ILLUMINATION 2.0: NEXT-LEVEL VISUALIZATION AND POLICY CREATION

MUKESH GUPTA, SR. DIRECTOR OF PRODUCT MANAGEMENT

AUGUST 22, 2017

In 2014, Illumio pioneered real-time application dependency mapping and visibility for micro-segmentation with Illumination. When we launched the Illumio Adaptive Security Platform (ASP), we believed that organizations wouldn't be able to build segmentation policy for their brownfield applications without an application dependency map (Illumio CTO PJ Kirner expounds upon why you need a map for security in a recent blog post). From our first version through today, Illumination has provided a way for organizations to use traffic flow visibility to build micro-segmentation policy, test it, and then start moving to enforcement – application by application.

THE EVOLUTION OF VISIBILITY

The first version of Illumination allowed central security teams to analyze application flows and manually add whitelist label-based rules to allow them. The sole goal was to help the customers build their micro-segmentation policies, and all the workflows in Illumination focused on that single goal. When we initially conceived of Illumination, we thought that customers would pair a limited number of workloads, build policy, and then migrate those workloads into enforcement. We were wrong.

As many of our customers have used Illumination to segment their data centers and cloud infrastructure, here's what we've learned since we first shipped:

1. **Policy Generation Can Be Really, Really Hard:** Illumination allowed security teams to analyze traffic connections one by one and, with a valid flow, add a rule in Illumio's whitelist label-based policy model. We've learned that applications are extremely interconnected and just a few hundred applications comprised of a couple thousand workloads can have millions of unique connections that need to be analyzed. The best way to get started is to automatically generate policy to allow those connections. This has the risk of allowing a connection that shouldn't be allowed (as you'll read below, we have tools to help with this); however, from this point onwards, customers can restrict lateral movement and immediately detect policy violations.
2. **Centralized Policy Creation Doesn't Always Work:** Workflows in Illumination were designed to help a central security team build micro-segmentation policies for the entire infrastructure. However, we learned that building micro-segmentation policies is difficult and time-consuming without delegating it down to the application teams that understand those applications. (Coming soon: Our VP of product Matthew Glenn's blog post about aligning segmentation with your organization. Stay tuned – it is a good read).
3. **Visibility Can Be Used for Compliance and Security Operations:** When we first shipped, visibility in Illumination drove micro-segmentation policy creation. However, once we added the context of labels and policy to traffic, this visibility became tremendously beneficial to compliance/audit and security operations teams. Compliance teams use visibility to generate reports that enable an auditor to finish his or her job faster and more efficiently. Security operations teams use visibility to quickly find policy violations, detect threats, and respond to those threats more effectively. In fact, some of Illumio's customers were able to detect hosts impacted by WannaCry through Illumio's visibility; any host that broke policy and tried to connect on SMB ports was quickly tracked down and remediated. Other customers found that some of their data center servers were listening to music from Spotify and were posting updates on Facebook. You should have seen the expressions on their faces when they discovered those connections.

We're constantly listening to and learning from our customers. Last year, we added App Group Maps to help application teams use Illumio and focus on just the applications and workloads that are important to them. Today, we are excited to announce the following new features under the umbrella of Illumination 2.0.

