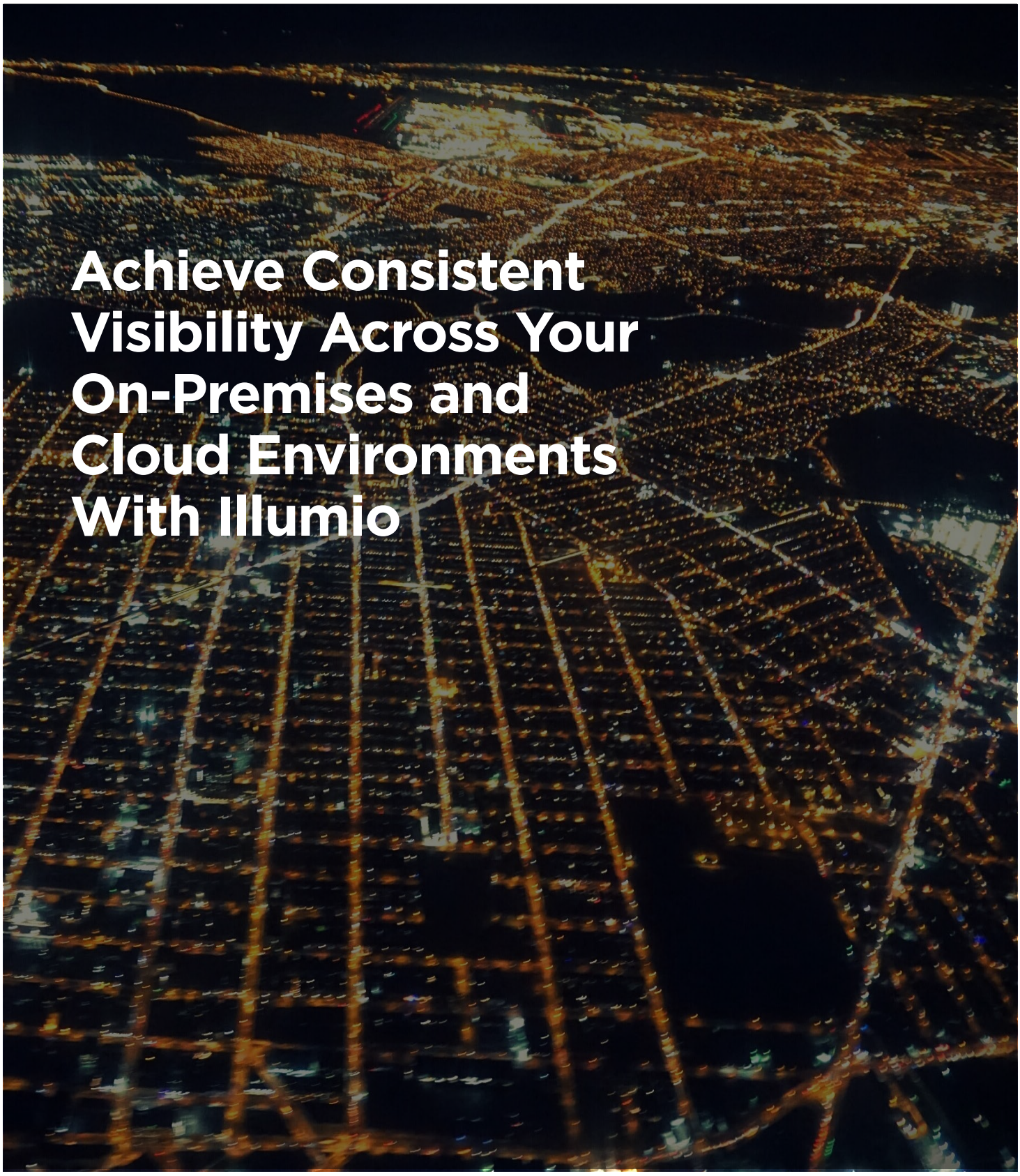
illumio

WHITE PAPER



Achieve Consistent Visibility Across Your On-Premises and Cloud Environments With Illumio

Managing Your Multi-Cloud Architecture

Today's enterprise IT resources extend beyond the four walls of locally managed, traditional data centers to a wide range of public cloud services. Organizations are increasingly moving to hybrid multi-cloud architectures consisting of on-premises data center and cloud-managed fabrics, which enable an elastic deployment of compute, storage, and network resources across any of these fabrics. This allows deployment and associated operational expenses to expand and contract along with fluctuating business requirements. You should not have to pay for a resource when it is idle.

