



# IoT Meets Security Monitoring at Ayla Networks

## Customer Problem

Ayla Networks is an IoT PaaS (Platform as a Service) company that builds enterprise-class, cloud-based software for the Internet of Things. As such, it has a major focus on securing connected products, the data they collect, and the applications they leverage. With a growing global customer base that includes numerous Fortune 1,000 companies, Ayla knows that delivering a fast and secure platform is essential.

As a security-conscious company running completely on AWS, Ayla takes a cloud-native approach to security and compliance with the goal of preemptively protecting customers against threats. While AWS has given Ayla incredible speed, efficiency, and ability to scale, keeping their platform secure and compliant within AWS is essential. Since IoT devices are often tied to an enterprise's infrastructure and typically store and transmit sensitive data, they can create vulnerabilities that companies may not be used to.

## The Solution

Every tool Ayla deploys must be lightweight (requiring very little computing power) and easy to manage with a small DevOps team. As a cloud-native threat management solution that can deploy on top of AWS, F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, met Ayla's requirements perfectly: It is extremely lightweight and enables them to deploy and scale securely at a moment's notice. It took Ayla's DevOps team just minutes to deploy, rule configuration was easy, and the time it takes their team to manage Distributed Cloud AIP on a regular basis is negligible.

In addition to delivering security at speed and scale, Ayla verified that Distributed Cloud AIP could support compliance in the cloud. Through its ability to provide key functions such as intrusion detection, continuous monitoring, real-time actionable alerts, and reporting (with complete audit trails), Distributed Cloud AIP has streamlined Ayla's entire compliance process, enabling them to meet requirements that include ISO 27001, SOC 2, and GDPR.



**Founded**

2010

**Headquarters**

Milpitas, CA

**Industry**

Internet (IoT cloud  
platform-as-a-service)

**Employees**

120

*“With [Distributed Cloud AIP] on our side, continuously making sure that security scales as we grow and that threats are detected the moment they crop up, we can say with confidence that our cloud is buckled down. Now we’re ready and excited for the growth that’s going to take place in the IoT space over the next several years!”*

**Adrian Caceres, CTO, Ayla Networks**

## Outcomes and Benefits

Using Distributed Cloud AIP, Ayla has been able to meet all of its security, compliance, and operational requirements. And given its ability to scale in real time, Distributed Cloud AIP is making sure Ayla can keep pace as their customer base continues to expand and the number of connected devices skyrockets.

## Threat Stack: Now Part of F5

Threat Stack is now F5 Distributed Cloud App Infrastructure Protection (AIP). If you’d like to learn more about this solution, the company’s Security Operations Center (including Distributed Cloud AIP Managed Security Services and Distributed Cloud AIP Insights), and more, feel free to contact our cloud security and compliance experts.

**Let our experts take your cloud security worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, [visit our website](#) today.**

