REVIEW: MICRO-SEGMENTATION WITH ILLUMIO

SPONSORED BY:

Author: Justin Warren

REVIEW: MICRO-SEGMENTATION WITH ILLUMIO

Contents

01 INTRODUCTION

PivotNine took a look at Illumio's approach to security and micro-segmentation, and gave the product a try. This whitepaper is the result of our high-level testing of the product's capabilities from an outsider's point of view.

We tested some common security scenarios, such as setting up multiple physical environments, a mix of on-site and cloud resources, production, test, and development environments, and a mix of Windows and Linux workloads.

Our goal with this review is to help customers understand the Illumio approach to micro-segmentation as compared to other, more traditional methods such as network-level firewall appliances.

About Illumio Adaptive Security Platform

Illumio ASP is an adaptive micro-segmentation solution that helps to prevent unauthorised communications across the data center and cloud. Through the automatic recommendation of micro-segmentation policies, the platform can create, model, and natively enforce these policies.

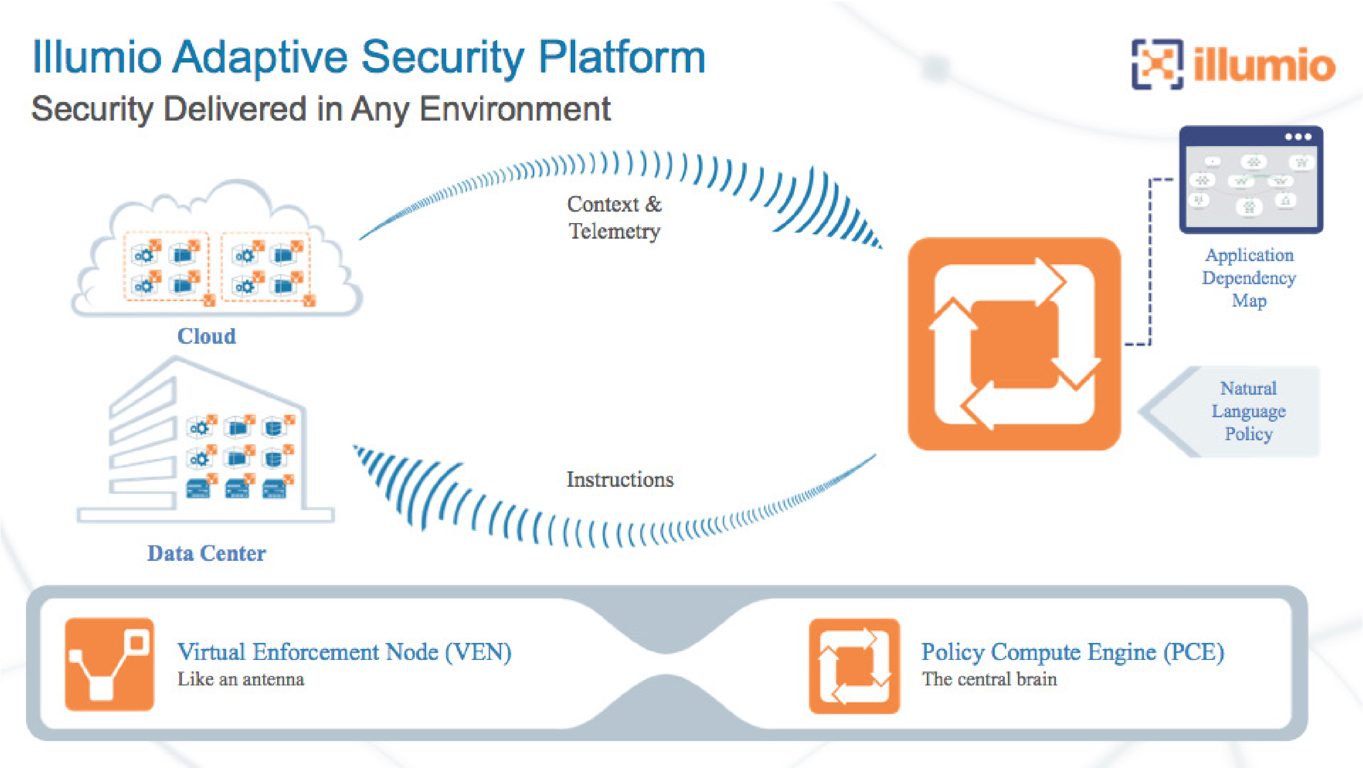


Figure 1. The Illumio Adaptive Security Platform

01

Illumio uses a central controller (the Policy Compute Engine, or PCE) that takes label-based security policy definitions and calculates per-host firewall configurations required to enforce the policy. Enforcement of the policy is performed using the native firewall capability of the host operating system, which Illumio calls a *workload*.

