



Muscogee Nation Casino and Resort drives operational resilience with Armis

The challenge

- Expanding visibility into assets and security status enterprise-wide
- Pinpointing and mitigating the riskiest vulnerabilities
- Sharing data across technical teams for faster, more efficient remediation response

The solution

- Provided real-time, accurate, and detailed visibility and insights into assets across all locations
- Prioritized vulnerability remediation by consolidating security intelligence from disparate security tools and real-world threat intelligence
- Integrated with Splunk to enrich threat investigation data

The results

- Surfaced 10,000 assets missed by traditional vulnerability scanning software
- Reduced time spent on manual processes with automated ticket routing to correct teams
- Inspected traffic to ensure general user access only to authorized AI apps
- Can detect vulnerabilities 2 weeks faster than before
- 10+ hours a month saved on average by quickly scoping vulnerability exposure with advanced search capabilities.

Industry: **Entertainment**

Location: **Tulsa, OK**

Size: **2,000+ employees**



Armis Centrix™ for Asset Management and Security



Armis Centrix™ for VIPR Pro - Prioritization and Remediation

Background

The Muscogee Nation Gaming Enterprises (MNGE) is owned and operated by the Muskogee (Creek) Nation in Oklahoma, the fourth largest tribe in the U.S. with over 100,000 citizens. A critical contributor to the tribe's economic prosperity, MNGE offers diverse entertainment and recreational amenities at its twelve locations, from electronic gaming and traditional casinos to fine dining and live concerts.

IT Security Manager Seth McLaughlin coordinates with multiple cross-functional technical teams to secure MNGE's sophisticated network, critical data, and gaming infrastructure. MNGE relies on VMware vSphere cloud computing and server virtualization platform for its digital framework. This unified, centralized environment consolidates the physical computing assets and Virtual Machines (VMs) that power internal operations and casinos to ensure business continuity in a fast-moving, high-stakes industry.



“Our scanning solution took a much longer time to uncover vulnerabilities and generate reports. In the meantime, we were missing potential exposures between scans. In contrast, Armis is always-on, constantly ingesting information and providing us with real-time visibility into risk...”

Seth McLaughlin,
IT and Security Manager,
Muscogee Nation Gaming
Enterprises

“Armis eliminates the guesswork and streamlines resolution. By automatically establishing ticket ownership, it has eliminated manual processes, saving the team as much as four hours per month.”

Seth McLaughlin,
IT and Security Manager,
Muscogee Nation Gaming
Enterprises

“VIPR Pro is a great tool to demonstrate our value to our finance team and CIO. The ability to tie a remediation campaign directly to how we’ve eliminated vulnerabilities over the last six months is a highly compelling way to tell our story.”

Seth McLaughlin,
IT and Security Manager,
Muscogee Nation Gaming
Enterprises

The Challenge

Looking to bolster the organization's resilience, McLaughlin collaborated with the CIO to find ways to incorporate AI and machine learning into MNGE's cybersecurity strategy. Their goal was to improve asset control and exposure management by gaining visibility across the entire estate. The primary focus was on reducing risk and shrinking the attack surface by uncovering security gaps and taking action to ensure the latest protection and prioritize remediation for business-critical vulnerabilities.

McLaughlin was already aware of the cloud-based, AI-powered Armis Centrix™ platform and was eager to test it out in the MNGE environment with a proof of value.

“What really convinced me to move forward with a POV was the agentless, passive asset identification of assets and deep packet inspection provided by Armis. This would give us a level of visibility we never had before,” he explained. “Our existing vulnerability scanner worked fine for scanning assets we already knew about. But if a new VLAN were to pop up on the network that the security team wasn't aware of, our solution would never see or scan the devices connecting to it.”

The Solution

McLaughlin decided to move ahead with the POV to test both the physical and virtual versions of Armis Centrix™ for Asset Management and Security and Armis Centrix™ for VIPR Pro – Prioritization and Remediation. The deployment was simple and straightforward: McLaughlin spent only three hours to get the platform up and running, with the help of easy-to-follow documentation.

While MNGE's existing tool performs scheduled, point-in-time active scans at casinos on different days, Armis Centrix™ provides always-on, real-time asset and risk discovery and visibility, delivering accurate, comprehensive intelligence. Armis Centrix™ for VIPR Pro – Prioritization and Remediation, part of the unified platform, goes beyond traditional vulnerability management by aggregating findings across multiple security tools and using AI to automatically prioritize what to fix first to stay ahead of evolving threats based on business risk.

