OUT WITH THE OLD: WHY WE NEED A DATA CENTER AND CLOUD SECURITY REVOLUTION

PJ KIRNER, CTO AND CO-FOUNDER, ILLUMIO

JULY 9, 2017

Revolutions happen for good reason. They're the result of a divergence of expectations and reality causing pent-up frustration that pushes the need for change. Old ways no longer align with new requirements and pressure reaches a boiling point where there is no other option but to make that change.

Evolutions in applications, the data center, and cloud have pushed security to the limits, where old ways like choke points and network based approaches no longer align with new requirements of application teams. These teams have gotten used to new models of resource utilization and application delivery — and there's no turning back. It's time for a revolution in security.

PRESSURE FROM THE DATA CENTER

We've seen the data center evolve rapidly in the past decade and a half, enabling us to better utilize resources, realize new levels of scale, and move faster than ever. Gone are the days of assuming your applications were more or less static and all lived in your private data center.

New levels of consumption, scale, and speed have created new challenges and pressure for security teams.

- Virtualization has abstracted core data center resources of compute, network, and storage, making workloads more portable and adaptable while making applications more scalable and resilient.
- Cloud has created on-demand, elastic environments allowing us to satisfy our on-demand infrastructure needs, making consumption easier and utilization more efficient.
- Containers are increasingly common in environments today, enabling a rapid way of developing, building, and packaging applications and services.

PRESSURE FROM APPLICATION

Infrastructure isn't the only area of evolution and innovation. We've seen similar change with the way we develop and deliver applications. Thanks to Continuous Integration and Continuous Delivery (CI/CD), our expectations throughout the Software Delivery Lifecycle (SDLC) have evolved. We now expect software to be developed and delivered faster and more fluidly than traditional release-based approaches. For many, gone are the days of distinct release cycles where teams could get into a room and plan the details for an upcoming go-live date. Every week and, in some cases, every day or even several times a day, new code is being developed and pushed into production.

Monolithic applications have been superseded by microservice architectures. The applications themselves and related service architectures have also become more complex and their components more connected. Applications are dependent upon data and services across the environment leading to exponentially more East-West communication than we have ever seen in the past. More interconnections mean more open pathways, which can lead to a larger attack surface to defend and more risk to the business. In addition, the ephemeral nature of containers, plus the connectedness across those environments, create a whole new set of challenges for security.

The DevOps movement has brought together developers and operations teams to fuel this need for application and infrastructure agility. But the first generation of this movement left security out of the loop. For many, engaging with security was seen as a hindrance to progress and the rapid deployments philosophy and, in some cases, caused security to be sidestepped altogether.

SECURITY HASN'T KEPT UP

The evolution in data center infrastructure and applications has fueled the movement of organizations becoming more software-driven and moving faster than ever before. Security has always been important, but as organizations become more dependent upon software to drive their business, it's becoming increasingly critical to get security right in order to minimize business risk. Getting it wrong can mean loss of data, impact to revenue, lasting effect on brand, and even penalties tied to compliance. Security has not kept up with the evolution we have seen across infrastructure and applications.

Traditional network-based, choke point solutions for enforcing policy are not only impractical, they can be downright impossible to architect around and deploy. With applications being a sum of their parts, sometimes distributed across data centers and even into the cloud, the complexity of consistently enforcing policy can be a huge challenge. Couple that with the fact that application infrastructure is becoming more and more dynamic, keeping policy in sync with movement and scale can be close to impossible.

One of the goals of evolving security is to shift the balance away from the attacker's advantage and leverage the strengths of the defender.

Even attackers have evolved to defeat the latest security approaches. Shifting the balance to the defender's advantage requires a model that moves from being reactive to threats to a model that proactively changes the game, giving the defender back control. In order to do that, we need to approach security in a new way and think differently about application environments and how we protect them.

Current security approaches can be a bump in the road, slowing down progress, if not an altogether roadblock. In continuing to follow the traditional path, there is risk that development teams will look for ways around security to continue moving forward at the pace they need to remain efficient.

This need for efficiency is one of the reasons we need to rethink security and better align it with the evolutions we've seen across the data center.

EVOLVING SECURITY FOR MODERN APPLICATION ENVIRONMENTS

While most security solutions today are based on old assumptions that things move slower and are more or less static, we know that reality is no longer true.

Even if you're not yet feeling the full impact, businesses are increasingly driven by software, applications are moving faster, and application environments are becoming more complex and heterogeneous — calling for a revolution in data center and cloud security.

Technologies like virtualization and IaaS have abstracted infrastructure to align better with application requirements. We need to think about security in a similar manner.

Seeing workloads in the context of the application and business processes is the best way to understand risk and build policy. It's also the only common language that all teams within the organization can understand. An application development team doesn't think about their app environment in the context of the network (IP addresses and ports). They think about it in the context of the components of that application, how they're related and how they work together. The same is true for business process owners who think about their process, the applications and services that are related, and how they all work together to address business requirements.

This shift in perspective is foundational and a first step to open the door to a new approach. It's the only way to create security that adapts for modern application environments that are spread across platforms and locations, dynamically moving and scaling to meet demands.