NIGC Tech Alert

ZERO TRUST: A Dynamic Approach to Cybersecurity

Zero Trust is a construct that executes the continuous progression of cybersecurity tactics that shift defenses from static, network-based boundaries to make points of concentration on organization users, assets and resources. Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate least privilege per-request access decisions in information systems and services in the face of network viewed as compromised (CISA.gov). As organizations' network trends to incorporating more remote users, cloud-based and bring your own device assets that are not maintained within the network boundary, Zero Trust Architecture (ZTA) can provide an excellent way to focus on protecting all IT resources (assets, services, workflows, network accounts). In tribal gaming, Zero Trust can play a pivotal role in minimizing the impact to the core organization – the gaming operation! As digital threats grow more sophisticated, cybersecurity management is a critical priority for organizations across all sectors — including tribal communities. Zero Trust, a "never trust, always verify" security framework, offers a proven approach to protecting sensitive data, networks, and identity assets while strengthening resilience against evolving cyber risks (TribalHub.com).

The benefits of Zero Trust in tribal gaming are many. ZTA can significantly impact a gaming organization by enhancing security and compliance. It requires continuous verification of every user and device, ensuring that no one is automatically trusted, which helps prevent unauthorized access and lateral movement of threats within the network. This approach limits the potential for cyberattacks and data breaches, because it segments networks and uses technologies like multi-factor authentication and real-time monitoring. By employing Zero Trust, casinos can reduce fraud risk, protect sensitive data, and build player confidence in their gaming experience. Zero Trust transforms casinos from potential targets into more secure environments, making them less susceptible to cyber threats.

The NIST ZTA is a cybersecurity framework that shifts the focus from traditional perimeter-based security to a model that emphasizes user identity, assets, and resources. It is defined in NIST Special Publication (SP) 800-207, which outlines deployment models, use cases, and the logical components of ZTA. This architecture aims to prevent data breaches and limit internal lateral movement by ensuring that trust is never assumed, regardless of the location of the user or device NIST offers free cybersecurity tools to assist with building a Zero Trust Architecture (NIST.Gov).

The National Indian Gaming Commission requires every tribal gaming operation maintain and seek to robust their tribal internal controls as well as system internal controls as it applies to their unique organization to ensure a strong cybersecurity strategy is employed in accordance with 25 CFR 543.20.

For more information on CISA's Zero Trust Maturity Model, please find it at:
https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf

For more information on NIST Zero Trust Architecture, please find it at:
https://www.nist.gov/publications/zero-trust-architecture

For minimum internal control standards, please find the NIGC IT Audit 25 CFR 543.20 Toolkit at
https://www.nigc.gov/images/uploads/training/Toolkit_ITAudit_Rev12_4.pdf

DIVISION OF TECHNOLOGY

December 2025