EXTRAHOP

Securing the Guest Journey and Protecting the Integrity of Gaming Operations

Keep Critical Technology and SaaS Applications Free from Threats and Disruption with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: From Guest Experience to Systemic Sabotage

The hospitality and gaming industry operates in a high-stakes environment where a single minute of digital downtime translates directly to thousands of dollars in lost revenue and a collapse in guest trust. By 2026, the sector will have evolved into a hyper-connected ecosystem of omnichannel guest experiences, AI-powered casino floors, and cloud-integrated property management systems (PMS). While these innovations drive operational excellence, they have exponentially expanded the attack surface, making cybersecurity a core component of brand reputation and operational survival. Hospitality operators face several critical friction points:

- **The Escalation of Nation-State and Destructive AI Attacks:** Geopolitically motivated actors and advanced ransomware groups have shifted from simple data theft to functional destruction. In early 2026, a destructive breach of a major global distribution system (GDS) demonstrated this reality by paralyzing booking engines for thousands of properties worldwide. A disruption to cage systems or slot machine networks can cost operators over $9,000 per minute, turning a state-sponsored event into a massive revenue crisis.
- **The Identity and Post-Compromise Crisis:** Advanced threat actors now prioritize the long-term exploitation of player loyalty programs and high-value guest identities. Using generative AI-powered vishing campaigns and deepfake impersonation, they bypass traditional authentication to navigate undetected from guest Wi-Fi segments toward high-value player rewards databases. Identifying this post-compromise behavior on the wire is the only way to prevent mass exfiltration of sensitive information.
- **The IoT and Surveillance Blind Spot:** Modern properties run tens of thousands of unmanaged endpoints, including smart TVs, digital locks, and 4K AI surveillance cameras, that cannot host security agents. This agent blind spot leaves specialized traffic invisible to traditional EDR tools. Attackers frequently use these unmanaged nodes as a foothold to disable security tools on adjacent systems, creating a massive visibility gap that violates core security principles.
- **Regulatory Rigor and Uptime Convergence:** 2026 mandates have fundamentally changed the compliance landscape. The rollout of PCI DSS 4.0.1 requires institutions to prove continuous, real-time behavioral monitoring across the Cardholder Data Environment (CDE). Simultaneously, state and tribal gaming commission mandates require rigorous auditing of network access to ensure the integrity of gaming operations.

KEY CAPABILITIES

Depth and Breadth of NDR Performance: Monitors interactions by decrypting and decoding over 90+ protocols at 100 Gbps to protect high-volume property management systems and automated casino floor operations.

The Definitive Data Source for the AI-Enabled SOC: Provides high-fidelity wire data for SOC automation, delivering unalterable ground truth to accelerate detection and remediation.

AI-Powered Cyber Threat Detection: Identifies lateral movement and ransomware targeting booking services and loyalty applications via machine learning and behavioral baselining.

Unified Agentless Visibility: Discovers all assets, including unmanaged IoT and cloud workload, without installing software or risking system stability.

Strategic Line-Rate Decryption: Analyzes TLS 1.3 and PFS to expose hidden threats without adding latency to sensitive financial or guest transactions.

High-Fidelity Performance Metrics: Troubleshoots disruptions and verifies SLAs using 5,000+ metrics for insight into guest Wi-Fi and booking engine performance.

Continuous Forensic Recording: Maintains unalterable transaction records for PCI DSS 4.0 and gaming commission mandates, accelerating incident reconstruction.

