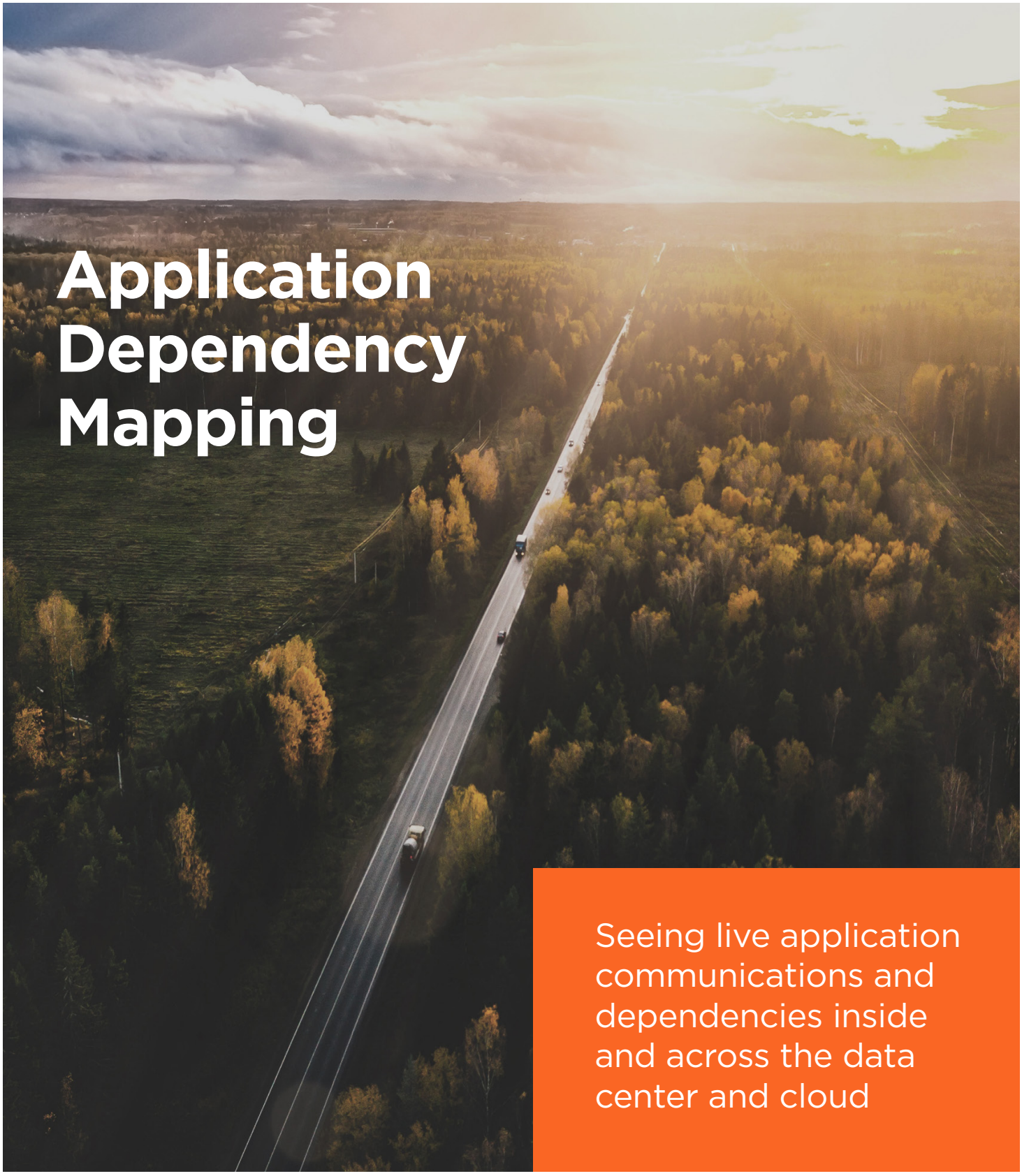
illumio

WHITE PAPER



Application Dependency Mapping

Seeing live application communications and dependencies inside and across the data center and cloud

Overview

Application context includes visibility into application components and relationships between those components within your data center and cloud environments. This is required to help you plan and implement your micro-segmentation strategy and protect your key business assets from threats like breaches and misuse.

Contents

This paper will help you understand:

How application dependency mapping is different 03

Why visualizing the application dependency map is critical 03

How application dependency mapping works 05

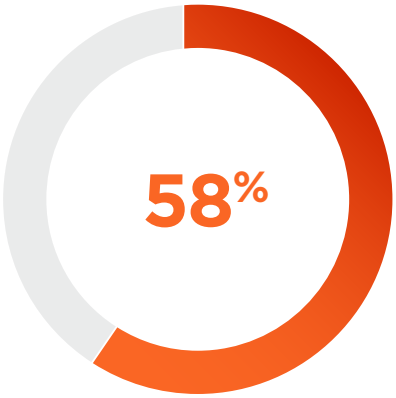
Benefiting from application dependency mapping 10

How to get started 14

illumio

How Application Dependency Mapping Is Different

Traditional network-based security tools to protect your dynamically changing application environment are too static and fail to give you the full picture in terms of context and application dependencies. Network-based visibility tools provide a map in terms of IP addresses, VLANs, and zones, but do not help to understand business application context. Visualizing web and database servers communicating with each other using MySQL inside a CRM application is more powerful than having the network path visibility in terms of IP addresses. With powerful insights into application topology, you can get an idea of how your business applications are interlinked — without worrying about underlying network infrastructure.



58% have no visibility into their East-West traffic in their data center or cloud environment

Why Visualizing the Application Dependency Map Is Critical

Modern data center technologies like software-defined networking (SDN), virtualization, and containerization techniques layered with automation and orchestration platforms have facilitated faster and more agile application development. On the other hand, it has become exponentially more difficult for your operations and security teams to keep track of your dynamic application environment and the existing security blind spots.

To understand and eliminate the security blind spots in your application environment, the first step is to visualize all your application components and how they are interconnected. Once you understand what your applications are, where are they hosted, and how they are interacting with each other, you can start to take control of your business assets and define your security posture.

