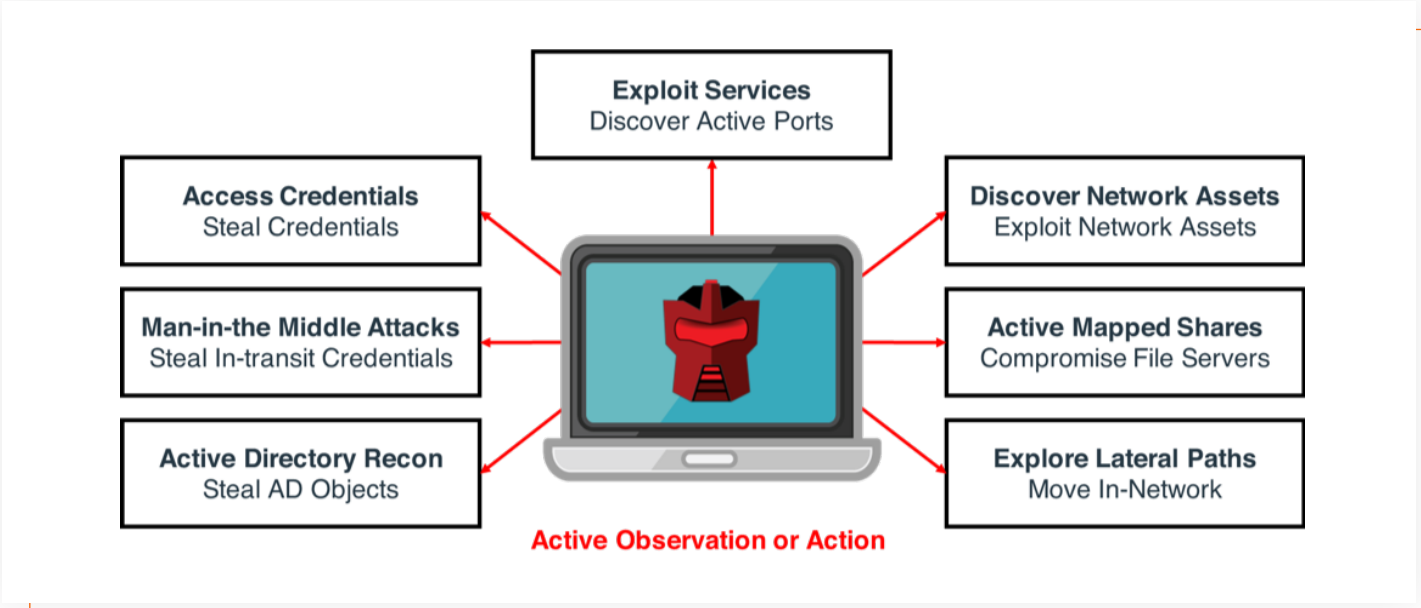
THE ATTIVO NETWORKS ENDPOINT DETECTION NET (EDN) FAMILY OF PRODUCTS

Attackers view every endpoint as a doorway to the inside of the network. Organizations understand this, so they use Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions to defend against attacks. However, advanced attackers have ways to evade these security controls to compromise an endpoint and infiltrate the network. Once inside, they use various tactics to establish a base from which to expand their foothold, many of which EPP and EDR solutions find hard to detect. (see figure 1.) Using these tactics, threat actors move laterally to infiltrate the network to achieve their goals.



The Attivo Networks® Endpoint Detection Net (EDN) solution, part of the ThreatDefend® platform, includes the ThreatStrike® functionality for endpoint threat detection and protection, the ThreatPath® solution for attack path visibility, the ADSecure solution for Active Directory (AD) defense, the Cloaking function to protect data and credentials, and the Deflect function to derail port and service scans. Together, they augment existing endpoint defenses by detecting the tactics and techniques that attackers use to move deeper into the network. Moreover, the solution works to misdirect, misinform, and deny attackers unrestricted lateral movement from the initially infected system. The EDN suite packages these solutions under one license to simplify the buying process. It is available as a standalone solution with the EDN Manager or as part of the ThreatDefend platform, which adds attacker engagement when used with the BOTsink® deception server decoys.

