Overcoming the PaaS Dilemma: What You Do Not See?

P2P3-W05: Overcoming the PaaS Dilemma: What You Do Not See?

Wayne Anderson, Enterprise Security Architect, McAfee

Overcoming the PaaS Dilemma: What You Do Not See?

Platform as a Service (PaaS) offers our industry both amazing opportunity and challenge. Without this advancement in cloud services publishing, all but the largest businesses would be challenged to harvest advancements in Machine Learning, the massive computation of model learning processing, stepped functions with zero overhead, even new applications of pre-constructed intelligence like Virtual Private Assistants. PaaS is one of a number of democratizing shifts in cloud services, making technologies whose early adoptions required massive server farms, teams of graduate level researchers, and government backing available to even the small startups using minimal capital.

As security professionals, this shift has a cost – by giving up control of the infrastructure and the underlying complexity, we also give up visibility to a number of the key points along the service route we have depended upon for control. Our "sensor grid" of indicators transforms as the Cloud Service Provider now retains these indicators, and our observable behaviors is limited to what our code produces, and to the service interfaces into and out of the service blocks.

Gathering at RSA Conference 2019, a group of professionals joined in a Peer to Peer session examining this challenge: What do you not see? And, just as importantly for the enterprise defender, how do you compensate in your security strategy?

Ahead of the session, the participants shared some basic information about their experience with cloud services. As a collective group, 72% of those participating indicated Azure as the primary cloud service provider with production platform services, with the remaining participants operating in AWS. Only one participant identified a provider other than these two for significant production applications. Across the group, a small number had a deployed production application using platform as a service for more than 24 months, with an even distribution of experience inside of that timeframe. This group, then, represented a variety of companies and at least two US government agencies with a range of experience in cloud engineering for protecting these new applications.

Underlining the challenges of Platform as a service, out of all of the participants in the room, only ***one*** participant asserted full integration of the production Platform as a Service applications to security operations. More than half of those participating identified that they were on the journey, today registering partial or incomplete integrations, with around a third stating that PaaS application's visibility was completely separate from traditional security operations. Exploring these statistics, the participants found their own demographic unsurprising, with stories of PaaS operating as "the wild west, kind of like the '90s when we had no firewalls".

A key question under discussion from the outset, the entire group could universally agree that individual enterprises have a duty to do "something else" – to invest in security controls and visibility to secure PaaS applications beyond Cloud Service Provider defaults. One participant remarked, "The CSP is not responsible for our data, it's not the CSP that will have to do the breach notification, or the CSP who has the privacy accountability." Despite recognizing this truth as a group, the question remained: why do we all understand and see the need for beyond-CSP controls but the self-same group self-identifies integration at far less than full visibility and readiness?

The business pace for Platform as a Service followed as a critical and repeated theme, "the business is asking for new service blocks," offered one senior architect in the room, with a cloud services security manager adding, "the PaaS applications have more responsive ways to meet business cases, but often require that operations includes groups which we have never worked with before." Exploring the demographic issues, the knowledge of patterns and practices for protecting PaaS applications was

identified as a gap by many in the room. One potential methods identified to cross that gap and raise PaaS application readiness includes the notion of a "12 Factor App" using the factors identified by the Heroku mobile PaaS application system.

Connectivity between PaaS applications emerged as a key opportunity for better standardization and readiness both for cloud publishers and companies consuming these application blocks. One security engineer from a large financial institution remarked, "[It's] not a flat network anymore, especially in the cloud… we own less of it." As the group dug into the challenge, the APIs themselves must be appropriately instrumented either by the CSP, or by the company to raise more visible indicators of application misuse. Many participants also indicated a false perception of greater security by the organization,resulting in less money and time being invested in the security of applications engineered on a cloud provider than an on-premise equivalent.

When prompted to consider just one thing to advise companies adopting Platform as a Service to consider as part of their security strategy, a variety of answers emerged. Some of those strategies included:

- Using a service to evaluate SaaS or software-component vendors deployed into PaaS environments
- Consider using a vendor toolkit for Cloud Access to build custom APIs for conditional access control for multi-nationals.
- Use tools like FAIR Risk approaches to help communicate to the business when practices like fast application deployments or poor development practices add to the company's risk profile.
- Use "converged" training with line of business participants to establish a shared language of risk so that those receiving reports or being asked to act on new cloud service requests understand the information being conveyed to make good decisions.
- Implement data security approaches like materialized views, event sourcing, and data integrity analysis to protect data "behind" PaaS applications.

As the session drew to a close, the challenge of securing Platform as a Service offered no easy or immediate answer. Participants from the variety of organizations represented recognized that a combination of development practice, security readiness, communication, and tools would be needed to protect the next generation of new business applications.