Mesh7

case study

codilime × MESH7

Building a microservices security platform for a disruptive startup

Our client, **Mesh7**, was a Silicon Valley-based startup founded by IT industry veterans and backed by venture capital funds. Mesh7 released its cloud-native observability application.

This solution examines communication between microservices, visualizes the connections between them, shows potential threats, and automatically applies security policies. With this product, Mesh7's ultimate goal is to **protect your microservices effectively while giving the user a clear overview of all the traffic** between them from a security perspective.

Challenge

As an application’s complexity grows exponentially (resulting from interconnected ephemeral, heterogeneous, and distributed workloads), so too do concerns about the security of such applications. Using cloud and third-party services, and exchanging sensitive information at Layer 7 over a network, had created dangerous blind spots:

- **Lack of real-time visibility** of the interactions between various workloads, cloud, and third-party services.
- **Lack of control** over the flow of sensitive data, both internally and externally.
- **Impossible to detect** anomalous behavior and unsanctioned changes in applications.
- **No real-time detection** of lateral threats and vulnerabilities at run time.

Challenge

Mesh7 decided to tackle these challenges by creating a complex platform to monitor communication between different workloads and apply automated security rules. The platform works on top of the customer’s infrastructure and ensures that no potential threat remains undetected.

CodiLime was chosen as an external technology partner to help Mesh7 build the product and keep the promises it has made to its clients and investors. Together we have succeeded in creating a product we believe will become the first-in-class solution for ensuring the security of microservices.

What we delivered

DevOps services 1

Frontend services 2

Network services 3

Network security services 4

Test automation 5

Results & benefits

Co-designed and delivered a service mesh platform that brings security and observability

Created and maintained CI/CD project

Created user-centered frontend solution (service graph, analytics)

Performed performance analysis, and optimized relevant areas (response to attack performance, data aggregation, memory usage)

Client’s testimonial

MESH7

Thanks to its expertise in networking technologies and Kubernetes, CodiLime has become our reliable technical partner helping us deliver the first-in-class product for monitoring security in microservices. CodiLime’s experienced project managers and engineers played an important role in releasing the final product and thus keeping promises given to clients and investors.

Amit Jain
CTO & Co-Founder
Mesh7, Inc.

The scope of the project

Thanks to the SaaS model installation, it takes mere minutes to onboard a customer. The product can be used in any type of workload, cloud or environment. The modern user interface clearly visualizes all the necessary information.

Short summary of the project:

- Created DDOS protection mechanisms
- Created a plethora of plugins for the observability ecosystem (service mesh, Istio)
- Created performance measurement toolkit
- Delivered policies generation mechanisms (api discovery, api validation, service discovery …) utilizing Envoy Proxy as insertion point
- Developed data enrichment mechanisms and plugins for Envoy
- GoLang control plane utilizing K8s operator

Mesh7 Cloud Security Observability

The scope of the project

Application Observability

Proactive Baselining & Anomaly Detection

- Proactively Detect Application breaches before it is exploited
- Zero-day

Application Security Graph (L4-L7+)

- Services Auto-Discovery
- L4 Flow Mapping
- L7 API Auto-Discovery
- Application Payload & Schema Discovery
- PII Data Flow Map
- Cloud services access
- Egress Services

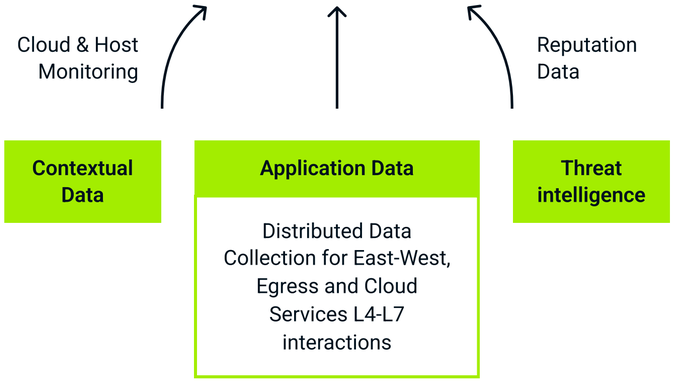
AI/ML Security Analytics

- Application Behavioral Analytics
- Application Data Risk Tracking
- Drill Down investigation of Events & Alerts
- SIEM Integration

Preventive Security Controls

- Protection against Breaches & Data Exfiltration
- Identity based API & PII Segmentation
- Block selective traffic
- Adaptive Rate Control
- Redact sensitive information

Intelligent Data Correlation & Mapping



Cloud Deployed

Zero Latency/Fail Open
Zero Changes to Applications

The scope of the project

Key benefits for all main stakeholders:

Security Team

- Immediately detects security threats and vulnerabilities; facilitates the implementation of appropriate security policies.

Cloud Ops Team

- Works with any type of platform - public, hybrid cloud or workloads (Kubernetes, VMware vCenter, AWS) while offering excellent scalability.

Compliance Team

- Manages compliance risk exposure detecting vulnerabilities and sensitive data leaks.

DevOps Team

- Rapidly improves an application’s security with zero impact on its latency.

The scope of the project

Application Observability is a response to security challenges related to distributed applications with increasing data in motion.
It correlates distributed data collection of east-west, egress, and cloud services with cloud and host monitoring data. Application observability provides four distinct benefits:

- An application security graph that provides L4-L7+ visibility into workload interactions along with auto-discovery of API payloads.
- A data flow map showing the flow of sensitive information in application environments.
- Baselining and continuous drift detection that sends alerts in real-time for any unsanctioned or anomalous application behavior.
- Intelligent security analytics and preventive security controls at L7+.

Technologies and tools

About CodiLime

codilime

Since 2011, CodiLime has been the engineering partner of choice for semiconductor companies, networking services, telecom services, and software solution providers.

We have come a long way – from a startup to a company that hires more than 350 top-notch software developers, network engineers, DevOps experts, and solution architects. **We focus on five N.E.E.D.S. - Networks, Equipment, Environment, Data and Security.**

We aim to link engineering talent with business domain expertise. Everything to provide our clients with delivery excellence and custom-tailored solutions.

Check out what our partners have said about us and how they evaluated our cooperation.

Go to about us page