SOLUTION BRIEF

ENHANCING XDR WITH THE ATTIVO NETWORKS® THREATDEFEND® PLATFORM

INTRODUCTION

Endpoint security solutions have gone through a significant expansion since the first antivirus solutions, adding host firewalls, host IDS/IPS, Endpoint Protection Platforms (EPP), and Endpoint Detection and Response (EDR) solutions. Current endpoint security innovation has evolved to Extended Detection and Response (XDR) solutions that correlate data from other security controls to improve endpoint defenses. The idea is simple: collect and connect data from other detection mechanisms to identify malicious activities and then stop them. While the concept is sound, there are still in-network attack techniques that can evade detection. The Attivo Networks ThreatDefend® platform provides security functions that augment XDR solutions, detecting and preventing advanced in-network attack techniques other solutions cannot detect. Additionally, the ThreatDefend platform records all attack activities and forensic data to develop organization-centric threat intelligence and fortify defenses.

WHAT ARE EXTENDED DETECTION AND RESPONSE (XDR) PLATFORMS

According to analyst firm Gartner, Extended Detection and Response solutions are "a unified security incident detection and response platform that automatically collects and correlates data from multiple proprietary security components."

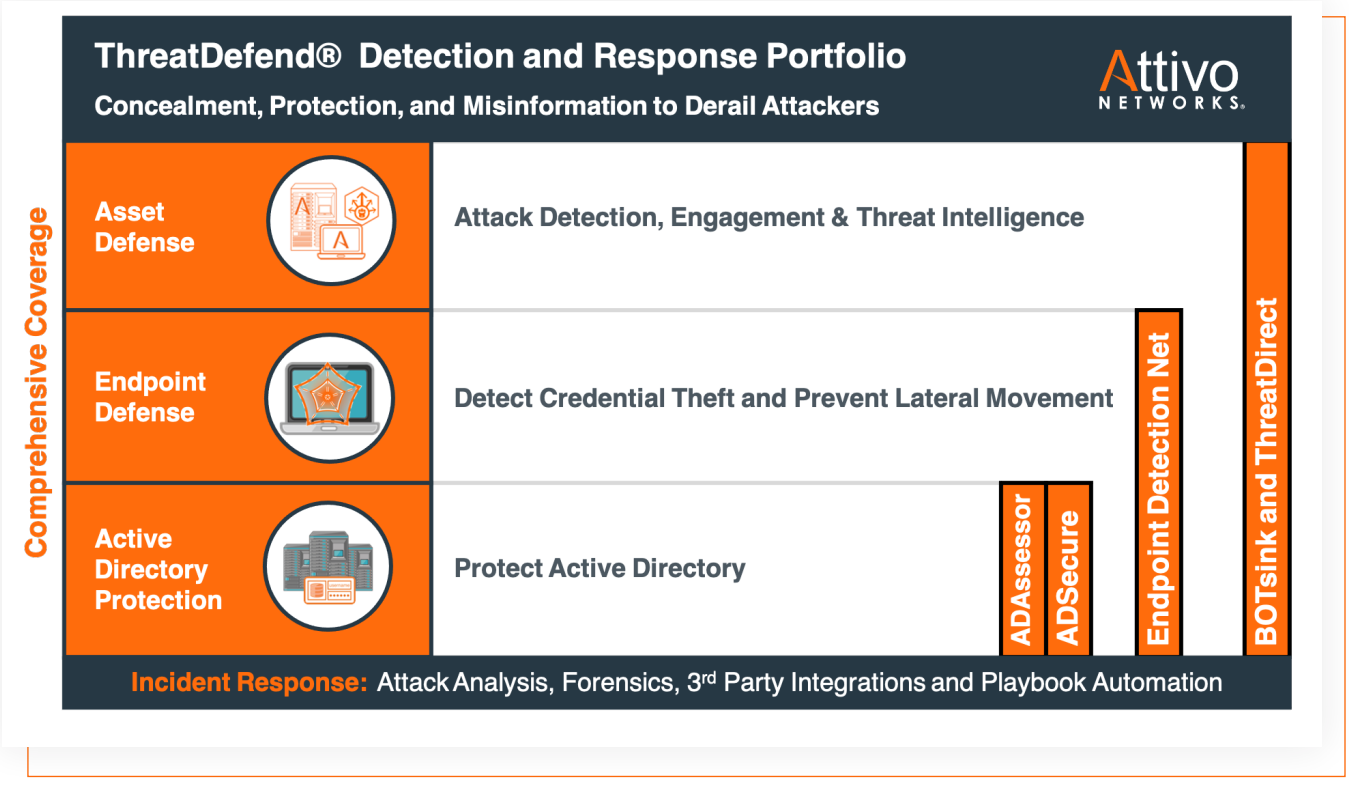
Emerging XDR products consolidate multiple security products into a cohesive security incident detection and response platform for the mainstream market. XDR offerings are a natural evolution of endpoint detection and response (EDR) platforms, which have become a primary incident response tool for security teams. XDR products improve security operations productivity and enhance detection and response capabilities by including more security components into a unified whole that offers multiple telemetry streams, presenting options for numerous forms of detection and concurrently enabling various response methods. XDR products can provide traditionally complex security operations capabilities, making them more accessible to security teams without the resources for more custom-made point solutions.