Better understand your business risk

In a survey conducted about the state of dynamic data center and cloud security for modern enterprise, 58 percent of respondents say they have no visibility into their East-West traffic in their data center or cloud environments and 25 percent of respondents do not know whether they have experienced attacks1. Dynamic and heterogeneous infrastructure results in poor

With powerful insights into application topology, you can get an idea of how your business applications are interlinked.

visibility into your lateral application traffic and allows bad actors to take advantage. They are able to breach your environment and stay undetected for an extended period of time while stealing business critical data.

With end-to-end visualization of all active traffic flows and all open ports and processes between the application components in your application environment, you can understand your attack surface, including:

- Critical business assets that need to be protected databases with sensitive customer information, your PCI or HIPAA-regulated servers, financial and payroll application servers, etc.
- Vulnerable and potential pathways that are available for intruders to attack
- Unexpected connections and unauthorized activity

Improve your security policy creation

The best way to effectively plan your security policies and guarantee application availability is to first understand your key assets and how they connect. Even with your security policies in place, without live visualization of your application environment, it is hard to predict the effectiveness of your policies.

With application dependency mapping, you can understand how all the applications are connected and develop your security posture by:

- Planning your segmentation strategy and creating effective security policies
- Modeling and testing your security policies with visual feedback for impact analysis
- Avoiding any mistakes due to policy misconfigurations that can compromise application availability and security

Meet your business compliance requirements

Live application dependency mapping has to be in real time and constantly monitored for all application traffic within your regulated environments like PCI, HIPAA, SOX, etc. Using this live visualization, you can:

- Have visual confirmation to ensure requirements are met across all compliance environments
- Pinpoint any violations to focus efforts for quick resolution
- Perform an easy audit of effectiveness of security policies

25%

do not know whether they have experienced attacks

[1] https://www.sans.org/reading-room/whitepapers/analyst/state-dynamic-data-center-cloudsecurity-modern-enterprise-36312

How Application Dependency Mapping Works

Understand your application environment

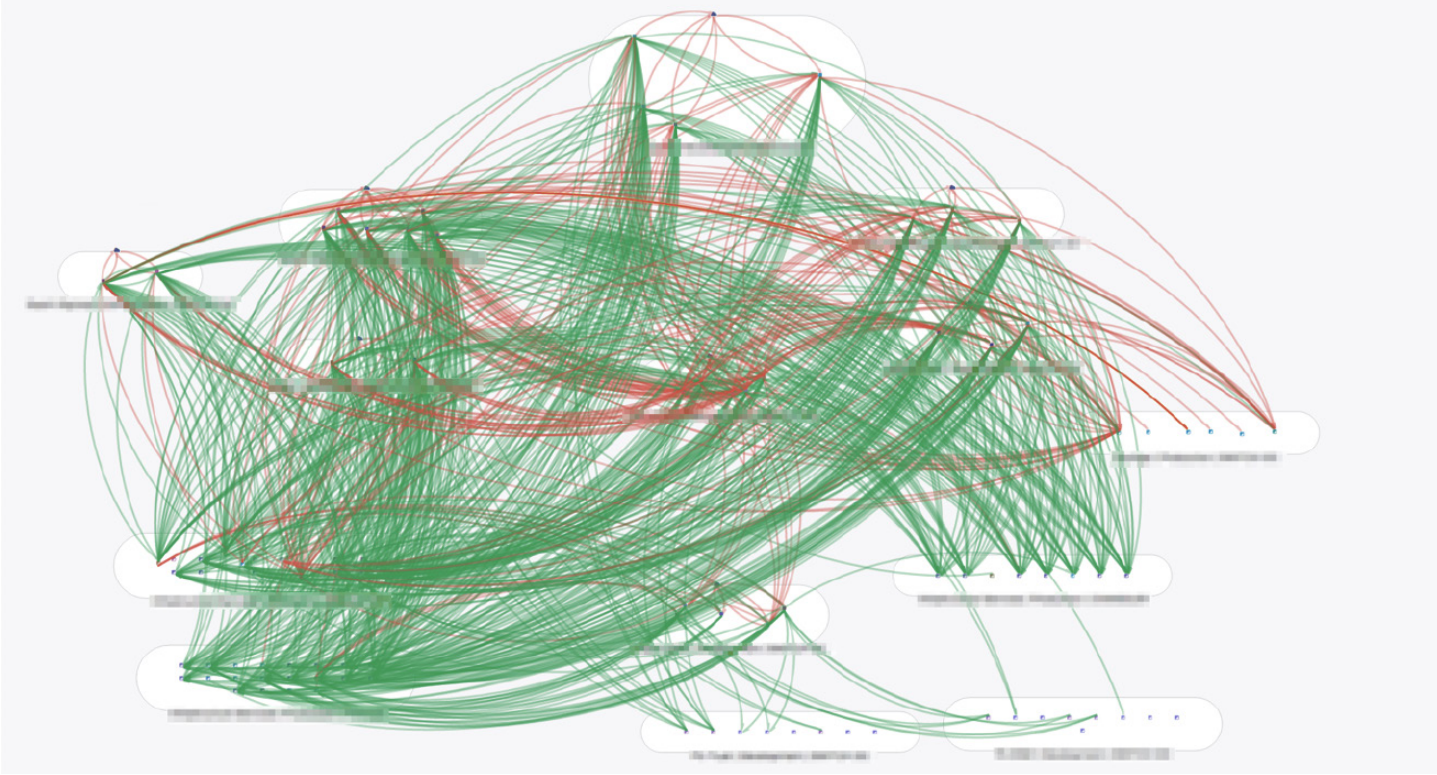
The first step to building an application dependency map is to identify existing workloads in your data center and cloud environment and map the interconnected applications, which includes:

- Workloads that are communicating with each other
- Ports being used by workloads for communication
- Processes that are running on the workloads

For example, if your web server is talking to a database server in your application, you can tell what ports and processes are being used to establish a connection between those servers.

