illumio

CASE STUDY

Global Law Firm Stops Ransomware With Illumio

From intrusion to containment in hours: How a company used Illumio to isolate a ransomware attack before it damaged the organization and its clients

Industry: Legal Services

Location: Global

Environment: Data center with about 1,000 servers running more than 30 applications

Challenge: Prevent lateral movement of a ransomware attack to protect data center operations and client data

Solution: Illumio Core

Benefits:

- Stopped the attack from causing significant damage to its IT systems or data
- Prevented the theft or encryption of any data, including any client records or legal files
- Avoided disruptions to its business operations and preserved its reputation

No one likes bad news. Then there is news no CIO ever wants to hear.

But at 4:00 PM on a Monday evening in late September 2021, the CIO of a global law firm was notified that the company was under attack by ransomware.

Malicious code snuck into the network through a URL in a phishing email that made its way onto a help desk workstation. The law firm's network was breached. In just a couple of hours, the ransomware had spread to 12 servers. Time was running out.

But this law firm had something that the cybercriminals weren't expecting: Zero Trust Segmentation from Illumio.

No More Lateral Moves — Or Any Moves

In seconds, the company used Illumio to shut down the ransomware attack. Once they identified the 12 compromised servers, they quickly set up a policy to "ring-fence" and isolate the infected machines, essentially dropping a box on the attackers to stop their movement through the network.

"Literally in a couple of drag-and-drop clicks, we were able to quarantine all the affected systems," explains the IT executive who led the law firm's incident response team. "We did it so quickly the attackers were locked out of the network before they knew what had happened. They had no way to jump anywhere else to evade us and keep spreading. Their fun for the evening was over."

The executive says the speed at which they were able to use Illumio to quarantine the compromised servers made all the difference.

"Our security consultants said they had never seen such a rapid — and effective — response to a ransomware breach," he explains. "In most cases, by the time a company realizes that it's being attacked and takes action with conventional methods to contain access, it is too late, and the ransomware has spread to hundreds of systems."

"The speed at which we were able to use Illumio to quarantine the ransomware made all the difference."

IT Executive
Global Law Firm

Helping Defeat a Ransomware Attack

While Illumio was pivotal in quickly quarantining the ransomware to keep it from moving through the network, it contributed to successfully defeating the attack in several ways, the executive says.

Illumio helped the law firm to:

- **Slow the Attack:** Before the attack, the firm had already greatly limited open pathways on its network by deploying Illumio's Zero Trust Segmentation access controls.
- **Track the Intruders:** By seamlessly integrating with its security information and event management (SIEM) tool, Illumio's communications telemetry helped provide a fuller view of the ransomware's spread.
- **Visualize the Activity:** Illumio's real-time application communications map across the law firm's hybrid cloud environment clearly showed the unusual network activity from ransomware chatter.
- **Quarantine Compromised Assets:** Illumio's simple rule generation capabilities made it easy to create a policy in less than a minute to isolate the infected servers in both the data center and a Microsoft Azure cloud service.
- **Aid the Investigation:** Illumio made it safe to access compromised server data and securely transfer it to an incident response agency for analysis.

In particular, the executive says that the microsegmentation they had already put in place with Illumio Core (Illumio's flagship product) made a profound difference. It proactively limited where the attackers could go and what they could do, finally trapping them in a ring-fence.

Illumio Core left the attackers a much narrower range of options and bought the company more time to track them down.

"If we hadn't already had Illumio Core in place with live enforcement policies, I think the attack could have been much more difficult to contain," he says. "The bad actors would have had more paths from the help desk workstation and spread much further, much faster, making our job of stopping them much more complex."

Defending Client Data and Organizational Reputation

Being able to stop ransomware is doubly essential for law firms, the executive says. They must not only protect their own organization, but law firms are bound by fiduciary duty to safeguard information about their clients and their legal cases.

"No law firm can afford to lose any of its clients' data in an attack, because that causes reputational harm which, in some cases, can be very difficult to recover from," he says.

For example, the executive knows of another law firm that suffered a major ransomware attack that exposed client data and forced them to take their network down for a month, significantly hurting its business and client confidence.

"Their exposure was huge. It is unclear how many clients or potential clients they may have lost as a result of the incident," the executive says. "I didn't want anything remotely similar to happen to us."

By being able to respond so quickly to stop its ransomware attack with Illumio, the law firm was able to:

- Prevent the attackers from causing significant damage to its IT systems or data
- Stop the theft or encryption of any data, including any client records or legal files
- Avoid disruptions to its business operations

And because no client data was stolen, the firm preserved its most precious asset: its reputation.

> "Our security consultants said they had never seen such a rapid — and effective — response to a ransomware breach."
>
> **IT Executive**
> **Global Law Firm**

Searching for Back-Office Security

The law firm executive says he is always looking for new ways to further improve the company's digital security and stay one step ahead of increasingly sophisticated cyberattacks.

"It's all about being able to close the loose ends on your network that offer attackers a weakness to exploit," he says.

Historically, the law firm has used multiple technologies for securing its data and systems, such as endpoint detection and response (EDR) tools, anti-virus software for employee laptops, and ransomware detection for file systems.

But before Illumio, it lacked strong methods for protecting "the back office" — all the applications and data that run its business operations — now living in both data centers and cloud platforms.

The executive recognized that microsegmentation would be a key way to bolster protection of these systems.

By being able to easily control and block pathways of travel down to the application level, the firm could greatly limit the "unlocked doors" that so often make it easy for cybercriminals to move around networks to steal data and hold companies hostage, he explains.

When he began his search for a microsegmentation platform, he found that conventional approaches for segmentation just didn't work the way they needed to.

> "If we hadn't already had some of our Illumio segmentation in place, the attack could have been impossible to contain."
>
> **IT Executive**
> **Global Law Firm**

"I wanted to gain better control over our network communications, but I knew I couldn't do it with methods like manually restricting access control lists on physical network switches," he says. "It just takes too much manpower to program those, and, then, how do you map all of that afterwards?"

Illumio solves these challenges, the executive says.

Based on extensive vetting and guidance from leading analyst firms, the executive selected Illumio to bring simple, scalable Zero Trust Segmentation to his organization.

"Illumio gives you the visibility and control over application communication flows in ways that you don't have with any other security solution," he says. "With Illumio, you can easily go through your policies and make updates and modifications as necessary."

The executive says Illumio's ability to seamlessly provide the same segmentation capabilities for cloud workloads as for on-premises data centers was also a big selling point.

"You can't just think about the confines of your own data center," he says. "Hybrid cloud computing is a reality today. Rather than be bound to a network hardware solution or a virtualization platform, we wanted to go with a best-of-breed SaaS platform that gives us the flexibility we need. I'd say Illumio is just that."

Certainly, the law firm is more than happy that Illumio was in place, ready to help it defeat ransomware and avoid damage to its operations, its clients and its reputation. It is now focusing on expanding Illumio to enforce policy across a much broader range of its IT estate.

"In this day and age, it's essential to implement microsegmentation to limit lateral movement from any attacker or malware that gets into your network." he says. "It is only a matter of time before you have your own breach. So you need to be prepared."

Stop Ransomware as Soon as It Strikes — With Illumio

- **Learn More:** www.illumio.com
- **Go Deeper:** How to Stop Ransomware Attacks eBook
- **Schedule a Chat:** Free consultation and demo

"I wanted to gain better control over our network communications, but I knew I couldn't do it with methods like manually restricting access control lists on physical network switches. It just takes too much manpower to program those, and, then, how do you map all of that afterwards?"

IT Executive
Global Law Firm

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.

Copyright © 2022 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.