“Our scanning solution took much longer to uncover vulnerabilities and generate reports. In the meantime, we were missing potential exposures between scans. In contrast, Armis Centrix™ is always-on, constantly ingesting information and providing us with real-time visibility into risk by monitoring connected device communication, anomalous activity, and unusual traffic patterns,” said McLaughlin.

The Results

Armis Centrix™ quickly proved its value by eliminating blind spots. It immediately discovered more than 10,000 assets that were missed by the existing tool, including servers in the vSphere environment.

In addition to identifying previously undetected assets, Armis has been instrumental in strengthening MNGE's overall security posture. The Armis Asset Intelligence Engine identifies cyber risk patterns and behaviors by monitoring billions of assets worldwide. It compares MNGE's traffic to this knowledge base and feeds the Armis Centrix™ platform with actionable intelligence that enables technical teams to detect, prioritize, and remediate real-time threats across the entire enterprise estate.

10,000

previously unknown
assets discovered

Save up to 4 hours

per month by streamlining
ticket assignments

Deployed in just 3 hours

10+ hours

a month saved scoping
vulnerability exposure

Operationally, Armis Centrix™ has been a big boon to MNGE's security team. The integration with Splunk, which only took five minutes to activate, enriches threat investigations by feeding Armis Centrix™ device data, risk assessments, and alerts directly into the Splunk Security Information and Event Management (SIEM) interface for faster remediation.

Moreover, the platform's AI-powered alert and exposure classifications automatically route tickets to the appropriate teams based on incident type and severity. For example, if a PCI device is on the wrong VLAN, a ticket is assigned to the networking team for manual triage.

"Armis eliminates the guesswork and streamlines resolution. By automatically establishing ticket ownership, it has eliminated manual processes, saving the team as much as four hours per month," noted McLaughlin.

Technical teams also use Armis Centrix™ to gain immediate visibility into corporate devices connecting to guest networks to prevent potential data exfiltration. Integration with MNGE's network mapper enables precise, real-time switch port tracking to locate and secure connected computing assets, helping to reduce discovery time down to minutes.

McLaughlin pointed out that Armis device and network data is made available to teams through dashboards with granular access controls. Users are only allowed to view asset information pertinent to specific tasks, such as desktop workstation refresh projects or tracking end-of-life devices. While he encourages users to complete Armis training on search and filtering capabilities, he provides convenient pre-built Armis dashboards as an alternative for busy team members.

In line with the MNGE's strategic investment in AI tools, McLaughlin's team uses Armis to ensure safe and compliant usage. The platform detects and reports on AI traffic in the network to help the team proactively identify and curb shadow AI.

Still in the early stages of Armis Centrix™ for VIPR Pro – Prioritization and Remediation implementation, McLaughlin has recently launched a remediation campaign. Using vulnerability data from a third-party audit, he uses Armis Centrix™ for VIPR Pro – Prioritization and Remediation to track remediation and plans to present a report to the board, highlighting successes with tangible metrics.

"Armis Centrix™ for VIPR Pro – Prioritization and Remediation is a great tool to demonstrate our value to our finance team and CIO. The ability to tie a remediation campaign directly to how we've eliminated vulnerabilities over the last six months is a highly compelling way to tell our story. Armis helps us ensure that our security strategy is being comprehensively deployed. We're looking forward to expanding our utilization of the technology," said McLaughlin.

To further strengthen the organization's exposure management strategy and as a complement to Armis Centrix™ for VIPR Pro – Prioritization and Remediation, McLaughlin is exploring Armis Centrix™ for Vulnerability Management Detection and Response, which focuses on discovery, profiling, and active monitoring of all connected as-sets and provides an undisruptive, intelligence-driven alternative to traditional broad network vulnerability scanning to continuously assess risks on every asset, eliminate lengthy scan cycles, and find and resolve vulnerabilities faster.

ARMIS™ from ServiceNow

See how leading organizations secure
their environments with Armis.

[See Armis Centrix™ in Action](#)

**Armis from ServiceNow, the cyber exposure
management and security company, protects the
entire attack surface and manages an organization's
cyber risk exposure in real time.**

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets—from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7. Armis is a privately held company headquartered in California.