nile

WHITEPAPER | GAMING & HOSPITALITY

Security, AI and Autonomous Operations:

Modern Networks That Help The House Win

How casino owners and operators can turn the odds in their favor using Nile's AI-driven, Secure Network-as-a-Service to protect revenue, run autonomously, and stay ahead of regulators and attackers, without writing hard checks.

Executive Summary

Two of the world's biggest casinos lost more than $115 million in ten days. Attackers got in through identity systems. But most of the damage came afterward, when the operators couldn't be sure which parts of their environment were still safe, and shut everything down to find out. For any casino owner, the question is no longer if an attack will happen, but whether you'll be able to keep the floor running when it does.

In September 2023, MGM Resorts and Caesars Entertainment were both compromised by the same threat actor through social engineering of help desk staff to subvert their identity provider. Once inside, the attackers had options. On a traditional network where security is layered on through firewalls, VLANs, NAC appliances, and dozens of overlay tools, knowing exactly what an attacker can and cannot reach takes days, not minutes. MGM made the only safe call available to them: shut services down. Hotel keys, reservation systems, and parts of the floor went dark because no one could confidently say which systems were still isolated from the breach. Caesars paid roughly $15 million to recover. MGM's reported losses topped $100 million. Neither outage came down to a missing security product. Both came down to how hard it is to vouch for an open-by-default network in the middle of an incident, even when network security wasn't the initial culprit.

Casinos are unique. They never close, they sit at the intersection of gaming, hospitality, and finance, and they run on tens of thousands of connected devices an owner does not directly control. Regulated gaming systems are typically already isolated, often physically or strictly logically separated to satisfy state gaming commission rules. The much larger attack surface is everything else, the hospitality, surveillance, payment, food and beverage, building, and guest networks that share infrastructure and routinely sprawl beyond the IT team's visibility.

This whitepaper is written for the people who run casinos, not the people who run networks or firewalls. It explains, in plain business terms, what a modern casino needs from its connected non-gaming infrastructure, why the legacy approach is no longer a safe bet, and how Nile's AI-driven, autonomous Network-as-a-Service narrows the blast radius of any future incident while improving operations, compliance, and the guest experience.

$8.4M
PER DAY OF DOWNTIME (MGM, 2023)

Zero Trust
PREVENTS BREACHES WITH SECURITY-BY-DESIGN

30-60%
TCO REDUCTION REPORTED BY NILE CUSTOMERS

The bottom line for owners

If your hospitality and operations network is more than five years old, the question is not whether you have firewalls. The question is what stays running, and what falls over the next time a human-targeted attack succeeds anywhere in your stack. Nile turns the network from a sprawling attack surface into a contained, monitored, predictable service that limits what any single intrusion can reach.

Table of Contents

01. What's at stake on the floor

A modern casino is one of the most demanding technology environments on Earth, and the non-gaming side of the network now carries most of the operational, financial, and reputational risk.

An integrated resort is not a single business. It is a hotel, a restaurant group, a sportsbook, a retail mall, a concert venue, a parking operation, and a regulated gaming floor, all running on one campus. The regulated gaming floor is typically air-gapped or strictly isolated under gaming commission rules. Almost everything else shares infrastructure, depends on connected technology, and cannot tolerate downtime.

What's connected to the network on a typical property

- Slot machines, electronic table games, and the casino management system that tracks every wager, win, and payout.
- Surveillance, thousands of high-definition IP cameras feeding the eye-in-the-sky, often a regulatory requirement that cannot fail.
- Hotel operations, property management, digital room keys, in-room entertainment, and back-office reservations.
- Payment infrastructure, card terminals, kiosks, ATMs, and cashless wagering apps under PCI DSS scrutiny.
- Food and beverage, point-of-sale, kitchen displays, inventory scanners, and digital menu boards.
- Building systems, access control, elevators, HVAC, lighting, and digital signage, all on the same IP network.
- Tens of thousands of guest phones expecting Wi-Fi the moment they walk through the lobby.

