

THREATDEFEND FOR CASINOS & GAMING

Securing player data, protecting transactions, and maintaining compliance in gaming environments

Relevant ThreatDefend Modules



Falcon EDR/XDR

Secure gaming terminals, POS systems, and staff or franchisee devices



Falcon Identity

Monitor staff, vendor, and third-party access to gaming platforms and hotel operations



Falcon Discover

Inventory casino floor, hotel, and back office infrastructure for risk mapping



Falcon Exposure

Remediate vulnerabilities in gaming software, payment apps, and cage systems



Cribl Stream

Enable PCI- and audit-grade logging across all gaming and hospitality environments



Corelight + Zeek

Monitor lateral movement and threat signals across segmented gaming and hotel networks

Top Cybersecurity Threats Facing Casinos & Gaming

1

POS Malware or Ransomware

Targeting payment terminals and cage systems during peak hours

2

Account Misuse

Compromised logins granting access to hotel, back office, or gaming platforms

3

Compliance Violations

Gaps in PCI, GLI, or gaming board audit readiness due to poor log visibility

Take Action

Casinos must align cybersecurity with operational uptime, guest privacy, and state or gaming board compliance requirements.

Why It Matters

A breach doesn't just stop the floor, it risks your license. ThreatDefend helps operators maintain trust, resilience, and regulatory standing across casino networks.