Workloads are connected to the PCE using a lightweight host-based agent (the Virtual Enforcement Node, or VEN). The VEN locally applies the holistic ruleset determined by the PCE, but remains out of the data path at all times.

Evolution Of The Network: Why Consider Illumio ASP

Enterprise IT systems have changed markedly since the early days of remote access to timeshare systems over VT220 terminals. Software has become more distributed as has the hardware that it runs on. We now have vast quantities of virtual machines running in data centres throughout the world, as well as embedded computers with full IP stacks that run on webcams, sensors, and drones.

This has increased the number of applications we need to protect from malicious actors seeking to ransom our data. With the amazing changes in both the number of devices and applications, and how they are connected, we should probably be changing the way we partition and secure the network to help keep all of these applications safe.

Network Boundary Segmentation

Some changes have been made, of course. We moved from perimeter firewalls and demilitarised zones to multiple segments inside the network, each protected by another firewall. We joined specific network zones together with VPNs when we couldn't physically place the devices near one another, and therefore within the same firewalled zone.

We also moved to multiple data centres, and then to cloud computing, where an application might span data centres, not just network boundaries. Microservices is causing another step change in volume and complexity of systems that need to be secured, all still managed by human operators, largely configuring firewall rulesets and access control lists by hand.

Managing Complexity

Add into this infrastructure nightmare the prospect of continuous integration and multiple code deployments a day, rather than one or two a year. Firewall changes don't have to happen inside a change window next month, they need to happen *constantly* to keep pace with developers continuously deploying new code into production. Organisations are driving the expectation for ever more frequent change in a vastly more complex environment than even five years ago in order to keep up with their competitors who are all doing the same thing. It's a dynamically complex environment.

The threats in this environment are also growing more numerous and sophisticated, as the criminal enterprise of hacking has become big business in its own

01

right. Where there is a profit motive, there is a drive to improve, and there are plenty of people with nefarious motives who are every bit as smart and capable as the white hat hackers.

This is the situation the modern security team faces every day. It is no longer possible for a human operator to manage their security systems unaided—not with any degree of responsiveness or reliability. Attempting to keep up inevitably results in misconfigured ACLs that block important traffic—or worse—allow malicious actors to gain access to important systems.

Interestingly, technologies like Illumio are tackling the dual issues of complexity and scale to provide useful new approaches to keeping systems safe.