XDRs function similarly to security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools. However, XDRs differ by levels of product integration at deployment and focus on threat detection and incident response use cases. While the SIEM market is mature, many organizations have not deployed SIEM tools, have failed or incomplete implementations, or only use SIEM for log storage and compliance. XDR products aim to solve the primary challenges with SIEM products, such as effective detection of and response to targeted attacks, including native support for behavior analysis, threat intelligence, behavior profiling, and analytics.

THE THREATDEFEND PLATFORM

The Attivo Networks ThreatDefend platform provides a customer-proven solution to prevent identity-based privilege escalation and detect attacker lateral movement. The platform's visibility programs deliver insight into credential and attack path vulnerabilities and Active Directory Domain, user, and device-level exposures for organizations implementing increased security based on least privilege access. The ThreatDefend platform's concealment technology derail attacks by hiding and denying access to the data, files, AD objects, and credentials threat actors seek.

Additionally, the solution's decoys obfuscate the attack surface, collect forensic data, automatically analyze attack data, and automate incident response through its 30 native integrations. The platform provides the most comprehensive in-network detection solution, deploying a detection fabric that scales to on-premises, cloud, remote worksites, and specialty environments such as IoT, SCADA, POS, SWIFT, and network infrastructure.



THE THREATDEFEND PLATFORM AND XDR

The Attivo ThreatDefend platform can augment XDR solutions in several ways. Besides acting as another data source for XDR, the platform offers the following benefits:

1. The EDN suite can definitively detect endpoint attacks like credential theft, privilege escalation, AD recon, ransomware behavior, and lateral movement attempts. The EDN suite feeds forward such detections to XDR solutions for correlation and response.
2. The EDN suite provides in-depth process and action details around attacks that help XDR solutions to remediate specific impacts caused by the attack at endpoints.
3. The ThreatDefend platform detects network attacks like MITM, network recon, and lateral movements reliably and definitively. When combined with information from the EDN suite, it provides actionable information around process, user, and host context. Organizations can use these to augment and enhance the XDR solution's response.
4. The ThreatDefend platform offers the capability to build a deception strategy to lure and lead attackers away from production assets. This function is highly beneficial to XDR solutions to use as part of the response to minimize the impact.
5. The Attivo ADAssessor solution empowers XDR solutions with exposure detections at the Active Directory level, which attackers could leverage to progress their attack.

CONCLUSION

XDR solutions are a logical next step forward in defending endpoints from attack. However, attackers have demonstrated that they can evade even the most sophisticated security controls. Once they compromise an endpoint, they can steal and reuse stored credentials, query Active Directory, move laterally, escalate privileges, and identify targets while avoiding detection. The ThreatDefend platform provides extra visibility, detection, and prevention controls that focus on these in-network attack techniques to augment any XDR solution, increase detection efficiency early in the attack cycle, and provide much-needed threat intelligence on attacker actions and indicators.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com