ATTIVO NETWORKS PARTNER INTEGRATIONS FOR AN ACTIVE DEFENSE

INTRODUCTION

An active security architecture is built upon the four core pillars of prediction, prevention, detection, and response, requiring solutions within each of these categories to share information and automate actions to build a stronger defense, improve policies, and to better meet compliance expectations.

This paper will outline how Attivo Networks® solutions fit into this eco-system to strengthen an organization's overall defense against cyber threats. The Attivo ThreatDefend™ Deception and Response Platform is built to detect in-network threats, disrupt an attack, and to defend against all forms of known and unknown attacks.

PREDICT THE ATTACK

Having a baseline understanding of one's security infrastructure, compliance requirements, associated threat risks, and exposure are first steps in establishing an organization's security posture and preparing for cyber threats. Each company's ultimate "attack score" differs, since some are more targeted due to the value of their information or critical infrastructure. Others may be driven by compliance requirements, noting that fulfilling such criteria should never be mistaken for having a lock-tight security system. Another consideration should be based on factors such as the ability to keep systems updated and, of course, the risk of human error.

DECEIVE. DETECT. DEFEND.

Windows XP-based systems are commonly used in critical infrastructures, which are not easily taken off-line for regular security patch and maintenance updates given their mission-critical nature. This is also compounded by end-of-life cycle product management where systems are often left operating well after a manufacturer stops updating its software.

Human error plays an equal role in creating security backdoors. Sometimes it is simply the mistake of clicking on a suspicious or malicious email or URL. Other times, misconfigurations or inherent use of default or weak passwords provides an entryway for attackers.

The Attivo solution provides organizations the ability to do vulnerability and attack path assessments through ThreatPath™. A common tactic is to use compromised credentials to gain network persistence and move laterally within the network from the initial infection point. The Attivo ThreatPath solution takes an attacker's view of the network and identifies the paths an attacker can take to compromise a target asset. The solution mitigates risks by providing extensive information to highlight incomplete policies and misconfigurations. This offers insight into the greatest points of vulnerability, allowing security teams the ability to place additional detection measures where needed. The ThreatPath solution can be used as a form of continuous testing to understand ongoing risks that arise from network and end-point changes.

PREVENTION

The security fundamentals start with preventing attackers from getting into the network. Typical prevention systems include firewalls, gateways, sandboxes, network access control, endpoint security, and other systems that keep track of attacks and block them from entering the network. Some will use intelligence to look for known patterns or signatures to identify these attacks.

The ThreatDefend Platform extends the value of prevention systems by manually or automatically sharing newly discovered attack information and signatures to block and isolate an attacker. The Attivo solution integrates with major prevention partners through APIs and/or their information sharing platforms. These integrations are fast and easy to set up and manage, either from the Attivo User Interface (UI) or the partner's information sharing platform.

DETECTION

A modern-day security posture assumes the network has been compromised and attackers are already inside. Zero-day exploits, ransomware/malware, stolen credential, man-in-the-middle activity, phishing, and insider compromises are just some of the many ways that an attacker can bypass perimeter security. With the ThreatDefend Deception and Response Platform, organizations gain unparalleled visibility into threats inside their network and into attacker lateral movements and tactics. The platform provides immediate value by detecting advanced threats as they propagate throughout the network, laying strategic decoys and lures to deceive, detect, and defend against attacks as they scan network clients, servers, and services for targets and seek to harvest credentials.