While there are many advantages of migrating to the public cloud, several challenges are associated with this effort, including maintaining consistent visibility and segmentation. Elastic services deployed on an as-needed basis across multiple cloud fabrics benefit the enterprise business model. Still, application-centric visibility remains a challenge — perhaps greater than when all resources are deployed entirely within an on-premises data center.

Visibility Challenges in Public Cloud

The public cloud is designed to abstract away customer visibility from the underlying hosting resources and network fabric. Resources are viewed and accessed in public cloud at Layer 3 and above, with no access to any of the lower networking layers directly managed in an on-premises data center. This means that traditional network-centric methods for gaining visibility into application behavior and associated traffic flows are not possible in the public cloud.

In a multi-cloud architecture, a fragmented approach to application visibility is common. For example, if you deploy several software-defined networking (SDN) solutions in an on-premises data center, they will provide some level of visibility into that environment's application and network behavior. But suppose you add several public cloud vendors to that architecture. In that case, you either have to push those on-premises SDN solutions out to the public cloud fabrics to get application visibility or use the proprietary tools offered by each public cloud vendor, resulting in visibility silos in each environment and a lack of correlation between them.

Application-centric visibility into traffic flows and dependencies requires a centralized solution that you can deploy across on-premises and public clouds without dependence on the underlying resources or fabric in each environment to enable that visibility. The goal is to learn how applications are connected. As your enterprise architecture scales, visibility should not be hindered by the limitations of the tools in one of the underlying fabrics.

So, the question is: How can you enable application-centric visibility across any data center and public cloud in a way that is 100 percent agnostic to the underlying fabric hosting your application workloads?

Cloud-Provided Tools vs. Third-Party Tools

All of the major public cloud providers offer specific, local security tools with various levels of policy control. If you implement a multi-cloud architecture that includes more than one public cloud provider and one or more on-premises data centers, then apply a segmentation architecture, you will have a siloed operational model across each hosting environment. Each environment's tools will live on a "segmentation island," distinct from all the others.

The segmentation tools in 'cloud provider A' generally do not integrate with the segmentation tools from 'cloud provider B.' And the segmentation tools included with SDN solutions for on-premises data centers are also local to those specific SDN vendors, not integrated with the public cloud provider segmentation tools.

In case of a security breach, you must correlate events and audit workloads across the entire architecture to block and isolate the threat. Without a centralized segmentation tool for controlling, defining, or quarantining compromised workloads quickly across the entire architecture, you will need to secure and troubleshoot each environment separately. These operational silos will only slow down effective threat remediation across the overall fabric and create bottlenecks to scale and audit an evolving segmentation architecture.

The resulting operational model will rely on a "swivel-chair" management approach. The Security Operations (SecOps) team swivels between the segmentation tools in all of the individual environments, attempting

to correlate and remediate a security threat using a collection of tools never designed to work together. The lack of centralized visibility can lead to long delays in SecOps threat remediation and a fragmented workload audit trail across the entire fabric.

Illumio: Consistent Application Visibility Across On-Premises and Public Cloud

While visibility and segmentation capabilities are available in cloud provider tools, SDN controllers, and traditional firewalls, these tools are designed to address networking-centric challenges (e.g., segmentation and visibility along network boundaries) and networking priorities (e.g., preventing distributed denial of service [DDoS] and address resolution protocol [ARP] spoofing attacks). They are not designed to prevent workload-specific threats like ransomware across 10,000 individual workloads.

To protect cloud workloads, you must implement visibility and segmentation directly at the workload level. Illumio Core does just that. It enables application-centric visibility directly at the workload level, independent of how you deploy underlying networking resources, across on-premises environments, public clouds and hybrid clouds. This frees SecOps teams from relying on network operations teams to provide visibility into application behavior.

