

WORLD-RENOWNED VEHICLE MANUFACTURER SEEKS SOLUTIONS FOR PROTECTING INTELLECTUAL PROPERTY

ORGANIZATION

A world-renowned vehicle manufacturer with world-wide operations.

SITUATION

Producing everything from jet aircraft to automobiles and motorcycles, this industry-leading manufacturer had recently created a fully dedicated cybersecurity team to protect their Intellectual Property “Crown Jewels.” Previously, information security was a distributed responsibility across their IT and Infrastructure teams.

They recognized that their existing security infrastructure was facing an escalating and evolving threat landscape with multiple levels of risk, including industrial rivals and state actors. They turned to the Attivo Networks ThreatDefend® platform to provide early and accurate in-network detection for a broad range of threats. The ThreatDefend platform defends against evolving threats and scales smoothly across a wide variety of attack surfaces. This solution also served to augment controls within their security stack versus replacing them.



SOLUTION

The Attivo Networks® ThreatDefend® platform provided the range of defense capabilities the manufacture sought. Given the varied nature of their expected threats, they looked to cover in-network visibility, early detection, lateral movement, Man-in-the-Middle (MitM) attacks, ransomware, and other malware threats. They required an accurate, comprehensive, and reliable solution that didn't overtly impact the workload of their incident response team. The organization was particularly interested in a solution that effectively worked for external and insider threats. Additionally, any new solutions needed to integrate with other components of their security stack seamlessly.

The ideal solution should be efficient, scalable, future-proof, and cover the full range of expected and unexpected threats. Attivo's ThreatDefend platform was a match on every point.

ATTIVO NETWORKS PRODUCTS

With a broad range of requirements, starting with detecting advanced threats in a dynamic environment, the installation began with a BOTsink® server to host decoys and management services. The ThreatDirect solution projected deception into remote locations worldwide without increasing their operational overhead or putting devices in remote sites, which was not always feasible. The ThreatStrike® solution placed decoy credentials and other deceptive assets on select endpoints within the organization to expand the detection footprint. The ThreatPath® solution provided additional protection, giving them the tools to identify misconfigured credentials and potential routes an attacker could use to traverse the environment to reduce the attack surface.

IMMEDIATE VALUE

Initial testing proved that the ThreatDefend platform met the company's needs across the full range of threat surfaces while adding minimal overhead to the information security team's operations. It also provided an additional layer of defense around critical R&D for both insiders and external threats. Integration with other security controls improved efficiency, and the platform's versatility gave them several options to integrate different security tools as their dedicated security posture matures.



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.