



# Stratasan's Security and Compliance Solution

## Customer Problem

Stratasan delivers web-based software and professional services that enable healthcare organizations to access information on healthcare markets and thereby establish a foundation for strategic planning, marketing, physician relations, and growth.

When Stratasan adopted F5® Distributed Cloud App Infrastructure Protection (AIP), formerly known as Threat Stack, on the recommendation of peers in the healthcare sector, they were a 15-person company with limited personnel and financial resources. Distributed Cloud AIP was a perfect fit for their HIPAA requirements given its ability to provide host-based intrusion detection. Since the platform was well documented and easy to set up, Stratasan had it rolled out and was using it within a couple of weeks of deciding to adopt.

## The Solution

As Stratasan began using Distributed Cloud AIP more systematically, they derived value that extended significantly beyond their original HIPAA requirements:

**Increased Visibility and Better Communication:** By integrating with Slack, they increased visibility into their systems without needing to continually log into Distributed Cloud AIP. They also received real-time alerts on who was doing what, where, and when—and they could communicate more effectively on how to remediate issues, improve operations, and ensure that Dev, Security, and Operations (DevSecOps) were driving towards common goals.

**Audit Records for HIPAA:** In addition to comprehensive monitoring and real-time alerts, Distributed Cloud AIP created an audit trail and reports that could be passed on to auditors.

**Containerization and Full-Stack Visibility:** While Stratasan doesn't necessarily plan to become fully containerized, Distributed Cloud AIP's container monitoring capabilities produced observability throughout Stratasan's stack and SDLC, strengthening security at all levels and phases.



**Founded**

2010

**Headquarters**

Nashville, TN

**Industry**

Healthcare Information  
Technology & Services

**Employees**

50

**Third-Party Expertise:** As a small team, Stratasan is budget conscious and doesn't have a dedicated security person. Adding Distributed Cloud AIP Managed Security Services has provided an effective, cost-effective way of leveraging third-party security insights and expertise so Stratasan can focus all resources on their core competencies.

*"[Distributed Cloud AIP] has been a great tool to have in our arsenal. We like the idea of sticking to our core business competencies—healthcare, healthcare marketing, and strategic planning—while being able to outsource other things that are valuable but simply outside our area of expertise. That's why we partner with [Distributed Cloud AIP]."*

**Brian Dailey, Stratasan's Co-Founder and CTO**

## Outcomes and Benefits

As Stratasan's needs have grown beyond their initial requirement for host-based intrusion detection and support for HIPAA, the company has derived more value from Distributed Cloud AIP. As Stratasan continues to evolve their infrastructure, scale their data processing capacity, and expand their customer base, they plan to stay with Distributed Cloud AIP to strengthen security and compliance, optimize operations, and achieve their overall business goals.

## About Stratasan

Stratasan is now part of Syntellis. This Nashville-based Healthcare IT and Services division has 50 employees.

## 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.**

