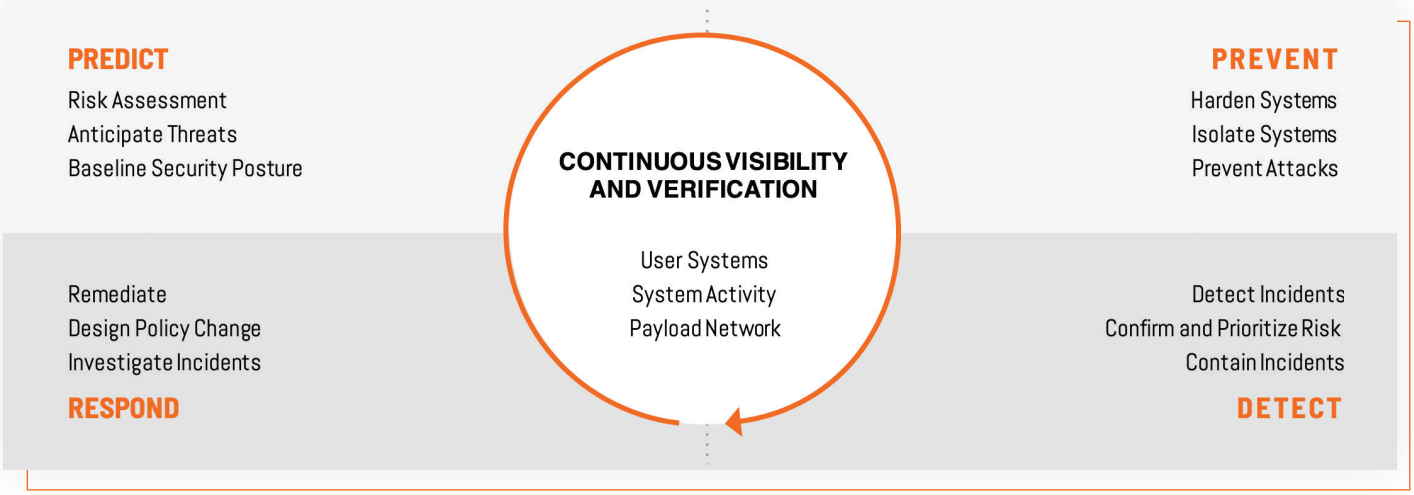
ATTIVO NETWORKS PARTNER INTEGRATIONS FOR AN ACTIVE DEFENSE

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 better meet compliance expectations.

The Attivo Networks® solutions fit into this eco-system to strengthen an organization's overall defense against cyber threats. The Attivo ThreatDefend® Platform detects in-network threats, disrupts an attack, and to defends against all forms of known and unknown attacks.



PREDICTION

A baseline understanding of one's security infrastructure, compliance requirements, associated threat risks, and exposure are the 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 focus on factors such as the ability to keep systems updated and, of course, the risk of human error.

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. End-of-life cycle product management compounds the situation, 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 merely the mistake of clicking on a suspicious or malicious email or URL. Other times, misconfigurations or inherent use of default or weak passwords provide an entryway for attackers.

The Attivo solution provides organizations the ability to do vulnerability and attack path assessments through the ThreatPath® solution. 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 capability offers insight into the most significant points of vulnerability, allowing security teams the ability to place additional detection measures where needed. The ThreatPath solution can act as a continuous monitoring process to understand ongoing and new risks from network and endpoint 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 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 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 that attackers will compromise the network and 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 attackers can bypass perimeter security. With the ThreatDefend Platform, organizations gain unparalleled visibility into threats inside their network and attacker lateral movements and tactics. The platform provides immediate value by detecting advanced threats as they propagate throughout the network during discovery, credential theft, lateral movement, privilege escalation, and data collection activities.