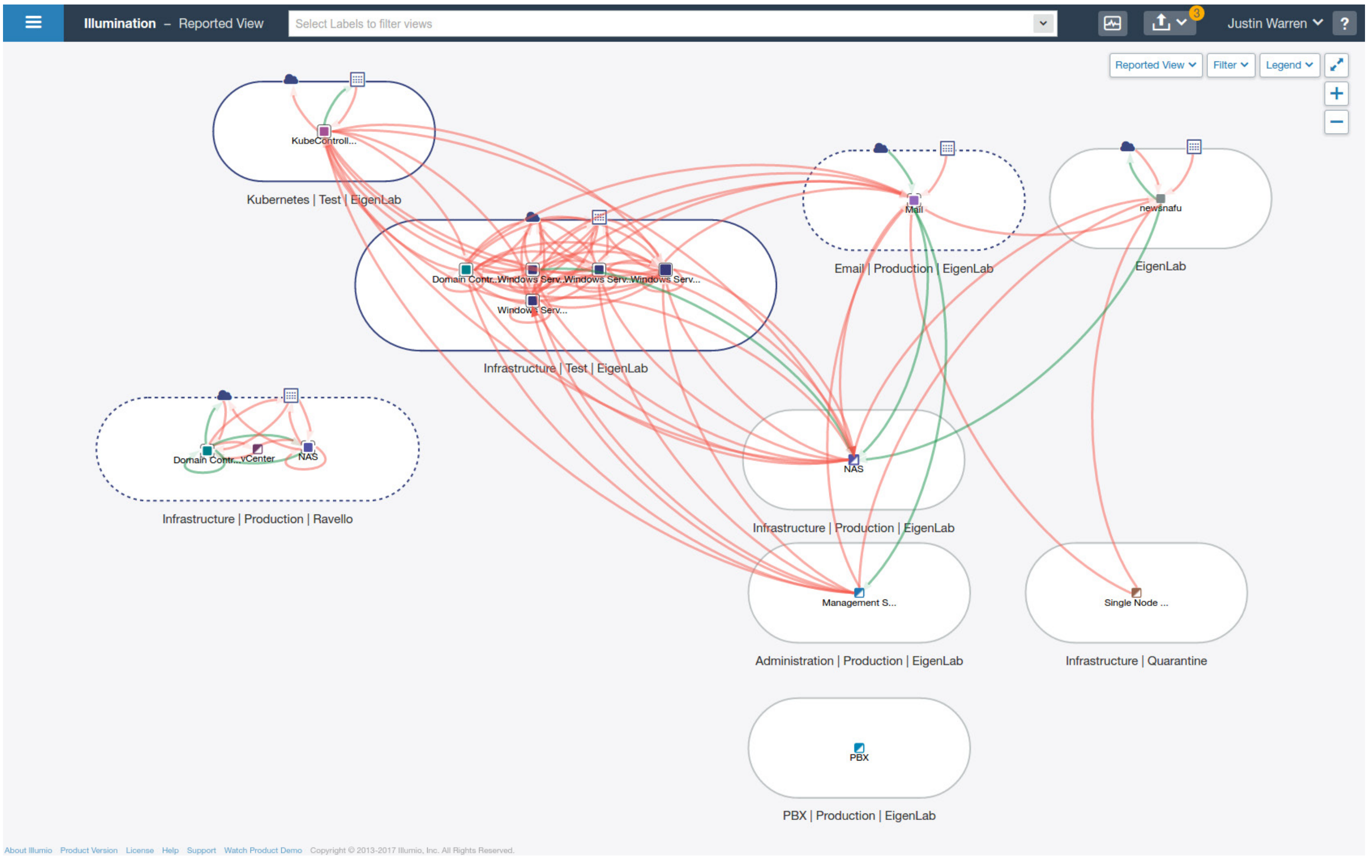
02

SITUATIONAL AWARENESS

The key to a good security system is situational awareness. Having situational awareness requires three things: accurate information about the environment, the ability to understand how this information relates to the bigger picture, and the ability to predict the likely future state of the system based on this understanding.

There is no shortage of systems and tools that provide individual pieces of information. Individual firewalls can tell you if a network flow violates an access control list, but they can't tell you which application that flow relates to or how important it is. It's also tricky to determine how overall security policy relates to individual rules in an ACL. When you have hundreds—or thousands—of rules on hundreds of firewalls, it's near impossible for a human to have an accurate picture of how they all relate, robbing you of situational awareness.

It's similarly difficult to be able to predict the effects of changing any one rule. How does it interact with all the other rules on this firewall, let alone all the other ones throughout the organisation? Will adding this rule break an important application? Will it interact with other rule and accidentally allow traffic through that should be blocked?



Illumination – Reported View
Select Labels to filter views
Justin Warren
?
Reported View
Filter
Legend
+
−
KubeControll...
Kubernetes | Test | EigenLab
Domain Contr...
Windows Serv...
Windows Serv...
Windows Serv...
Windows Serv...
Infrastructure | Test | EigenLab
Mail
Email | Production | EigenLab
newsnafu
EigenLab
Domain Contr...
vCenter
NAS
Infrastructure | Production | Ravello
NAS
Infrastructure | Production | EigenLab
Management S...
Administration | Production | EigenLab
Single Node ...
Infrastructure | Quarantine
PBX
PBX | Production | EigenLab
About Illumio
Product Version
License
Help
Support
Watch Product Demo
Copyright © 2013-2017 Illumio, Inc. All Rights Reserved.

Figure 2. The Illumination View

02

Illumination

Modern Windows and Linux operating systems have quite robust firewall mechanisms built into them. They are also capable of providing high quality information about network traffic seen by the host. Illumio takes advantage of this built-in capability using what it calls *Virtual Enforcement Nodes* (VENs) installed on each host. These simply connect the host-based firewall mechanisms to a central Illumio controller called the *Policy Compute Engine* (PCE).

