# Cisco Secure Network Analytics + Splunk

- **Enhance Network Visibility:** Use the network as a sensor for comprehensive traffic visibility.
- **Reduce Data Volume:** Compress network telemetry by 6-8x, simplifying analysis and reducing costs.
- **Improve Threat Detection:** Apply behavioral analytics and machine learning to identify threats.
- **Integrates with Public Cloud:** Supports AWS and Azure telemetry for hybrid environment security.

## Unified Network Detection and Response for Enhanced Security

Cisco Secure Network Analytics (SNA), combined with Splunk Enterprise Security (ES), offers a powerful and unified solution for the Security Operations Center. SNA leverages the network as a sensor, consuming flow data directly from your infrastructure to provide comprehensive visibility into network activities without the need for additional probes or sensors.

The solution applies advanced behavioral analytics and machine learning to identify suspicious and malicious activities, delivering high-fidelity security insights directly into the Splunk platform. This integration helps you reduce data volumes by compressing raw network telemetry, making it easier for security teams to understand and respond.

Ideal for enterprises with mature security operations, regulated industries, and government agencies, this offering enhances threat detection, supports compliance, and offers seamless integration with both on-premises and cloud environments. Together, Cisco SNA and Splunk provide a comprehensive, cost-effective approach to network security and incident response.

## Advanced Network Monitoring and Threat Detection

Cisco SNA stands out for its comprehensive and efficient approach to network detection and response. Key functions include:

- **Network as a Sensor:** SNA consumes network flow data directly from your infrastructure, providing visibility without additional probes or sensors.
- **Data Compression:** Proprietary de-duplicating and stitching turn raw network telemetry into meaningful network conversation records, reducing data volumes by 6-8x.
- **Behavioral Analytics and Custom Rules:** Advanced analytics and machine learning create a running baseline of network behavior, identifying threats. Custom rules support security, compliance, and network operations needs.

**General Ledger of Network Telemetry:** Incident responders use SNA as the record of all network activity, quickly tracing incidents, including lateral movement and data exfiltration.

- **Seamless Integration:** SNA integrates smoothly with Splunk ES, enhancing threat detection and incident response capabilities without increasing Splunk costs.

This solution offers deeper visibility, advanced analytics, and efficient data management without additional probes, agents, or decryption.

> “Now we can identify vulnerabilities in our systems we weren’t able to before with other platforms. With Splunk, we have what we need to improve our security strategy and better protect Soriana’s assets and information.”
>
> **– Sergio Gonzalez, CISO, Soriana**

Enhance your security operations with the combined power of Cisco Secure Network Analytics and Splunk.

Learn more