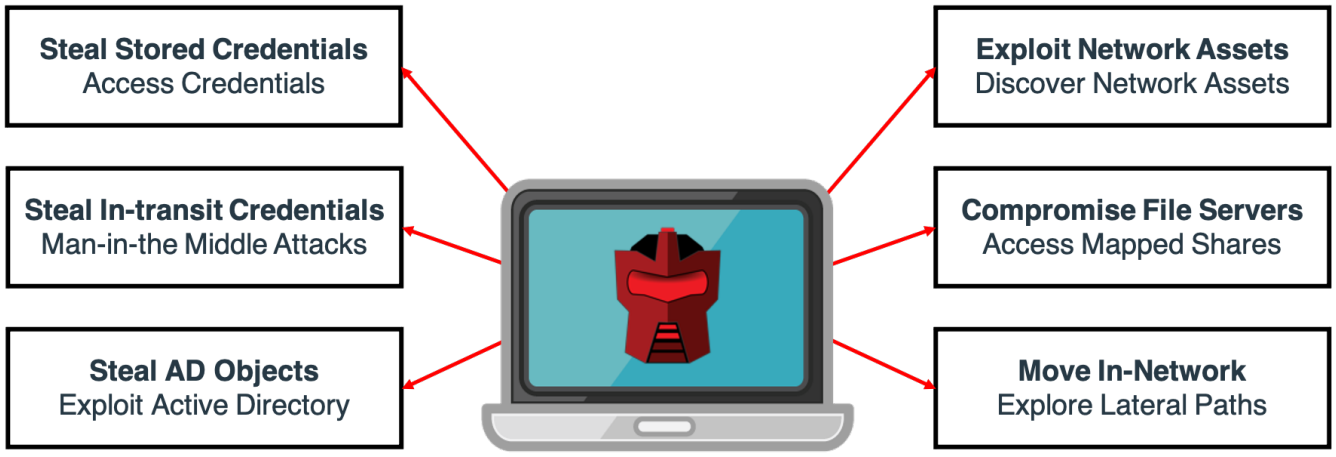
DATASHEET

AMBUSH ATTACKERS AT THE ENDPOINT WITH THE ENDPOINT DETECTION NET SUITE

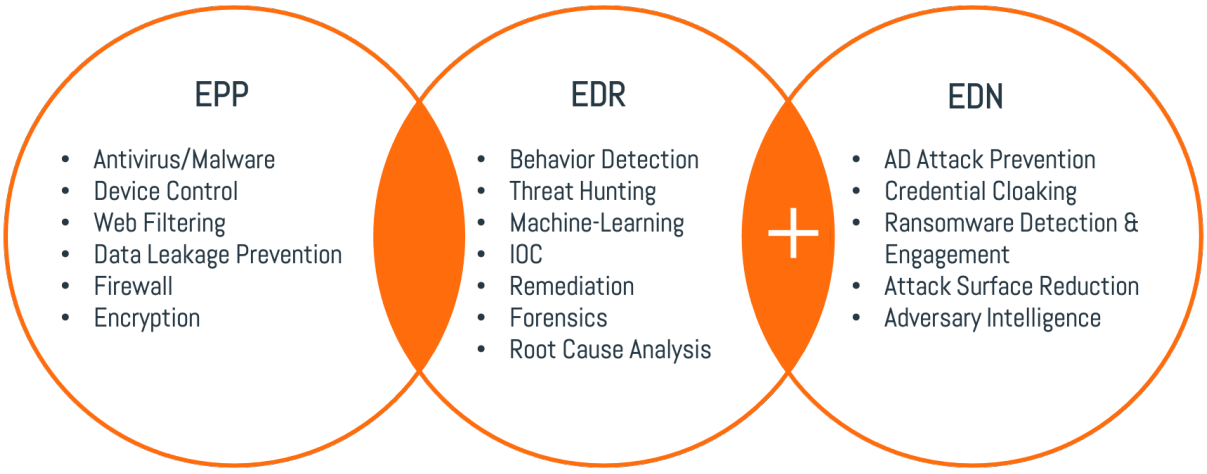
INTRODUCTION

The endpoint is the primary avenue for an attacker to infiltrate an organization. Whether through malware, social engineering, or other attack methods, once attackers bypass existing security controls and compromise an endpoint, they have an entry point into the network. Attackers use several tactics that allow them to move laterally and escalate privileges to break out from their entry point and stealthily extend their reach into the organization for nefarious purposes. Logically, stopping an attacker at the endpoint can severely limit their effectiveness.