Telemetry information is sent from the VENs to the PCE (over encrypted channels, of course) which PivotNine investigated using the cloud-based Software-as-a-Service (SaaS) deployment method. The PCE is also available in an on-site mode for customers with more restrictive deployment needs and the functionality is identical to the cloud-based PCE.

This telemetry information provides the first requirement for situational awareness. Illumio's *Illumination* view provides the second: understanding of the bigger picture. The Illumination view is a node-and-flow graph view of how workloads connect to each other.

This view provides an *application dependency map* showing the workloads and flows in the context of the applications to which they belong, rather than an infrastructure-centric view of which physical assets sit where.

You'll naturally see patterns of connections between workloads in an application—web servers connecting to app servers connecting to databases, for example—and also between applications, particularly in microservices environments. You might also discover connections between systems that you didn't know about.

Perhaps applications are connecting to each other in ways that aren't immediately obvious, exposing interdependencies you weren't fully conscious of. You might even discover services you didn't know existed or thought had been decommissioned. Making the invisible visible is a powerful way to expose hidden risk that can then be addressed in a systematic way.

Application Dependency Mapping

Showing how applications are composed of a set of related services is particularly important as organisations move to microservices architectures. Applications can span physical systems in multiple network zones, in multiple data centres, even multiple clouds. Using a firewall/chokepoint approach becomes unwieldy as service connections are forced to route via arbitrarily provisioned choke points instead of connecting from service to service in a clean way.

The application-centric approach from Illumio helps the network and security teams to get out of the way of the application without compromising the security of the system.

Illumio uses a *default deny* approach to security, so we need to have an understanding of which systems are permitted to connect to others. This is a kind of *need-to-know* or *need-to-connect* principle; if a system has no need to connect to another one, it isn't allowed to by default.

03

A NEW APPROACH TO SEGMENTATION

Micro-segmentation is the process of creating smaller compartments than the traditional internal/external or production, test, and development compartments separated by firewalls. Smaller compartments keep threats contained, and reduce the degree of damage that can be wrought if something goes wrong within any one compartment.

Flexible Granularity

Illumio allows you to go several steps further than the traditional broad compartments by providing for a flexible method for *granular* segmentation. A very specific policy that only applies to a single port/protocol connection between two extremely high value assets can coexist with another policy that allows any-to-any communication for hosts within a development application. Tight security controls can be applied where necessary, while agility in the development cycle is not sacrificed in an effort to maintain security.

Illumio supports extremely fine-grained segmentation, down to the Windows process level if required, not just at device boundaries or to specific network ports. Windows systems make extensive use of dynamic port allocations through its RPC mechanisms, which are important for administrative and internal Windows functions. Blocking them would break functionality, but allowing them isn't as simple as for port-based networking connections. Illumio is able to secure access between RPC endpoints because it understands Windows networking at the process level.

The traditional production, test, and development compartments are still easily implemented with Illumio. Unlike data centre firewalls, the visualization and dynamic enforcement of the broad policy can validate that the intended policy matches the actual policy with minimal configuration and no maintenance.

Role-Application-Environment-Location

The flexibility of segmentation comes from Illumio's labelling mechanism for defining groupings of workloads. This is a multidimensional way of describing workloads as logical groupings, rather than having to deal with security policy at an individual workload level or at physical network boundaries.

The *Location* is used to describe the location of the workload, while the *Environment* is used for the

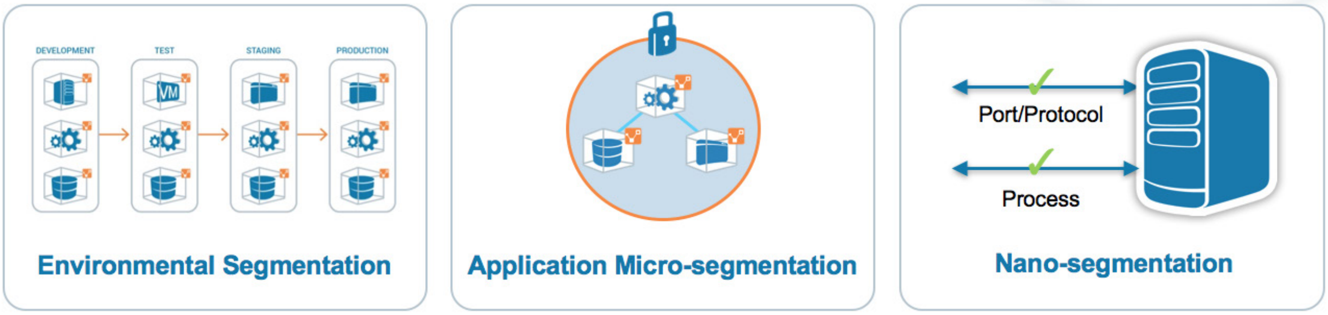


Figure 3. Types of Granular Segmentation

software development life cycle (SDLC) stage of the application. The *Application* is just a logical grouping of related workloads that form an application, and the *Role* is the role each workload performs as part of that application.