Hundreds of thousands of devices, most of them outside the operator's direct control, any one of them a potential way in. The pattern is well established. In March 2021, attackers compromised the cloud platform behind 150,000 connected surveillance cameras, including those at corporate offices, hospitals, and prisons. The Federal Trade Commission settled with the vendor in 2024 over the underlying security failings. In March 2024, the Daixin ransomware group hit Omni Hotels, taking room keys, point-of-sale systems, and reservations offline across the chain for nearly a week. The pattern is consistent: an opening on the periphery, then movement into the operational systems that guests touch every minute.

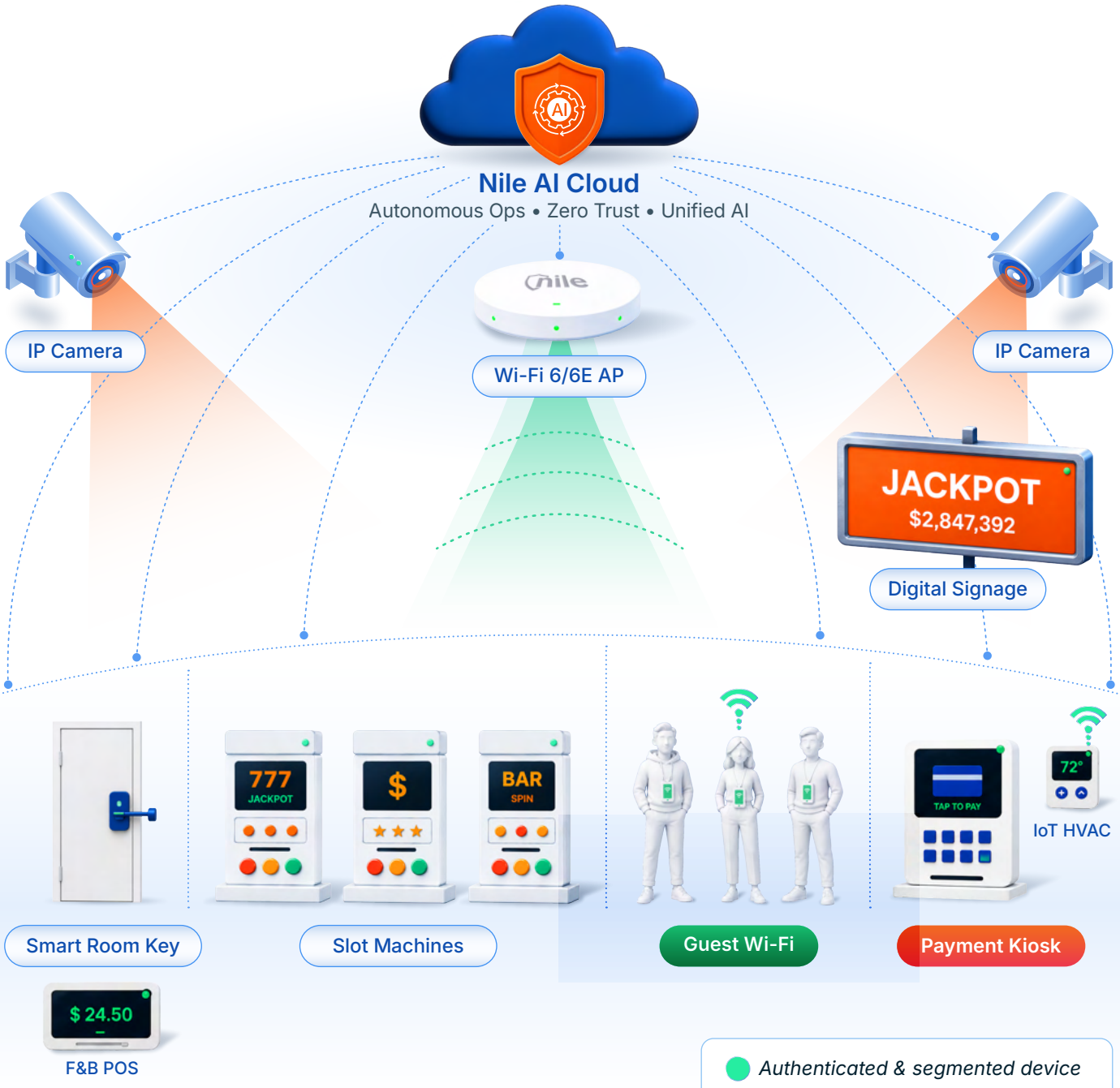
This is no longer a problem human teams can solve manually. The volume of network events, the speed at which attackers move across cloud and on-premise systems, and the regulatory expectation of continuous monitoring have all outgrown what even a fully staffed IT and security organization can keep up with on its own. The casinos that fared worst in 2023 and 2024 were not the ones without people watching. They were the ones whose architectures gave a single intrusion access to too much.

