illumio

SOLUTION BRIEF

Contain Ransomware With Zero Trust Segmentation

Illumio stops breaches at their source, proactively protecting IT and OT environments

The ransomware threat

Ransomware attacks aren't going away. In fact, according to Forrester, ransomware is the top cause of breaches for many industries is the top cause of breaches for many industries, such as business services, construction, manufacturing, utilities, and telecommunications.

Attacks can happen across businesses of all sizes and industries. When they do happen, the impacts can be catastrophic:

- The total cost of ransomware attacks is expected to reach **$265 billion** by 2031.
- It takes on average **277 days** to identify and contain a breach. .
- The total cost to recover from a ransomware attack is around **$5.2 million**.

Ransomware attacks are not only costly — they negatively affect an organization's reputation. Customers need to be confident that they can trust an organization with their data and that the business will be resilient against a cyberattack. This lack of confidence from customers can exacerbate ransomware's impact on the business and the ability to fully recover after a breach.

The solution

Ransomware protection isn't just a product – it's a plan and a process. Gartner expects that by 2025 30% of nation states will pass legislation that regulates ransomware payments, fines, and negotiation. This has a major impact on how preparations should take place.

A multi-pronged approach is required to ensure that an organization is successful. Following a framework such as the NIST Cybersecurity Framework (CSF) can help prepare for the worst.

> "By blocking and eliminating server-to-server threats, Illumio will reduce our attack surface by at least 80%. "
>
> **– François Lepage, Director of Cybersecurity and Infrastructure The Master Group**

Illumio Zero Trust Segmentation

Zero Trust Segmentation (ZTS), also called microsegmentation, is a key component to any ransomware containment strategy and supports frameworks such as NIST CSF. Illumio ZTS limits east-west lateral movement. This level of control can contain the attack at its entry point, ensuring attackers cannot spread through an environment.

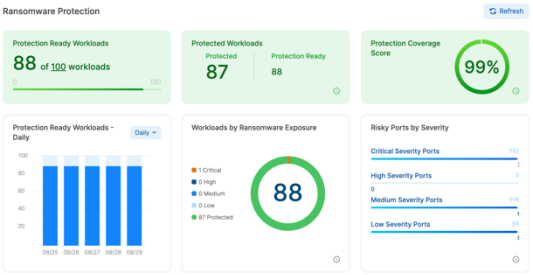
By eliminating the ability for attacks to spread with Illumio ZTS, EDR and XDR solutions have the time they need to detect. This prevents cyber disasters and enables business to continue forward, unimpeded by attempted attacks.

Illumio works across the hybrid environment, whether on-premises or in cloud-based containers, VMs, endpoints, and more. This ensures that there are no silos or blind spots. It also keeps policy consistent across the environment which is key to the success of ransomware containment.

Stop ransomware with Illumio

Identify risks

Eliminate silos with complete visibility into security risks and dependencies across the hybrid environment providing key intel to define the containment strategy and prepare for threats.

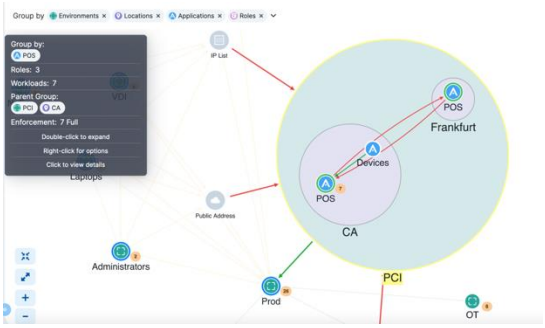


Build cyber resilience

Illumio's host-based segmentation approach allows you to block all unused and high-risk ports and protocols, rapidly and at scale. This proactively reduces the ransomware attack surface to protect operations, revenue, and reputation.

Protect high-value assets

It's quick and easy to quarantine compromised systems. Contain ransomware at its entry point — without complex detection methods or making changes to the network. Implement application ringfencing to allow access based on least privilege to protect critical assets.



Illumio aligns to the NIST CSF

A key to success against ransomware is identifying a plan. NIST CSF is the gold standard of frameworks with five functions that make up the pillars of a successful program:

- **Identify –** Map connections between applications and devices
- **Protect –** Deny rules block unused and high-risk ports
- **Detect –** The application dependency map identifies risk and optimizes EDR solutions
- **Respond –** Integrate with existing SOAR workflows for automated containment
- **Restore –** Build long term security with a true Zero Trust model

Illumio ZTS for ransomware containment

Illumio stops ransomware from causing a major business failure by reducing the attack surface and containing attackers at the source. This prevents ransomware from reaching critical systems and data.

Illumio ZTS limits a breach's impact, helping to maintain business resilience and preserve the organization's reputation.

Learn more about containing ransomware with Illumio ZTS

Visit:
illumio.com/use-case/ransomware-containment

About Illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Zero Trust Segmentation Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.