THE EDN MANAGER AND THE THREATDEFEND PLATFORM BOTSINK SERVER

The EDN Manager is a virtual on-premises or cloud appliance that centrally manages and administers the standalone EDN solution. It configures the ThreatStrike, ThreatPath, ADSecure, Cloaking, and Deflect components of the EDN solution and alerts on any interaction with these assets. The EDN Manager offers detection, analysis, visibility, and partner integrations for automated incident response actions and intelligence sharing. The EDN Manager functions identically to the full BOTsink server, but does not offer decoys for engagement or collect the full gamut of forensic evidence of the attacker's activities. Organizations that wish to capture all attacker activity should use the BOTsink server.

The ThreatDefend platform BOTsink server offers a more robust deception solution. Besides managing and administering the EDN components, it also provides full Operating System virtual network decoys as engagement servers that the attacker can interact with as a conventional system. These decoys record all attacker activity at the disk, memory, and network layers for a complete picture of the attack. Organizations can utilize the built-in machine learning to customize these full OS virtual machine decoys, import golden images as decoys, emulate IoT or specialized devices, emulate cloud technology decoys like serverless functions, and even create decoy routers or switches.

THREATSTRIKE® FUNCTION – ENDPOINT PROTECTION AND DEFENSE

Threat actors compromise systems to reach sensitive data by stealing passwords and hashes that they use to move laterally within the network and escalate privileges.
The Attivo Networks ThreatStrike functionality hides and denies unauthorized access to credentials by binding them to applications, preventing unauthorized access. The functionality's deception technology dynamically plants fake credentials, lures, and deceptive network shares onto production endpoints as breadcrumbs to misdirect and mislead attackers, derailing their activities as they try to advance their attack. The Cloaking function hides data, credentials, and AD objects to prevent attacker compromise. The ThreatStrike functionality can also install in service mode to periodically renew the timestamps of the credentials for increased authenticity. When in service mode, it collects forensic information from the endpoint to capture attack activity data in memory.

In standalone EDN mode, the EDN Manager generates alerts when attackers interact with fake credentials, AD objects, and shares. The EDN Manager can then use the deflect functions (described later) or native partner integrations to isolate the infected system.

If the attacker uses the fake credentials on a production system, it will fail and create an alert. When used with the BOTsink server, the ThreatStrike solution decoy credentials, shares, and disinformation also lead to network decoy systems for engagement. Once the attacker interacts with the decoys systems, they record all attacker activity for analysis and threat intelligence development. The BOTsink native integrations also allow for automated isolation of the infected system to accelerate incident response and limit the attacker's ability to move around.

THE THREATPATH SOLUTION – ATTACK SURFACE REDUCTION

The Attivo ThreatPath solution provides continuous attack path vulnerability assessment of likely lateral movement avenues that an attacker would take to compromise a network based on misconfigured systems and misused or orphaned credentials. The solution exposes and provides topographical visual graphs showing the paths an attacker would traverse through the internal network once they engage with their first endpoint system and the locations of systems susceptible to compromise. Clickable drill-downs provide detailed views of the weaknesses and IP addresses for hosts that the organization needs to isolate or fix. They can then use this information to remediate exposures and gain insight into prime locations where they can deploy deceptive credentials. The UI provides actionable insights that work to strengthen policies and prevent attacker lateral movement. Additionally, ThreatPath users gain continuous assessments of the network and are alerted when new paths open to critical assets.

The ThreatPath solution can natively remediate these attack paths or activate integrations with workflow and incident management systems like Service Now and JIRA inside the dashboard. The solution's in-depth data on the compromised asset simplifies incident workflow management, and double-click integrations automate trouble ticket creation and notifications. Customers benefit from visibility into these workflows, closed-loop remediation, and reporting to record compromised systems handling.