What downtime really cost MGM

Public reporting estimated revenue losses of roughly $8.4 million per day during the 2023 attack, about $100 million across ten days. The initial breach came through social engineering of the IT help desk to compromise identity systems, not through the network itself. MGM then deliberately took many connected services offline to contain the spread, which is what guests experienced as the outage. The lesson isn't that any single product would have prevented the initial breach. The lesson is what it costs to operate a network you can't quickly vouch for under pressure, when there is no way to trust in the network.

The lesson isn't that any single product would have prevented the initial breach. The lesson is what it costs to operate a network you can't quickly vouch for under pressure, when there is no way to trust in the network.

EVERY DEVICE. EVERY SEGMENT.
ONE NETWORK. AUTONOMOUSLY MANAGED.



02. Can Its Network Really Help the Casino?

Three audiences. One non-gaming network. Zero room for compromise.

A casino's non-gaming network has to satisfy three audiences at the same time: regulators who require provable controls on the systems that touch wagering, payments, and personal data, business leaders who require revenue and guest experience, and IT teams who need something they can actually run with the staff they have. The requirements below reflect what gaming commissions, payment processors, and modern attackers are now forcing onto every property.

Wired Connectivity

- **Always on.** Gaming and surveillance must run 24/7/365. Switch failures and reboots translate directly into lost revenue and regulatory exposure.
- **Built for surveillance and cashless gaming.** Multi-gigabit access and 25/100 GbE uplinks are now baseline, not a luxury.
- **Power for everything.** Cameras, phones, badge readers, access points, and signage all draw power over the network, across thousands of ports, reliably.
- **Hard separation of regulated traffic.** Gaming systems are typically isolated under state gaming commission rules, often on dedicated infrastructure. Nile is built for the much larger non-gaming environment that surrounds it, and is designed to interoperate cleanly with whatever segmentation regulators require.

Wireless Connectivity

- **Pervasive, high-density Wi-Fi.** Friday night sees tens of thousands of guest devices on the floor at once. Wi-Fi 6E/7 performance and seamless multi-floor roaming are now table stakes.
- **Hardened wireless for staff.** Beverage servers, security, valet, hosts, and housekeeping all rely on it, and need a different, more secure profile than the guest.
- **Compliant guest network isolation.** Regulators expect guest Wi-Fi to be fully segmented from gaming systems, with documented encryption and key rotation.
- **Always-on rogue detection.** Rogue access points and evil-twin attacks must be caught and shut down automatically, not weeks later in a log review.

Security

- **Zero Trust by default.** Every device, every user, every connection authenticated before it gets an IP address. The era of "trust the network because it's behind the firewall" is over.
- **Containment, not just prevention.** If a kiosk, camera, vendor device, or guest endpoint gets compromised, it must not be able to reach the payment, player-data, or operational systems. Limiting what each device can reach is the single highest-leverage control on the non-gaming side of the property.
- **IoT visibility and control.** From slots to thermostats to signage, every device must be identifiable, classified, and policed. You cannot protect what you cannot see.
- **Identity-based access.** Permissions follow the user or device, not the cable they happen to be plugged into.
- **Audit-ready by design.** PCI DSS, AML obligations, state-specific gaming commission technical standards, and privacy laws all require evidence that controls actually work, on demand. Continuous monitoring and an immutable audit trail are built into the service, not an add-on, so evidence is ready when an examiner asks.

03. Why the legacy network is a bad bet

Most casinos are running a network designed twenty years ago and patched ever since. It is costing real money every quarter, even when nothing visibly breaks.

The traditional approach is a stack of switches, access points, controllers, firewalls, NAC appliances, RADIUS servers, VLANs, and overlay tools that nobody fully understands and nobody can fully defend. The result is the worst of both worlds: high cost and high risk.