Deployed as an agent anywhere that workload is hosted in the operating system's user space and residing entirely in the management plane, Illumio does not modify the kernel in any way, thus not incurring any throughput concerns in the data plane. This allows you to harvest application and traffic flow information without impacting resources or performance, and then create an application dependency map of all workloads across data centers, private clouds, public clouds and hybrid clouds. The result is centralized visibility and auditing capabilities across all hosting environments (Figure 1).

APPLICATION DEPENDENCY MAP

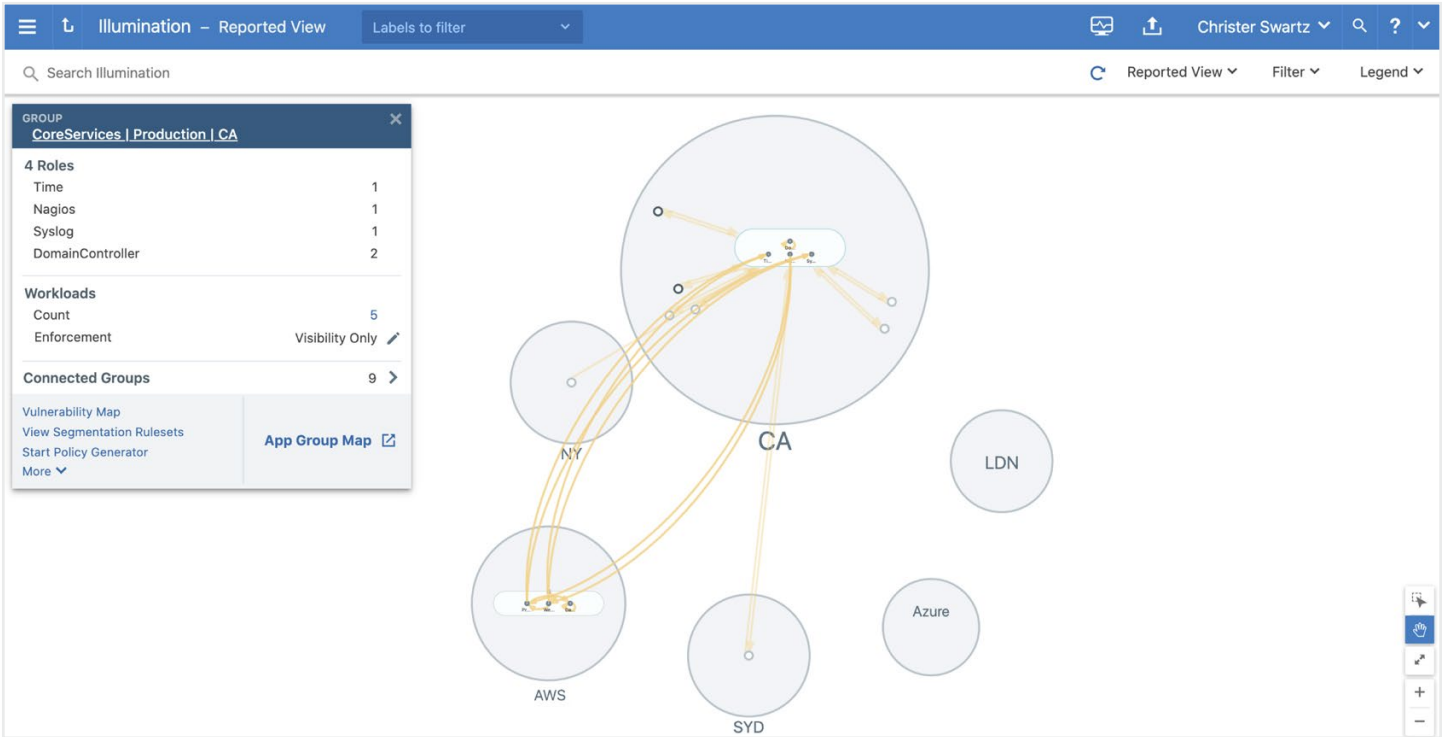


Figure 1

illumio

Metadata-Driven Policies

A workload is not associated with a single IP address across its lifecycle, and policy can no longer be defined against specific IP addresses since they are ephemeral. Something else needs to be used to identify a workload.

