illumio

SOLUTION BRIEF

IT / OT Convergence

Securing the integration of cyber-physical systems

Business transformation is driving the adoption of automation and digitalization. In many industries, we are seeing business needs for the convergence of IT and OT.

Healthcare:

- Connected medicine
- Telemedicine
- Record management integration

Energy:

- Supply management
- Delivery optimization
- Big data analytics

Manufacturing:

- Supply chain automation
- Non-stop production
- Automated logistics

Recent incidents show that an attack on any part of an organization can have wider effect. This can result in a hospital not being able to treat patients, energy not being delivered, or a manufacturer suffering substantial losses.

New connected technology is being developed to optimize the delivery of essential services. However, some cyber-physical systems are older and use out-of-support equipment.

It is critical that any attack on either the IT or OT environment can be contained to maintain the delivery of services.

A new approach

Modern cyber-physical devices need increased connectivity which means that we cannot guarantee the safety of the network they are connected to.

This means we need to move away from traditional network-based security.

New cyber-physical systems use operating systems like Linux and Windows and so take advantage of the native firewall to protect each individual asset.

As standard, the firewall is likely to be configured using traditional network constructs which do not provide the granularity required to protect individual assets.

> “When implementing cybersecurity requirements, grid and DER planners should build cyber defenses with the goal of surviving an attack while maintaining critical functionality.”
>
> **US Department of Energy**

The Illumio approach

Illumio has a five-step model that takes an asset-centric approach to understanding the properties, risk, and state of each device and then applies the appropriate protection without affecting the OS kernel.

Step 1

Collect connectivity data from IT and OT devices to map interdependencies

Step 2

Enrich with asset and vulnerability scanning data

Step 3

Apply easily understandable labels based on function and risk

Step 4

Enforce policy based on least privilege and risk using the native firewall on IT and supported OT devices

Step 5

Enforce using network switches for legacy systems

Building a resilient infrastructure

Using this approach not only provides the visibility to understand exactly what systems exist but also how they are communicating. By controlling how critical systems communicate, threats like ransomware can be contained. This makes the infrastructure tolerant to attack and will maintain the delivery of critical services.

Across all industries, new regulations are being created to protect critical national infrastructure. While there is variation, they all contain the same core attributes:

- Build policy based on risk
- Map the interdependencies of all IT and OT systems
- Segment the infrastructure to contain an attack and maintain service delivery
- Focus on protecting the asset instead of the network

The Illumio model protects your IT/OT convergence and helps you comply with regulations.

Secure your IT/OT

Learn more about how Illumio can help you protect your network and achieve compliance.

https://www.illumio.com/products

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.