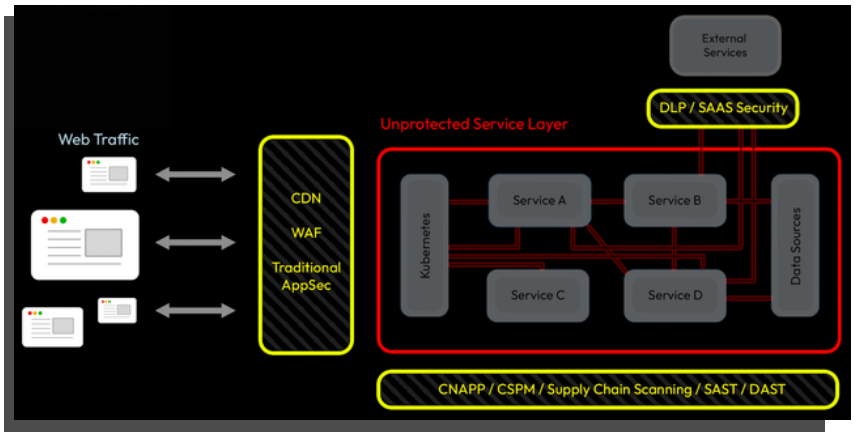
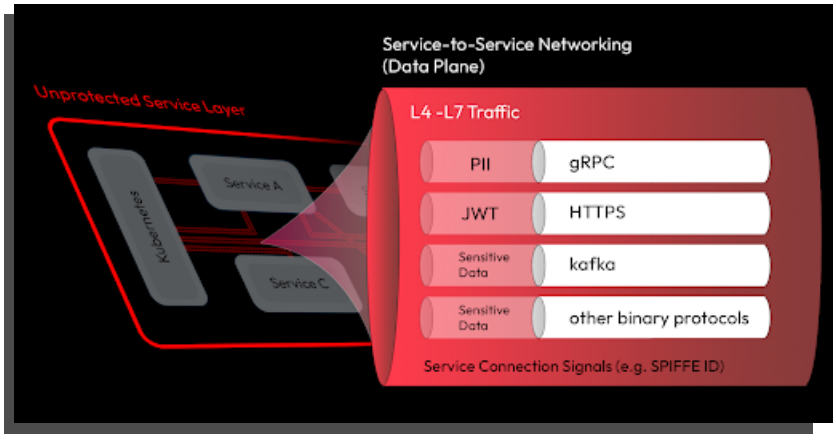
LeakSignal Service Layer Security

Microservices and Serverless Architectures Require a New Security Solution

The challenge with microservice architectures is that the environment and the applications are dynamic and virtualized. Traditional security approaches such as agents and firewalls don't insert cleanly. Securing the edges (e.g. with WAF) and the infrastructure (e.g. with CNAPP) provide some protection, but dynamic application logic and the constant flow of sensitive data through the service layer must be observed and protected too.



LeakSignal's novel approach monitors and protects the service layer by inserting into the data plane - the new networking layer for microservices. With this lightweight approach, security teams achieve visibility to risks, assessment of their severity, and mitigation.



KEY BENEFITS

INSTALLS IN MINUTES

Installs as a lightweight WebAsembly module into existing ingress, sidecar, and ambient mesh proxies, giving engineering and security teams instant visibility to assess the data plane security posture.

AGENTLESS

LeakSignal's Inline Response Manager (IRM™) is built to process all outbound content, which allows for unique data protection and audit capabilities that identify exactly what sensitive data was accessed.

INSTANT OUTCOMES

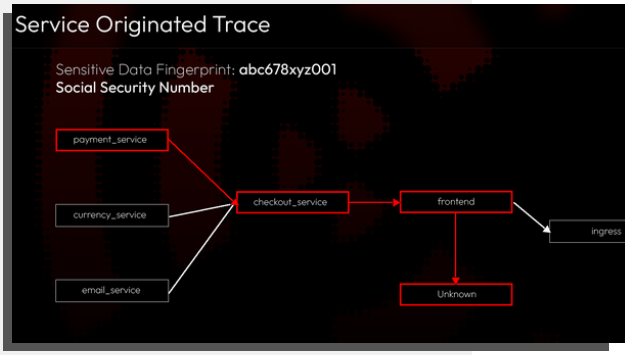
Automatically maps all services and sensitive data in real-time. After analysis, improved posture management is achieved through prioritization, microsegmentation and configuration hardening.

LeakSignal Product Overview

VISIBILITY AND PRIORITIZATION

LeakSignal monitors data flows between microservices and outside systems to:

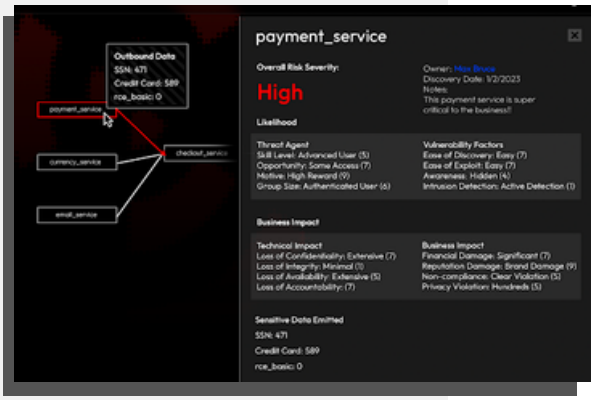
- Map service interactions and decorate them with posture indicators and sensitive data tracing.
- See exactly where sensitive data is originating from and flowing to.
- Prioritize security teams efforts in securing microservices.