The ThreatPath solution operates the same in standalone EDN mode or with a ThreatDefend platform deployment.

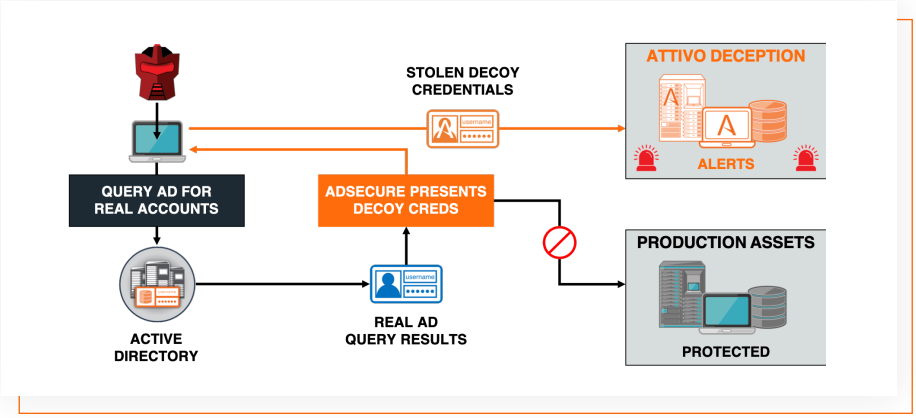
THE ADSECURE SOLUTION – ACTIVE DIRECTORY PROTECTION

The ADSecure solution defends essential Active Directory (AD) objects from an attacker's data gathering activities, such as user and system accounts, privileged groups members, domain controllers, service principal names

(SPNs), and others, without interfering with the production AD environment. The module sits at every endpoint and identifies unauthorized queries to the AD controller, replying with deceptive data, hiding the privileged credentials, and altering real credentials values. The solution also hides local accounts that are members of the Local Administrator group to protect against horizontal privilege escalation. No matter what tool the attackers use, the data they receive misleads them.

When used in standalone EDN mode, the EDN Manager generates alerts and collects all the relevant telemetry from the activity. This data includes the application that executed it and the actual query. The EDN Manager can then isolate the system with the deflect function or the native partner integrations.

With a ThreatDefend platform deployment, the ADSecure module augments the existing AD defense capabilities the platform already offers, such as deceptive credentials based on production accounts and decoy AD servers. In this mode, the ADSecure solution returns AD objects for any unauthorized queries that lead attackers to the BOTsink server network decoys for engagement and forensic collection. The BOTsink server's partner integrations also allow for automated isolation to limit attacker movement.

