CASE STUDY

LAW FIRM CHOOSES ATTIVO NETWORKS THREATDEFEND® PLATFORM AS A MANAGED SERVICE

ORGANIZATION

A New England (US) based law firm specializing in commercial, regulatory, and litigation work.

SITUATION

The firm's CIO attended presentations on deception technology by the Attivo Networks® team and independent journalists and analysts at several cybersecurity conferences. They recognized the benefits deception could bring to their security stack and reached out to Attivo Networks for more information on the ThreatDefend® platform.

As a law firm, they were especially concerned with protecting their client's private information and intellectual property. This concern put an emphasis on detecting insider threats, stopping lateral movement in the case of an intrusion, and protecting their data from ransomware or other malware that could damage files.

The firm relied on a reputable Managed Security Service Provider (MSSP) for their information security needs. The Attivo team educated the MSSP on the ThreatDefend solution and the value it could add to this firm's security stack. Attivo Networks® worked closely with the MSSP and the customer to successfully integrate deception into the MSSP's existing workflows.

Based on references, demonstrations, 3rd party endorsements, and an agreeable method of integration with their MSSP, the firm chose to deploy the ThreatDefend® platform.

ATTIVO NETWORKS IMPLEMENTATION

The deployment placed deception throughout their headquarters, including endpoint deceptive lures with the ThreatStrike® solution, and relied on the ThreatDirect® deception forwarder solution to protect remote locations. Additionally, the deception solution was integrated with their existing MSSP provided security solution for seamless operations.

The firm installed an Attivo Networks BOTsink® appliance in their corporate headquarters and configured it to send alerts directly to their MSSP's SIEM. This gave them the base to project deception throughout their environment and allowed an easy integration with their 3rd party sourced security tools.

To protect the endpoints and deliver defenses against insider threats and malware attack, they deployed the ThreatStrike solution to the user workstations and internal servers. To extend deception and offer the same level of defense into the field as they enjoyed at headquarters, they deployed the ThreatDirect solution into satellite offices for protecting remote workers.

SOLUTION

The Attivo Networks ThreatDefend® platform gave the firm the tools and visibility they needed to prevent identity-based privilege escalation, detect lateral movement and thwart insider threats. The solution also provided an effective means to disrupt the spread of ransomware and related malware.

Active Directory domain, user, and device-level exposures for organizations seeking increased security based on least privilege access. The ThreatDefend platform's concealment technology derails attackers as they can no longer find or access the data, files, AD objects, and credentials they seek.

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. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend capabilities tightly align to the MITRE ATT&CK Framework, and deception and denial are now integral parts of NIST Special Publications and MITRE Shield active defense strategies. Attivo has 150+ awards for technology innovation and leadership. www.attivonetworks.com.