Once you have all your workloads in your environment showing upwith all their interdependencies, the next step is to group them for easy understanding.

VISUALIZE APPLICATION COMMUNICATION



Organize your application environment

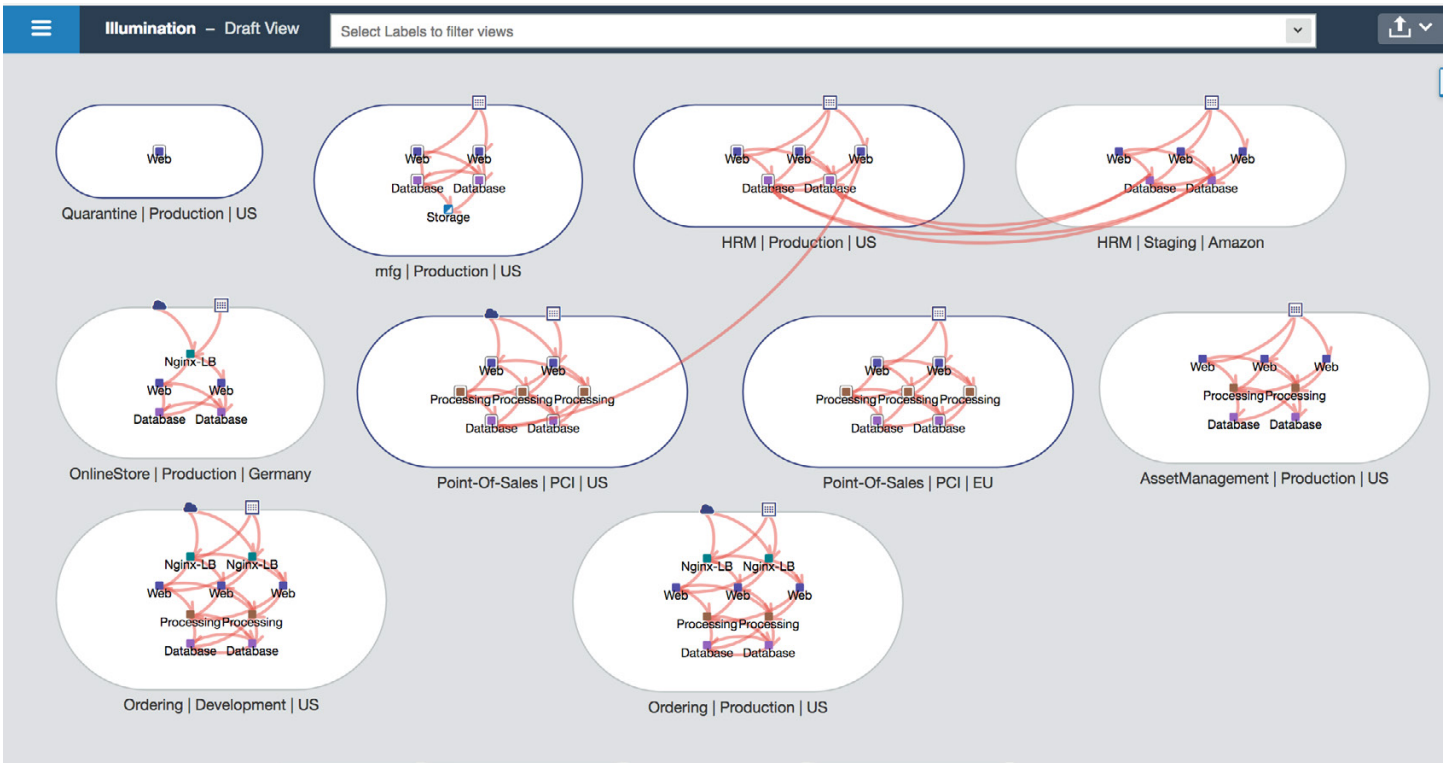
Once you have the map of all application dependencies, you can start adding labels to identify the workloads and group them in terms of common metadata like which application they belong to, the location (data center, cloud, geographical zones, etc.) and environment (development, production, staging, etc.) they are hosted in, and their role (web, database, processing, etc.).

All the context and telemetry, like which IP addresses, ports, protocols, processes, and services are used by workloads to communicate with each each other, are shown in a relational graph.

The whole map is developed without relying on underlying network infrastructure and does not show any networking equipment in the application traffic paths.

Now you have a complete map with all applications and their dependencies in real time and the next step is to start defining your security posture.

