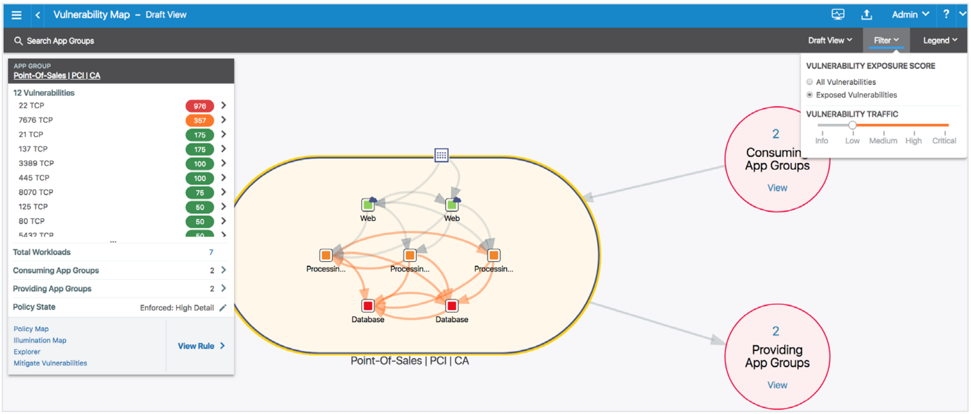
SOLUTION BRIEF

ILLUMIO ADAPTIVE SECURITY PLATFORM®: VULNERABILITY MAPS

ENABLING VULNERABILITY-BASED MICRO-SEGMENTATION

The Illumio Adaptive Security Platform (ASP) delivers micro-segmentation to prevent the spread of breaches inside data center and cloud environments and to meet regulatory compliance standards such as SWIFT, PCI, GDPR, and HITRUST. Why micro-segmentation? The perimeter doesn't stop all bad actors from getting inside data center and cloud environments. Regardless of how many detection technologies organizations use, something is bound to get through – a new virus, a phishing email, or a bad actor working at a company.

With the addition of vulnerability maps to Illumio ASP, security teams can now see exactly where their data centers and clouds are most vulnerable. Application dependency mapping and third-party vulnerability analysis deliver increased situational awareness with visibility to the potential application connections that a bad actor can leverage. This is the first time that vulnerability data has been tied to real-time application traffic.



APP GROUP
Point-Of-Sales | PCI | CA

12 Vulnerabilities

22 TCP	976
7676 TCP	357
21 TCP	175
137 TCP	175
3389 TCP	100
445 TCP	100
8070 TCP	75
125 TCP	50
80 TCP	50
5432 TCP	50

Total Workloads 7

Consuming App Groups 2

Providing App Groups 2

Policy State Enforced: High Detail

Policy Map
Illumination Map
Explorer
Mitigate Vulnerabilities

View Rule

VULNERABILITY EXPOSURE SCORE
○ All Vulnerabilities
● Exposed Vulnerabilities

VULNERABILITY TRAFFIC
Info Low Medium High Critical

Illumio ASP vulnerability map.

With Illumio ASP vulnerability maps, you can:

- Visualize a map of your applications and their associated software vulnerabilities within them.
- Compute an East-West exposure score based on the number of application workloads that can communicate with a vulnerable port.
- Classify vulnerable workloads based on the role they play in an application, the application that they are part of, their environment, and location.
- Visualize paths to high-value assets.

Organizations can use vulnerability mapping insights to prioritize patching or to create vulnerability-based micro-segmentation policies that act as compensating controls that help teams meet compliance regimens.

Vulnerability-based micro-segmentation enables you to:

- Strengthen micro-segmentation policies to reduce vulnerability exposure.
- Prioritize micro-segmentation policy based on application context.
- Stop threats from moving laterally via vulnerable workloads.

