ThreatGuard

DATASHEET

APCON

Advanced Network Security Monitoring and Threat Detection Software

ThreatGuard Security Software

ThreatGuard is APCON's network security monitoring software, delivering real-time threat detection, deep packet inspection, and intrusion analysis through a single platform. Combining live and recorded traffic analysis, intrusion detection, AI-assisted investigation, and automated alerting, ThreatGuard gives security teams complete visibility into their network. It is available as standalone software on customer-provided hardware or fully integrated on APCON's IntellaStore® IV security appliance.

Designed for the Security Professional

ThreatGuard is designed for network security administrators, Security Operations Center analysts, and information technology and network operations teams in enterprise, government, industrial, and critical infrastructure environments. These teams need visibility beyond firewall logs and endpoint alerts. ThreatGuard provides insight down to the packet level.

Network Security at the Packet Level

ThreatGuard performs deep packet inspection to identify malicious patterns, unusual protocols, and application-layer behaviors that surface-level monitoring misses. It analyzes live and recorded traffic, extracts session metadata, maps connected devices into an interactive connection graph, and automatically records both the sessions and the context investigators need when something of interest occurs.

How ThreatGuard Works

ThreatGuard ingests live traffic from a SPAN port, network TAP, or the IntellaStore® IV, applies Deep Packet Inspection, and runs it through a continuous intrusion detection engine. When a threat is identified, email or mobile push alerts are sent and packet captures can be initiated. Administrators investigate through dashboards, a connection graph, and an AI-assisted chat interface that turns network events into actionable intelligence.

Why Network Visibility Matters

Time between compromise and detection is measured in days, and perimeter defenses alone leave a critical gap: the network itself. ThreatGuard closes that gap with continuous monitoring, automated detection, and the tools to investigate and respond quickly. For organizations that cannot afford the cost of a breach, ThreatGuard is not optional; it is essential.

Capture What Matters, Get Notified Instantly

ThreatGuard gives administrators precise control over what gets captured and when. Pre-defined conditions, including specific addresses, protocols, traffic volumes, behavioral patterns, or matched threat signatures, automatically initiate packet captures when user-defined criteria are met. Capture files are managed directly within ThreatGuard: configure auto-start recordings, upload existing capture files up to 50GB for analysis, rotate and age out older captures, and buffer data to keep only the most relevant traffic. When a threat is detected, email alerts are dispatched immediately, and the APCON Mobile App delivers push notifications so administrators can respond from anywhere.

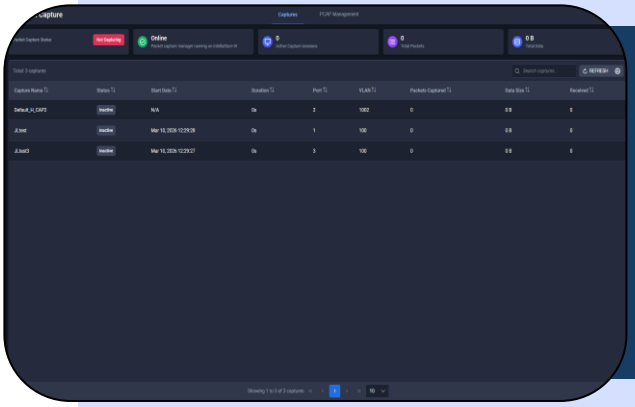

Figure 1: Packet Capture Status

The Best of Both: AI Chat and Rule-Based Detection

ThreatGuard combines the precision of defined detection rules with the interpretive power of artificial intelligence. ThreatGuard integrates with industry-standard intrusion detection rule sets, and administrators can upload custom rules and scripts to extend coverage for unique environments or organization-specific threat models. The built-in chat interface lets analysts query live and recorded data in natural language to understand what the data is showing, and translate complex network activity into clear, contextual answers that accelerate investigation for the entire security team.

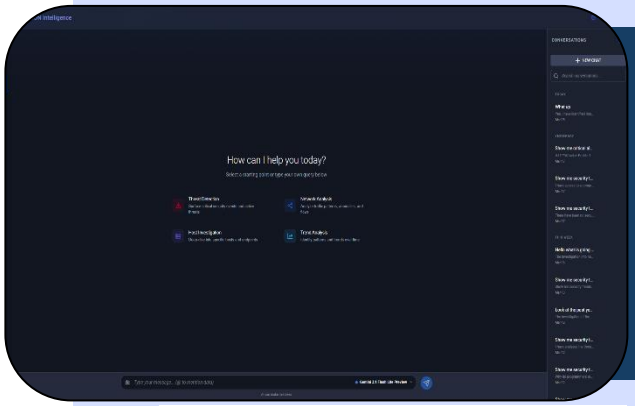

Figure 2: APCON Intelligence

Get Insight into What Traffic Is on The Network

ThreatGuard's dashboards display metadata for every session on the network, including source and destination addresses, protocols, time duration, and data volume. When a dangerous address is involved in a breach, that context is immediately visible, giving analysts a direct path to the relevant traffic. The Connection Graph maps every connected device in a visual representation of the network to pinpoint suspicious access and focus investigations. ThreatGuard also monitors certificate compliance, highlighting expired certificates on the Connections screen with a single-click status overview.