The Solution: RevealX Network Intelligence

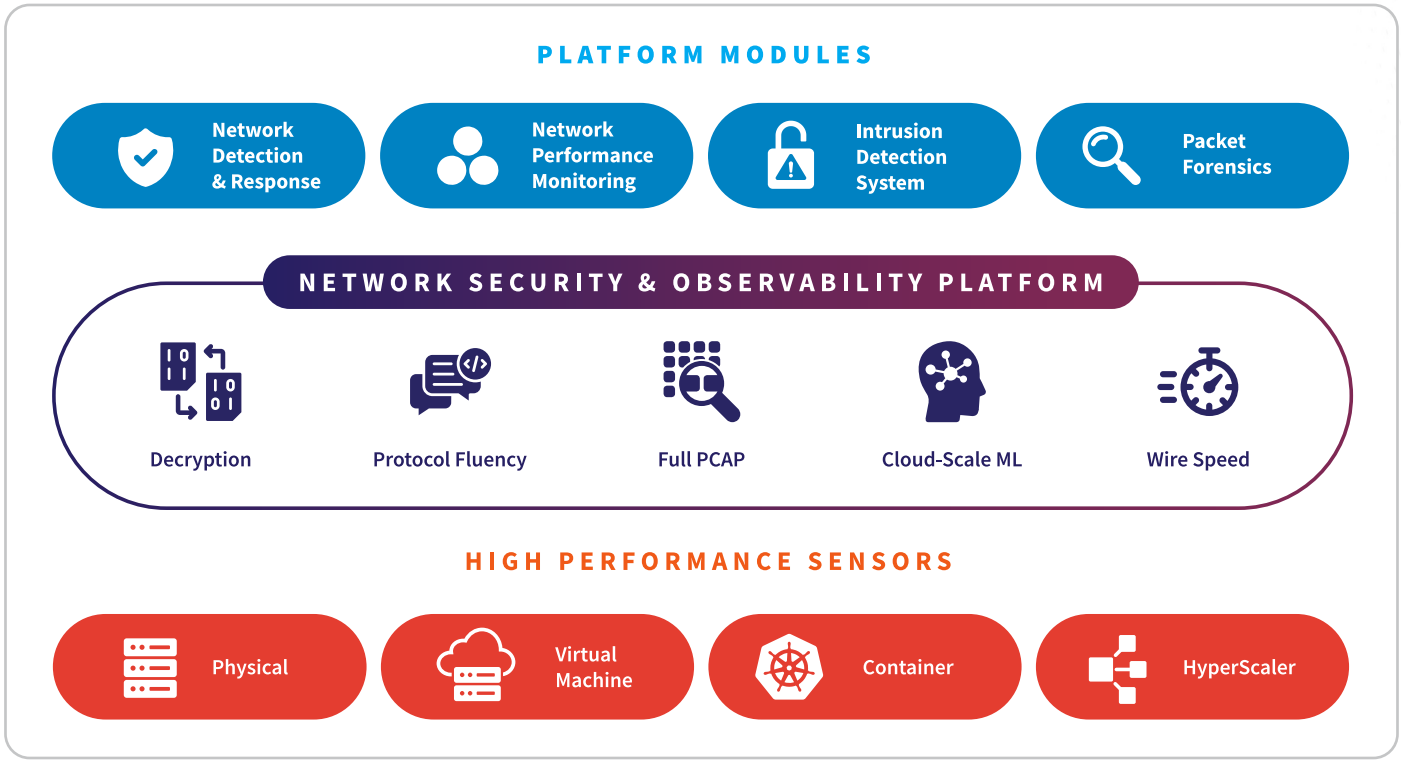
ExtraHop RevealX provides the network intelligence required to secure high-value guest data, maintain gaming floor integrity, and ensure operational continuity. By delivering a unified view of converged IT, IoT, and OT environments, RevealX enables security and network teams to detect sophisticated threats. It ensures availability across mission-critical systems, including property management systems (PMS), automated gaming floors, and reservation networks.

Neutralizing destructive attacks or digital sabotage requires stopping actors before they execute malicious commands. By monitoring the wire rather than relying on vulnerable endpoint agents, RevealX detects lateral movement and credential abuse as attackers pivot from guest Wi-Fi or compromised vendor portals toward high-value property assets. This agentless approach ensures that even if an unmanaged device such as a digital lock or RFID system is compromised, the platform identifies the anomalous behavior in real time. Security teams can then isolate affected segments to preserve financial transaction integrity and prevent ransomware-induced shutdowns.