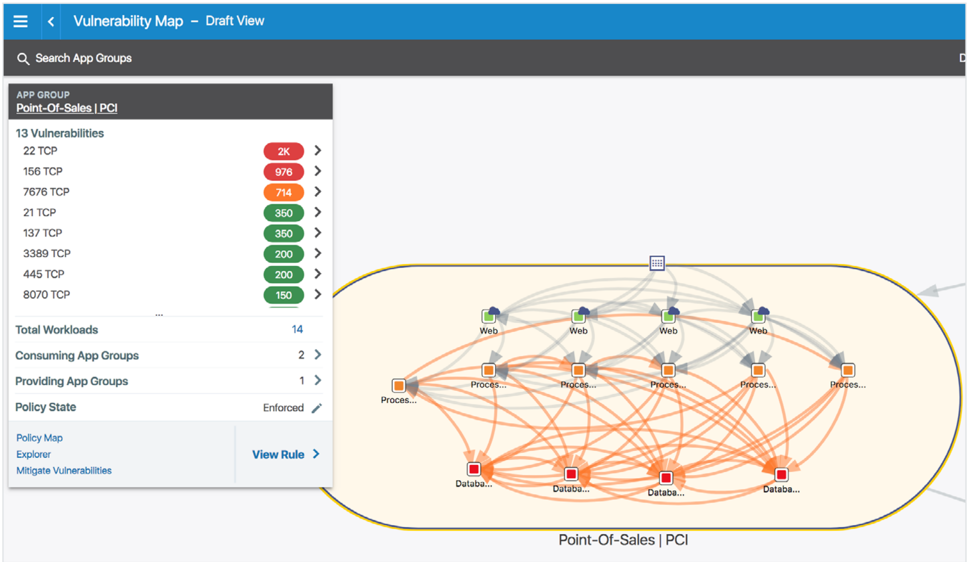
UNDERSTANDING VULNERABILITIES IN APPLICATION CONTEXT

Vulnerability maps give organizations an application-centric, dynamic view of vulnerabilities across all bare-metal, virtualized, containerized, and cloud environments. Illumio combines Illumination®, its industry-leading application dependency mapping service, with vulnerability data from leading third parties to provide real-time visualization into how vulnerable workloads are communicating with one another. With the combination of vulnerability data and application traffic in real time, vulnerability maps contextualize how vulnerabilities may be exploited by bad actors and help you prioritize your security decisions.

Visualize Vulnerabilities in Applications

Vulnerability maps provide a list of vulnerabilities in an application and the security context for those vulnerabilities. Application security context includes:

- A list of workloads on which the vulnerability is present.
- A vulnerability exposure score that is the total number of workloads that can reach a vulnerable port
- Whether the vulnerability is reachable from the Internet.



APP GROUP
Point-Of-Sales | PCI

13 Vulnerabilities

22 TCP	2K
156 TCP	976
7676 TCP	714
21 TCP	350
137 TCP	350
3389 TCP	200
445 TCP	200
8070 TCP	150

...

Total Workloads	14
Consuming App Groups	2
Providing App Groups	1
Policy State	Enforced

Application vulnerability map with list of existing vulnerabilities and dependencies.

Discover Workload Vulnerability Scores

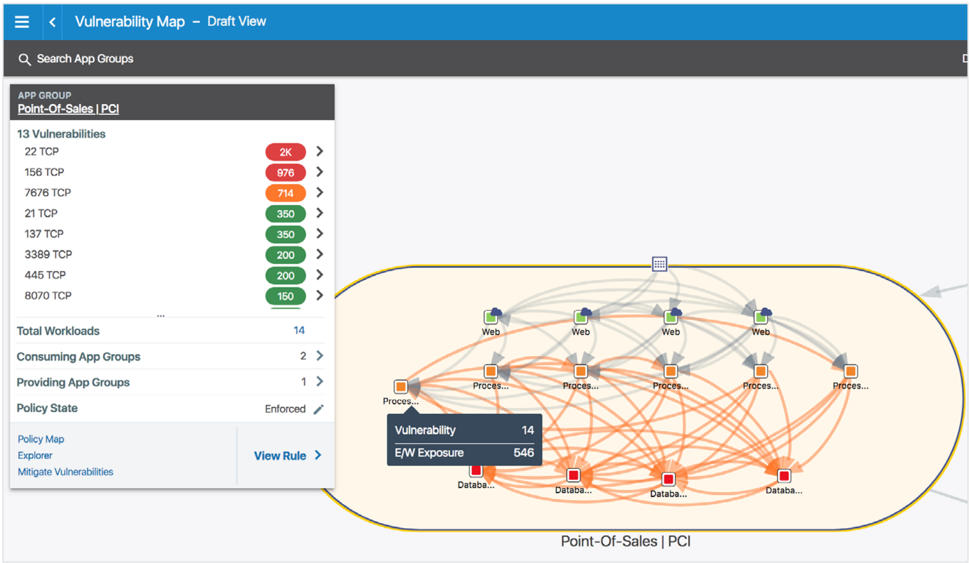
Illumination discovers and maps connectivity between workloads across all of your environments. Vulnerability maps overlay the application dependency map with a vulnerability score of the workload. The vulnerability score is the sum of Common Vulnerability Scoring System (CVSS) – scores of all vulnerabilities on the workload that are reachable from other workloads. At a workload level, vulnerability maps let you see a list of vulnerabilities on a given workload, whether there was any traffic into that vulnerability, and the details of the vulnerability such as name and CVSS score.