Using labels to identify a workload makes it easy to track a workload across its entire lifecycle, providing relief from the onerous task of trying to track and identify workloads in the face of frequent IP address changes. Policies can be implemented quickly and are highly available, auditable, and reliable, regardless of how fast or broad the architecture expands. Deployment is fully automated and orchestrated, so workloads come online with labels and inherit policies.

Cloud-Native Visibility Across Multi-Cloud and Hybrid Clouds, Without Agents

Cloud-native applications can present other unique visibility challenges that usually do not occur in on-premises data centers — such as serverless environments, cloud-managed database services, and containers. These cloud resources do not allow third-party agents to be deployed.

Illumio CloudSecure provides unmatched real-time visibility into cloud workloads without the need for software agents (Figure 2).

With CloudSecure, you can:

- See cloud traffic flows across multi-cloud and hybrid cloud environments, eliminating blind spots. Proactively discover vulnerabilities across multi-cloud and on-premises environments.
- Gain deep insight into application behavior based on what did and what can happen inside and across clouds. Respond faster to policy changes and emerging risks.
- Easily program and enforce security policies across cloud-native applications and resources. Maintain a consistent security posture regardless of the environment.

When coupled with Illumio Core, CloudSecure delivers comprehensive visibility and control across all clouds and data centers, with the ability to build and enforce unified security policies spanning diverse computing infrastructures.

AGENTLESS VISIBILITY

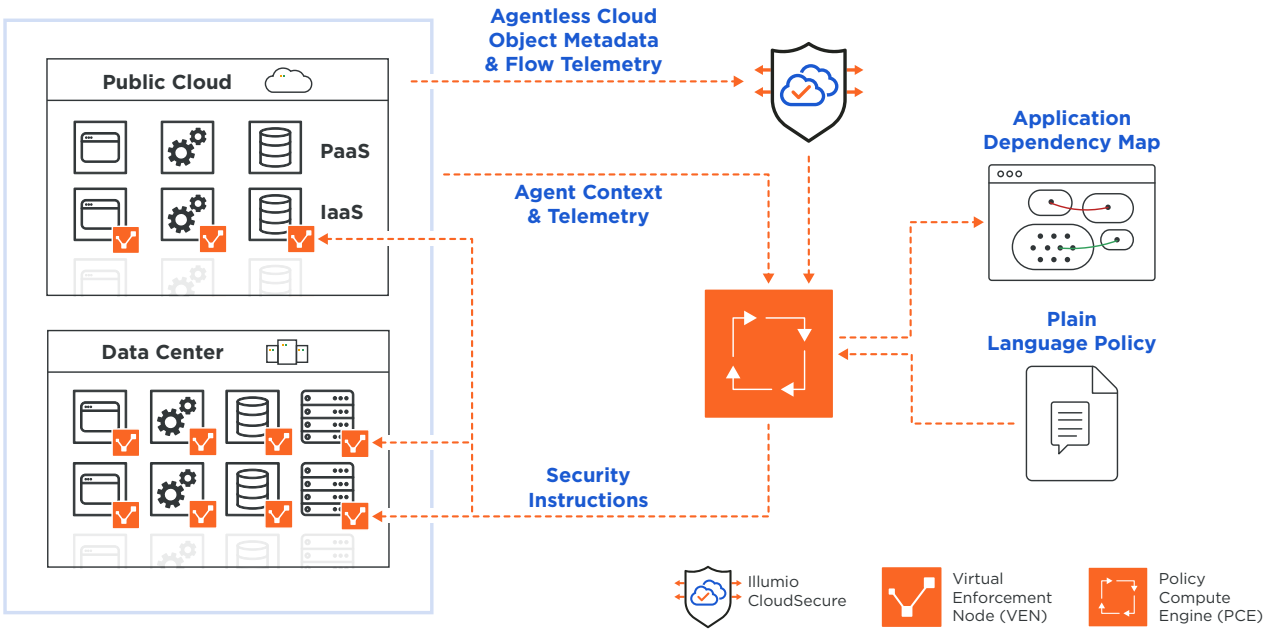


Figure 2

illumio

Segmentation Scalability

Workload segmentation solutions should not impose scaling limits on the hosting architecture. Segmentation solutions at the network layer were designed with network scaling numbers in mind, such as VLANs with a local scaling limit of no more than 4,095 unique VLAN IDs. The number of unique segment IDs in a hypervisor-based segmentation solution assumes the traditional tiered model of workload resources across a cluster of servers, enabling coarse-grained segments with an upper limit of segments enforced either at the visibility or enforcement layer.

