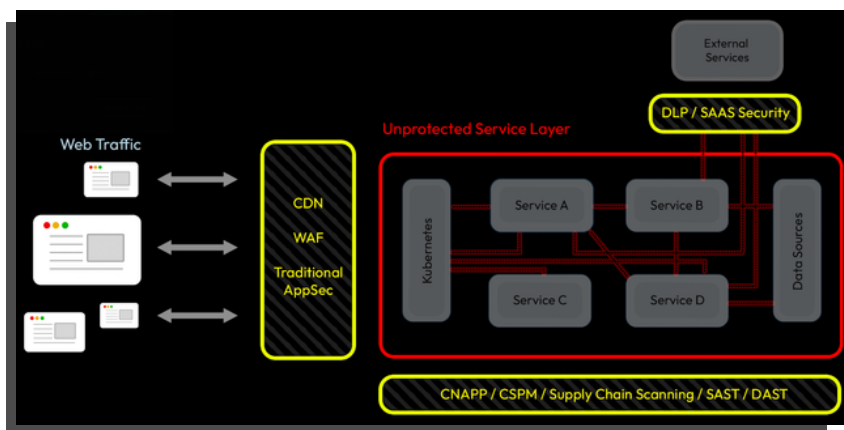


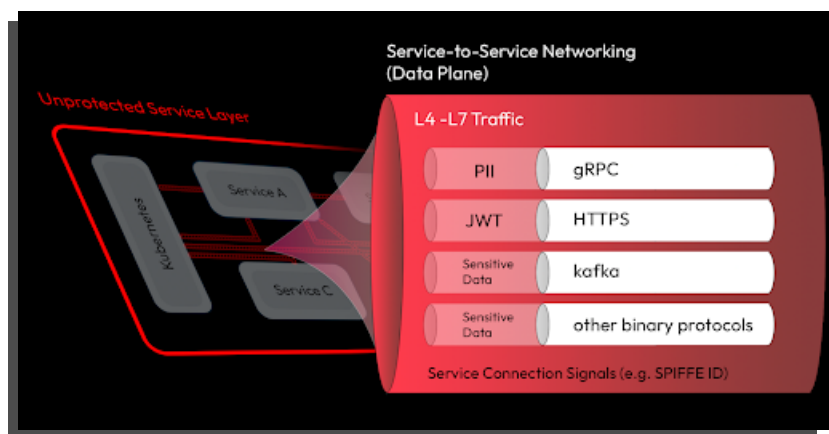
# LeakSignal Service Layer Security

## Microservices and Serverless Architectures Require a New Security Solution

As organizations transition to the next generation of Application Development & Platform technologies, most find themselves at a loss for the 25%+ of the infrastructure they now can't see - the microservices data plane. This makes meeting attestation and compliance requirements difficult if not impossible because the new protocols leveraged in these mesh environments go unmonitored and unprotected, with many executives unaware that this has even happened. If you have microservices running, and they transact in sensitive data, there is a massive vulnerability: If someone gets an API key - even by mistake - they can access anything that service can access.



**LeakSignal** has developed an in-line and at scale analysis, detection, control, and reporting technology that deploys natively within the servicemesh. Scanning response data as it's emitted from microservices and identifying potential data abuse, control failures, and data exfiltration. LeakSignal's Envoy Inline Response Manager (IRM) gives organizations the ability to observe and protect sensitive data as it traverses and is being emitted from these environments along with alerting and remediation capabilities.



### KEY BENEFITS

#### REDUCE BREACH TIME AND EXPOSURE BY UP TO 90%

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

#### DATA ATTESTATION AND COMPLIANCE SIMPLIFIED

LeakSignal's Envoy IRM is built to process all outbound content, which allows for unique data protection and audit capabilities that identify exactly what sensitive data moves, is encrypted and accessed.

#### INSTALL IN MINUTES

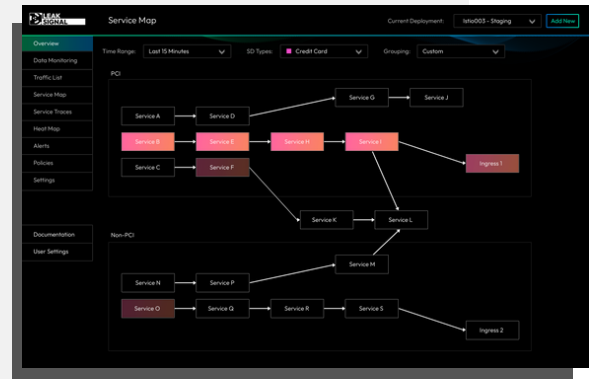
Installs as a lightweight WebAssembly module into existing ingress, sidecar, and ambient mesh proxies, giving engineering and security teams instant visibility to assess the data plane security posture.