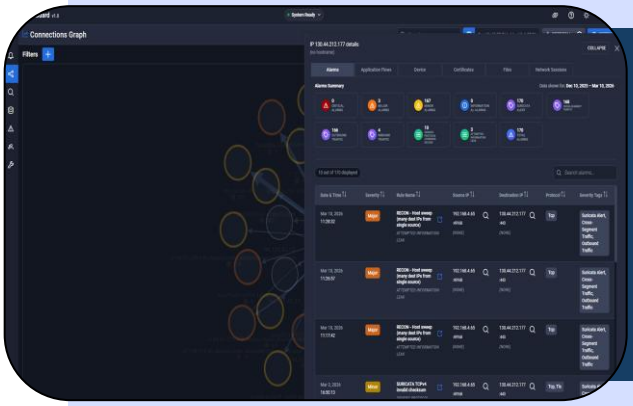

Figure 3: Connections Graph

Application Visibility and Threat Intelligence

ThreatGuard uses deep packet inspection to identify which applications are being accessed across the network and by whom, going beyond ports and addresses to reveal actual application usage. Teams can query by application, correlate users to services, and quickly identify unauthorized activity. This feeds into ThreatGuard's network intrusion detection system, which continuously evaluates traffic to identify known threat signatures and behavioral anomalies. ThreatGuard aggregates network metadata and security logs into a single location for analysts to query without hunting through multiple systems, and dashboards display network activity, threat alerts, session metadata, and the connection graph at a glance.

Figure 4: Applications Dashboard

ThreatGuard on the IntellaStore® IV

For organizations seeking a turnkey deployment, ThreatGuard runs on APCON's IntellaStore® IV, an appliance that pairs ThreatGuard's detection capabilities with high-performance hardware designed for network security and traffic monitoring. The IntellaStore® IV comes with ThreatGuard pre-installed and pre-integrated, delivering everything needed for full network visibility and threat detection in a single compact appliance with no additional hardware configuration required.

Figure 5: IntellaStore® IV with ThreatGuard

The IntellaStore® IV works in tandem with ThreatGuard. IntellaStore® IV's traffic optimization layer collects raw traffic from multiple sources, filters out noise, and delivers only relevant data for processing; this maximizes detection accuracy while reducing storage and compute overhead. With 24 high-speed monitoring ports that support 1G/10G/100G, and up to 32TB of onboard storage, the IntellaStore® IV handles high-volume environments without dropping packets or missing events.

At its core, the IntellaStore® IV is a network visibility platform with an advanced security solution built in. The APCON Intelligent Processor runs ThreatGuard locally, combining APCON's traffic collection and optimization capabilities with ThreatGuard's deep inspection, intrusion detection, and investigation features, all in one device. For teams that need both network visibility and threat detection without managing multiple systems, the IntellaStore® IV with ThreatGuard is the complete solution.

A Natural Fit for Your Security Stack

ThreatGuard integrates with existing security infrastructure rather than replacing it. It complements firewalls, endpoint detection tools, and zero-trust architectures by adding the layer most environments lack: deep visibility into actual network traffic. ThreatGuard aggregates threat data and session metadata in one place to enrich existing security workflows with the network context needed to accelerate triage and response. Rather than adding complexity, ThreatGuard makes every security tool already in place more effective.

Ready for What's Next

ThreatGuard expands with the networks it protects. As traffic volumes grow and topologies evolve, ThreatGuard adapts by supporting high-throughput environments, expanding monitoring coverage, and integrating new detection rules without requiring a platform replacement. Regular software updates keep detection capabilities current with the latest threat signatures and security standards, so organizations are never defending against today's threats with yesterday's tools.

Get Started with ThreatGuard

Network threats do not wait, and neither should your visibility. ThreatGuard gives security teams the real-time detection, deep inspection, and investigative tools they need to stay ahead of threats before they become incidents. To learn more about ThreatGuard, request a product demonstration, or speak with an APCON solutions specialist; visit **apcon.com** or contact your APCON sales representative. Discover why organizations trust APCON to deliver the network visibility and security performance their infrastructure demands.

How to Order

ACI-9510-001	**ThreatGuard Security Software**
ACI-4235-IS4-2-1	**IntellaStore® IV Appliance with ThreatGuard**

All IntellaStore® IV features and specifications are subject to change. Contact APCON for current standalone hardware validation and support.

Recommended Hardware Specifications

RAM	**32+ GB (recommended)** **24 GB (minimum)**
CPU	**16+ Cores (recommended)** **8 Cores (minimum)**
Storage	**2TB+ SSD (recommended)**
OS	**Alma Linux 10+**

APCON, Inc. *▪ 9255 SW Pioneer Court, Wilsonville, Oregon 97070*
+1 503–682–4050 ▪ 1–800–624–6808 ▪ @APCON ▪ company/APCON ▪ apcon.com