Overlay tunneling solutions used in SDN architectures have a much higher limit of possible unique IDs, such as 16 million possible unique IDs for VXLAN. But any attempt to use these solutions to segment directly at every workload — making every workload its own segment — will run into significant operational challenges.

For example, if you have 4,000 workloads and 1 VLAN is assigned to each workload, managing this number of VLANs at the upper scale via any SDN controller will be challenging. Trying to assign a unique VXLAN ID to each of 10,000 workloads across a hybrid cloud architecture will create an even greater operational challenge. Using these non-workload-specific tools will result in broad segments at the network layer in which all workloads in a given segment will have open access to all other workloads in that same segment.

With the many options available for hyperscale workload architectures in the public cloud, you need the ability to implement segmentation at the workload level. The high scale of workload segments should be easy to centrally manage, audit, and troubleshoot. Illumio Core supports well over 100,000+ workload segments. The most extensive and complex workload hosting architectures can enforce policy directly at the workload — before any packet even reaches the network layer.

Integration With Firewalls

While workload-centric segmentation is agnostic to tools in the underlying fabric, there are instances where it is of value to exchange information from the workload layer to network devices, such as firewalls and load balancers. Illumio Core can exchange context with Palo Alto Networks firewalls, where Illumio is the source of truth for metadata-to-IP mappings. Illumio's four-dimensional labeling system tracks which workloads are assigned a given IP address and the labels can be used to define human-readable, metadata-driven policy.

Illumio sends these mappings to Palo Alto Networks firewalls for populating Dynamic Address Groups on the firewall. This means that if a public cloud architecture contains Palo Alto Networks virtual firewalls, Illumio can exchange metadata information with those firewalls, enabling the same human-readable policy at both workload and network layers.

Illumio can also exchange context with virtual load balancers from F5 and AVI, allowing control of policy for traffic passing through these load-balancers.

Visibility Into Cloud Containers Environments: Standard and Proprietary

Illumio Core also extends visibility and policy enforcement to containers environments. It deploys a containerized version of the agent on hosts in container environments, orchestrated by Kubernetes or OpenShift.

The public cloud generally supports two kinds of container hosting environments: standard Kubernetes environments Amazon Elastic Kubernetes Service (AWS EKS) and Azure Kubernetes Service (AKS). Illumio agents can be deployed on workloads in these environments in public cloud.

Each cloud provider also supports a second kind of container hosting environment, one in which the provider manages most of the underlying hosting and clustering hosting and scaling details, allowing customers to simply deploy code. But these environments, such as Amazon Elastic Container Service (AWS ECS) and Azure Container Instance (ACI), are generally serverless —

where agents cannot be deployed. Illumio CloudSecure delivers visibility into serverless, proprietary container environments, consuming flow telemetry and logs from public cloud accounts to create application-layer visibility within and outside of the environments.

Using one central solution to manage and operationalize segmentation across all workloads eliminates the inefficiencies of a siloed approach where one set of segmentation tools is used for a traditional compute environment and a different set is used for containers.

Conclusion

Illumio extends full workload visibility and segmentation to the public cloud, delivering consistent enforcement across your entire hybrid cloud architecture. You no longer have to sacrifice visibility for scalability. Blind spots and network dependencies for workload segmentation are a thing of the past. See all traffic, end-to-end, into all possible compute environments and achieve consistent security across even the largest hyperscale architectures.

Illumio, the pioneer and market leader of Zero Trust Segmentation, stops breaches from becoming cyber disasters. Illumio Core and Illumio Edge automate policy enforcement to stop cyberattacks and ransomware from spreading across applications, containers, clouds, data centers, and endpoints. By combining intelligent visibility to detect threats with security enforcement achieved in minutes, Illumio enables the world's leading organizations to strengthen their cyber resiliency and reduce risk.

Gartner peerinsights™

See what customers have to say about Illumio.