The Legacy Reality	What It Actually Costs the Business
Dozens of disparate boxes from multiple vendors, each with its own license and support contract.	Capital costs rise every refresh cycle. IT teams spend more time integrating than innovating, and finger-pointing slows resolution when something breaks.
Security bolted on through VLANs, NAC appliances, and overlays.	Misconfiguration is the leading cause of breaches. Lateral movement between segments is rarely prevented in practice, which is what made the 2024 Omni Hotels and similar hospitality-sector incidents so disruptive once attackers were inside.
Manual operations, patching, upgrades, troubleshooting all done by hand.	Outages are common, mean time to repair is hours or days, and the network team becomes a bottleneck for every other initiative on the property.
No real performance accountability. Vendors sell hardware, not outcomes.	When the floor goes slow on a Saturday night, no one is contractually on the hook. The casino absorbs the loss.
IoT and guest devices share infrastructure with regulated systems.	One compromised camera, kiosk, vendor device, or guest endpoint becomes a path to point-of-sale, room-key, and reservation systems, the pattern seen across hospitality breaches from 2021 through 2024.

Casino owners are increasingly being asked to write larger checks for the same architecture that just failed publicly for the largest operators in the industry. There is a smarter bet.

04. The Nile difference

A network delivered as a service. Zero Trust built in, not bolted on. Run by AI, not by people. Autonomous networks that deliver security and savings.

Nile is a revolutionary new company that has rebuilt the enterprise network from a clean sheet. Nile delivers wired and wireless LAN as a fully managed, AI-driven autonomous service, with Zero Trust security and a financially backed performance guarantee built into the foundation.

1 The network becomes a service, not a project

Nile delivers everything, the access points, the switches, the sensors, the management software, the AI operations, the security controls, as a single subscription. No licenses to negotiate. No vendors to chase. No NAC, RADIUS, or DHCP appliances to size and patch. Nile designs the network for the property, deploys it, and operates it from its cloud.

What that means for the owner: the network shifts from a capital expense and a perpetual integration problem to a predictable operating cost. Customers report total cost of ownership reductions of between 30 and 60 percent versus their previous architectures.

2 Zero Trust is built into the network, not layered on

Every Nile network ships with Zero Trust as a default behavior, not an upgrade. No device, guest phone, slot machine, surveillance camera, employee laptop, contractor's tablet, communicates on the network until it has been authenticated and explicitly authorized. Each authorized device is then placed in its own isolated segment, what Nile calls a "segment of one", so a compromise of any single endpoint cannot spread.

Identity-based microsegmentation, continuous agentless fingerprinting of unmanaged IoT devices using DHCP attributes, MAC/OUI, protocol behavior, and flow telemetry, native access control that replaces standalone NAC appliances, integrated DHCP, always-on rogue detection, and a fully managed Secure Guest service that keeps visitor traffic completely off the corporate network, all included, configured, and continuously updated.

How Nile limits the next hospitality-sector incident

Nile does not replace identity and access management. Where Nile changes the equation is on the day of an incident. Because every device, user, and connection on a Nile network is explicitly authorized in advance, and because every access rule is configured and documented in a single portal rather than scattered across hundreds of switches, controllers, and overlay tools, a security team can verify what is and isn't reachable in minutes, not days. The reach of any single intrusion is constrained by design to what that one identity or device is authorized to touch. Just as importantly, the operator can vouch for it. 'I know this system is protected' becomes a defensible statement, not a hope. That is what changes whether the floor stays up through an incident or has to go dark.

05. AI and autonomous operations: the third revolution

The first shift was wired-to-wireless. The second was on-premise-to-cloud. The third, and the one that decides which casinos survive the next decade, is human-operated to Autonomous Operations with AI.

Nile's network is not just managed by software. It is operated by an AI system that ingests live telemetry from every access point, switch, and sensor across every Nile customer in the world. That collective signal is what allows a single property's network to behave more reliably, more securely, and more cheaply than any human team could deliver.

For a casino, the implications are immediate and measurable.

Predictive uptime: prevent the outage instead of explaining it

Most network outages don't appear suddenly, they announce themselves quietly first. A radio drifting off channel. A switch port logging unusual error rates. A controller starting to swap memory. Human teams catch these signals after the symptom hits the floor; AI catches them before. Nile's operations engine flags degrading components, runs the diagnostic, and either remediates automatically or opens a pre-investigated ticket so a human only ever sees the issues that genuinely need a human.

