THE NEXT VERSION: ADAPTIVE SECURITY GOES DEEPER AND BROADER

PJ KIRNER, CTO AND CO-FOUNDER, ILLUMIO

APRIL 14, 2015

Today, we are launching the next version of the Illumio Adaptive Security Platform (ASP) with extensions that enable greater control and provide more enforcement points across the data center to protect your data and applications.

It has been about five months since we unveiled Illumio and we have been busy working to further our vision of adaptive security by building upon the power of the dynamic Relationship Graph that the Illumio platform continuously computes.

COMPUTED SECURITY AND THE RELATIONSHIP GRAPH

The Illumio team created a platform to secure computing in dynamic and distributed data centers and any public cloud without any dependency on the underlying infrastructure.

We started with the premise that the specification of security policies (written in plain English) can be separated from the implementation details (their translation to IP-based rules) to keep up with application and environment changes. This allowed applications and their permitted interactions to be captured and maintained even as the chosen underlying hardware (VM vs. bare metal) and OS (Linux vs. Windows) differed, or the network (different data centers and public clouds) changed.

At its core, Illumio ASP relies on its ability to build and understand the application topology using a dynamic model of relationships between the workloads inside and across multi-tier applications deployed anywhere.

In our parlance, we call this the Relationship Graph and it is kept accurate by continuously discovering changes in the context of individual workloads. This dynamic graph enabled us to build services on top of it—like visualization of all application traffic through Illumination, the computation of fine-grained inbound and outbound security rules to be enforced on every workload, and the encryption of data with IPsec between any set of workloads.

The platform automatically adapts to the smallest change in workload state by reconciling the appropriate implementation policies on the affected workloads. It removes the need for manual intervention to account for changes and naturally reduces the likelihood of errors.

BROADER AND DEEPER CONTROL WITH THE RELATIONSHIP GRAPH

The latest version of Illumio ASP extends adaptive security to additional enforcement points.

We saw the ability to mine context from deeper inside the workload—the individual processes running on them—as a natural extension to the Relationship Graph. This means we can increase the granularity of the security model by describing application interactions not just between workloads but also down to individual processes. This will also lead to the ability to secure container-based application deployments.

Illumio ASP can now nano-segment applications in data centers or clouds to a level where different processes within a workload could be part of different applications. As an example, Illumio ASP allows you to segment the ERP and the HR applications across multiple process instances running on a single workload, but serving the two different applications, without having to compromise on security and data segmentation policy.

A COORDINATED APPROACH TO SECURITY POLICY AND INTELLIGENCE

Today we also announced a strategic partnership with F5 Networks, as part of the Illumio vision of a coordinated approach to provide security policy and intelligence across the entire data center. The inclusion of F5 load balancers allows Illumio ASP to broaden its security enforcement beyond just the host. The Illumio Policy Compute Engine (PCE) enables the F5 load balancer as an additional coordinated point of enforcement by programing ACLs directly into the F5 load balancer. This allows security policy to be enforced on data flowing into and out of the load balancer and to be automatically reprogrammed when workloads on either side of the load balancer change.

As an example, a single F5 load balancer can be segmented across multiple application environments (staging vs. production) by programming policies for the virtual IPs serving the two environments on the appliance, preventing unauthorized access and data leakage across those environments. As a result, the Relationship Graph is richer as it brings third-party components into the security model and effectively lowers the attack surface inside data centers even further. This also enables businesses to better utilize their existing IT investments by allowing them to participate in an adaptive and coordinated security model rather than just being managed and operated as point solutions and by bringing previously opaque components into the segmentation model.

OUR VISION GOES EVEN FURTHER

Virtual machines and Amazon created a much more dynamic model for computing resources and enabled businesses to go faster. Containers like Docker and Mesos are paving the way for the next wave of such improvements. At Illumio, our vision is that security should match the speed of applications and adapt to the changes in your business.

Our customers benefit from removing complexity while improving their security posture, all without the need to add any hardware. We will continue to extend our adaptive security model to more elements of the infrastructure while staying true to our credo of “security that works anywhere.”