# LeakSignal Envoy IRM Product Overview

## VISIBILITY AND PRIORITIZATION

LeakSignal monitors data flows between microservices and outside systems to:

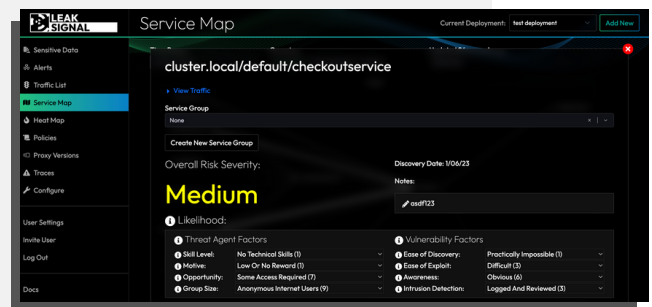
- Map service interactions and decorate them with posture indicators and sensitive data tracing.
- See exactly where sensitive data is originating from and flowing to.
- Prioritize security teams efforts in securing microservices.



## ASSESSMENT

LeakSignal's risk assessment capabilities empower teams with:

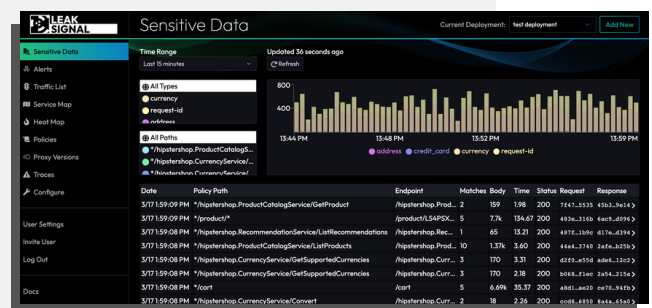
- Risk severity across the service mesh and comparison to baseline.
- Enforce strict compliance, security requirements, and frameworks, such as WAF and OWASP Top Ten.
- Data tracing that follows data elements through the service mesh to calculate exposure radius.






## PROTECTION

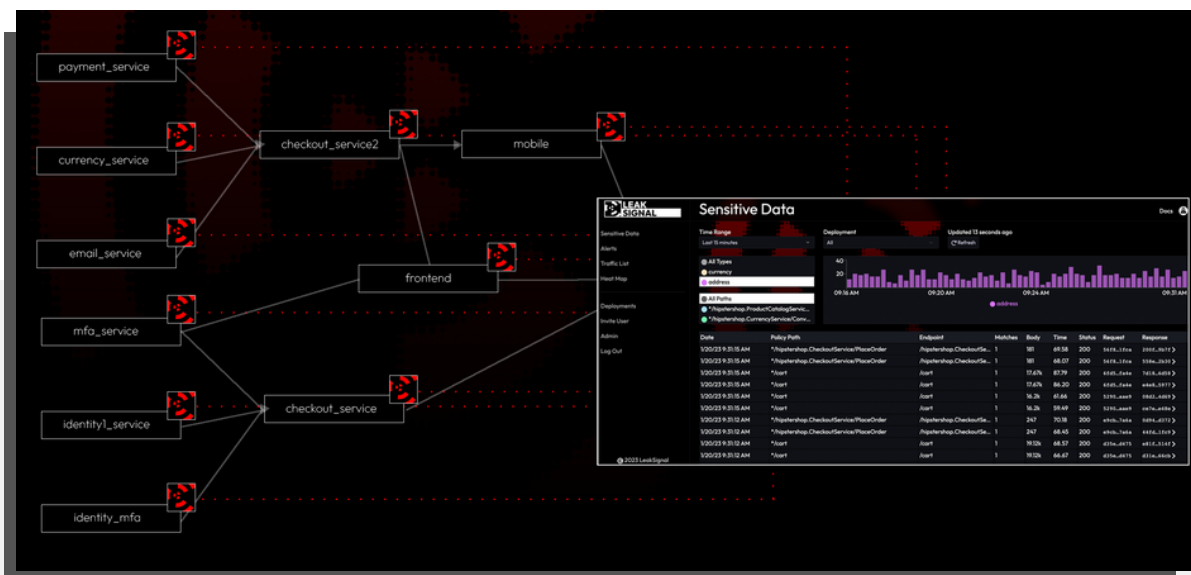
LeakSignal is deployed inline in the data plane allowing teams to:

- 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 Envoy IRM: 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.