Organizations add defenses such as Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions to defend against such incursions, but attackers exploit gaps in their coverage to slip through. As a capability of the Attivo Networks ThreatDefend® platform, the Attivo Endpoint Detection Net (EDN) suite covers these gaps and acts as a force multiplier to Endpoint Protection Platforms and Endpoint Detection and Response solutions to truly lock down the environment, strengthening defenses to ambush and stop attackers at the endpoint.



ENDPOINT DETECTION NET AS A FORCE MULTIPLIER FOR EPP/EDR



Current endpoint security consists of two complementary controls, EPP and EDR. EPP solutions deploy on the endpoint to protect against file-based, file-less, and other types of malware, through prevention and investigation and remediation capabilities. EDR solutions monitor and record activity on endpoints, detect suspicious behavior and security risks, and respond to internal and external threats. Organizations use both to prevent and investigate attacks at the endpoint. However, attackers have demonstrated that they can bypass these protection mechanisms to infiltrate the network. With the EDN suite, organizations can extend their EPP and EDR solution capabilities to defend the environment better and prevent attackers from misusing credentials, leveraging Active Directory, and moving laterally. Additionally, organizations can leverage native integrations within the Attivo partner ecosystem to automate incident response for blocking, isolation, and threat hunting. The solution is available for purchase as part of the ThreatDefend platform.

AMPLIFY ENDPOINT PROTECTION CAPABILITIES

The EDN suite strengthens endpoint defensive capabilities by stopping credential theft and misuse to prevent unauthorized access early in the attack process. The solution detects and alerts on attack tactics that attackers use once they manage to compromise a system to spread to other devices on the network. The EDN suite helps organizations reduce the cost and damage of the attack and minimizes the personnel needed to respond to incidents. The following table lists the problems the EDN suite solves and the value it brings.

The Problem	How EDN Helps	EDN Value
Unauthorized AD queries Attackers query AD from an endpoint to extract information on privileged domain accounts, systems, and other high-value objects.	Return fake Active Directory results, making an attacker's automated tools untrustworthy and redirecting the attacker's efforts into a decoy environment.	Defend AD against information theft and exploitation while obfuscating the addressable attack surface.
Local credential theft Attackers steal stored or in-memory credentials to reuse for access on production assets.	Credentials are hidden and bound to applications to prevent unauthorized access. Attackers are lured to the decoy environment with fake credentials for engagement, alerting, and forensic collection on their activities.	Prevent credential theft-and-reuse attack activity, detect lateral movement, and collect threat intelligence.

The Problem (cont.)	How EDN Helps (cont.)	EDN Value (cont.)
Exploit mapped shares Attackers access mapped shares on the endpoint to compromise the file server (such as with ransomware)	Decoy file shares and systems misdirect attackers that follow these mapped shares to decoys for engagement.	Early detection and protection against attacks that move across mapped directory shares.
Network reconnaissance Attackers scan network segments and endpoints to find production assets and available services.	Decoy respond to scans with systems that appear identical to production assets but are instead virtual landmines that attackers engage with instead of a production asset.	Obfuscate the attack surface so attackers can't accurately map the network.
Steal credentials in transit Attacks conduct Man-in-the-Middle attacks to steal credentials as they traverse the network.	Network decoys detect MitM activity on every network segment where they have an IP address.	Early detection and alerting of in-network MitM attacks.
Traverse lateral attack paths Attackers leverage stored or orphaned credentials, or endpoint policy misconfigurations to move from system to system.	Provide visibility to at-risk credentials and avenues of lateral movement, as well as the insights needed to remove or remediate them before attackers leverage them.	Reduce the attack surface by gaining visibility and pre-emptively remediating attack paths.

THE ATTIVO NETWORKS THREATDEFEND PLATFORM

The Endpoint Detection Net solution is available for purchase standalone or as part of the ThreatDefend platform, which is a comprehensive solution that accurately and efficiently guards against credential theft and detects, misinforms, and misdirects lateral movement attacks across all primary attack vectors. With the ability to detect attacks against Active Directory and other network systems, organizations gain the knowledge to efficiently identify and derail attacks, reducing dwell time and preventing attackers from establishing a foothold.

The ThreatDefend product portfolio works by creating a detection fabric that is interwoven throughout the entire network infrastructure, from user segments, data centers, cloud, specialized networks, or remote locations to create a virtual layer of land mines and lures designed to confuse, slow down and misdirect an attacker. When an attacker engages with a decoy through network scans, stolen deceptive credentials, or other methods, organizations receive a high-fidelity alert so that they can quickly and confidently respond to incidents.

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.