Of course, you could use your own labelling scheme for what each label category refers to—perhaps a logical location makes more sense for your applications—but the important point to note is that the labels provide multiple axes for defining micro-segments that a particular set of security policy applies to.

Abstraction and Automation

By using these axes for labelling, security rules can be applied to groups of workloads—large or small—on a logical basis. While extremely complex rulesets can be defined for specific circumstances, common situations—such as permitting administration traffic from a dedicated administration network—can be addressed with quite simple rules applied to a broad scope.

The PCE does the hard work of generating the specific firewall configuration required by each workload, instead of human operators having to manually craft individual ACL rules. These generated rules are specific to each workload, and applied by its VEN, so they are consistent across the environment. This situational awareness means the PCE can define the minimum set of configuration required to achieve the desired policy result, and you can concentrate on defining security policy from an application-centric perspective.

Working at a higher level of abstraction is part of what enables systems to scale. By using these logical groupings, it's easy to change which set of rules apply to a given workload, or entire groupings of them, simply by changing labels. For example, as an application moves through its software development life-cycle, different security rules can be applied simply by changing the *Environment* label of all workloads for that application.

The use of software labels and dynamic host-based security policies makes Illumio an ideal fit for modern, heavily automated environments. Labels can be applied to new workloads as they join the environment, so the right security policy is applied to them immediately. There's no separate build step to configure security when commissioning new systems, which is particularly important for the modern ephemeral cloud and container-based environments. All systems become protected immediately and consistently.

As systems move through the development process, they can be quickly changed to have the right policy based on the application need just by changing a couple of labels. Policy is consistently applied because the details are taken care of by the PCE's automation, and you can keep the development speed high without compromising on security.

04

SECURITY POLICY DESIGN

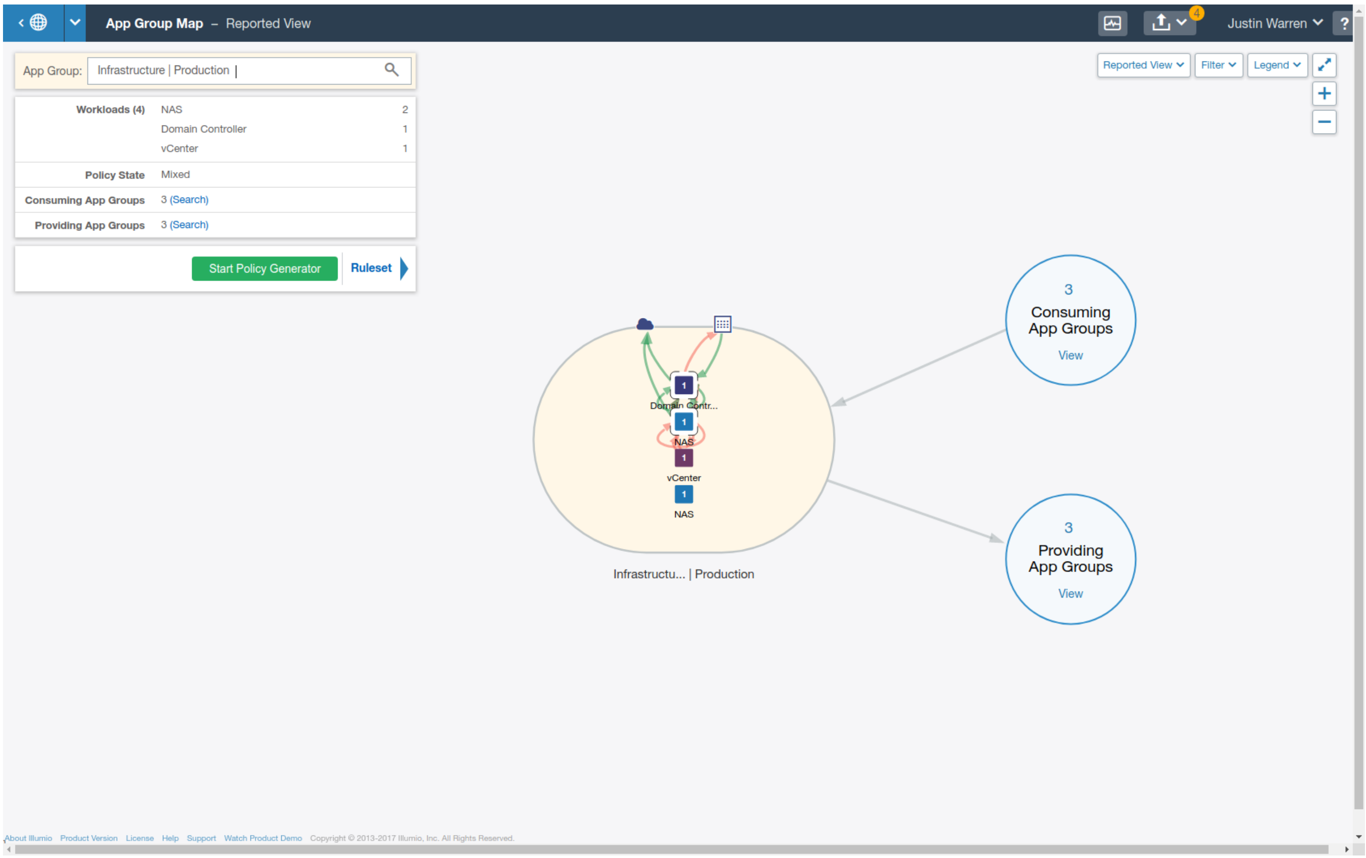
With our first two requirements for situational awareness established, we can move on to the third point: the ability to predict the future state of the system. There are two major stages where this is important: initial policy setup and making changes.