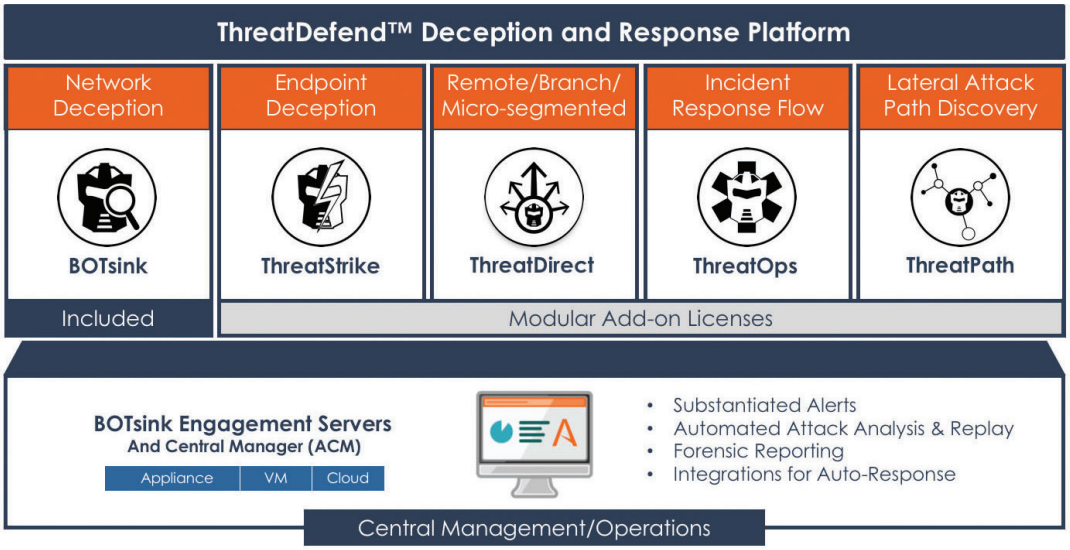
The decoys attract and detect attackers in real-time raising evidence-based alerts while actively engaging with them so that their lateral movement and actions can be safely analyzed. For authenticity, the decoy systems run real operating systems, full services, and applications, along with the ability to completely customize the environment by importing the organization's golden images and applications. As a result, the platform provides a "hall of mirrors" environment that is baited with lures and traps, while making deception decoys completely indistinguishable from company assets.

By inserting deception into all key areas that attackers target for reconnaissance, the deception deployment appears as part of the production environment in multiple layers.

Endpoint deceptions provide easy and highly effective detection against attacks seeking to harvest credentials by redirecting them to deception assets. The platform can even monitor for attempted use of inactive, disabled, or black-listed cloud credentials on partner services. Additionally, high interaction deception can be instrumental in slowing a ransomware attack and providing the time advantage to stop the attack before it can cause extensive damage.

The solution integrates with Active Directory, so deceptive assets are part of any query results the attacker extracts from the servers. This provides visibility if an attacker breaches the AD servers.

The Attivo Adaptive Deception Campaigns apply machine learning to keep the network and endpoint deceptions fresh, for easy deployment, and ongoing maintenance, and can utilize partner integrations or any software delivery mechanism to easily deploy endpoint deceptive credentials. These deceptions can be distributed within all types of networks including endpoints, user networks, server, data center, ROBO, cloud, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications.



RESPONSE

Traditionally, organizations utilize many tools that operate in isolation making it a challenge to quickly respond to an incident. In some cases, an organization must send attack files to vendors to create signatures, causing delays in preventing the attack from spreading. However, when the Attivo solution identifies an attack, it provides immediately actionable information by recording all attacker activity within the environment. The ThreatDefend Deception and Response Platform is designed to simplify and expedite incident response, creating full attack forensic analysis and providing information to promptly block and quarantine the attack.

