USE CASE

Attivo NETWORKS
A SentinelOne Company

ENDPOINT DETECTION NET (EDN) SUITE USE CASES

Now more than ever, it is critical for organizations to protect their endpoints and prevent attackers from spreading throughout the network. Most will use various forms of Endpoint Protection Platforms and Endpoint Detection and Response solutions to defend endpoints from attacks. The Attivo Networks® Endpoint Detection Net (EDN) suite provides capabilities that complement these existing endpoint security solutions. It achieves this by ambushing attackers at the endpoint, detecting them early in the attack cycle, hiding and denying unauthorized credential access, and misdirecting attackers from moving laterally through the network. The EDN suite creates an environment where every endpoint becomes a decoy, designed to disrupt an attacker's ability to break out and further infiltrate the network. It does this without requiring agents on the endpoint or causing disruption to the regular endpoint or network operations. The solution's ability to collect forensic data on all attack activity gives organizations company-centric adversary intelligence to enhance their security posture and strengthen defenses.

The following use cases highlight the capabilities that the EDN suite provides.

PROTECT ACTIVE DIRECTORY (AD) DATA FROM THEFT AND EXPLOITATION

Attackers query AD from an endpoint to extract information on privileged domain accounts, systems, and other high-value objects. They use this information to compromise accounts, elevate privileges, and move laterally to access critical organizational data. The EDN suite returns fake Active Directory results, making an attacker's tools and reconnaissance untrustworthy while redirecting the attacker's focus and efforts into a decoy environment. The organization gains early alerting on attempts to access AD data while obscuring the attack surface, misinforming the attacker, and misdirecting the attack.

PROTECT ENDPOINT CREDENTIALS FROM THEFT AND MISUSE

Attackers steal stored or in-memory credentials to reuse for access to production assets. The EDN suite hides credentials and binds them to applications, stopping an attack early in the process and blocking attackers from gaining unauthorized access. The solution creates deceptive credential lures that breadcrumb attackers into a decoy environment for forensic threat intelligence collection. The organization can then use this adversary intelligence to strengthen defenses.

PREVENT ATTACKERS FROM TRAVERSING AND EXPLOITING MAPPED SHARES

Attackers access mapped shares on the endpoint to compromise the file server (such as with ransomware). The EDN suite creates hidden shares that lead to decoy file servers that alert on the activity while recording it. If the attack involves ransomware, the high-interaction deception occupies the malware, giving the organization time to respond while limiting the damage to decoy files with no production value.

REDUCE THE EFFECTIVENESS OF NETWORK RECONNAISSANCE

Attackers scan network segments and endpoints to find production assets and available services. The EDN suite disrupts attacker discovery attempts to find other systems to compromise by misdirecting port and service discovery scans to network decoys for engagement. These decoys also obfuscate the attack surface with systems that appear identical to production assets.

REDUCE THE ATTACK SURFACE AVAILABLE FOR ATTACKER EXPLOITATION

Attackers leverage stored or orphaned credentials, or endpoint policy misconfigurations to move from system to system. The EDN suite preemptively identifies and remediates these lateral attack paths before attackers can use them, reducing the available attack surface while improving existing defenses.

DETECT AND PROTECT AGAINST MAN-IN-THE-MIDDLE ATTACKS

Attacks conduct Man-in-the-Middle attacks to steal credentials as they traverse the network. The EDN suite detects MitM activity with decoys on every network segment, giving the organization early alerting on the event while feeding attackers fake credentials that lead to decoys. Attempts to use these credentials generate alerts while the decoys collect forensic evidence for later analysis.

SUMMARY

The use cases highlighted above showcase the capabilities that the EDN suite provides for organizations to bridge coverage gaps and improve security. The EDN suite portfolio includes the ThreatStrike® solution for credential concealment, deceptive lures and mapped shares, the ThreatPath® assessment tool to identify credential exposures and lateral paths, the ADSecure module to protect against unauthorized Active Directory queries, and the Deflect function to misdirect port and service discovery scans to decoys. These capabilities provide the means to strengthen existing defenses, detect and alert on attackers as they attempt to move from an endpoint, misinform them as they gather information, and misdirect them to decoys for engagement when deployed with a BOTink® deception server. The solution works in tandem with existing EPP, and EDR controls to defend the endpoint more effectively, acting as a force multiplier to detect and deny attackers the ability to move deeper into the network while remaining undetected.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, a SentinelOne company, provides Identity Threat Detection and Response (ITDR) and cyber deception solutions for protecting against identity compromise, privilege escalation, and lateral movement attacks. Through data cloaking, misdirection, and cyber deception, the platform efficiently prevents attacks across Active Directory, cloud environments, and devices.