For an owner, this is the difference between **a guest experience that quietly works and a Saturday-night incident bridge with the COO on it.**

Zero Trust Based Threat Prevention with AI, Eliminate Human Errors

Modern attacks no longer announce themselves with obvious malware signatures. They look like a slightly unusual login pattern from a service account, a kiosk reaching out to an IP it has never spoken to before, or a camera attempting a connection during the wrong shift. These are exactly the patterns AI was built to find. Nile's AI learns from operational and security signals across its global service footprint, distinguishing normal behavior from anomalies in seconds, not weeks.

Pair that with the Zero Trust segmentation already in place, and the result is closed-loop containment: the AI sees the anomaly, isolates the offending device automatically, and alerts the team, all before a human could finish reading a SIEM alert.

Autonomous everyday ops: solve the IT-staffing problem

Casinos have always struggled to staff and retain network specialists. The job is exhausting, the talent pool is thin, and the floor doesn't sleep. Nile collapses the day-to-day: configuration drift, firmware patching, capacity planning, RF tuning, port resets, certificate rotations, segmentation policy enforcement, and audit-log generation are all handled by the service. Local IT shifts from running the network to running the business, onboarding a new restaurant, opening a new tower, integrating a loyalty platform.

Network intelligence that compounds

When Nile's AI detects, diagnoses, or remediates an issue at one customer, the lesson is applied across the entire customer base. A casino that joins Nile in 2026 inherits every problem already solved for every other Nile customer, including hospitals, universities, and Fortune 500 enterprises. The same problem does not happen twice, anywhere.

Backed by a guarantee

Nile is the only enterprise network that contractually commits to wired and wireless availability, coverage, and capacity. If the AI-driven service does not perform, Nile is financially accountable. That kind of accountability does not exist in the box-and-license model the industry has lived with for thirty years.

06. Nile Delivers Outcomes Against Stringent Requirements

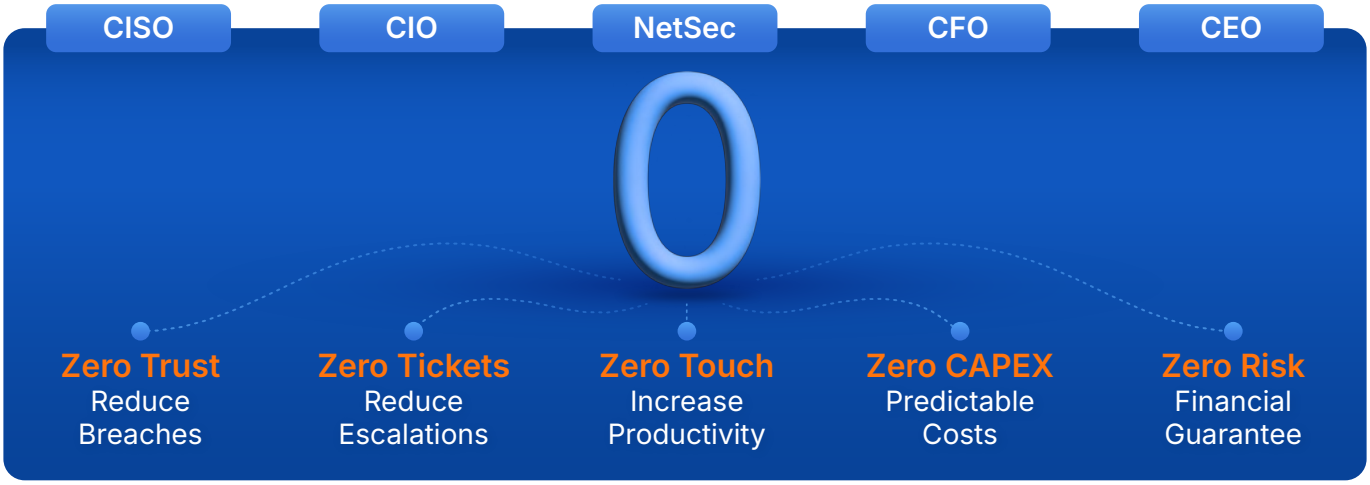
Every requirement in Section 02 is addressed natively by Nile's secure Network-as-a-Service.