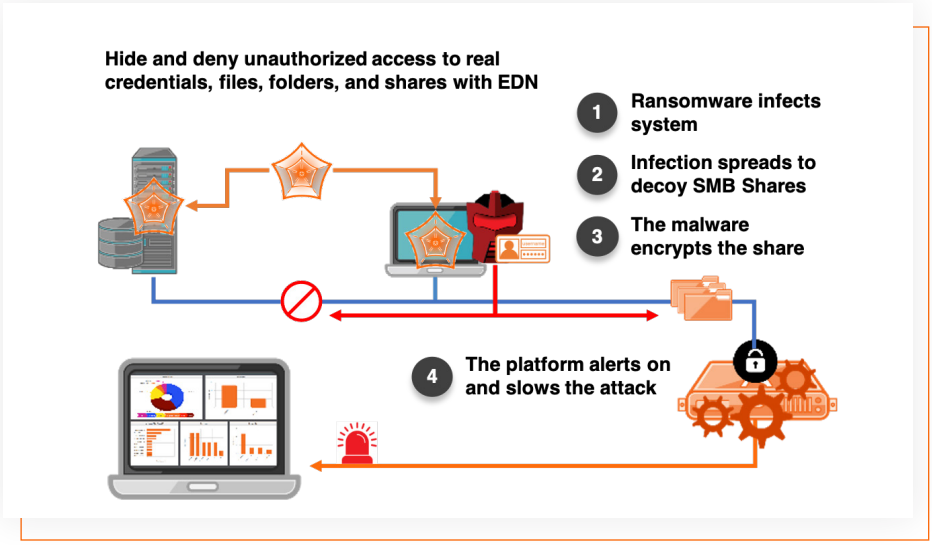


RANSOMWARE MITIGATION – LIMITING DAMAGE AND MOVEMENT

The EDN solution includes technology to mitigate ransomware attacks. This function hides and denies access to credentials, AD objects, production files, folders, and removable media on the endpoint from ransomware discovery, preventing the malware from encrypting user data and limiting its ability to spread via attached storage devices. The solution also hides the production mapped shares on the host and only shows decoy file shares, credentials, and AD objects to the ransomware as it tries to move around the network and encrypt files.

In a standalone EDN solution deployment, the EDN Manager generates alerts for every activity that attempts to enumerate the local files, folders, or tries to move to the shares. It can then isolate the system with the deflect function or the native partner integrations as part of the IR process.

When used with the BOTsink server, these mapped file shares lead to network decoy servers populated with fake data. As the ransomware encrypts the files on the phony file shares, the decoys keep feeding the malware a never-ending stream of data to stall and occupy it, delaying the attack while alerting security teams. Additionally, the BOTsink server has native integrations with existing security solutions that can automatically isolate the infected system to give security teams time to remediate the incident.



DEFLECT FUNCTION – MISDIRECTING AND MISINFORMING ATTACKERS

The EDN solution includes a deflection feature that misdirects attackers attempting to find and connect to host ports and services. This feature also makes it difficult for them to fingerprint systems accurately. Attackers fingerprint systems by sending probes to a host to determine what ports and services it has open and running to identify hosts to compromise. They establish the type of server it is (web server, SMB server, Active Directory controller, FTP server, etc.) and the attacks they can use to compromise its services based on the software versions. For example, a few years ago, attackers targeted SMBv1 with the WannaCry ransomware using the Eternal Blue exploit. The deflect function detects these probes and forwards any traffic that touches a closed port to a different IP address while generating an alert. This function does not interfere with any running services or open ports, so it does not disrupt a production server's functionality.

Because the deflect functions can redirect both inbound and outbound traffic, organizations can use it as a way to isolate a system from the network by redirecting all outbound traffic only to decoy IP addresses, no matter what port. This feature limits all traffic only to decoys for engagement and prevents the attacker from communicating with any production system, in effect quarantining it to the decoy environment only.

In a standalone EDN deployment, the destination IPs are ones that the EDN Manager monitors. It alerts the security team to any traffic that touches these IPs and then closes the communications while optionally isolating the system.

When used in tandem with a BOTsink server in a full ThreatDefend platform deployment, the deflect functions sends the traffic to ports and services on network decoys that the attackers interact with, thinking they are real systems. For example, when the attacker probes for a web server on a system that is not running it, the deflect function forwards the traffic to a decoy web server that responds to the communications as if it was the system the attacker probed. The decoys can then record all of the attacker's activities while alerting the security team and optionally isolate the system automatically with native integrations.

CONCLUSION

The EDN Suite is a powerful solution that adds visibility, protection, and detection to derail attack tactics that evade existing security controls. Whether an attacker is stealing credentials, pulling critical accounts and information from AD, traversing network shares, discovering ports and services to attack, or other activities, the EDN solution reveals these actions and protects against credential misuse, unauthorized access, and subsequent lateral movement at the endpoint. The flexibility of the solution gives security teams an option to deploy it either in standalone mode or as part of a broader ThreatDefend platform deception fabric. The full platform adds forensic collection and other capabilities to the detection functions of EDN. By adding the EDN suite to existing EPP and EDR solutions, organizations can strengthen their endpoint defenses and deny attackers a foothold into the network.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com