ASSESSMENT

LeakSignal's risk assessment capabilities empower teams with:

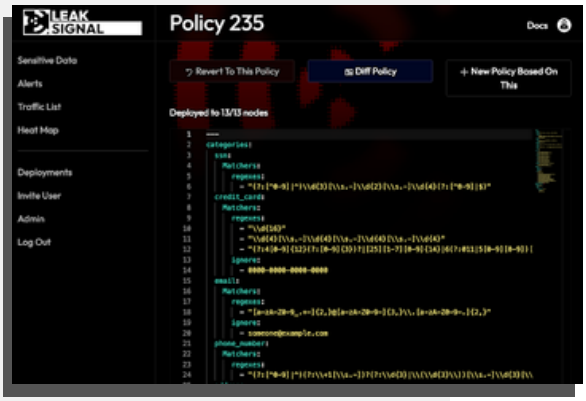
- Risk severity across the service mesh and comparison to baseline.
- Enforce strict compliance, security requirements, and frameworks., such as WAF and OWASP Top Ten.
- Data tracing that follows data elements through the service mesh to calculate exposure radius.



PROTECTION

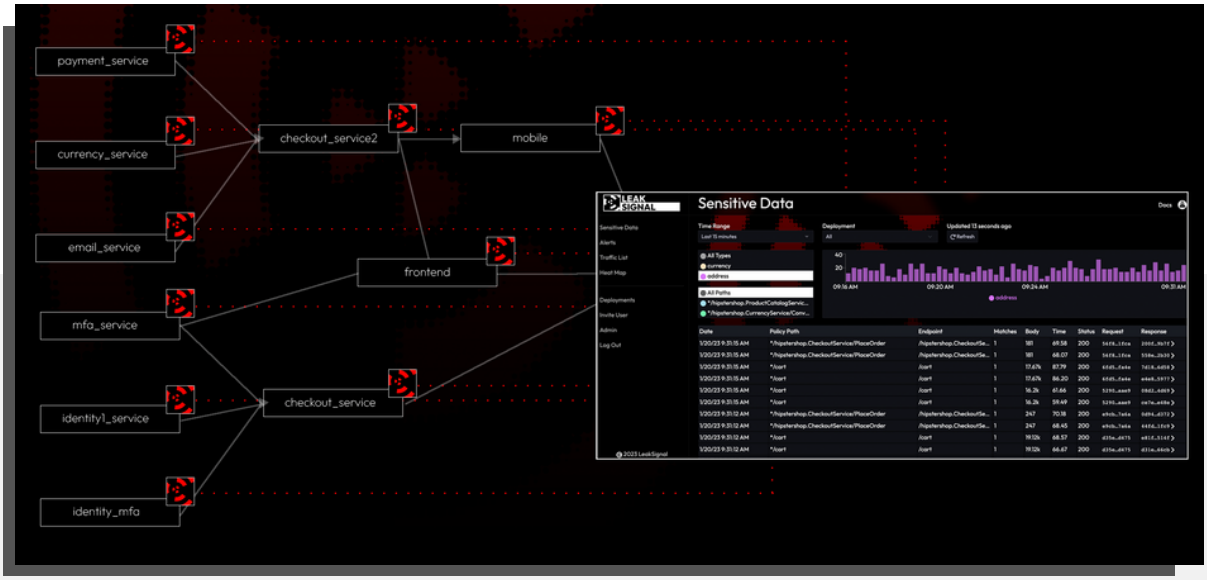
LeakSignal is deployed inline in the data plane allowing teams to:

- Explicitly match sensitive data that is important to an organization and apply policy, including blocking and redaction.
- Implement segmentation and service protection through SBAC and implicit (learned) or explicit service permissions.
- Prevent lateral movement, probing, and abuse.



LeakSignal: How It Works

- **LeakSignal SENTRY** is configured as a WASM module into service mesh proxies and ingress controllers.
- **LeakSignal COMMAND** runs in the cloud or self-hosted. It maintains policy, coordinates data tracing, and calculates alerts.
- **LeakSignal OTEL & SIEM** modules are used in place of LeakSignal COMMAND to send in-filter telemetry to desired aggregation platforms.



SCALABILITY

LeakSignal is embedded in the service routing layer, so it is automatically scaled by the mesh controller - there is no separate layer to coordinate, manage, or scale.

RELIABILITY

LeakSignal Sentry runs in a WASM VM built-in and is supported by Envoy. Because it is running in this VM sandbox, it operates in parallel to the service traffic (except for blocking/redaction) and won't take down the service traffic if there is policy failure.

INTEGRATION

LeakSignal emits base metrics through Envoy via OpenTelemetry and Prometheus. Alert tracing can be sent to SIEM and other aggregation platforms.