Illumio Core: DNS-Based Segmentation That Works

Enabling DNS-Based Visibility and Segmentation

Extend segmentation policy beyond your data center and public or private cloud environments to consistently secure workloads identified by fully qualified domain names (FQDNs) – including managed services, Platform as a Service (PaaS), and containers. Illumio Core™ now supports management and visibility of DNS-addressable services with adaptive segmentation policy that seamlessly follows the workload and automatically adjusts based on its domain name.

Why Illumio?

Illumio Core delivers segmentation to prevent the spread of breaches and to meet regulatory compliance standards such as SWIFT, PCI, and GDPR. Because the perimeter doesn't stop all bad actors from getting inside data centers and cloud environments – or even through to your PaaS providers, managed services, or containers – segmentation from Illumio restricts access to critical systems to only authorized entities.

Gain visibility and control of DNS-addressable services

Illumio Core delivers a full range of DNS-enabled segmentation:

- Enforce segmentation for managed services, PaaS, and containers: Allow only selected workloads to access cloud resources (e.g., secure containers pulling images from unmanaged repositories that don't have a fixed IP address like Amazon RDS).

- Control internet access (on-premises or in the cloud): Restrict workloads' access to services on the internet.

- Centralize visibility by enriching Illumio's application dependency map: See which services are accessed by workloads and collect DNS data as part of traffic flow summaries for anomaly detection.
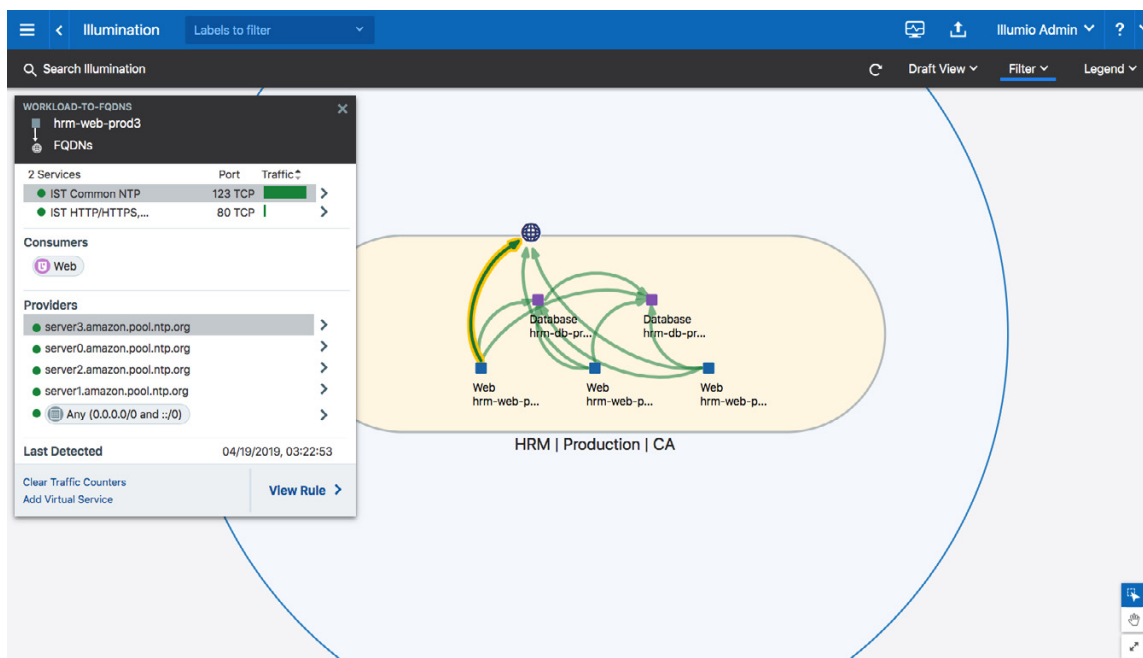
Illumio Core application dependency map: Create an Illumio policy object to represent the FQDN.

illumio

DNS-based segmentation that works

Illumio Core secures your applications by delivering visibility into application dependencies and enforcing policybased ringfencing to restrict access, even outside your network – and now to any DNS-addressable service or platform. These services can be visualized, tracked, and enforced alongside other applications in your data center, public cloud, or private cloud. With Illumio's host-based approach, security follows the workload wherever it runs, without rewriting firewall rules or modifying your infrastructure.

Illumio Core delivers a full range of DNS-enabled segmentation:

- No firewall rule writing required: Centralize and distribute DNS-based rules on the workload as close as possible to the source.

- Adaptive security: Conform policy to any changes in domain name via DNS mapping ingestion at the workload, without the complexity of manual or script-based firewall rewriting (e.g., if domain name stays the same but the IP address changes).

- Lock down outbound communications and reduce risk: Allowlist outbound services with DNS-based enforcement for your application rather than allowing all outbound communications. This mitigates the risk of applications (or people) potentially communicating with a malicious server identified only by a domain name.

- Centralize visibility: View communications from workloads to any workload reachable via a URL in the context of your cross-environment application dependency map.

- Wildcard support: Construct DNS-based policy using wildcards to capture a range of domains or subdomains, such as *.redhat.com.

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.

Follow us on:

illumio