



Safe Internet Access

Policy Enforcement Without Network Disruption

Inspect, detect and enforce internet access policies across traffic, users, applications and IOC's

From Network Traffic to Actionable Policy Enforcement

Service providers need precise control over internet access while meeting regulatory and security requirements. Underscore's Safe Internet Access (SIA) provides deep inspection and policy enforcement without disruptive changes to routing, firewalls or client configurations.

SIA works in passive tap or inline deployments to inspect traffic at L3–L7, identify behaviour and policy violations, and take preventive action. Policy violations can trigger user-facing notifications and connection termination; inline mode can drop offending communications in real time.

Built for high-throughput service-provider environments, SIA supports HTTP, HTTPS, SSH, Telnet and email protocols, IPv4/IPv6, asymmetric routing and traffic inspection up to 40 Gbps, with real-time alerts, threat-intelligence correlation, policy management and operational

Benefits

- Drop-in deployment without client reconfiguration or disruptive network redesign.
- Enforce regulatory blocking and internet-use policies without service interruption.
- Inspect and control traffic across supported protocols, including HTTPS, QUIC and secure DNS services.
- Investigate with live network graph analytics, grouped alerts and ATT&CK context.
- Monitor appliance health and deployment status from one console.
- Manage rules, blocklists, retention and archives centrally.
- Correlate source and destination IOCs with real-time threat intelligence.

Core Capabilities

Deep Packet Inspection & Policy Enforcement

- L2–L7 inspection and configurable policies help service providers enforce safe, compliant internet access. Passive tap and inline deployment options support non-disruptive monitoring and real-time preventive action.

Real-Time Network Visibility

- A live network graph provides Centrality, Communities, Paths, Similarity and Structure views for investigating relationships and activity. Grouped alerts and live-tail monitoring support ongoing investigation.

Threat Detection & ATT&CK Context

- Source and destination IOCs are correlated with threat intelligence in real time. Alerts are automatically mapped to MITRE ATT&CK tactics and techniques for attack-chain context.

Policy, Blocklist & Retention Management

- Manage the full SIA ruleset from the console, maintain IPv4/IPv6/FQDN blocklists, import large IOC sets, configure retention and archive data to Amazon S3 or a local server.

Network Graph with Live Analytics

- Explore the live network through five analytical lenses — Centrality, Communities, Paths, Similarity and Structure. Use the same graph canvas to focus investigations on relationships and activity that matter.

MITRE ATT&CK Mapping

- Automatically map alerts to MITRE ATT&CK tactics and techniques. The ATT&CK matrix highlights active areas of the attack chain so operators can understand observed activity in context.

Live Health

- Monitor CPU, memory, storage, network and deployment health in real time, including per-core counters, warning and critical bands, and an auto-reconnecting feed.

Policy Management

- Manage the complete SIA ruleset from the console. View SID, message, action, endpoints, tags, classtype and priority; create rules with a guided builder; enable, disable or draft rules; and delete safely with protected-SID guards and timestamped backups.

Blocklist Management

- Manage blocked IPv4, IPv6 and FQDN entries across dedicated tabs. Fast search, bulk removal and file upload support large IOC imports.

Data Retention & Archiving

- Configure custom retention for flow statistics, alerts and raw data by days, weeks or months. Schedule automated purge or secure archiving to Amazon S3 or a local server.

Alerts

- Use grouped views to bucket events by rule, source, destination, conversation, sensor, severity, category or action. Live tail streams alerts as they fire with pause/resume, rate meter and auto-reconnect. Block an offending IP directly from an alert row.

Threat Intelligence Integration

- Check source and destination IPs and other IOCs such as domains against Underscore threat intelligence in real time. Malicious and suspicious verdicts are surfaced on hosts, alerts and the network graph

Deployment

- Passive tap mode, inline deployment; single-arm mode; L2 failover; IPv4/IPv6 support; asymmetric routing; up to 40 Gbps traffic.

Key Advantages

Feature	Value Delivered
Network Graph with Live Analytics	Five graph lenses for live relationship and activity investigation.
MITRE ATT&CK Mapping	Automatic tactic and technique mapping with active areas highlighted.
Live Health	Live CPU, memory, storage and network health with warning/critical bands.
Policy Management	Guided rule creation, lifecycle controls, protected deletion and backups.
Blocklist Management	IPv4, IPv6 and FQDN lists with search, bulk removal and file upload.
Data Retention & Archiving	Custom retention plus scheduled purge or archive to S3 or local server.
Alerts	Grouped/live-tail alerts, auto-reconnect and direct IP blocking.
Threat Intelligence Integration	Real-time IOC verdicts surfaced across hosts, alerts and the graph.

About Underscore:

Unlocking Cyber Resilience in the digital realm. Our robust platform combines proactive prediction, powerful forecasting, prioritizing risk, providing unparalleled real-time insights to keep you ahead of threats and assuring business continuity.

Contact Us:

info@underscorecs.com
Tel. +91-9811344253