Eliminating device security threats at scale with context-driven visibility, risk assessment, and access control

Case Study

Ozarks Electric Cooperative is a non-profit electric utility headquartered in Fayetteville, Arkansas, with district offices in Springdale, Arkansas, Stilwell, Oklahoma, and Westville, Oklahoma. The Cooperative serves the states of Arkansas and Oklahoma.

How can an electric cooperative company protect its IT and IoT infrastructure across the corporate, regional, and substation networks?

To proactively mitigate security risks, the cooperative's board of directors set a mandate to have a set of effective security controls in place that would provide access control and visibility to all devices on the network especially on their far-flung substation network which were identified as critical threat vectors for malicious hacking activity. Another key mandate was to identify approved devices and automatically remove any devices that were unauthorized.

As a corporation, Ozarks is closely aligned with the CIS 20 controls framework, so the chosen platform had to ensure that Ozarks gained complete adherence to the CIS framework especially around Network Access and Segmentation (CIS 1.6, CIS 14.1 etc.). With a small network team, a completely automated platform with deep machine learning capabilities was of the utmost importance to the client so that the system could take over most of the tasks around device identification, classification, and risk management thus allowing the team to focus on strategic initiatives. Ozarks also recently migrated to Juniper Mist access points, hence integration with Mist to drive access control was a critical need.

The Utility realized that its existing IT and IoT infrastructure required a contextual solution that would help them address their multiple challenges around device visibility, alert management, SOAR integration, network segmentation, and access control, while retaining full control on the policies that control access.

ozarks ELECTRIC COOPERATIVE

Profile

Industry
Utilities

Region
United States

Year Founded
1938

Click here to visit the Ozarks Electric website

Challenges

- Enable visibility and control across the distributed network
- Identify unauthorized devices to reduce the attack surface
- Orchestrate actions using existing security tools
- Ensure compliance with CIS security controls

Solutions

- Netskope Device Intelligence

Results

- Accurate device threat analysis and risk assessment
- Enriched alerts by sharing device intelligence with SIEM and SOAR platforms
- Seamless integration with existing Juniper Mist infrastructure for network micro-segmentation and access control
- Adherence to NIST and CIS frameworks

The solution: Netskope Device Intelligence

Netskope's award winning HyperContext® platform is an AI-based, agentless solution, that provides contextualized visibility and analytics for all devices, and uses this intelligence to segment the network, correlate threats, and vulnerability propagation across interfaces, and automate access control.

- Advanced device identification, classification, and modeling abilities ensure 100% device visibility which leads to accurate threat analysis and assessment of risk that a device poses to the organization. Accurate identification leads to improved efficiency in remediation.
- Greater device intelligence coupled with higher accuracy in threat and risk assessment enables Netskope to provide actionable intelligence for Incident and Problem management in the ITIL framework and ensures adherence to NIST and CIS frameworks.
- Netskope supercharges existing Network Operations with an integrated product offering with its partners such as Juniper Networks to provide next-gen access control and network micro-segmentation capabilities.

As with most security and IT organizations, the Utility is resource constrained. Using inefficient tools causes tremendous strain and fatigue in SecOps personnel. The client's vision is to utilize Netskope HyperContext to accurately catalog and assess device threats & risks and provide meaningful, actionable insights from a device-centric view, thus dramatically enhancing process efficiencies, automate alert and risk management, and eliminate operations fatigue for the Utility's IT organization.

Netskope demonstrated its ability to not just provide device visibility and analytics but also mitigate security threats by driving remediation at individual device level. Using the Netskope Device Intelligence solution, the client discovered several devices that had unrestricted corporate access and were not visible earlier. The IoT insights captured IT, network and security controls, enabling the client to move rapidly to a zero trust model with complete control over network access and threat remediation. Selecting the Netskope Device Intelligence solution also allowed the client to adhere to CIS critical security controls requirements, while adding capabilities around network micro-segmentation and access control.