illumio

SOLUTION BRIEF

Protect Critical Assets With Illumio

Illumio secures high-value critical assets by blocking all access by default and only allowing approved access

Critical assets need unique protection

High-value critical resources like legacy mainframes, proprietary hardware, sensitive scientific machinery, or classified government devices require a much higher level of security than other assets.

This is because they're at risk for a variety of motivations:

- Holding the resource ransom
- Disrupting the infrastructure
- Siphoning resources for free cryptomining

But it's not always easy to secure critical assets — compliance requirements and existing architectures can often prevent the installation of third-party security software.

Breach costs for any critical asset are too high to risk assuming it's beyond the interest of cybercriminals. Organizations must prioritize the unique security needs of their critical assets.

Contain breaches with Illumio

Breaches are inevitable. And while traditional prevention and detection tools are still necessary, they will never be perfect.

Illumio Zero Trust Segmentation (ZTS) fills this gap by providing breach containment. Illumio offers real-time visibility to see and secure network exposure, automates security policy at the workload regardless of the underlying environment, and applies consistent security across your network.

Breaches will happen – but Illumio ZTS will stop them from spreading, allowing operations to continue despite a breach.

> "With Illumio, we now have the proper protections in place to stop lateral movement and keep hackers from accessing our critical applications and data."
>
> **– Edwin Leong**
> Data Security Architect
> MGM China

How to secure critical assets

It's essential that resources in the surrounding environment can't access critical assets. Exceptions to this blanket deny-all policy can be enabled to carefully control which traffic is allowed and in what direction.

With this, security teams can create a protective barrier around critical assets with granular control over permitted traffic types, users, and teams with all other traffic denied.

Without deploying any security software onto assets, Illumio ZTS offers three essential controls to secure critical assets:

- Complete visibility of traffic in and out of critical assets
- Consistent policy using asset ringfencing
- Enforcement Boundaries to set an initial deny-all policy with granular exceptions

Visibility into network traffic

It's impossible to secure what you can't see. Before deciding exceptions to deny-all rules for critical assets, security teams must get visibility into the network's current traffic.

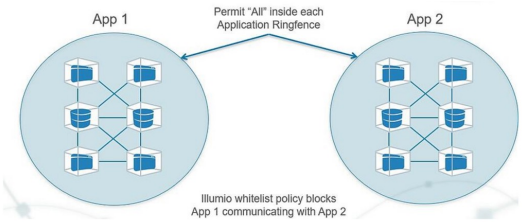
Visibility must be specific to application, users, and teams — not just network addresses or port numbers.

Illumio's application dependency map shows what traffic is currently active in and out of critical assets at any scale. With this insight, security teams can set policy for what should be allowed or denied.

Ringfence critical assets

Illumio enables the creation of a ringfence around all resources using the same label.

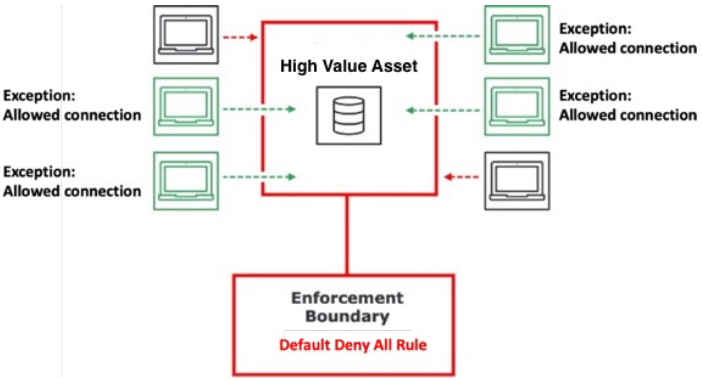
For example, if some critical assets are labeled "App 1" and others are labeled "App 2," Illumio will define each collection of like-labeled resources as a single entity and apply a common policy for all resources within it. This creates a least-privilege access model between each ringfence.



Ringfences allow security teams to visualize and enforce policy on critical assets without needing to know where they're located or the networking details of where they're hosted. It doesn't matter if ringfenced assets are on different networks or in different geographies — Illumio enforces policy by viewing them as a single group.

Illumio Enforcement Boundaries

Illumio Enforcement Boundaries allow an initial deny-all policy to be defined for high-value critical asset. Then, security teams can define granular exceptions to that blanket deny-all policy.



This gets done without deploying any security software onto critical assets, ensuring security doesn't impact operations.

Even if one asset gets breached, Illumio ensures it can't spread to any other assets.

Learn more about protecting critical assets with Illumio ZTS

Visit: illumio.com/solutions/critical-asset-protection

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches 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.