illumio

SOLUTION BRIEF

Visibility Across the Hybrid Attack Surface With Illumio

Map all communication and traffic between workloads and devices with Illumio Zero Trust Segmentation

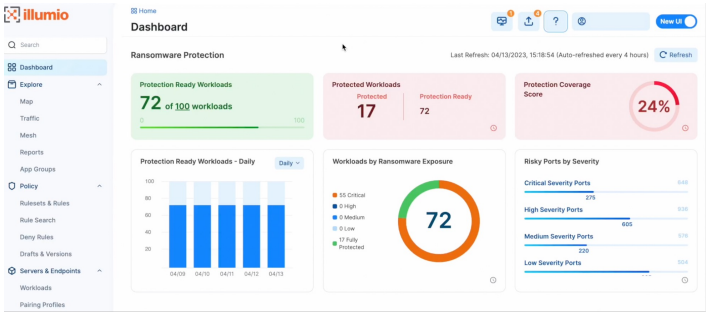
Visibility is essential to Zero Trust security

Zero Trust is changing cybersecurity – instead of trying to identify what is bad and stopping it, it's now essential to identify what is good and allow it access to assets. This is because it's far easier to block everything bad and only allow things that are safe. To achieve this, security teams must be able to identify what each asset is and what that asset is communicating with to determine the risk around each asset and take remediation steps.

Not being able to see resources and how they communicate make it difficult to determine which policies to put in place to stop an attack. In the era of AI-based attacks, it's key to be agile and react quickly.

The ability to simply create dynamic security rules for each individual asset is just not possible using a traditional network firewall model. A lack of understanding of where rules need to be applied combined with a complex management process makes this legacy model obsolete.

Illumio's Application Dependency Map shows a map of connectivity, and the Illumio Ransomware Protection Dashboard provides the context and status of each system.



> "It doesn't matter how complex it is, Illumio's map brings to light what's communicating with what and clearly shows which communications shouldn't be happening."
>
> **– Edwin Leong**
> Data Security Architect
> MGM China

Global compliance mandates require visibility

Almost all security directives and compliance standards require visibility of assets and their connectivity. This is especially true of mixed IT and OT environments. Mapping the interdependencies between IT and OT devices allows operators to understand what connections exist and which protocols are being used.

With this information, rules can be put in place to only allow permitted connections, preventing attacks from reaching the critical assets that, if compromised, could cause a societal impact.

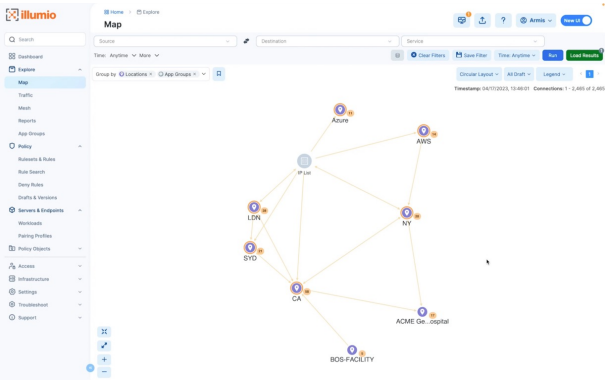
As more organizations are being impacted by regulations, organizations need a simple approach to understanding risk. Illumio provides a straightforward approach to visibility to implement the required security policies.

3 steps to see and stop high-risk connections with Illumio

1. Map interdependencies

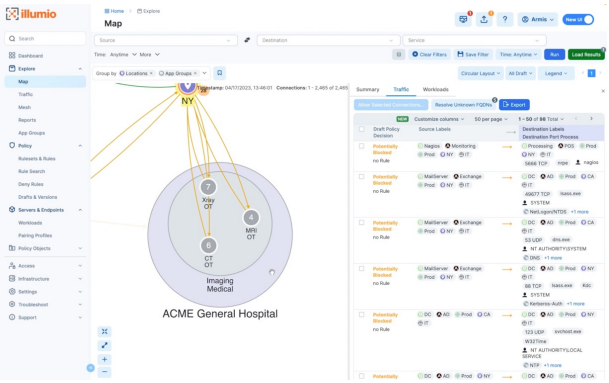
The first step to understanding potential risk, as defined by both regulators and common sense, is to map the interdependencies of assets. This applies to workloads, both data center and cloud located, endpoints, and OT assets.

Illumio gathers data from each asset, the network, and third parties to display the interdependencies on a simple-to-understand map.



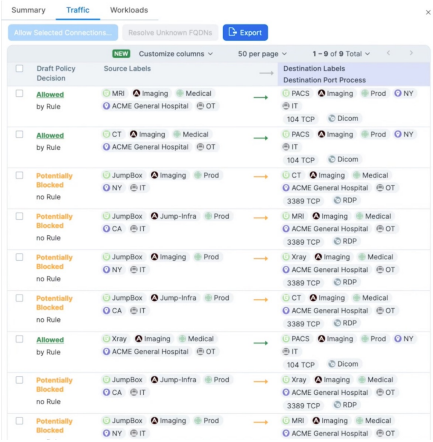
2. Identify risk

Next, understand the potential risks. By understanding each device, its vulnerabilities, and the protocols being used, it's easy to identify which connections to allow and which ports to open.



3. Audit ports and protocols

Ransomware can only propagate using existing protocols and open ports. The most popular for this is RDP using TCP Port 3389. If you can identify all the places that RDP exists, you can then decide whether to allow or deny it on an asset-by-asset basis by simply clicking on the link.



Visibility is essential to resilience

Attacks often spread using the paths that you cannot see. AI-based attacks will identify any open ports and vulnerabilities that exist. To prevent these types of attacks from becoming successful and potentially disrupting services, it's critical to be able to understand the risk and take steps to contain an attack.

Illumio provides a dynamic, real-time view of the connectivity and status of communications not available in other security solutions.

Learn more

Visit:
Illumio.com/solutions/asset-mapping-visibility

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.