CASE STUDY

CASE STUDY: LAW FIRM CHOOSES ATTIVO NETWORKS DECEPTION TECHNOLOGY 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 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.

SOLUTION

The Attivo Networks ThreatDefend platform gave the firm the tools and visibility they needed to address their primary concerns of detecting lateral movement, thwarting insider threats, and providing an effective means to disrupt the spread of ransomware and related malware.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.

ATTIVO NETWORKS PRODUCTS

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.In order 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.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in network attacks. The Attivo ThreatDefend® Deception Platform offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 90 awards for its technology innovation and leadership.

www.attivonetworks.com