WiNG

Aporeto and the Future of Cloud-Native Security

MAY 17, 2017 PETER WAGNER SECURITY

The micro-service architecture is the future of applications. Infrastructure is evolving to better support micro-services. DevOps methodologies are transforming the people-and-processes equation. We've written extensively about these trends, and their interaction here (http://wing.vc/perspectives/essays/microservices-containers-and-the-digital-dialectic) and here (http://wing.vc/blog/devops-and-the-digital-trialectic).

But amidst the micro-service mania, there remains a deep-seated concern about the security of distributed applications built according to this architecture. Would the explosion of interfaces exponentially expand the attack surface? Would the reuse of code create new attack vectors? Would existing security tools be powerless and blind to micro-service interactions?

At Wing, we initiated a deep investigation of next generation security approaches for the cloud-native world several years ago. We have found several interesting schools of thought. Some sought to apply classical approaches like network security to this new world. They invented ways to discern and control container network connections, and keep pace with the scale and velocity of changes in a micro-service-based application. Others focused on the contents of the container itself, and developed methods to identify vulnerabilities in micro-service code before it reached deployment. There is definitely value in these approaches, and they will have a place in cloud-native infrastructures and software development pipelines.

When we met Dimitri Stiliadis and Aporeto in 2015, we recognized a different line of thinking. Dimitri saw the rise of micro-services not as a source of problems, but rather as an enabler for better security. The Aporeto system was conceived to utilize increasingly available application metadata and service-to-service interfaces to create a vastly simpler, automated path to securing applications. Not only would Aporeto provide the basis for secure system design, it would also help bridge the gap between developers and security operations. In Dimitri's view, trends that at first

blush looked like sources of greater risk would actually be the keys to superior security.

We led Aporeto's seed financing in late 2015, and ever since have worked intensively with Dimitri, co-founders Satyam Sinha and Amir Sharif, and the rest of the team. The Aporeto concept has been relentlessly validated with well over one hundred customers in the cloud-native application world, and the product has been carefully crafted in response to their feedback. Now is an exciting time for the company, as it launches its beta program and begins its go-to-market efforts in earnest. We are pleased to welcome Matt Howard and our friends at Norwest Venture Partners to the Aporeto team as part of the recent Series A financing, and look forward to working closely together in the next phase of company-building.

The ultimate vision for Aporeto is an audacious one, which was of course a key motivation for Wing to get involved. If highly granular, automated security can be brought to bear at the application level, will companies still need to make the same massive investments in traditional static, brittle security technologies? Many tens of billions of dollars of security budget will be in play. As more and more applications embrace the micro-service architecture, Aporeto has the opportunity to become a truly strategic security provider for the cloud-native enterprise.

---

http://wing.vc/blog/aporeto-and-the-future-of-cloud-native-security
© 1990 — 2018 Wing, Menlo Park, CA