LABEL AND GROUP APPLICATION WORKLOADS



Secure your application environment

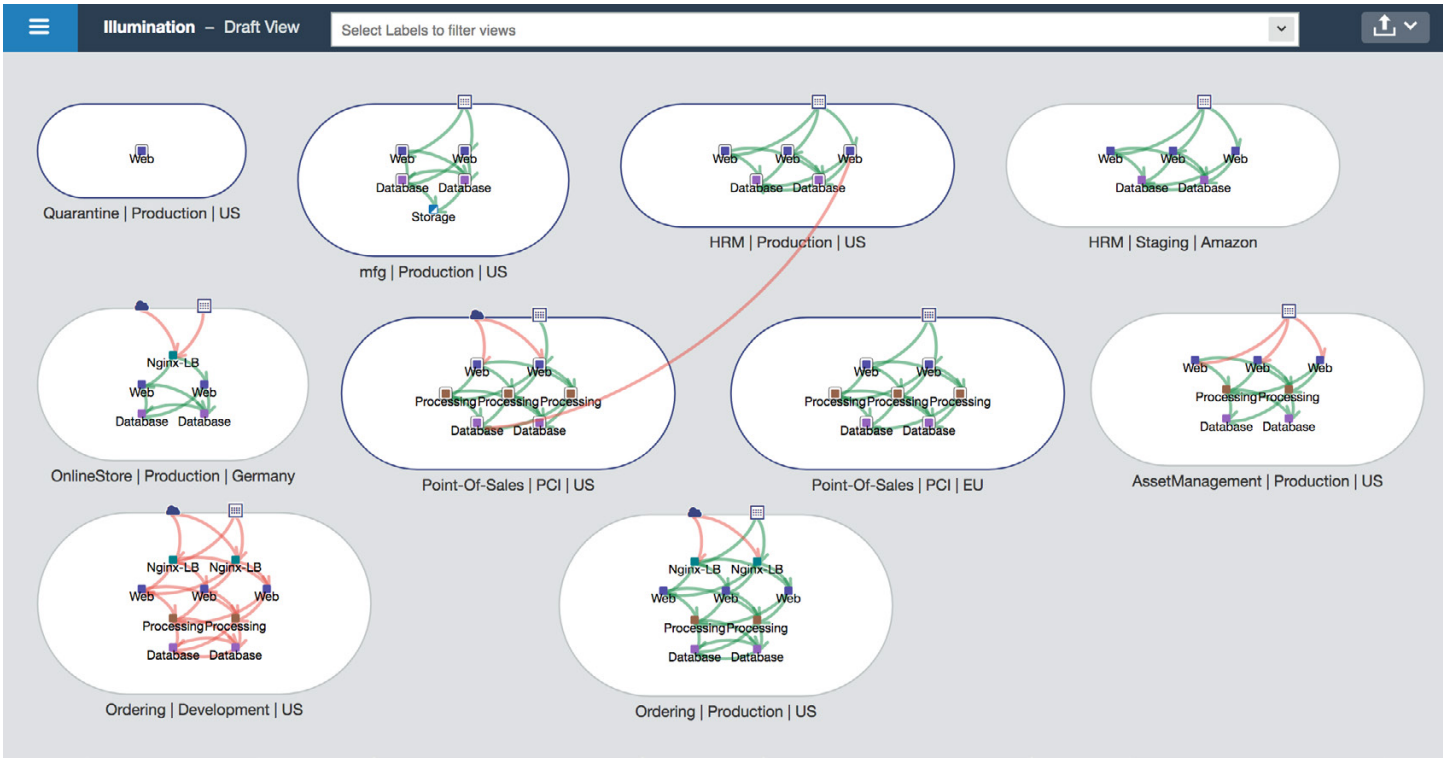
Lack of consistent segmentation strategies across on-premise data centers and private, public, or hybrid cloud environments enables intruders to pass perimeter protections, breach, and remain undetected for an average of three to six months before being discovered[2]. The longer it takes to detect and contain a data breach, the bigger the impact and the more expensive it is to resolve – this could range anywhere between $5-8 million[3].

Application dependency mapping gives you insight into all the attack vectors that an attacker can use and helps visualize all the open pathways they can use to breach your critical business assets.

Once you have insights into your application dependencies within your data center and cloud, you can now start instrumenting security policies to defend your application topology and test those policies to make sure the attack surface exposure is minimized. You can develop your quarantine strategy to take fast action to remediate in case of any breaches.

With your security strategy in place, the next step is to ensure that your security policies adapt to any workload or application architecture changes.

SECURE APPLICATION WORKLOADS



[2] Reference: Ponemon Institute's 2016 Cost of Data Breaches study
[3] Reference: Ponemon Institute's 2016 Cost of Data Breaches study

illumio

Adapt to changes in your application environment

Static data centers are a thing of the past. With the advent of cloudcomputing coupled with virtualization and automation, modern data centers have become highly dynamic with a heterogeneous mix of baremetal and virtual servers across on premise data centers and clouds.

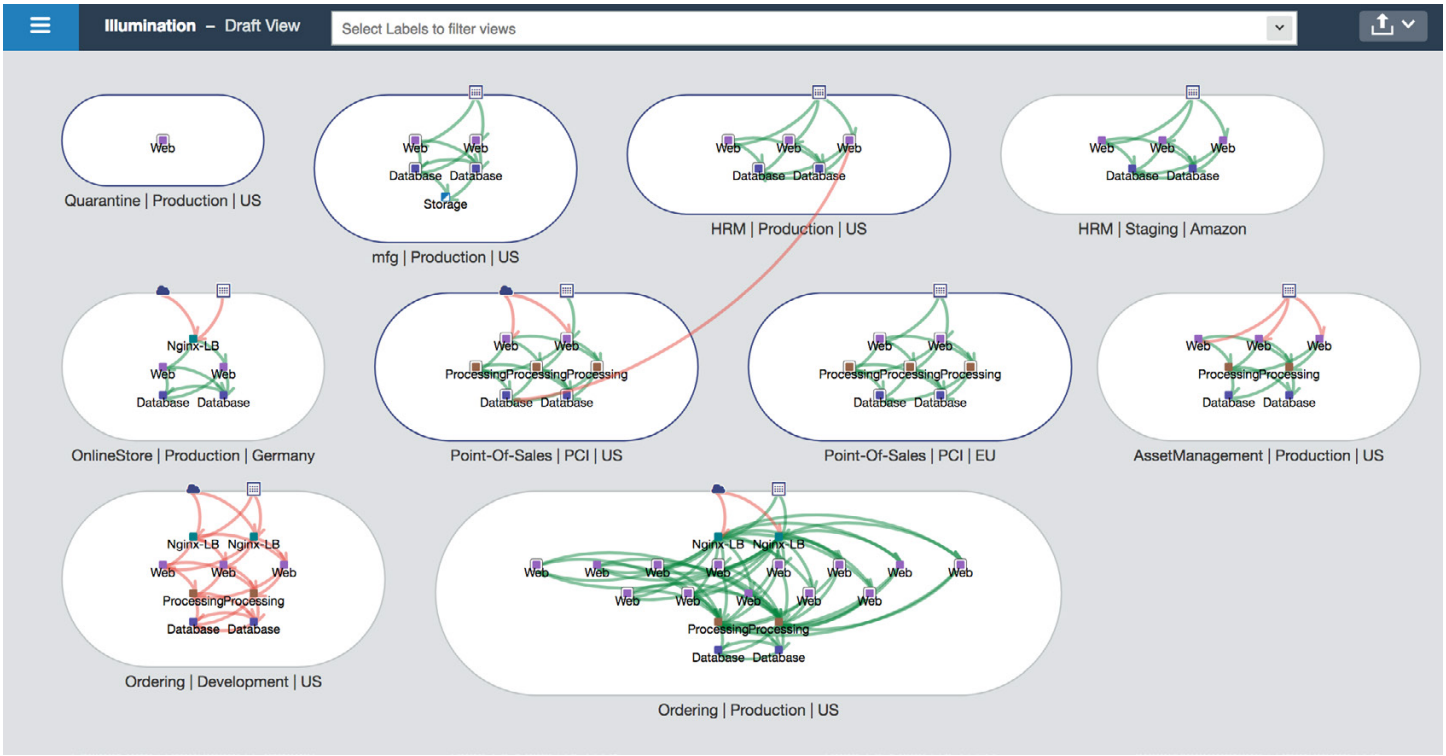
With real-time visibility into your application dependencies, all the blind spots created due to heterogeneity in the application infrastructure are eliminated.

