THE GREAT DIVIDE

PJ KIRNER, CTO and Co-Founder, Illumio
OCTOBER 21, 2014

As data centers grow increasingly complex and dynamic, businesses are facing a maelstrom of security risks. We can no longer trust the concept that a magical boundary will protect our data centers.

About nine years ago, I was working as a distinguished engineer for Juniper, one of the leading network security companies in the world. The longer I worked there, the more my customers' network perimeters slowly crumbled. Next-gen firewalls began to detect Skype and Google Docs. Infrastructure-as-a-Service and cloud alternatives made traditional choke-point security services impossible to implement. But it wasn't until I left that I could fully address the divide between that old world and the new world, where change is constant.

In this new world, data center virtualization accelerates the spin up of compute, storage, and networking services. Self-service IT and the DevOps culture of continuous delivery further increase the pace. Yet, during all these advances, security was left behind, often stalling forward progress. The SecOps folks are now forced into the unenviable position of having to say no to cloud architectures while everyone else is saying yes.

Illumio was born from this chaos.

We are not about making the network or infrastructure better (or virtual)—we are fundamentally decoupled from those constraints. Illumio's adaptive security system is leading the way from the static security model of the past to the increasingly dynamic data center of today. This is where it starts to get exciting.

Three truths and the great divide

1. We live in a world of constant change. We must embrace this, with all its challenges and benefits.

Data centers of the past were very much tied to their physical environment. Applications ran on bare metal, with directly attached storage and physical wires connecting these machines. That world was static.

Today our data centers have to keep up with countless changes. With continuous application delivery, new versions are being deployed more rapidly than ever before. Server virtualization allows workloads to move more easily and frequently, and to dynamically scale. Infrastructure as a Service enables almost anybody to provision and deploy servers and applications.

Traditionally we depended on the infrastructure for reliability, but as we build bigger and more complex data centers, infrastructure failure cannot be avoided. For this reason, Google long ago adopted the philosophy that new software architectures must be developed to run reliable applications on top of fundamentally unreliable infrastructure.

While the data center has undergone all these changes, security has been shackled to static and choke-point models. And it holds us back. We are not realizing the full benefit of our technology investments in the dynamic data center.

We knew that Illumio's security architecture needed to embrace and enable change.

By having a security system that adapts to our choices, we are more productive, we can put things anywhere, and we are freed from centralized control and rigid organization. We can scale more easily.

To achieve this, we knew our system must be **decoupled** from the network and the infrastructure. Being decoupled allows us to deliver a security solution that works consistently all the time, across all types of changes in the data center environment.

We also knew the system must be fully **distributed**. Traditional network security systems often steer traffic to a centralized choke point that has little to no context. Because of large-scale requirements, often only a portion of your workloads can actually be processed and secured. This brute-force mechanism also leads to blind spots, false positives and a greater attack surface.

To address those limitations and deliver sufficient coverage with enough flexibility, we put security in places that were traditionally difficult. We can now see into places that were previously hidden. This is much like having a matrix of bodyguards in every room of a hotel, instead of just the front-door security—it is a collective all working together under one set of directives.

2. Automation is not enough. Intelligent systems drive us forward.

Automation only masks complexity. IT has many systems that interact and most of us spend a lot of energy trying to make it all work. We add layers of automation and abstraction in attempts to hide or manage problems. These layers pile on top of each other and create a weak foundation that cannot support growth.

Simply virtualizing the old model in the new world was not going to cut it. The way forward had to be wholly different. It had to be intelligent enough to adapt to this completely different world, where speed and responsiveness are the new table stakes.

For an intelligent system to take effective action, it needs good data at its foundation. It needs a rich understanding of the world in which it operates. It needs **context**.

Many forms of context are required, and they must be combined to paint a complete picture. Our system gathers context about the workload itself, the relationships and communication between the workloads, and the environment in which the workload operates.

Next, we knew the solution required a system that was **dynamic** and **responsive**.

We created a language and policy model to align with the way users and data centers operate: a simple yet powerful, declarative, label-based system. This is not an additional layer on the old-world model, rather, it is a brand new approach.

The Illumio system continuously feeds context and relationship data into the declarative policy model and recomputes the graph to ensure a consistent security policy. We unburden the user from implementing every change…because in such a dynamic world, it would be absurd to expect a person to understand and remap all the dependencies and relationships with every change. With Illumio, people specify the policy and our security platform implements it.

3. The world is hybrid. Security needs to **work anywhere**.

As software and things that are "as-a-Service" become increasingly important, APIs are connecting countless different environments and creating a myriad of security challenges.

We all know that systems bound to one platform or working in a single ecosystem fail to succeed in this heterogeneous and hybrid world. We need the freedom to choose the right tools and systems. And we need these to work seamlessly, on demand, without concerns around divergence, inconsistencies, and errors creeping in.

Today's security system needs to work with us, not against us. It should go where we want to go and do what we need it to do.

We built our system to work on any computing platform, including bare-metal servers and virtual machines. The system also works in any environment, including enterprise data center, Amazon Web Services, Google Compute Engine, Microsoft Azure, and OpenStack.

Traveling the great divide

These three fundamental truths are woven into everything we do at Illumio. We have made the trek across the great divide, and the benefits are enormous. The best tool for the journey is an intelligent system that provides a uniform experience and makes the most of advances in the data center.

The team here at Illumio is very proud of what we're launching today and I look forward to sharing more as we continue delivering solutions for the new world.