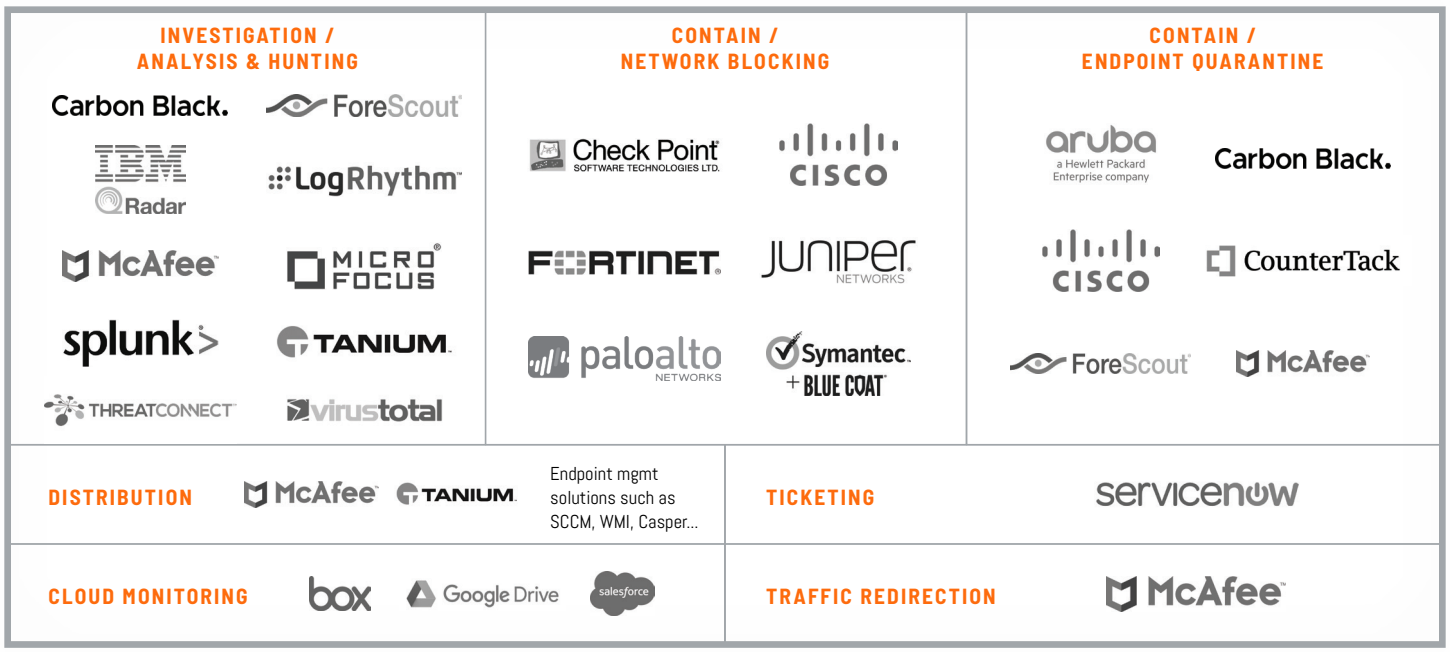
Attack forensic analysis includes information on infected systems and C&C addresses, so that security teams can promptly address the incident. The information also provides the detail to understand what phase in the "Kill Chain" the attacker was in and specifies additional information so that SHA1 and forensic artifacts can be researched in other devices. Integrations with malware database companies, such as VirusTotal, provide additional attack reporting enrichment. Specific partner integrations will even redirect traffic to deception assets for further visibility.

For streamlined incident response, organizations can deploy the Attivo ThreatOps™ solution to build and automate threat defense playbooks. These playbooks are based on integrations with existing security infrastructure and create automated and repeatable incident handling processes. With integrated solutions that enable blocking, network quarantining, network access

control, endpoint isolation, or threat hunting, the playbooks can automate an incident response action from start to finish, including creating IT service tickets for remediation. Because the ThreatDefend Platform has an available API, security teams can access functions from their existing tools, increasing security operations efficiency. By leveraging these automations, organizations reduce the time-to-respond to critical incidents and make it easier for less skilled staff to leverage a playbook to respond to an incident quickly.

ACTIVE DEFENSE PARTNERS

Native integrations for information sharing and automated response



SUMMARY

The Attivo ThreatDefend Deception and Response Platform plays a critical role in empowering an active defense with real-time threat detection, attack vulnerability assessments, attack forensic analysis, and the integrations to dramatically accelerate incident response. Partner technology integrations serve as a force multiplier for existing technologies, processes, and resource productivity. These integrations ultimately reduce the time to detect and respond to a malicious threat actor. Attivo Networks will continue to expand its platform and native partner integrations to deliver the fastest detection and incident response to stop attackers in their tracks.

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