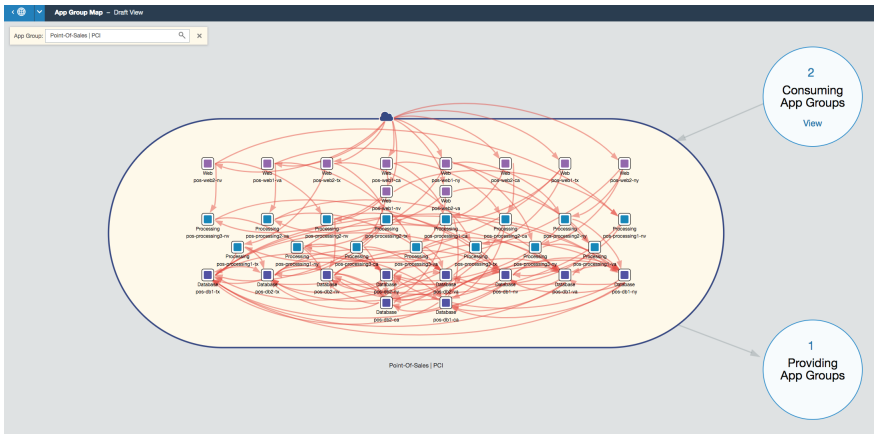
NEW FEATURES, ADVANCED VISIBILITY

INTRODUCING POLICY GENERATOR

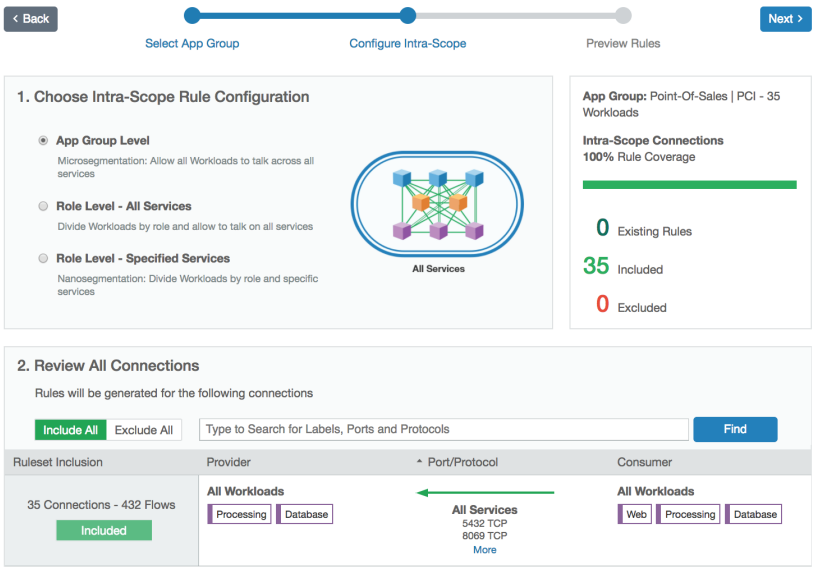
Years of customer feedback loops and lessons learned have given way to key insights about policy:

- Writing policies flow by flow in a large environment isn't really scalable. (If you want proof of how one of our competitors does it flow by flow, watch this video).
- Centralized security teams don't always know the specifics of how applications work; when writing security policies, they couldn't validate whether flows were right or wrong. This has driven the desire to extend policy creation out to application teams who have details of their applications.
- Application teams might have opinions about how applications should be secured, but they don't have experience in creating security policies (e.g., firewall rules) – and putting application teams through segmentation policy school isn't really an option.

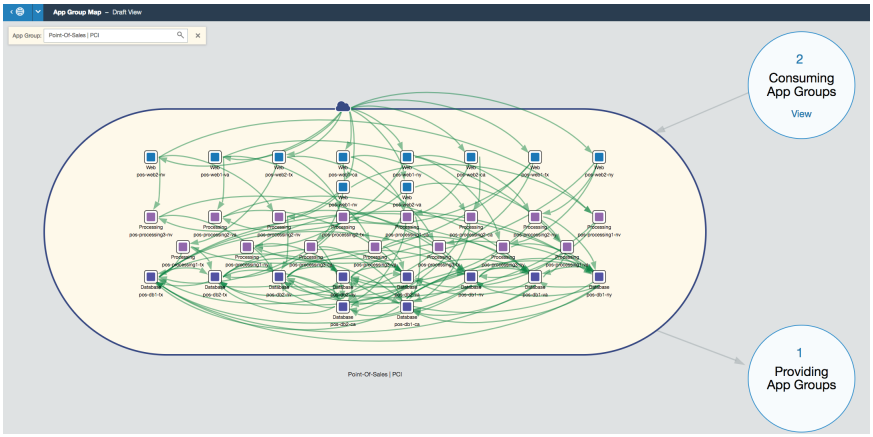
That's why we created Policy Generator.



Application dependencies without security policies in a single application.



Security policy recommendations for micro-segmentation.



Application dependencies without security policies in a single application.

Policy Generator drastically reduces the time, training, and resources required to write micro-segmentation policies.

It uses custom-built algorithms and network traffic history to automatically generate label-based micro-segmentation policies. Policy Generator allows customers to dial in their desired level of segmentation granularity at the application, application tier, or all the way down to the port/protocol level. Once the desired level of policy is selected, Policy Generator automatically generates conforming micro-segmentation policies in minutes. What's more, the micro-segmentation policy is natural language – something that any application team can read and understand.

Policy Generator can be used with role-based access control (RBAC) to delegate policy creation to the respective application team. Security teams can perform a final check before promoting the policy created by the application team into production, so the policy can follow the software development lifecycle (SDLC).

Policy Generator allows large organizations to get to a fully micro-segmented data center and cloud infrastructure with significantly reduced time and resources.

It also allows customers to iteratively develop segmentation policies. For instance, an organization can generate an initial micro-segmentation policy. In a few weeks or months, Policy Generator can be run again to generate policies that accommodate new flows, or adjust granularity to tighten the policy down to the port/protocol level (a.k.a. nano-segmentation).

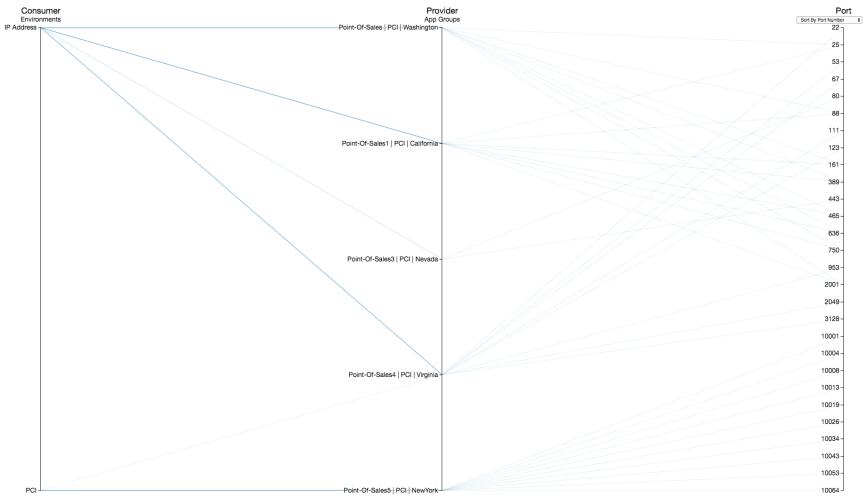
INTRODUCING POLICY GENERATOR

Explorer enables security, operations, and compliance teams to create traffic queries. Here are some examples that we have seen:

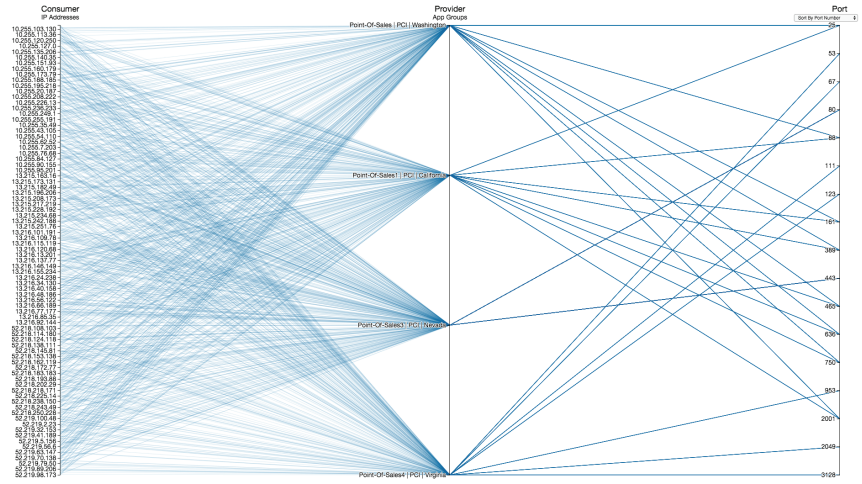
- A compliance team can use the Explorer tool to quickly download the list of connections flowing into their PCI environment. They can then deliver that report to a QSA to help pass a PCI audit.
- A security operations team could ask for all the traffic flows between the “Dev” and the “Prod” environment on SSH and database ports so that they can have app teams justify the connections.
- An operations team can pose queries like, "Tell me about all of the flows between servers in two different data centers," which can be used to identify remote application dependencies, or to determine if a data center outage could impact the availability of an application in general.

Organizations are using Explorer to find the 'needle in the haystack' across millions of flows to identify hidden policy violations or security threats.

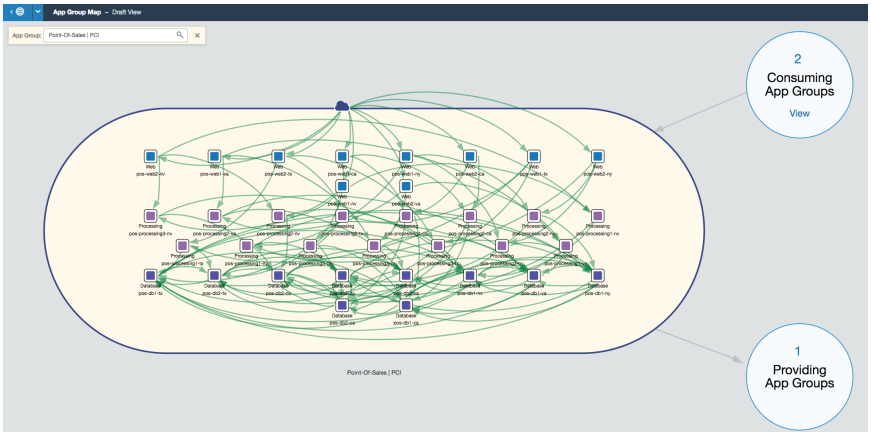
Explorer allows users to approach traffic in a very different way. Users can look at traffic associated with any set of labels using a parallel coordinate map (pictured below). Then a user can ‘click’ through points on the parallel coordinate map to get to the traffic that is interesting. They can then download the list of flows into a CSV, but include the label context to the connections for both the sources and the destinations. Explorer also adds the context of policies to each connection to quickly inform if the connection is allowed by your policy or not.



Identify any policy violations and security threats.



View of all communications into your PCI environment.



Ask a question about your PCI application traffic.

SEE IT LIVE AT VMWORLD 2017

We embarked on this journey to provide real-time application dependency mapping and visibility for segmentation three years ago. Since then, other vendors in the micro-segmentation market have realized the importance of visibility and application dependency mapping. Last year, nearly all of them tried to fill their product gaps by trying to build or acquire a solution. While other companies are at the start of their journey, we're excited to take visibility to a new level by adding Policy Generator and Explorer to Illumination.

Illumination 2.0 enables organizations to use these visibility features to more efficiently micro-segment and secure their data center and cloud infrastructure, while also allowing them to use this visibility for operations, compliance, and security operations workflows.

We'll be showcasing these new features at VMworld 2017. If you're headed to the show, come visit us at booth #800 for a live demo.