Gain Visibility with an East-West Exposure Score

An East-West exposure score offers a unique approach to measure the level of risk in your applications. It is a patent-pending measurement that combines the criticality of vulnerability with the exposure to other hosts in your environment. It is calculated by an algorithm that includes the:

- Severity of the vulnerability.
- Number of workloads that can connect to a vulnerable port.
- Vulnerabilities on connecting workloads (upstream risk).
- Potential paths through which bad actors can reach the vulnerability.

It also accounts for other data including application values.



APP GROUP
Point-Of-Sales | PCI

13 Vulnerabilities

22 TCP	2K
156 TCP	976
7676 TCP	714
21 TCP	350
137 TCP	350
3389 TCP	200
445 TCP	200
8070 TCP	150

Total Workloads	14
Consuming App Groups	2
Providing App Groups	1
Policy State	Enforced

Vulnerability	14
E/W Exposure	546

Workload vulnerability score and East-West exposure score.

VULNERABILITY-BASED MICRO-SEGMENTATION: MODELING AND MITIGATING THE IMPACT OF THREATS

Vulnerability-based micro-segmentation builds upon the application security context provided by vulnerability maps. It combines traffic visibility with vulnerability information, and computes optimal micro-segmentation policy to reduce the exposure of those vulnerabilities.

Model Optimal Security Policy: Policy Generator

Illumio ASP shows how vulnerable a host is through the exposure score. This helps your security teams in prioritizing patching to address those vulnerabilities. In many cases, a security team does not have the ability to patch without application teams agreeing to the upgrade/patch. In other cases, there is a hesitancy to patch during a production freeze – or when there is no patch available for a zero-day vulnerability.

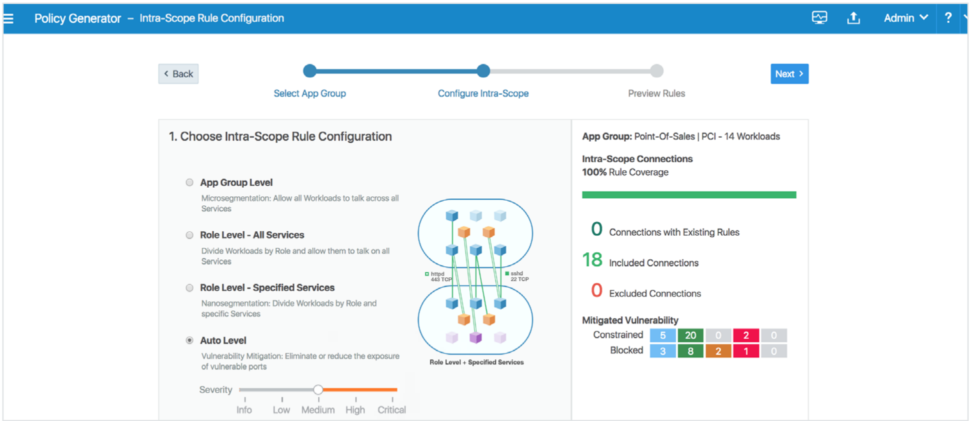
Policy Generator leverages vulnerability data and traffic visibility to generate micro-segmentation policy recommendations that reduce or eliminate the exposure of vulnerable ports and thereby prevent bad actors from exploiting them. Using Policy Generator, you can model micro-segmentation policies by optimizing around vulnerability scores provided by an organization's vulnerability management software such as Qualys.

For instance, you can choose the most granular form of segmentation for your "high" and "critical" vulnerabilities. In turn, this will create highly granular rules around those vulnerabilities and create more coarse rules for vulnerabilities that are lower in criticality. This creates micro-segmentation policies that are compensating controls for those vulnerabilities and that satisfy compliance requirements.