Your security policies must move at the same pace as application infrastructure changes for your applications to be scalable, highly elastic, and agile to meet customer demands.

Real-time application dependency mapping helps with:

- Expanding to new geographies and new data centers
- M&A activities leading to data center consolidation
- Commissioning and decommissioning servers

ADAPT TO CHANGES IN APPLICATION WORKLOADS



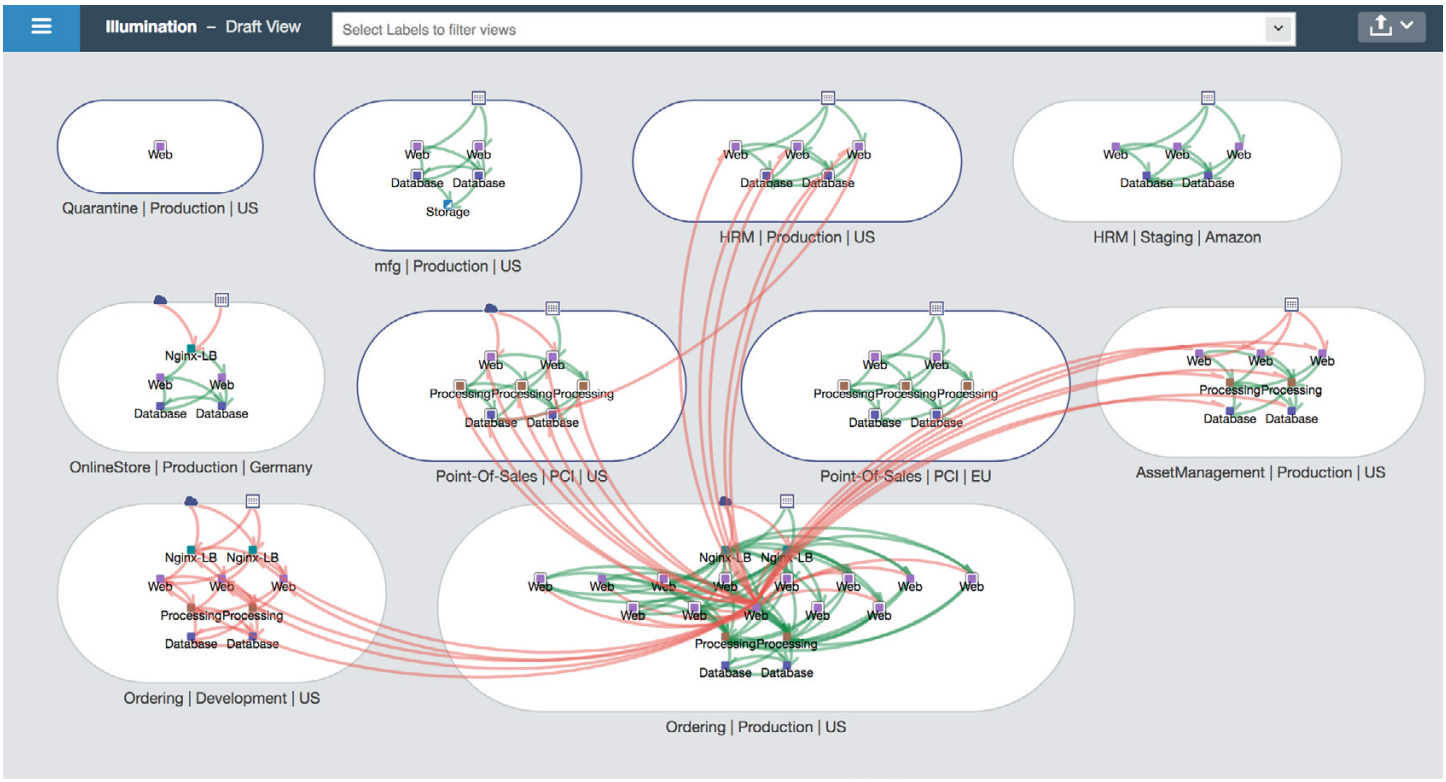
Identify non-conforming behavior in your applications

Knowing what applications exist in your environment and how they are interlinked can help you derive some baselining of your normal application environment. Once you understand what "normal" operation looks like, you can start to monitor and detect for non-conformance or unauthorized activity that could be dangerous or could potentially suggest a compromise of your critical business assets.

You could notice some traffic flows between two servers that are not authorized to talk to each other; for example, a development environment server talking to a production environment server over SSH. With this insight, you can take remedial action to block this flow and make adjustments to harden the defenses of your environment.

Once you understand what "normal" operation looks like, you can start to monitor and detect for non-conformance or unauthorized activity that could be dangerous.

