CASE STUDY

UK FINANCIAL SERVICES COMPANY CHOOSES ATTIVO NETWORKS TO ENHANCE ITS SECURITY STACK WITH DECEPTION TECHNOLOGY

ORGANIZATION

A respected UK based trading and investment firm.

SITUATION

Operating in the financial services sector, the organization must comply with a range of specific regulations, which made data security a top priority. The organization considered early and accurate detection highly important and had additional concerns with identifying lateral movement.

Due to the structure of their organization, management had particular concerns with targeted attacks against their executives with a possible compromise leading to a more serious breach. This concern made endpoint defense equally important, including an ability to perform forensics and to identify command and control traffic in case an attacker managed to get into their environment.

The organization was familiar with deception technology from a previous installation of a competing solution. As they became familiar with Attivo deception technology, they realized the advantages that the ThreatDefend offered over their existing solution. The Attivo deception offering proved itself able to meet their full range of requirements while offering improved effectiveness, efficiency, and scale.

SOLUTION

The Attivo Networks® ThreatDefend™ platform provided the range of capabilities the organization required. Given the regulatory environment they operate in, high-fidelity alerts, risk mitigation, and forensics were all critical. The platform also offered direct integration with their existing security stack, which increased the information security team's efficiency by enabling both automated and manual responses. They were also looking to replace their current firewall vendor, and the ThreatDefend platform offered native integration with their selected replacement.

ATTIVO NETWORKS PRODUCTS

The organization selected a physical Attivo BOTsink server, deployed in their local data center, to serve as the platform for the deception solution. They implemented the ThreatDirect solution to project deception into their remote offices without requiring additional appliances. With a need to protect their endpoint and provide forensic capabilities, they selected the ThreatStrike solution for deployment across the organization. The ThreatStrike solution also gave them the endpoint forensics capabilities that they needed and could mitigate both credential theft and malware threats. They also chose to deploy the ThreatPath solution for the capability to reduce their attack surface by identifying and mitigating potential compromise routes within their environment. Lastly, they heavily leveraged the automated response capabilities included in Attivo's ThreatOps solution.

IMMEDIATE VALUE

The organization believed in the benefits of deception technology and saw immediate improvements over their previous deception solution, with false positives dropping to virtually zero while the coverage expanded to encompass their entire environment. The incident response team also noticed improvements in efficiency and leveraged the option to initiate manual or automated responses as needed.

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 100 awards for its technology innovation and leadership.

www.attivonetworks.com