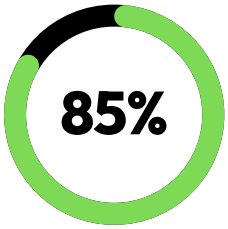
Microservices and Serverless Architectures
Require a New Security Solution

The increasing adoption of serverless and microservice environments has brought to light the shortcomings of existing security solutions, which weren't designed with this new architecture in mind.

To protect organization's most important asset - sensitive and confidential data - LeakSignal developed an in-line and at scale data classification, remediation, and reporting technology. LeakSignal deploys natively within the service mesh, and is the first to provide layer 4-7 data visibility and protection in machine-to-machine and cloud native architectures.



of companies say they are modernizing their apps to a microservice architecture

Delivering Immediate Value to Your Business

Complete Sensitive Data Monitoring

- Identify unknown data exposure in test/stage environments.
- 100% source of truth auditing on data exfiltrated from microservices and APIs.
- Discover how sensitive data flows across organizational boundaries and cloud environments.

Simplified Data Attestation and Compliance

- See past legacy controls and significantly reduce Incident Response times.
- 100% coverage on sensitive data access after MFA.
- Data Security Posture Management (DSPM) capabilities for microservices.

Optimized Security Posture

- Enforce Service-based Access Control (SBAC) across all sensitive data flows.
- Automatically redact sensitive data during an attack, before it falls into the wrong hands.
- Easily integrate with existing SIEMs and cloud native monitoring solutions.

LEAK SIGNAL

Take control and set limits on sensitive data access

LeakSignal is the first to provide layer 4-7 data visibility and protection for microservices environments, allowing security teams to take control and set limits on sensitive data access. Using LeakSignal, organizations achieve:

Visibility and Prioritization

LeakSignal monitors data flows between microservices and outside systems to:

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

Assesment

LeakSignal's risk assessment capabilities empower teams with:

- Risk severity across the service mesh and comparison to baseline.
- Strict compliance and frameworks, such as WAF and OWASP Top Ten.
- Data tracing through the service mesh to calculate exposure radius.

Protection

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

- Match sensitive data and apply policy, including blocking and redaction.
- Implement segmentation and implicit or explicit service permissions.
- Prevent lateral movement, probing, and abuse.

Complete visibility and security of microservice environments

Traditional Solutions	LeakSignal
✗ Built for non-mesh architecture	✓ Scales with 1000's of services through native insertion
✗ Visibility on API traffic only	✓ Visibility on all traffic emitted from a service, APIs, protocols, and more
✗ Existing edge protections WAF, Bot, CDN	✓ Additional mitigation capabilities after edge bypass
✗ DLP and DSPM only see half the problem	✓ Aligned to DLP and InfoSec covering what existing solutions can't see
✗ Only operate on HTTP protocol	✓ Support for all L4-7 mesh-based protocols (API, gRPC, kafka, redis, binary)

About LeakSignal:

LeakSignal redesigned network level cybersecurity for microservices and service mesh technologies because traditional defenses are incompatible with the newer microservice architectures. LeakSignal provides enterprise-grade security solutions that are open, cloud-native, performant and lethal in their ability to stop cyber attacks.

leaksignal.com | sales@leaksignal.com

Now Available on:

awsmarketplace

Microsoft Azure