Policy Generator

Illumio provides a *Policy Generator* which automates much of the initial setup. Instead of configuring rules individually, Policy Generator uses the Illumio *App Groups* feature to find and analyze groupings of traffic and automatically generates rules that would permit this traffic.

This is the power of having both high quality information about the environment (situational awareness, step one) and a holistic view of the system (situational awareness, step two). Illumio can accurately predict what policy will be effective—and automatically generate it for you—because it has good information about your environment as a whole.

App Groups are based on your choice of how to use labels to group applications. Applications are not



App Group Map – Reported View

App Group: Infrastructure | Production

Workloads (4)	NAS	2
	Domain Controller	1
	vCenter	1
Policy State	Mixed	
Consuming App Groups	3 (Search)	
Providing App Groups	3 (Search)	

Figure 4. Policy Generator and App Groups

limited to any particular physical location or network boundary. For example, the web, processing, and database workloads in your ordering application, in development could belong to the same App Group, even if some of the web workloads ran in the cloud, the processing workloads ran in a colocation facility, and the database workloads ran in your private data centres.

Policy Generator can then analyze the data flows between workloads and automatically generate rules for you based on the flows already occurring between these App Groups. The wizard style interface steps you through creating the rule sets for each App Group instead of having to do it manually, and you can be as permissive, or restrictive, as you like. If you want to ensure that database systems only ever talk to other systems on specific ports, including workloads within the same App Group, you can permit only those specific services for workloads in the database App Group.

It's usually best to start with a few simple catchall rules for known safe traffic and then gradually add tightly scoped rules to allow additional traffic, depending on your security posture and the assessed risk.

Modelling and Testing Micro-Segmentation Policies

Most of a security team's work involves making changes to the existing policy definitions that protect the environment in order to respond to changes needed by applications. To make good changes, we need to be able to predict their effect on the environment, and Illumio provides an easy-to-use way to do this as part of its Illumination view.

With Illumio, you can simply switch from *Reported View* to *Draft View* to see what the effect of policy changes will be. If the effect isn't what you want, you can change your policy definitions before provisioning them. Existing configuration is not affected until you're ready to provision the changes into the live environment.

The visual display of the Illumination view makes it easy to see the effect of policy changes before they are implemented. When you make a series of changes to a complex set of rules, one of the concerns is that you might inadvertently block important traffic, or accidentally allow traffic that should be prevented.

This is very difficult with traditional ACL-based firewalls. While it is generally obvious when important traffic is suddenly blocked—thanks to all the panicked phone calls that tend to occur—it's much less obvious if unintended connections are suddenly allowed.

