PARTNER BRIEF

Microsoft Azure

Attivo NETWORKS

ATTIVO NETWORKS INTEGRATES WITH MICROSOFT AZURE SECURITY CENTER TO PROTECT AZURE IOT EDGE

Attivo Networks has partnered with Microsoft to give organizations detection and visibility in the Azure IoT Edge against attackers trying to compromise devices while remaining undetected. Together with the Attivo Networks ThreatDefend® platform, the Azure Security Center for IoT provides adaptive threat prevention and intelligent threat detection and response across workloads running on premises, on edge, in Azure, and in other clouds.

HIGHLIGHTS

- Early and Accurate Threat Detection
- Attack Analysis and Forensics
- Quick and Easy Deployment
- Threat Intelligence Development

THE CHALLENGE

Attackers target IoT devices as a means of breaking into a network. Whether through a misconfigured security permission or an exposed IoT device that can't run security software, attackers look for opportunities to compromise a system and get inside. Once attackers have established a foothold, they will move laterally throughout the network, expanding their footprint until they can find the data they are looking for and complete their mission.

Organizations encounter difficulties in detecting attackers moving inside the network, particularly with IoT devices that may not log activity or have the means to send telemetry data to a SIEM. They need a more robust way to detect these invaders without relying on recognizing known signatures or analyzing patterns of behavior. This method of detection uses deception to trick attackers into revealing themselves and engaging with decoy IoT devices that can forensically capture valuable attack information while alerting on their activity. This early detection leads to faster incident response to deny attackers free reign to move around undetected while recording forensic evidence on their activities to develop rich threat intelligence for improved security.

THE ATTIVO THREATDEFEND PLATFORM AND MICROSOFT JOINT SOLUTION

The integration between Attivo Networks and Microsoft Azure Security Center for IoT leverages the platform's ability to create a fabric of deceptive assets that proactively deceive and redirect attackers into revealing their presence. Security teams can also deploy ThreatDirect® forwarders in remote IoT Edge devices from the Azure IoT Hub console and scalably project deception across the enterprise cloud, IoT, industrial, and medical networks to protect their entire infrastructure. When attackers target IoT edge devices, attempt to conduct reconnaissance or move laterally, they will discover decoy assets that appear identical to production systems. The platform redirects any active attacker observation to the deception environment while raising an engagement-based alert that automatically notifies the Azure Security Center for IoT of their presence.

ATTIVO NETWORKS THREATDEFEND PLATFORM

Recognized as the industry's most comprehensive deception platform, the solution provides network, endpoint, and data deceptions and is highly effective in detecting threats from all vectors such as reconnaissance, stolen credentials,Man-in-the-Middle, Active Directory, ransomware, and insider threats. The ThreatDefend Deception Platform is a modular solution that covers network and endpoint detection. The Attivo BOTsink engagement servers, decoys, lures, and breadcrumbs provide detection for the network, while the Endpoint Detection Net portfolio consists of the ThreatStrike® endpoint lures, ThreatPath® for attack path visibility, and the ADSecure module protect at the endpoint. Together, these create a comprehensive early detection and active defense against cyber threats

SUMMARY

The Attivo ThreatDefend Platform and Microsoft work together to enhance detection and response for Azure IoT Edge. Since the intelligent edge is a prime target for attackers, Azure IoT Edge actively addresses the inherent risks by collaborating with innovative security companies that are effective at efficiently detecting attackers in these emerging environments. The integration provides customers a reliable way to quickly and confidently detect, redirect, and respond to in-network attackers.

By implementing these solutions jointly, organizations can confidentally detect in-network threats targeting their Azure IoT Edge devices and respond to them quickly to mitigate the risk of large-scale breaches.

ABOUT ATTIVO NETWORKS®

Attivo Networks® provides real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response.

www.attivonetworks.com

ABOUT MICROSOFT® AZURE IOT EDGE

Azure IoT Edge is a fully managed service built on Azure IoT Hub. Deploy cloud workloads—artificial intelligence, Azure and third-party services or business logic—to run on Internet of Things (IoT) edge devices via standard containers. By moving certain workloads to the edge of the network, devices spend less time communicating with the cloud, react more quickly to local changes and operate reliably even in extended offline periods.

https://azure.microsoft.com/en-in/services/iot-edge/