IDENTIFY BREACHES AND ROGUE BEHAVIORS

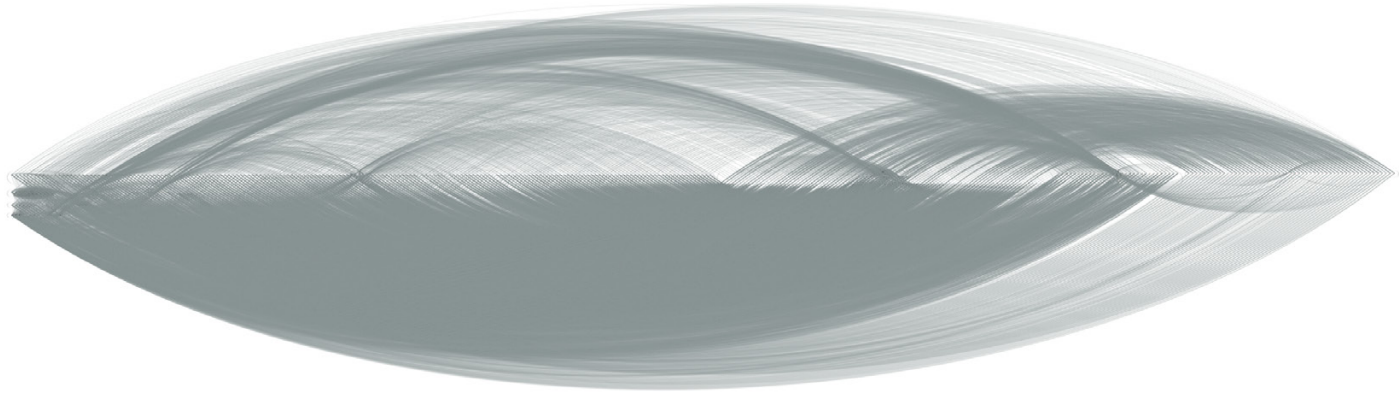


Benefiting from Application Dependency Mapping

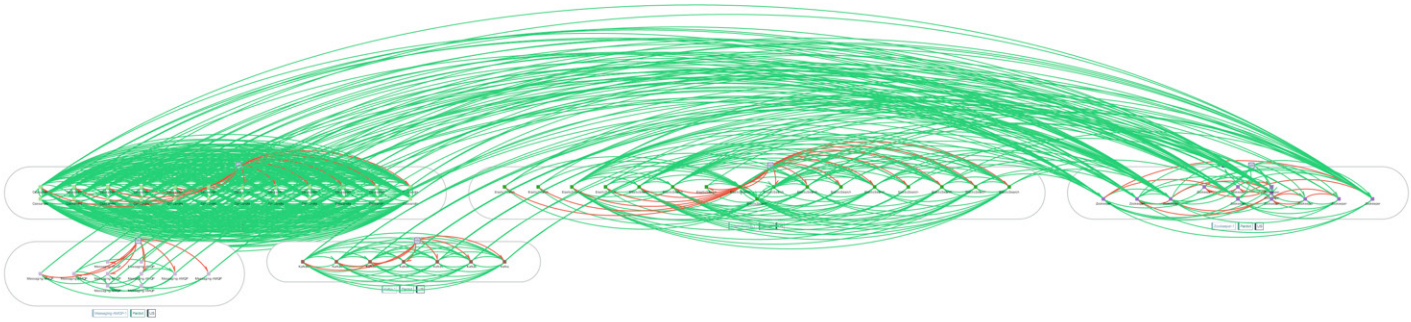
Reveal your applications

Take control of your infrastructure with real-time visibility. Reveal all the application dependencies that help you identify the interactions between components, services, ports, and processes in your data center and cloud environments, and understand your application topology.