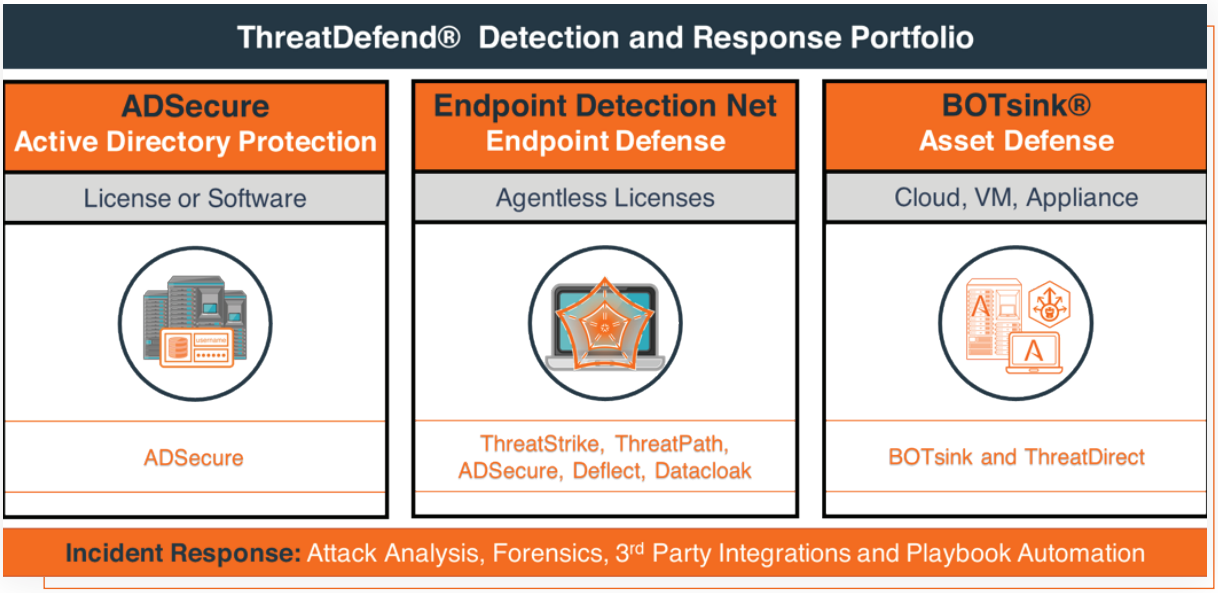
The platform detects attackers in real-time, raising evidence-based alerts while actively engaging with them to analyze their lateral movement and actions safely. The platform protects the organization at the network, on endpoints, and in Active Directory, whether on-premises, in the cloud, or at remote sites. Its deception and concealment technologies hide and restrict access to sensitive or critical data while redirecting attacks to full operating system decoys for engagement.

By operating at all critical areas that attackers target, the platform denies, detects, and derails in-network attacks from the earliest phases of the attack cycle, crippling the attacker's ability to remain undetected.

The Endpoint Detection Net (EDN) suite of products provides easy and highly effective denial, detection, and redirection against attacks targeting the endpoint. The solution identifies credential risks that allow attackers to move laterally between systems, hides

and restricts access to local files, folders, network or cloud-mapped shares, and local administrator accounts to prevent attackers from exploiting them. It also identifies unauthorized Active Directory queries, hiding sensitive objects, and returning decoy data that misdirects the attack to an engagement environment that collects forensics to develop threat intelligence. The EDN suite is particularly effective against ransomware attacks, preventing it from accessing local data, redirecting it to decoy mapped shares, and stalling the attack by feeding the malware endless decoy data to give security teams time to respond to the attack.

The ThreatDefend platform applies machine learning for easy deployment and maintains the freshness of network and endpoint decoys. It can utilize partner integrations or any software delivery mechanism to deploy the EDN suite easily. The components operate within all types of networks, user networks, servers, data centers, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications.



