

MSSP WORKS WITH LARGE METROPOLITAN PUBLIC SCHOOL DISTRICT TO USE DECEPTION FOR NETWORK VISIBILITY

ORGANIZATION

A large metropolitan Public-School District.

SITUATION

The school district had an established relationship with their Managed Security Service Provider (MSSP) to protect the district's endpoints and network infrastructure. The MSSP also provided dedicated Security Operations Center (SOC) personnel and remediation capabilities for the district. They saw Attivo's ThreatDefend platform as an ideal solution to complement their existing capabilities and improve visibility into the district's environment.

SOLUTION

The Attivo Networks® ThreatDefend™ platform easily integrated into the existing security infrastructure provided by the school district's MSSP. The solution consisted of several BOTsink server appliances deployed at strategic locations within the district, several ThreatDirect virtual machines to project deception into remote sites, an Attivo Central Manager at the MSSP's site for management and reporting, and several hundred instances of the ThreatStrike solution to protect specific endpoints.

The MSSP enlisted Attivo's Professional Services team to aid in the deployment and to provide additional training on the integrated solution, and the solution was architected to enable easy expansion and scaling to cover additional endpoints and network segments.

ATTIVO NETWORKS PRODUCTS

With a focus on detection in a managed environment, the installation started with BOTsink® servers to provide decoys, and ThreatDirect™ to allow them to project those decoys seamlessly into remote locations. The ThreatStrike™ solution placed deception credentials and other deceptive assets on the endpoints throughout the organization for protection, and Attivo Central Manager allowed the MSSP to centrally manage the entire deployment.

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