VIEW CONNECTED APPLICATIONS IN A DATA CENTER



UNDERSTAND APPPLICATIONS AND DEPENDENCIES



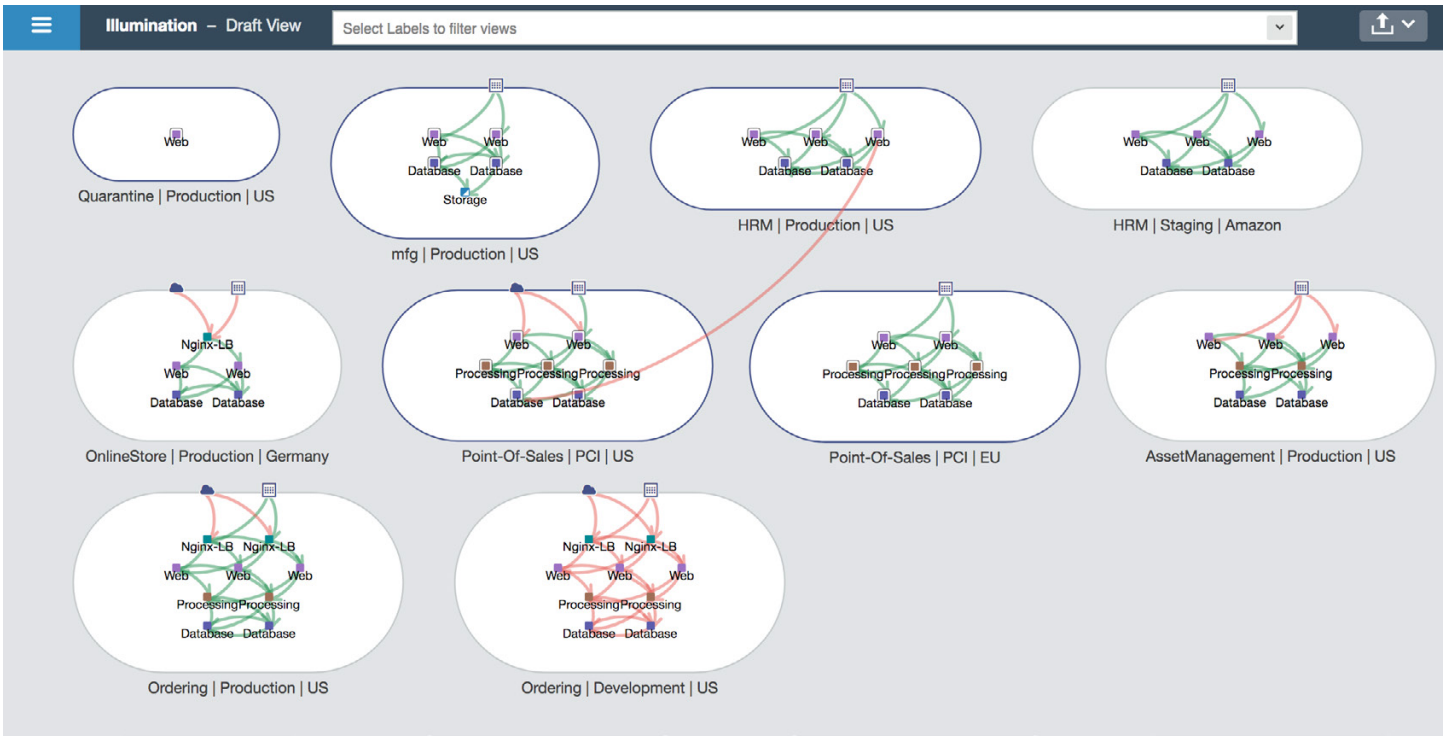
Plan your segmentation strategy

Once you understand the application topology that you are protecting, you can identify your high-value critical assets and plan your security strategy to defend them. You have a map of attack vectors that the intruders can use to breach your infrastructure, which you can use to plan your segmentation strategy. Refer to "How to Build a Micro-Segmentation Strategy" for security strategy ideas.

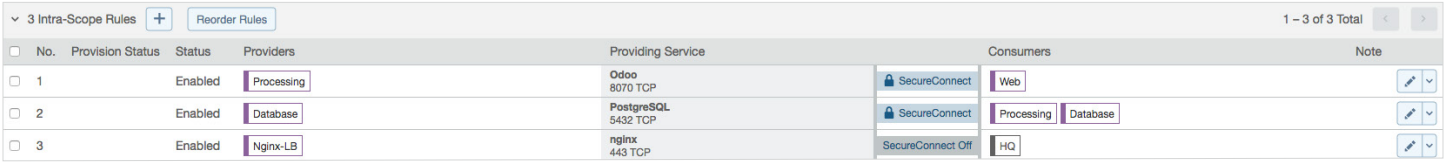
Test and fine-tune your security policies

With your segmentation strategy in place, you can build security policies to protect your assets. With the aid of real-time application dependency mapping, take the time to test and fine-tune your security policies and protect your active environment from any misconfigurations that could compromise availability and security.

VIEW CONNECTED APPLICATIONS IN A DATA CENTER



CREATE AND TEST SECURITY POLICIES



illumio

Enforce your security policies

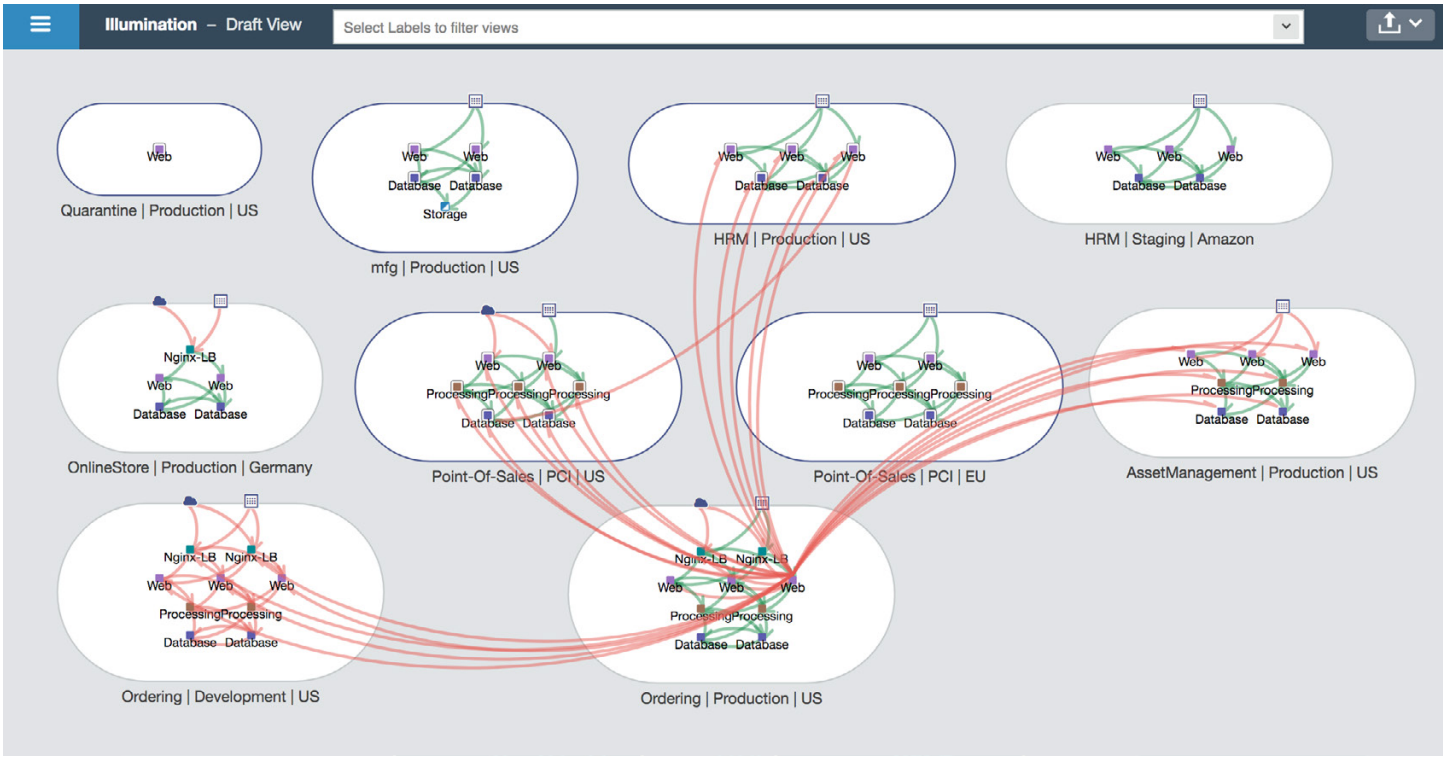
Once you have a baseline of your application traffic and security policies in place for all the possible attack vectors, put your segmentation strategy into enforcement. You are now ready to make application dependency mapping work for you.