There is no checklist of optional add-ons, no fragmented tech stack, and no claim that Nile replaces controls that gaming regulators require on the gaming network itself.

Casino Need	Nile Capability	Business Outcome
24/7 wired availability for gaming and surveillance	AI-driven self-healing on hardened, redundant switching, with a financially backed availability SLA	Predictable uptime on the floor; outages prevented before they hit guests
High-density, multi-story Wi-Fi	Wi-Fi 6E/7 APs with continuous, AI-tuned RF optimization and seamless roaming	Consistent guest experience that drives loyalty and on-property spend
Hard isolation of non-gaming hospitality and operations traffic	Identity-based microsegmentation with default-deny, complementing whatever isolation gaming regulators require	Cleaner audits across PCI, privacy, and gaming commission technical reviews of the non-gaming environment
IoT and OT device sprawl (cameras, slots, signage)	Continuous agentless fingerprinting (DHCP attributes, MAC/OUI, protocol behavior, flow telemetry) and per-device isolation ("segment of one") for unmanaged endpoints	A compromised IoT device cannot become an entry point to anything else
Threats hidden in normal-looking traffic	AI anomaly detection trained across Nile's global customer base, paired with automatic containment	Attacks caught and isolated in seconds, not in the post-mortem

Casino Need	Nile Capability	Business Outcome
PCI DSS, gaming commission, and privacy compliance	Built-in encryption, native NAC, immutable audit trails, continuous AI posture monitoring	Lower compliance burden, fewer findings, faster regulator response
IT staff shortage and rapid expansion	Autonomous operations handle patching, tuning, and policy; cloud service scales by adding hardware	30-60% TCO reduction; new space online in days, not quarters

Casinos always have to balance audience engagement and satisfaction with risk. It's a high stakes game, and the outcomes have to be extremely compelling for the Casino to place the bet. With Nile's secure NaaS solution, no matter who the stakeholder is, the outcomes are very promising.



07. Why this resonates in the boardroom

Revenue Protection

The largest non-gaming financial event most casinos will face this decade is a connected-systems outage or hospitality breach. Nile's Zero Trust architecture narrows what any single intrusion can reach, and AI-driven operations catch the early signals of failure before they reach the floor. The performance guarantee provides recourse if the network underperforms. One avoided day of property-wide disruption more than pays for the service.

Guest Experience

A guest whose Wi-Fi drops in the lobby or whose digital room key fails tells the story to others. Nile's high-density Wi-Fi, AI-tuned roaming, and Secure Guest service are designed for the moments when guests judge the property hardest, at peak occupancy and during major events.

Regulatory Standing

Gaming commissions, PCI DSS auditors, and privacy regulators are converging on the same expectations: documented segmentation, identity-based access, encrypted management, continuous monitoring, and a clean audit trail. Nile delivers all of them by default, with AI-generated evidence that can be handed directly to a regulator.

AI-readiness for the rest of the business

The casinos that win the next decade will be the ones whose loyalty programs, cashless gaming, video analytics, and personalization engines all run on AI. None of those initiatives perform on a network that is itself manually operated and constantly congested. Nile gives the rest of the property the high-performance, intelligently managed foundation those investments need to actually pay off.

08. The smarter bet for the modern casino

Casinos run on a simple principle: control the environment, manage the risk, protect the experience.

The non-gaming network is the modern embodiment of that principle on every part of the property that is not the gaming floor itself, and legacy infrastructure is quietly costing operators real money every quarter, with bills measured in hundreds of millions when something goes wrong. Nile gives owners a different option: a network delivered as a service, with Zero Trust security and AI-driven autonomous operations built in, backed by a financial performance guarantee, and priced as a predictable monthly cost.

Next Step

Nile offers casino operators a structured assessment of current wired, wireless, and security posture, mapped to gaming-specific requirements with a clear business case for transition. The conversation starts with the floor and the business, not a hardware diagram.

About Nile

Nile builds the world's most secure networks and delivers them as-a-service, becoming a force multiplier for IT.

Ready to Get Started?

Let's Talk ↗