LogRhythm™

SaaS and Cloud Native Definitions and Best Practice

- a concise guide

a cloud community eBook

LogRhythm

1. Introduction

There's a disconnect in how we talk about applications that are no longer hosted within our own data centre.

When speaking with customers, we've observed that 'software as a service' (SaaS) and 'cloud-native' are terms that tend to be bundled together and used interchangeably at times.

There are instances where we hear that SaaS tends to be 'all things cloud' — but that is not necessarily true.

It's important to discuss the differentiation between these two terms because they mean different things and carry different implications for software and security.

Here's the result of our observations.

3. Definitions:

- **SaaS (Software as a Service):**
  - Delivered over the internet
  - Accessible via a web browser
  - Includes Google Workspace, Salesforce, Zoom, etc
  - Features:
    - Accessibility from anywhere
    - Multi-tenancy
    - Automatic updates
    - Subscription pricing
    - Scalability
    - Integration capabilities

- **Cloud Native:**
  - Approach leveraging cloud principles for application development
  - Promotes scalability, flexibility, and continuous product delivery
  - Characteristics:
    - Microservices architecture
    - Use of containers (e.g. Docker)
    - Orchestration via platforms (e.g., Kubernetes)
    - Embraces DevOps practices
    - Built for resilience
    - Uses cloud-specific services and APIs

3. Understanding the differences:

In simple terms, SaaS is about how software is delivered, while cloud-native is how software is built and deployed.

4. Securing your SaaS applications:

- **Inventory everything:** Understand every SaaS application in use. Consider both officially sanctioned apps and those used informally by employees.
- **Establish basic security controls:** Address common breach causes like misconfiguration and social engineering. Implement Single Sign-On (SSO) and multi-factor authentication (MFA).
- **Conduct Red Team exercises and pen tests:** Regularly test and verify security, especially since SaaS applications have unique access points like APIs.
- **Choose the right partners:** Opt for SaaS providers that prioritize security, offer effective disaster recovery options, and provide robust incident response tools.

5. Key Takeaways:

- **Cloud-native and SaaS are two inherently different things:** these are not competing, and they do not have to overlap — they are truly orthogonal concepts. As stated earlier, you can have applications that are cloud-native, SaaS, both, or neither. Keep this in mind as you adopt technology.
- **Choosing your vendor is the most important piece:** when you adopt SaaS technology, you're adding that vendor to your circle of trust. Your data is at risk if you don't follow proper controls and practices for that application, or if your vendor doesn't properly secure it.
- **80/20 rule for SaaS security best practices:** if you follow pareto principles, there are handful of quick wins that will lead to a lower volume in opportunities for hackers to attack your organisation.

LogRhythm™

About LogRhythm

LogRhythm Axon offers a cloud-native SaaS SIEM platform. It blends the advantages of both SaaS and cloud-native approaches, freeing security teams from infrastructure management to focus on threat detection and response.

For more on securing cloud applications, consider reading **‘Why Insights Matter for Cloud Application Security.’**