IPS

Intrusion Prevention System

Kognitive Networks' Intrusion Prevention System (IPS) is a powerful, real-time defense against cyber threats. Built to monitor and protect your network traffic, the Kognitive IPS leverages advanced threat detection using Talos rulesets, blocking malicious activity before it can impact your business operations.

Advanced Threat Detection

Kognitive's IPS leverages both signature and anomaly-based detection to identify and mitigate threats. Continuous scanning across multiple network layers ensures comprehensive defense against known and emerging risks. Using Talos rulesets, threat protection signatures and patterns are consistently updated and provide market leading defenses to protect your most vital network resources.

Automated Risk Mitigation

The system autonomously executes real-time actions, **blocking malicious traffic** and adjusting firewall rules in response to emerging threats. Supporting volume and type-based notifications with the capability to quarantine bad actors, this proactive response minimizes the burden on IT teams while accelerating threat resolution.

Secure Threats Dashboard

Kognitive's IPS provides in-depth telemetry and **real-time alerts** through a secure cloud portal. This visibility offers actionable insights, empowering faster threat detection and response to maintain network security while ensuring compliance with security protocols and standards.

Comprehensive Security for your Network

Zero Trust Network Access (ZTNA)

As the cornerstone of a secure architecture, Kognitive's ZTNA framework enforces a strict **never trust, always verify** approach, validating users and devices before granting access to the cloud portal and connected resources. With Integrated Access Management (IAM) and Multi-Factor Authentication (MFA), risk of unauthorized access is minimized at every entry point.

Edge and Cloud Security

Simplifying the deployments with an **integrated firewall and content filtering** enables consistent enforcement of security policies across edge and cloud environments. This dual-layered approach safeguards network integrity, reducing vulnerabilities in distributed setups.

Deep Packet Inspection (DPI) and Content Filtering

As part of the next-gen firewall, the DPI engine inspects data payloads, **recognizing usage patterns and signatures** in over 2000 applications to detect hidden threats. Content filtering further reinforces security, blocking access to malicious websites and phishing domains across 50+ categories.

Information Security is woven into every layer of your network with Kognitive Networks' powerful multi-level solutions. Reach out to **sales@kognitive.net** to see how the integrated Intrusion Prevention System provides seamless security, from the edge to the cloud.