Supporting digital modernization and meeting stringent regulatory demands requires total network visibility. A real-time view across gaming floors, hotel clusters, and cloud-managed booking engines allows teams to stay ahead of outages and breaches. Because log and endpoint data are modifiable and often disabled by advanced threats, the network provides the only immutable source of truth that cannot be subject to tampering or evasion.

RevealX decodes over 90+ protocols at 100 Gbps to provide persistent visibility across unmanaged IoT, surveillance systems, and POS terminals where agents cannot be installed. A key differentiator is the ability to perform line-rate decryption of TLS 1.3 and PFS. This ensures attackers cannot hide lateral movement or digital credit card skimming within encrypted payment integrations or booking APIs. By integrating NDR and NPM, teams can troubleshoot guest Wi-Fi latency or active ransomware staging before revenue streams are interrupted. This independent observation provides the foundation for a Zero Trust Architecture and ensures continuous compliance with PCI DSS 4.0.1 and evolving gaming commission audit requirements.

ExtraHop NDR Platform



NDR Technology Use Cases for the Hospitality & Gaming Industry

Nation-State Attacks	Detects stealthy lateral movement and data staging in long-term campaigns targeting high-value player databases, financial settlement systems, and global reservation networks.
Threat Detection & Response	Investigates hidden threats across converged IT/IoT environments, filling visibility gaps in property management systems (PMS) and casino management systems (CMS) where logs fail.
Threat Hunting	Leverages behavioral baselining to find signature-less anomalies in specialized gaming traffic (e.g., G2S, SAS) before they impact cage operations or floor integrity.
SOC Modernization	Unifies SOC/NOC workflows and uses AI prioritization to reduce alert fatigue, accelerating response times for high-traffic environments like sportsbooks and online gaming platforms.
Incident Response & Investigation	Delivers forensic visibility into unmanaged IoT devices (smart locks, RFID) and provides unalterable records of administrative commands for rapid root-cause analysis.
Lateral Movement	Uses peer-group clustering to catch attackers pivoting from guest Wi-Fi segments toward critical Cardholder Data Environments (CDE) or high-limit room controllers.
Cloud Workload Security	Provides agentless visibility for cloud-integrated booking engines and mobile app backends, discovering shadow IT and unmanaged assets across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse and OAuth token theft in real time. This focuses on mission-critical developer workstations and secure administrative gateways to stop attackers who use voice-based social engineering to bypass traditional MFA.
Ransomware Attacks	Identifies early-stage ransomware patterns, such as file staging or unusual encryption, to isolate hosts before exfiltration of player loyalty data or systemic floor shutdowns.
Unmanaged Devices	Fills the visibility gap for thousands of unmanaged endpoints, including 4K AI surveillance cameras, digital signage, and slot machines that cannot host security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity even when endpoint agents are disabled, ensuring persistent visibility across legacy POS systems and HMI kiosks.
AI Security	Monitors interactions with generative AI tools used for dynamic pricing, personalized marketing, or automated concierge services to prevent prompt injection or data leaks.
Operationalizing Zero Trust	Acts as the independent observer, detecting policy drift and providing empirical proof that network segmentation between guest, employee, and gaming zones is effective.

NPM Technology Use Cases for the Hospitality & Gaming Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing clear visibility into latency for high-frequency sportsbook transactions and mobile guest check-in apps.
Operational Resilience	Resolves infrastructure degradation before it hits guest experience or gaming continuity, ensuring 24/7 availability for mission-critical CMS and surveillance services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between hotel operations (IoT), IT network teams, and third-party vendors.
Migrate Workloads to the Cloud	Maintains performance during PMS or ERP migration by auto-mapping dependencies and using on-premises baselines to validate successful cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for booking APIs, payment gateways, and real-time inventory systems.
Forensic-Grade Investigations	Combines long-term metadata with scalable PCAP for an unalterable record, enabling deep-dive analysis into past Black Friday outages or telemetry drops.
Application Performance Monitoring	Complements APM by decoding 90+ protocols (including G2S and HL7 for resort clinics), providing real-time insights into command processing time vs. network latency.