Micro-segmentation can be a quick win against bad actors trying to exploit vulnerabilities. For each suggested micro-segmentation policy, Policy Generator indicates:

- Before and after lists of exposed vulnerabilities.
- The number of workloads that can still reach that vulnerability.
- The East-West exposure score.

Even if you do not want to fully enforce a vulnerability-based micro-segmentation policy, you can test it and receive an alert when a policy is violated. This ensures that you do not break your applications and alerts you if a new traffic pattern emerges – a possible indicator of a breach in progress.



1. Choose Intra-Scope Rule Configuration

○ App Group Level
Microsegmentation: Allow all Workloads to talk across all Services

○ Role Level - All Services
Divide Workloads by Role and allow them to talk on all Services

○ Role Level - Specified Services
Nanosegmentation: Divide Workloads by Role and specific Services

● Auto Level
Vulnerability Mitigation: Eliminate or reduce the exposure of vulnerable ports

Severity: Info, Low, Medium, High, Critical

App Group: Point-Of-Sales | PCI - 14 Workloads

Intra-Scope Connections
100% Rule Coverage

0 Connections with Existing Rules
18 Included Connections
0 Excluded Connections

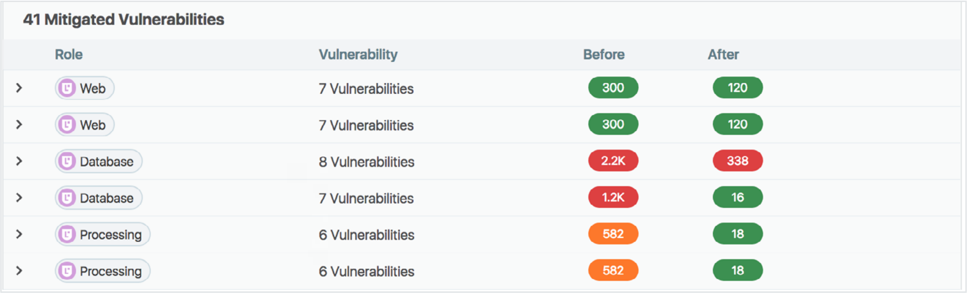
Mitigated Vulnerability

Constrained	5	20	0	2	0
Blocked	3	8	2	1	0

Automated vulnerability-based micro-segmentation policy recommendations.

Mitigate Threat Impact

Vulnerability-based micro-segmentation enables you to write label-based, dynamic micro-segmentation policy for each application to eliminate or constrain the exposure of ports with vulnerabilities. As new workloads come up in your environment or migrate from one location to another location or cloud, the workloads are programmed with security policy minimizing the exposure of vulnerable ports – and outbound policies that restrict their ability to connect to vulnerabilities on downstream workloads/applications. As vulnerabilities are patched on an ongoing basis, Policy Generator can be run again to consider new traffic flows and the latest vulnerability data to adjust micro-segmentation policies for maximum effect.



41 Mitigated Vulnerabilities

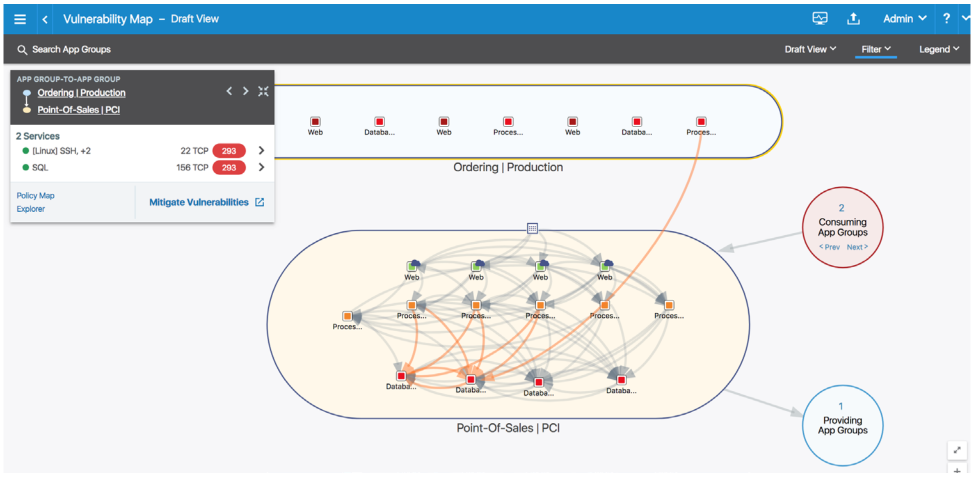
	Role	Vulnerability	Before	After
>	Web	7 Vulnerabilities	300	120
>	Web	7 Vulnerabilities	300	120
>	Database	8 Vulnerabilities	2.2K	338
>	Database	7 Vulnerabilities	1.2K	16
>	Processing	6 Vulnerabilities	582	18
>	Processing	6 Vulnerabilities	582	18

