Use Case Solutions for Federal Tribes and Casinos

The Problem

Federal tribes and casinos operate in a complex environment with the need to comply with multiple layers of regulations.

These entities must adhere to tribal, federal, and sometimes state regulations, all while ensuring their operations align with the strict standards set forth by governing bodies like the National Indian Gaming Commission. This regulatory landscape demands that their IT infrastructure be secure and compliant with various requirements including Tribal Readiness, Gaming Machines, Surveillance, and Information Technology to name a few.

Ransomware attack losses on casinos of tribal communities are staggering, exceeding millions of dollars per incident.[2]

Additionally, over the past three years, ransomware groups have targeted tribal casinos across North America, leading to operational disruptions and the theft of sensitive data.[1] The estimated financial losses from these [ransomware] attacks are staggering, exceeding millions of dollars per incident.[2]

Another challenge is the highly segmented nature of their operations. Casinos often function as separate entities from the tribes themselves, each with its own business needs. However, from an IT standpoint, the security measures are typically centralized, meaning a small team is tasked with managing the cybersecurity needs across multiple locations and business units.

This centralization can lead to inefficiencies and vulnerabilities, as the IT team must balance the need to secure the entire network while respecting the autonomy of each casino or business unit.

To more effectively manage these complexities, IT teams must:

- Segment IT Infrastructure: Ensure that different parts of the casino and tribal operations are separated to prevent one breach from affecting everything.
- Balance Security and Operations: Secure each department, like finance or HR, without disrupting daily activities.
- Maintain Compliance: Stay updated with and adhere to all relevant regulations without overextending limited resources.

These pain points create a challenging cybersecurity landscape where maintaining both security and compliance is a constant balancing act.

1. Cybersecurity Dive. November 2023.
2. SecurityAffairs. November 2021.

The Solution:
Force Multiply Your Security Teams' Efforts with BeyondTrust

In the face of shrinking federal budgets and a limited pool of cybersecurity talent, Federal Tribes and casinos are increasingly turning to security software as a practical solution to protect their operations.

It's becoming much easier and more cost-effective to invest in robust technology than to try and recruit additional personnel.

By equipping a small-but-mighty IT staff with advanced security tools, such as privileged access management and secure remote access technologies, tribes and casinos can significantly amplify their security efforts across disparate, siloed, and geographically dispersed environments. This approach not only hardens the overall security posture, but also helps retain current employees by reducing the pressure to increase headcount, making the most of existing resources to address the ever-growing need of identity-driven security.

Remote Support

Acts as a powerful force multiplier, enabling teams to maximize help desk efficiency and scale their operations with ease.

Endpoint Privilege Management

Provides a comprehensive solution to lock down vulnerable endpoints, minimize the attack surface, and offer IT teams powerful tools to manage and secure their environments effectively.

Password Safe

Allows organizations to protect their privileged credentials across the board, ensuring that unauthorized access is prevented, and compliance requirements are met. It can scale to meet the security needs of any organization.

Privileged Remote Access

Provides the necessary tools to ensure that both internal IT staff and third-party vendors can securely access the systems they need, no matter how geographically dispersed.

Identity Security Insights

Offers a comprehensive, continuous assessment of risks and paths to privilege across your entire identity landscape.

For smaller IT teams with limited resources, BeyondTrust acts as a powerful force multiplier.

Remote Support

Key Capabilities:

- Depth and Reach of Privileged Access Management: Allows internal IT staff to securely manage privileged access
- Secure Access and Troubleshooting: Offers both attended and unattended access to troubleshoot, update, and support various devices.
- VPN-less Secure Remote Access: Protects against unsecure remote access points by providing a secure, VPN-less tool that audits every session.
- Auditing & Compliance Initiatives: Provides comprehensive logging of all session activities, including real-time reporting and detailed video logs, to maintain compliance.

Endpoint Privilege Management

Key Capabilities:

- Least Privilege Enforcement: Enforces least privilege policies by allowing users to run only the applications and processes they need, and only for the finite amount of time required.
- Application Control: Defines and enforces strict policies on which applications can run, using Trusted Application Control (TAP) to ensure only approved software is executed.
- Operational Efficiency: Simplifies the management of user permissions, reducing the workload on IT teams and streamlining operations.

Password Safe

Key Capabilities:

- Centralized Credential Management: Easily stores and manages privileged passwords in one secure location to prevent misuse.
- Automated Password Rotation: Sets passwords to rotate automatically at regular intervals or after each use, reducing the risk of unauthorized access.
- Just-in-Time Access: Grants privileged access only when it's needed and for a limited time.

Privileged Remote Access

Key capabilities:

- Secure Remote Access for IT Administrators: Securely connects to critical systems without exposing sensitive credentials.
- Third-party Vendor Access: Allows vendors to access specific resources securely, without compromising the integrity of your systems.
- Auditing & Compliance: Ensures that your operations adhere to all necessary regulatory standards, to secure federal funding and maintain trust with stakeholders.

Identity Security Insights

Key capabilities:

- Holistic Risk Assessment: Provides a complete view of all human and machine identities, privileges, entitlements, and potential misconfigurations, to simplify attack surface management across all business units.
- Proactive Threat Detection: Understands how attackers might exploit multi-stage paths to privilege, enabling you to disrupt potential breaches before they escalate.
- Rapid Deployment and Actionable Insights: Allows deployment of the solution in less than an hour using out-of-the-box connectors.

Next Steps

By implementing BeyondTrust's solutions—tribes and casinos can substantially harden their security posture, reduce risks, and improve operational efficiency. This not only safeguards their businesses but also positions them for sustained growth and financial stability, ensuring they can continue to thrive in a complex and evolving regulatory landscape.

BeyondTrust is the global cybersecurity leader protecting paths to privilege with an identity-centric approach. We are leading the charge in transforming identity security and are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at www.beyondtrust.com.

TRIBALHUB
2025 PROUD ASSOCIATE MEMBER