Identify cyber attacks

Once the attackers breach your perimeter, they can move unimpeded laterally in your data center and wreak havoc on your infrastructure. Having visibility helps you to quickly pinpoint anomalous behavior and isolate compromised assets that are behaving out of profile. Once quarantined, your security team can investigate them for forensics and perform remediation.

Having visibility helps you to quickly pinpoint anomalous behavior and isolate compromised assets that are behaving out of profile.

IDENTIFY THREATS AND QUARANTINE ROGUE WORKLOADS

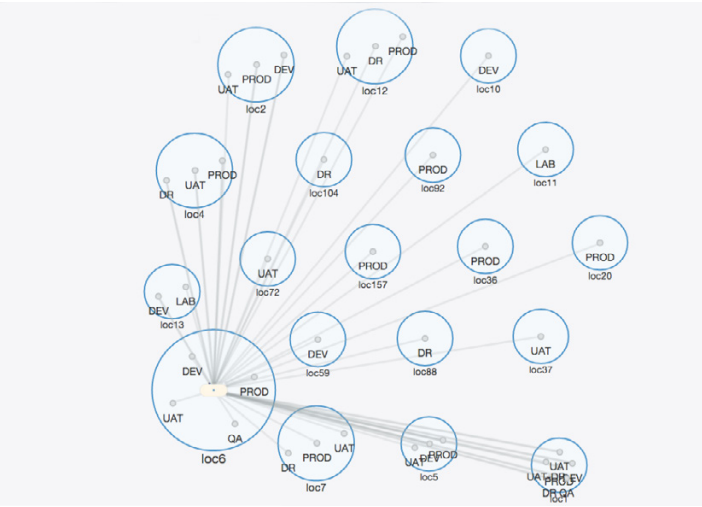


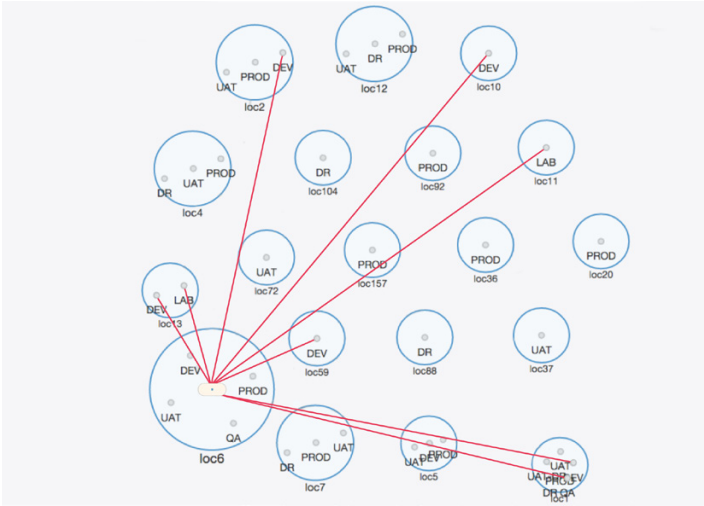
Isolate development and production environments

Separating your business-critical application environment into development, testing, staging, and production and ensuring that these environments are segregated from each other can be difficult given that these environments and applications can be dynamic and span multiple environments or data centers. Having connections like SSH open between development and production environments can potentially compromise your application by providing an open path for hackers to breach and bring down your infrastructure.

With real-time visibility into compliance environments, you have knowledge of the context of the workload.

PINPOINT DEVELOPMENT AND PRODUCTION COMMUNICATION VIOLATIONS



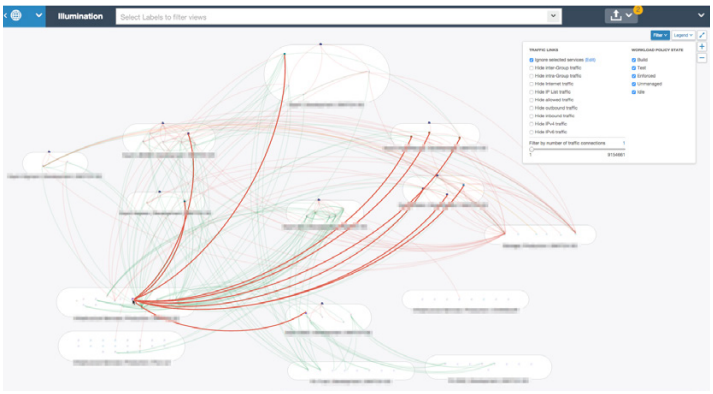


illumio

Reveal PCI compliance violations

With real-time visibility into compliance environments, you have knowledge of the context of the workload. Information about what the workloads are talking to and on what ports and processes can help isolate traffic flows occurring between compliant and non-compliant workloads. With situational awareness, you can take actions to enforce security policies to block these traffic flows.

REVEAL COMPLIANCE VIOLATIONS



How to Get Started

Planning your security strategy to protect critical assets starts with visualization of your application dependencies. Get a visual application dependency map of all your business assets, identify your most valuable assets, develop security policies to proactively defend them, and identify compromised assets for quick remediation. Visualizing and taking control of your environment helps you get ahead as a defender.

Illumio Core™ can help you achieve visibility into all your application dependencies in your data center. Illumination, the visibility component of Illumio Core, provides a real-time interactive application dependency map of all your lateral traffic across your onpremise data centers and private, public, or hybrid cloud environments. This relationship graph will help you take the next steps required to secure your environment and limit your attack surface, protecting your assets from threats and breaches.

If you'd like to get started, go to www.illumio.com for more information or contact us for a live product demo.

Application dependency mapping checklist

- ☑ Identify your key assets that could be potential targets
- ☑ Understand how your assets are interlinked – what are the ports and processes they are using to talk to each other
- ☑ Plan and test security polices required to protect your infrastructure
- ☑ Model and test to understand the effectiveness of your security policies
- ☑ Baseline your normal infrastructure traffic and identify aberrant and nonconforming traffic behavior

illumio

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.