing infrastructure already in place, giving coverage across the entire enterprise.
SUMMARY

The Attivo ThreatDefend Platform plays a critical role in empowering an active defense with in-network threat detection and native integrations to accelerate incident response dramatically. Together, Attivo Networks and Cisco provide joint customers with significant improvement in their active defense strategy.

Information sharing and incident response automation to block and quarantine an active attack can dramatically reduce the risk and impact of a potential breach. The Attivo Networks ThreatDefend platform allows for the real-time detection and identification of reconnaissance activities and early lateral movement infections that are often the first step in a sophisticated breach strategy. Configuring BOTsink engagement servers to integrate with the Cisco pxGrid, ISE, ASA, and FTD delivers an effective and efficient solution for early threat detection, prompt incident response, and the derailing of cyberattacks. The added Cisco-based deception features further aid in authenticity and comprehensive coverage. Together, Attivo Networks and Cisco Systems can increase network defenses in an operationally efficient manner.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides organizations of all sizes with an active defense for early and accurate threat detection. The Attivo ThreatDefend® Platform delivers comprehensive detection for on-premises, cloud, and specialized attack surfaces with a deception fabric designed to efficiently misdirect and reveal attacks from all threat vectors. High-fidelity alerts are backed with company-centric threat intelligence, automated attack analysis, and forensics; native integrations streamline incident response. The company has won over 130+ awards for its technology innovation and leadership.

www.attivonetworks.com

ABOUT CISCO SYSTEMS

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected.

www.cisco.com