illumio

SOLUTION BRIEF

Illumio Keeps Critical National Infrastructure Up, Running and Compliant

Water, utilities, manufacturers and power stations make tempting cyber targets. Now they can be secured with Zero Trust segmentation.

For Critical Infrastructure, Uptime Is Critical

What happens if critical national infrastructure systems — water, utilities, power stations and key manufacturing facilities — are taken down by cyberattacks?

That frightening question is increasingly at the top of the agenda for governments and boards of directors. Clearly, cybercriminals have critical infrastructure in their crosshairs. The ransomware payout for seizing control of such systems is extremely high.

Since the advent of the global pandemic, cybercriminals have stepped up the number, frequency and types of attacks they launch. If left unchecked, these hackers can threaten not only infrastructure providers, but also the national economies they support.

In response, the European Union created the Network and Information Security directive. It aims to establish national frameworks that will enhance cybersecurity across the EU. While the directive should help protect critical IT assets, it also burdens critical infrastructure providers with a new compliance challenge.

Zero Trust for Zero Downtime

The Illumio product suite provides pioneering capabilities to help utility operators and manufacturers create new security defenses against ransomware and other cyberattacks.

Importantly, Illumio helps ensure that segmentation security efforts don't inadvertently block services for applications and systems.

Segmentation stops attackers and their malware from moving laterally. This reduces both the attack surface and overall risk by lessening the impact of a breach.

Illumio gives critical infrastructure organizations the ability to deploy Zero Trust segmentation in a simple progression. Illumio streamlines policy creation, and policies can be deployed on a step-by-step basis. What's more, each policy can be tested on live traffic before enforcement — a feature few other vendors can offer.

Illumio also helps infrastructure providers control spending. Illumio products deploy quickly and safely, reducing a project's overall cost — without disruption or the need for infrastructure changes.

Illumio's Key Benefits

How Illumio helps keep critical infrastructure secure

Risk-Based Visibility
Map all communications across applications, devices and cloud platforms. Know your vulnerable pathways to prioritize your security efforts.

Ransomware Containment
Block unsafe network communications and integrate Illumio data into SIEM and SOAR tools. Prevent attacks from spreading.

Simpler Policy Creation
Define a policy to automatically generate the required rules. Enforce the policy in any cloud, data center or network. Gain full control over what talks to what.

How Illumio Speeds the Journey to Zero Trust

Simplify enforcement, gain visibility, stop attackers

With Illumio's risk-based visibility and automated policy generation, infrastructure organizations can quickly secure high-value assets, protect themselves from ransomware, and contain the spread of any attack.

Illumio technology gives organizations visibility into all ports, processes and connections used by application workloads, including interrelationships and potential vulnerabilities. It uses this information to compute and enforce accurate security policies that automatically adapt to application and infrastructure changes.

Many data centers in the infrastructure sector are designed as large, flat networks to allow for easy connectivity among systems. But this provides a larger attack surface for cybercriminals.

Once an attacker has compromised the perimeter of a network, they can gain access several ways, such as with malware, ransomware, stolen credentials and default passwords.

Without Illumio, criminals are free to move around a network. Staying hidden for weeks or even months, they map an organization's high-value assets and decide when to strike. When they do, their actions can have catastrophic results.

But with Illumio's segmentation approach, organizations can stop these attackers and their malware from moving freely through a network. Illumio reduces the attack surface and overall risk by lessening the impact of a breach.

By using Illumio, critical infrastructure providers can dramatically accelerate and simplify their journey to Zero Trust with automated enforcement of security policies across the entire organization. They gain the control needed to stop an attack from turning into a cyber disaster.

> "With Illumio, we had production assets enforced and under control in months, fulfilling our need to move faster and further toward our Zero Trust posture."
>
> **— Andrew Dell**
> **Chief Information Security Officer**
> **QBE Insurance Group**

Protect Key Industries

Learn more about how Illumio keeps critical national infrastructure safe, running and compliant.

Visit: www.illumio.com

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.