RESPONSE

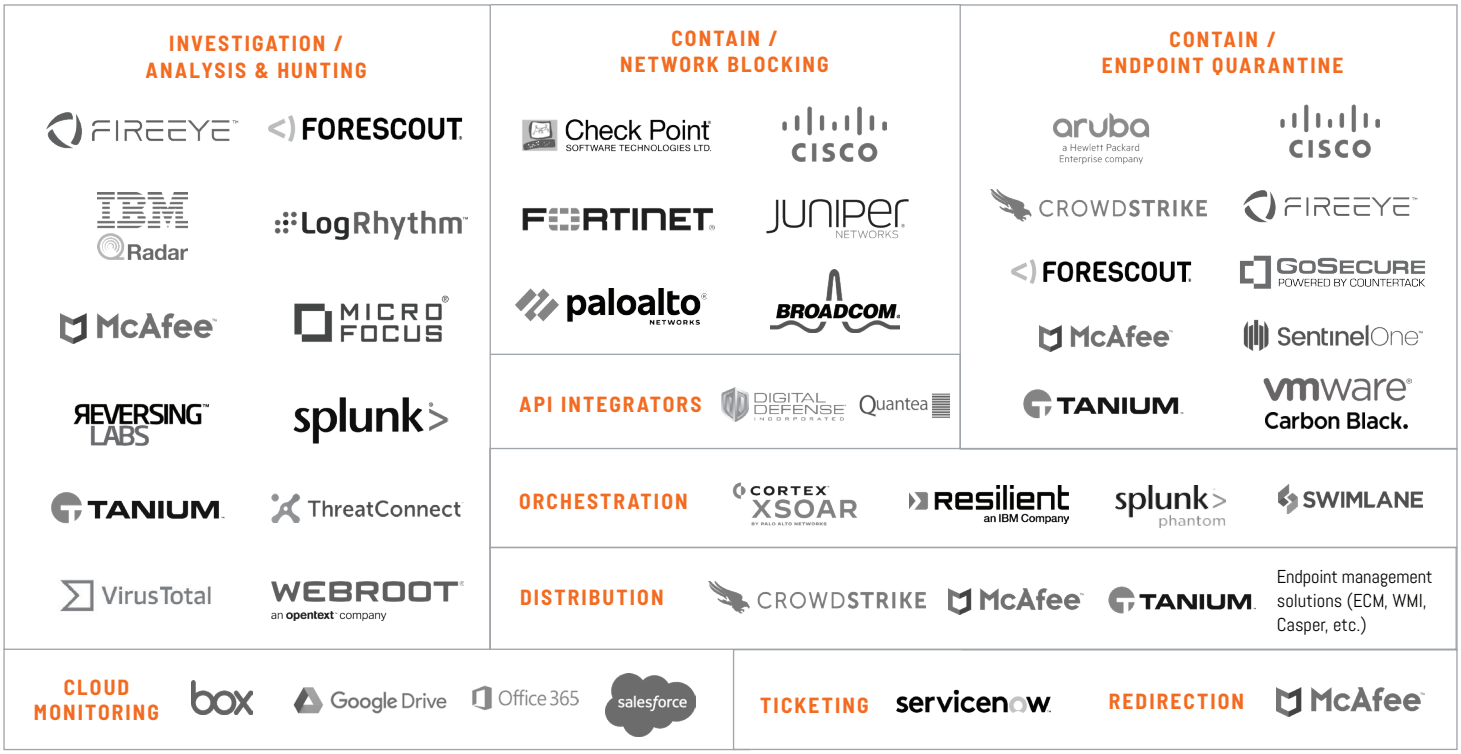
Traditionally, organizations utilize many tools that operate in isolation, making it challenging to respond to an incident quickly. In some cases, an organization must send attack files to vendors to create signatures, causing delays in preventing the attack from spreading. However, when the Attivo solution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

Attack forensic analysis includes information on infected systems and command and control (C2) addresses so that security teams can promptly address the incident. This information also provides the details to identify the tactics, techniques, and procedures (TTPs) of the attacker and specifies additional indicators of compromise (IoCs) to find infections in other devices. Integrations with threat intelligence database companies, such as VirusTotal and Webroot, provide additional attack reporting enrichment. The EDN deflect function redirect traffic to deception assets for further visibility or native endpoint isolation.

For streamlined incident response, organizations can use 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®, the leader in cyber deception and lateral movement attack detection, delivers a superior defense for revealing and preventing unauthorized insider and external threat activity. The customer-proven Attivo ThreatDefend® Platform provides a scalable solution for derailing attackers and reducing the attack surface within user networks, data centers, clouds, remote worksites, and specialized attack surfaces. The portfolio defends at the endpoint, Active Directory and throughout the network with ground-breaking innovations for preventing and misdirecting lateral attack activity. Forensics, automated attack analysis, and third-party native integrations streamline incident response. The company has won over 130 awards for its technology innovation and leadership. For more information, visit www.attivonetworks.com.

ANP0120420
www.attivonetworks.com