CASE STUDY

MAJOR ENERGY PROVIDER CHOOSES ATTIVO NETWORKS SOLUTIONS TO PROTECT CRITICAL ASSETS

ORGANIZATION

A Large Public Energy Utility Company

SITUATION

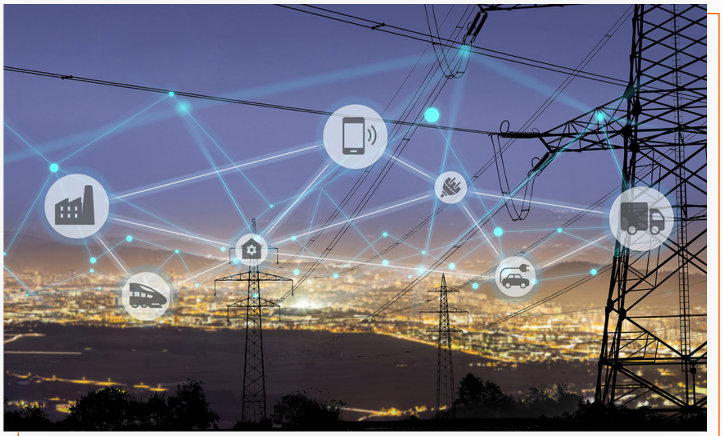
The Director of Cybersecurity for a large public energy utility organization had confidence in their perimeter security but realized they needed better visibility into their internal network in the event of a compromise or when facing an insider threat.

Existing perimeter defenses were not providing adequate visibility into the organization's complex network environment. Their environment was diverse, with systems and topologies unique to their business, such as SCADA systems and the typical user and datacenter spaces. Therefore, any solution they implemented needed to scale and detect intruders in this diverse environment without adding excessive workload to the Information Security team.

They chose to take a proactive approach with a complete defense-in-depth posture. After extensive research, the Director decided to implement a layer of deception to detect and slow attackers who made it past the perimeter.

SOLUTION

The organization chose to implement the Attivo Networks® ThreatDefend® platform, including the BOTsink® server and Attivo Central Manager, to gain more comprehensive visibility into their network environment. The ability to clearly detect a breach and thwart an attacker early in the attack cycle were significant driving forces behind their adoption of the Attivo solutions. Additionally, they added the Endpoint Detection Net (EDN) suite of products to expand their active defense capabilities further.



ATTIVO NETWORKS PRODUCTS

The organization selected the full range of Attivo Networks® ThreatDefend® products, including BOTsink® servers, the Attivo Central Manager, and the EDN suite of products allowing the company centralized control and management in a single system.

IMMEDIATE VALUE

The Director had done extensive research and determined that implementing deception technology would be the most efficient and cost-effective way to add the required detection capabilities. Once deployed, they quickly discovered some misconfigurations and other issues in their environment, giving an almost immediate return on investment. Further, the Attivo Networks® solution required no additional staffing. The organization found that their existing security team could easily deploy and maintain the solution without impacting their everyday responsibilities. Integration with their existing security infrastructure gave improved visibility with minimal overhead.

The organization added deception proactively to improve visibility and threat response capabilities rather than responding to a security incident, putting them in a more proactive posture. The Attivo Networks® ThreatDefend® platform includes native integrations with 3rd party security applications, enabling the organization to seamlessly mesh deception into their existing security infrastructure, feeding their SIEM and ticketing systems directly, improving efficiency and effectiveness. In addition, the system has quickly identified existing misconfigurations and proven to be very effective in testing, leaving the organization confident it will detect and respond to a sophisticated attack or insider threat.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com.