Microsoft and Attivo Networks Team Up to Protect Azure IoT Edge
Company Background

Innovation that Shifts Power to the Defender

- Innovator in Detection, Leader in Deception Technology
- Shipping Since 2014: Customer Proven at Scale
- #31 on the Deloitte Fast 500™
- Customers Across All Major Verticals & Sizes Including 50%+ midmarket and multiple within the Fortune 10
- Global Operations & Customer Success Programs
Azure IoT Edge

A fully managed service built on Azure IoT Hub that enables IoT devices to run cloud services, process data, and communicate with sensors, even with intermittent network access.

- **Certified IoT Edge hardware**: Works with Linux or Windows devices that support container engines.
- **Runtime**: Free and open-source under the MIT license to give more control and code flexibility.
- **Modules**: Docker-compatible containers from Azure services or Microsoft partners to run business logic at the edge.
- **Cloud interface**: Remotely manage and deploy workloads from the cloud through Azure IoT Hub with zero-touch device provisioning.
The Challenge

Attackers can gain access to the Azure IoT Edge to compromise devices while remaining undetected.

Attackers can move laterally and spread to other IoT devices or containers to escalate their attacks.

Organizations lack visibility and detection capabilities across all their IoT devices and network segments to identify unauthorized activity.

Organizations struggle to gather threat intelligence from IoT devices gain better detection and improve security.

IoT devices can not run traditional endpoint security solutions.
The Attivo Networks Solution

Misinform and Misdirect Attackers to Decoys for engagement

- Deploy decoy Azure IoT modules from a BOTsink® deception server for early and accurate threat detection
- Deploy ThreatDirect® forwarders in remote IoT Edge devices from the Azure IoT Hub to scale deception across the enterprise cloud, IoT, and OT networks
- Collect forensic and company-centric threat intelligence on attacks targeting the organization to gain visibility on methods and intent to strengthen security.
Optimized Threat Detection of Attackers Targeting Azure IoT Edge Devices

1. Install BOTsink GE in Azure
2. Install ThreatDirect in Edge
3. Project decoys
4. Deploy deceptive creds on access
5. Connect to ASC

- Attivo ThreatDirect
- IoT Decoy Edge Gateway
- Azure IoT Edge
- Azure IoT Hub
- Azure IoT Modules
- Azure Decoy Historian
- Azure Decoy HMI
- Azure Decoy OPC Server
- Attivo Decoys
- Attivo IoT Protocols
- Azure Decoy
- Azure Decoy
- Azure Decoy
- Azure Decoy
- Azure Decoy
Why Azure IoT Edge with the Attivo ThreatDefend Platform?

Customer Value

- Early and accurate threat detection across Azure IoT Edge modules
- Raises engagement-based alerts that automatically notify the Azure Security Center
- Projects deception at scale across the enterprise cloud, IoT, industrial and medical networks
- Gathers forensics and company-specific intelligence to strengthen defenses