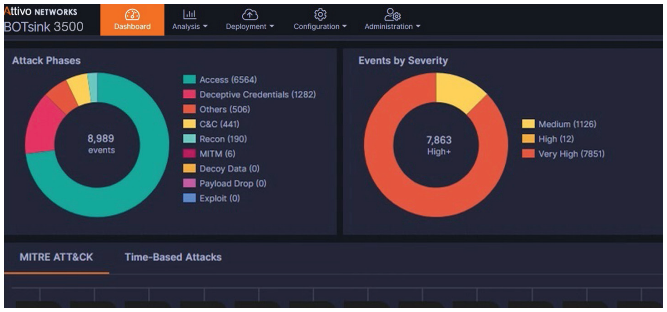

Attivo Networks

ThreatDefend Platform v5.0

Security pros will find the Attivo ThreatDefend Platform a comprehensive detection product that uses machine learning to customize decoys based on the systems, applications, and environments into which it has been deployed and adds endpoint components to hide data and deflect port and service scans to decoys. In other words, this unique design makes every endpoint part of the deception fabric. The platform campaigns drive early and accurate detection of in-network attackers, providing the visibility and adversary intelligence necessary to understand and derail threats early in the attack cycle.

Attivo ThreatDefend features automation that significantly reduces the complexity otherwise expected with a deception platform. The Self Learn Wizard analyzes an environment and intelligently profiles VLANs to configure decoy campaigns automatically. These decoys are developed by customizable, out-of-the-box templates that automatically match the services, operating systems, and naming conventions within an environment, simplifying the process for security teams and getting them running quickly.

Active Directory has become a common target for attackers and ThreatDefend mitigates this potential vulnerability by forming defenses at both the endpoint and network levels. The platform looks for unauthorized queries from any Active Directory system and returns decoy objects that lead to network decoys. Overlapping network and credential deceptions enable corroboration between different decoys and make the information contained within them look real. Security teams may also add deceptive credentials while hiding legitimate accounts and data. This added layer of deception protects actual production data, gives adversaries the kind of information they expect to find, and then leads these same adversaries directly into deception environments. Every time attackers touch closed ports while looking for open services, the endpoint forwards them to decoys that respond to their connection requests. These redirections force adversaries to engage and reveal their presence. Thus, while these adversaries tie themselves up with deception, misdirection, and misinformation, the environment remains protected against fingerprinting and exfiltration.

There are more than 32 partner integrations that let security teams create customizable, repeatable, automatic or manual playbooks and conduct deep, forensic investigations on captured deception information. Investigative capabilities include analyzing memory forensics captured and reported from the attacking endpoints. ThreatPath operates as a particularly valuable investigation tool that continually shows current and new credential exposures, including privileged account paths, and the misconfigurations that are causing them. This view breaks down the locations of decoy and real credentials letting security teams control, manage and remediate actual production environment vulnerabilities and exposures. Analysts may query this view to filter information according to their preferences and generate reports that they can then share with executives.

Overall, security pros will find the Attivo ThreatDefend Platform a flexible, highly scalable deception product. It uses full OS decoys that function like trap servers, an approach that covers a wide variety of use cases, including both cloud and local deception. The scalability extends to remote sites, where decoys remain physically separated at main headquarters while providing coverage at the remote location. The advanced deception abilities first detect adversaries during reconnaissance, before steering them away from the real environment and into the deception environment. ThreatDefend supports a variety of deployment options, including the ability to operate within specialized environments, making this dynamic and powerful solution suitable for any organization.

The platform costs $40,000 and includes 24/7 phone and email support. Professional support services are available for an additional fee.

– Katelyn Dunn

DETAILS

Vendor Attivo Networks

Price $40,000

Contact www.attivonetworks.com

Quick Read

What it does ThreatDefend conceals sensitive data and privileged accounts from attackers to deny their accounts and exploitations while defeating discovery, lateral movement, credential theft, and privilege escalation activities.

What we liked It supports a variety of deployment options, including the ability to operate within specialized environments, making this dynamic and powerful product suitable for any organization.

Adapted from SCMagazine.com, October 2020 • www.scmagazine.com
(#S088202) For more information about reprints and licensing, visit www.parsintl.com/publication/sc/