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 end-points.

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 off as an insider, they will establish a foothold and move laterally throughout the network until they complete their mission. Once attackers bypass 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 uses deception to deceive threats into revealing themselves and once engaged, can capture valuable attack forensics that can be used 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
DECEPTION FOR 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 deception technology 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 deception in the network, the attacker need only make one small engagement mistake to reveal their presence. By being present at both the network and endpoint layers, deception technology 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. Deception also addresses alert and log fatigue by only generating engagement-based alerts that are substantiated with threat and adversary intelligence.

Advanced distributed deception platforms also save time and energy by providing automated analysis of each attack, capturing the attacker’s Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IoCs); and by providing valuable, actionable, intelligence of the attack for improved incident response and to better fortify the network.

THE ATTIVO THREATDEFEND AND CISCO JOINT SOLUTION

Recognized as the industry’s most comprehensive deception solution, the ThreatDefend platform is comprised of the Attivo Networks BOTsink® deception servers, ThreatStrike™ endpoint deception suite, ThreatPath™ for attack path visibility, ThreatOps™ for repeatable response playbooks, DecoyDocs™ for data loss tracking, ThreatDirect™ for deployment flexibility in micro-segmented, remote, cloud, or branch environments, and the Attivo Central Manager (ACM) for enterprise deception and threat intelligence management. Together, these solutions create a comprehensive early detection and continuous threat management defense against information security threats. The BOTsink solution and the ThreatStrike suite are the main integrations with Cisco solutions.

The Attivo Networks BOTsink deception solution 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 is based on a deception engagement server that lures attackers into engaging before they can infiltrate company production servers. The BOTsink solution uses dynamic application and server-level deception techniques, including the ability to deploy 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 and in private and public cloud environments. The BOTsink deception servers are also designed to detect both reconnaissance and targeted attacks.

The ThreatStrike Suite includes deceptive credentials, lures, and mapped drives for ransomware attacks that bait and lead the attacker to the BOTsink solution engagement server. The engagement server captures the Indicators of Compromise (IoC) and full Techniques, Tactics, and Procedures (TTPs) of the attack. Security teams can install
the ThreatStrike Suite at endpoints within the BOTsink solution user interface or through existing software delivery mechanisms for easy, frictionless deployment. When an attacker attempts usage of these credentials, the BOTsink solution raises a high-fidelity alert, enabling the security operations team to take quick incident response actions.

Offered as a virtual machine or a container application, the ThreatDirect solution allows organizations to scale their deception deployment to remote and branch offices, the cloud, and to 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 ISR 4000, ASR 1000, and Cisco Catalyst 9000 series devices that run a hypervisor and can host VMs natively. This 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 what is happening in the network, such as who is connected, which applications are installed and running, 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 are integrated to offer customers a collective defense 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 that allows 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 solution is dispersed across the network to lure the attacker into engaging with it. Once engaged, the attack continues to play out safely in the BOTsink solution’s deception environment, which in turn identifies the infected endpoints, the attacker IP address, and generates attack signatures to automatically send on to the Cisco pxGrid platform. The BOTsink platform will then initiate endpoint policies through the ThreatOps solution to enforce the automated blocking and quarantining of the devices. This prevents the attacker from completing their mission and provides organizations with an efficient solution to quickly detect and respond to active cyberattacks.

CISCO ISE INTEGRATION TO AUTOMATICALLY QUARANTINE INFECTED END-POINTS

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

Cisco 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 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 can be completed in minutes, like the Cisco ISE configuration. The process begins with the ThreatDefend Platform identifying a threat that has bypassed traditional prevention systems and has started to infect machines on the network. Once the threat engages with the deception decoys, the attack can be safely played out and analyzed in a quarantined 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. Using one API for open automated data sharing and control, pxGrid can help 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 be seamlessly integrated with pxGrid to share contextual information with each other. Intersystem communications occurs 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 enables IT and security vendors to use pxGrid to share context with other Cisco platforms that use pxGrid, 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 DECEPTION

The ThreatDefend platform offers several features to enhance deception functionality specifically with Cisco products. The BOTsink deception server can project Cisco IOS decoys for router and switch deception. Using the IOS decoys allows organizations to plant deceptive router 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 ThreatStrike endpoint deception suite includes credentials, mapped shares, and ransomware bait. The deceptive credentials are username and password combinations stored on endpoints. They are specifically designed to be 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 to be router credentials and stored where attackers can steal them.

REMOTE DEPLOYMENT WITH CISCO

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

- **Cisco ISR 4000, ASR 1000 series routers** and **Catalyst 9000 series switches** run the Attivo **ThreatDirect** solution locally on the remote.

The ThreatDirect solution is a VM forwarder mechanism for scaling to remote or branch offices, micro-segmented networks, and cloud environments. Cisco ISR 4000 series & ASR 1000 series routers support running the ThreatDirect solution within the built-in hypervisor while Catalyst 9000 series switches can run the ThreatDirect container application to provide coverage on a per-VLAN basis. This allows for scaling deception to remote sites with the existing infrastructure already in place, giving deception 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 dramatically accelerate incident response. Together, Attivo Networks and Cisco provide joint customers significant improvement in their active defense strategy.

Information sharing and the automation of incident response, for blocking and quarantining an active attack, can dramatically reduce the risk and impact of a potential breach. Attivo Networks deception technology 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 features that enhance Cisco-based deception further aid in authenticity and comprehensive deception coverage. Together, Attivo Networks and Cisco Systems can increase network defenses in an operationally efficient manner.

**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 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