Hospitality & Gaming Compliance & Regulatory Use Cases

Cardholder Data Security	Global	PCI DSS 4.0.1	Continuous CDE Monitoring: Detects unauthorized payment scripts or exposed PAN in real time. RevealX validates Requirement 6.4.3 to identify digital skimming via line-rate analysis.
Cybersecurity Maturity	Global	NIST CSF 2.0 (PCI Alignment)	Detection and Response: Powers Detect (DE) and Respond (RS) functions. Identifies blast radius in real time to spot and scope anomalies.
Gaming Operations Integrity	US (Tribal)	NIGC MICS	Internal Control Validation: Automates discovery and logging of gaming system access. Ensures compliance by monitoring proprietary protocol anomalies.
Regulatory Best Practices	Global	NIST SP 800-53 (NIGC Support)	System Integrity (SI): Essential for Audit and SI control families. Provides continuous monitoring (CA-7) to detect unauthorized changes.
Guest Data Privacy	Global	GDPR / CCPA	Data Breach Notification: Attributes personal data access paths. Provides forensic evidence of scope to meet strict notification windows.
Financial Crime Prevention	Global	AML / FATF	Anomalous Transaction Monitoring: Flags protocol abuse at cages or digital wallets. Correlates user behavior with high-value financial flows.
Digital Perimeter Integrity	US (NV)	Nevada Reg 5	Perimeter Integrity: Validates that gaming and surveillance networks remain isolated. Provides forensic proof of integrity to prevent sanctions.

Customer Benefits: Ensuring Guest Experience and Operational Resilience Across the Modern Hospitality Ecosystems

Visibility into network truth is the cornerstone of every modern guest protection and operational resilience framework. Complete, real-time visibility from RevealX is vital for ensuring the sub-second response times required for automated check-in systems, sportsbook transactions, and real-time gaming floor monitoring. By monitoring the wire, hospitality and gaming operators safeguard against cyber threats and protocol anomalies that could jeopardize property-wide uptime, cage liquidity, and broader brand reputation.

The transition to smart hotels and AI-integrated casino floors provides the agility required for rapid innovation, yet it often creates exploitable blind spots in the transaction path. RevealX enables hospitality organizations to embrace a digital-first approach while maintaining operational resilience across legacy property networks and distributed supply chains. By observing actual traffic flows, including PMS, POS, and G2S, instead of relying on modifiable logs, firms gain the definitive, forensic evidence needed to satisfy global regulatory audits for PCI DSS 4.0.1 and NIGC MICS.

RevealX provides essential visibility for the expanding ecosystem of unmanaged devices and third-party maintenance connections in modern resorts. Monitoring these unknowns, from digital locks and RFID systems to slot machine controllers and IP cameras, eliminates the blind spots inherent in agent-based security. RevealX identifies lateral movement and credential abuse before they compromise safety systems or the exfiltration of sensitive player loyalty data. With RevealX, hospitality and gaming firms gain real-time discovery and classification of every entity on the network to ensure guest experiences and public safety remain uninterrupted.

> "Developers aren't antisecurity; what they are is anti-friction. With RevealX, we're removing that friction traditionally associated with security and becoming part of their development cycle. That's a win-win across the board."
>
> **DAN MCDANIEL**
> Chief Architect & Information Security Officer
> A Leading Software Gaming Manufacturer

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments:
Home Depot | Ulta Beauty | Seattle Children's Hospital

Or contact us to schedule your personalized demo and security assessment.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com