Security and Compliance on AWS ARM Architecture

AWS Graviton2 instances are powered by ARM architecture, which can handle a wide range of cloud-native workloads with improved efficiency. This combination promises a significant increase in cloud performance over comparable instances as well as material reductions in cost.

As cloud-native companies, and those migrating workloads to the cloud, seek to take advantage of these benefits, security leaders will need to ensure that they maintain their organization's security and compliance posture. With F5® Distributed Cloud App Infrastructure Protection (AIP)'s, formerly known as Threat Stack, out-of-the-box (OOTB) support for ARM architecture, organizations can do both.

Security and Compliance that Follows Your Workloads

The decision to move to a cloud instance like Graviton2 can often be made solely from a business perspective, related to scaling services and lowering costs. As a result, security teams are often informed post-transition and left scrambling to find the right tools to secure new environments. Security leaders need to be ready to empower the business when these types of technology innovations occur.

The Distributed Cloud AIP solution delivers OOTB support for the ARM architecture, allowing organizations to migrate workloads, without sacrificing their cloud security and compliance coverage. Likewise, organizations can realize the business benefits of Graviton2 coupled with Distributed Cloud AIP's unique combination of telemetry collection, behavioral rules for known threats, and ML-powered detection-in-depth, providing more than just anomaly detection. Additionally, our in-house SOC is available for 24/7/365 security coverage for your cloud hosted workloads, to include those running on Graviton2.

Organizations leveraging Distributed Cloud AIP continue to be well-prepared for business-led technology shifts. Likewise, infrastructure performance improvements and cost-savings opportunities, like those inherent in ARM architecture, provide an opportunity for IT and security leaders alike to proactively suggest the adoption of modern technology stacks that deliver scalability and financial benefits to their organizations—all without sacrificing security or compliance.

How It Works

Distributed Cloud AIP's Agent is a multi-architecture agent that is compatible with both x86 and ARM architecture, and a wide range of operating systems. All host-based event types will be supported, including audit, file integrity monitoring, Linux host, login, and threat intelligence. This agent can be installed on the following operating systems:

- Amazon Linux (version 2)
- CentOS (version 8.2)
- Debian (version 10)
- Red Hat Enterprise Linux (version 8.2)
- Ubuntu (versions 18.04, 20.04)

Additionally, the Distributed Cloud AIP agent can be deployed through a wide range of leading configuration management tools such as Chef, Ansible, Puppet and Salt.

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 and compliance worries off your shoulders, so you can get down to business. To learn more or to schedule a demo, visit our website today.