Before and after vulnerabilities mitigation using micro-segmentation.

AN INTEGRATED APPROACH TO SECURITY

Detect Vulnerability Exposure in Context of an Application

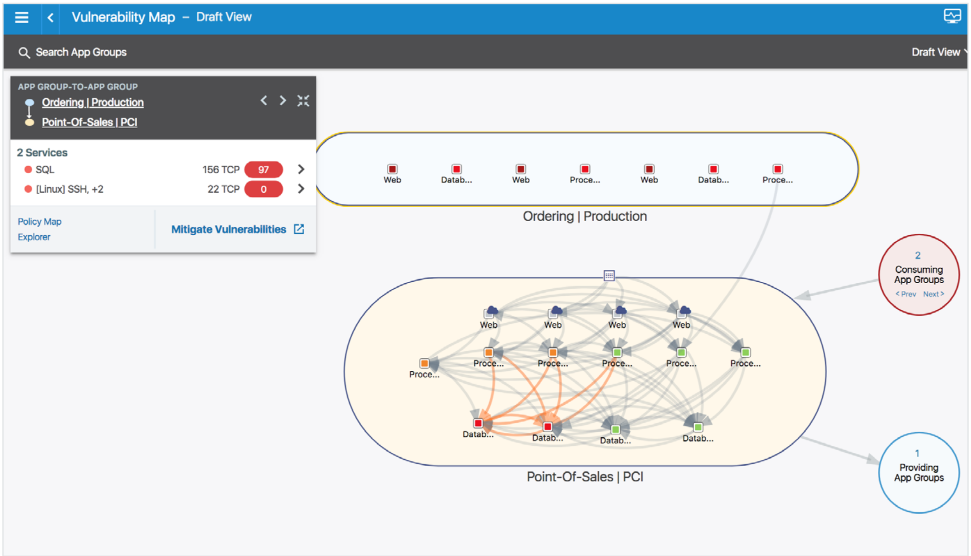
Vulnerability maps show real-time connectivity between workloads that can be compromised and provide an East-West exposure score that indicates the level of exposure of vulnerable ports on hosts to other workloads in your computing environment. You can use this information to prioritize patching and produce reports of unpatched workloads by application, environment, location, and even workload role.



Vulnerability exposure in the context of applications.

Deploy Micro-Segmentation Policy to Mitigate Threat Impact

Not all detected vulnerabilities can be addressed by patching. In many cases, there may be a production freeze, no available patch, or the application team is unwilling to patch and they sign off on the risk. Policy Generator combines traffic visibility and third-party vulnerability analysis with label-based dynamic micro-segmentation policies that can be used as compensating controls for unpatched workloads. Using Policy Generator, you can model the effects of suggested policy, examine the details of constrained and eliminated vulnerabilities, and deploy dynamic label-based micro-segmentation policies.



APP GROUP-TO-APP GROUP
Ordering | Production
Point-Of-Sales | PCI

2 Services

● SQL	156 TCP	97
● [Linux] SSH, +2	22 TCP	0

Vulnerability-based micro-segmentation to mitigate threat impact.

ABOUT ILLUMIO

Illumio, the leader in micro-segmentation, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use Illumio to reduce cyber risk and achieve regulatory compliance. The Illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with micro-segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information about Illumio, visit www.illumio.com/what-we-do or follow @Illumio.

- Engage with Illumio on Twitter
- Follow Illumio on LinkedIn
- Like Illumio on Facebook
- Subscribe to the Illumio YouTube Channel

CONTACT US

For more information about Illumio ASP and how it can be used to achieve visibility behind the firewall, email us at illuminate@illumio.com or call 855-426-3983 to speak to an Illumio representative.

Illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com