Intrusion

intrusion.com | 888-637-7770

Shield Sentinel

High-Throughput Network Observability for Large-Scale Infrastructure

Gain scalable visibility into high-capacity network environments without introducing latency, operational disruption, or inline risk. Shield Sentinel is purpose-built for environments operating at **100 Gbps and beyond**, enabling organizations to capture and retain valuable network telemetry for security operations, forensic investigation, compliance initiatives, and long-term traffic analysis, all through efficient metadata collection, flow summarization, and passive monitoring architecture.

Built for Visibility at Scale

Shield Sentinel operates passively through network TAPs or port mirroring, allowing organizations to observe network traffic without placing an inline appliance in the production path. Rather than attempting to perform deep inline inspection or enforcement, Shield Sentinel focuses on efficiently recording and summarizing high-volume network metadata.

Captures metadata across:

- TCP traffic
- UDP traffic
- ICMP traffic
- DNS queries and responses
- Network flow activity

This approach enables organizations to retain actionable visibility into large-scale network environments while minimizing operational overhead. Shield Sentinel leverages modern kernel-level networking technologies, including **eBPF and XDP**, to support efficient high-throughput packet decoding and metadata collection within demanding network environments.

Why Organizations Deploy Shield Sentinel

- **High-Throughput Network Observability:** Designed for environments operating at 100 Gbps and beyond, enabling scalable monitoring of large trunk circuits and high-capacity network infrastructure.
- **Passive, Out-of-Band Deployment:** Operates independently from production traffic flows, allowing organizations to collect network telemetry without introducing inline latency, routing complexity, or enforcement risk.
- **Efficient Metadata Collection:** Rather than storing massive full packet captures, focuses on collecting summarized network metadata and DNS activity that can be retained, exported, and analyzed more efficiently over time.
- **DNS and Flow Visibility:** Comprehensive recording of DNS requests, responses, and network flow metadata provides valuable context for security investigations, compliance workflows, and historical analysis.
- **Flexible Data Export:** Supports exporting collected telemetry as structured data that organizations can load into SIEMs, analytics platforms, data lakes, or internal investigation workflows.
- **Supports Security Operations and Threat Hunting:** Telemetry generated by Shield Sentinel can support broader security operations, incident response, threat hunting, and forensic investigation efforts when combined with existing security tooling.

How Shield Sentinel Works

Shield Sentinel passively monitors mirrored network traffic and extracts summarized metadata from observed communications at high throughput. Rather than functioning as an inline enforcement platform, Sentinel focuses on scalable collection and retention of network telemetry that organizations can analyze internally or integrate into downstream analytics workflows.

Captured metadata may include:

- Source and destination communications
- Protocol information
- DNS requests and responses
- Connection timing and flow details
- Traffic volume metrics

This information can be exported in structured formats for integration into SIEM platforms, investigation pipelines, compliance workflows, or long-term network visibility initiatives. Because Shield Sentinel operates out-of-band, **production traffic continues uninterrupted even if the monitoring platform becomes unavailable.**

Who Benefits from Shield Sentinel

- **Carriers and Service Providers:** Monitor high-capacity trunk circuits and customer environments while maintaining operational separation from production traffic flows.
- **Enterprise Data Centers:** Improve visibility into large-scale network activity for operational analysis, compliance initiatives, incident response support, and historical traffic investigation.
- **Security Operations Teams:** Leverage scalable DNS and flow telemetry to support investigations, threat hunting workflows, and broader security analytics initiatives.
- **Government and Critical Infrastructure:** Deploy passive monitoring capabilities within sensitive environments where operational stability and separation from production systems are critical requirements.

VISIBILITY WITHOUT RISK

Shield Sentinel delivers high-throughput network observability through passive out-of-band monitoring — no inline latency, no production disruption, no enforcement risk.

Shield Sentinel vs. Traditional Monitoring Approaches

Capability	Shield Sentinel	Traditional Full PCAP Approaches
High-Throughput Metadata Collection	●	○
Passive Out-of-Band Monitoring	●	●
Reduced Storage Requirements	●	○
DNS and Network Flow Visibility	●	●
Structured Telemetry Export	●	○
Optimized for Large Trunk Circuits	●	○
Full Packet Capture Storage	—	●

● Native Capability ○ Limited or Resource-Intensive Capability — Not Applicable

This comparison reflects the architectural differences between Shield Sentinel and traditional full packet capture platforms. Rather than functioning as a full PCAP storage platform, Shield Sentinel focuses on scalable metadata collection, reduced storage overhead, efficient telemetry retention, and high-throughput observability for large-scale network environments.

About INTRUSION Inc.

INTRUSION Inc. delivers advanced cyber threat intelligence, network visibility, and prevention technologies designed to help organizations strengthen operational awareness and reduce security risk across on-premises, cloud, and endpoint environments. The Shield platform provides organizations with scalable network enforcement, visibility, and telemetry capabilities built for modern distributed infrastructures.

Contact Us

888-637-7770
info@intrusion.com
www.intrusion.com