Individual workloads—or groups of them—can also be placed in Test mode which will report on provisioned policy violations without enforcing them. This can be a useful step for testing out policy changes, or adding in new systems, before converting workloads to fully protected *Enforced* mode.

Testing policy changes before deployment provides operators with confidence that changes have been made correctly and to see likely traffic disruptions before they occur.

05

THE FUTURE OF DATA CENTRE AND CLOUD SECURITY

The complexity of modern environments is growing and for humans to keep up we need to move to higher levels of abstraction and automation. The scope and scale of a modern microservices environment requires a fundamentally different approach than long lists of ACL rules on a bunch of independent firewalls.

However, we need to be able to transition to the new way of working without completely rebuilding from scratch. Few established organisations get the chance to build a completely new environment from the ground up, though for those that do, a flat network with Illumio providing security close to the workloads, rather than using a lot of firewall-based chokepoints, is clearly a good choice. Besides, you already have all the firewalls you need to control east-west application traffic. The host-based firewall capabilities in modern operating systems are robust and are available wherever these operating systems are deployed, be it on-site or in the cloud.

This approach can even keep unwanted traffic off the network completely, making an existing investment in other security devices last longer.

The sophistication of attackers is also increasing. Lateral movement is a common goal and attackers have a range of automated tools at their own disposal, therefore limiting our defense to traditional approaches places us at a disadvantage. Micro-segmentation helps keep the risk of lateral movement to a minimum so at least if an attacker does breach one security barrier, they are less likely to be able to get very far. Illumio can also improve situational awareness of what normal application traffic looks like so that a breach is that much more obvious.

Tools like Illumio help to ensure security policy works as intended and is correctly applied. Using APIs helps us automate systems and helps us to work at a level of abstraction that is easier to understand as humans, while we leave the tedious configuration details to computers that are, quite frankly, better at it.

Just as we mostly don't hand-tune assembly code any more, configuring line-level ACLs on firewalls seems hopelessly outdated for the vast majority of use-cases. Too much of security involves using hand tools in an age of automated factories. While it's comforting to know you can roll up your sleeves and fix things by hand if you need to, it shouldn't be what we do on a day-to-day basis.

About The Author

Justin Warren is Founder and Chief Analyst of PivotNine. He has worked with many well-known companies around the world, including ANZ, Australia Post, IBM, NetApp, Nutanix, Pure Storage, Suncorp, Telstra, and VMware as well as a variety of startups including Atomist, Datera, Elastifile, and Illumio.

Justin regularly contributes to *Forbes*, *iTnews*, and *CRN Australia*. He also hosts the popular podcast *The Eigencast*, which focuses on the business of enterprise IT.

Justin holds an MBA from Melbourne Business School, and is a graduate member of the Australian Institute of Company Directors.

About PivotNine

PivotNine Pty Ltd is a specialist IT consulting firm based in Melbourne, Australia.

PivotNine helps customers to evaluate and select technology products, and to implement effective organisational structures and processes.

PivotNine assists vendors with marketing positioning and messaging, with a focus on data driven marketing methods.

Contact

Global Headquarters
enquiries@pivotnine.com
https://pivotnine.com

Reproduction and distribution of this document in any form without prior written permission is prohibited. The information in this document is from sources believed to be reliable. PivotNine disclaims all warranties as to the accuracy, completeness, or adequacy of such information. If any legal issues are discussed in this document, let's be clear that it's not legal advice; PivotNine is not a law firm, and we make no claims that we provide anything even resembling legal advice, so if you want actual legal advice, go and hire a lawyer. PivotNine is not a financial adviser. Do not tumble dry. You should consider seeking independent legal, financial, taxation or other advice to check how information in this document relates to your unique circumstances. PivotNine shall have no liability for errors, omissions, or inadequacies in the information contained in this document. PivotNine is not liable for any loss caused, whether due to negligence or otherwise arising from the use of, or reliance on, the information provided directly or indirectly in this document. This document may, or may not, set fire to your datacentre. The opinions expressed in this document were made at a particular point in time based on information available at that time, and we reserve the right to change our minds as new information comes to hand. If you actually bothered to read this far, send us a note at ilovelegalese@pivotnine.com. PivotNine and the Circular Device are trademarks of PivotNine Pty Ltd. All other trademarks are the property of their respective owners.