illumio

EBOOK

CUSTOMER STORIES

Better Cybersecurity Begins With Real-Time Visibility

Learn how leading organizations use Illumio's comprehensive, real-time visibility and Zero Trust segmentation to defeat ransomware and other cyberattacks

Taking on Modern Security Threats: Why Visibility Is the Critical First Step

Cyberattacks can officially be added to "the only things in life that are certain" list.

Over the past two years, major ransomware attacks have taken hold of critical data worldwide while taking news headlines by storm. In 2020, ransomware cases skyrocketed by 150 percent over the previous year. Breach numbers are on track to break records this year — and it's no surprise that ransomware is a huge contributor, having become the most common type of attack.

Reports about these breaches often cite unknown servers, unpatched systems or misconfigured firewalls as contributing factors. Many cyberattacks succeed because IT teams lack the visibility needed to identify and eliminate these risks before attackers can take advantage of them.

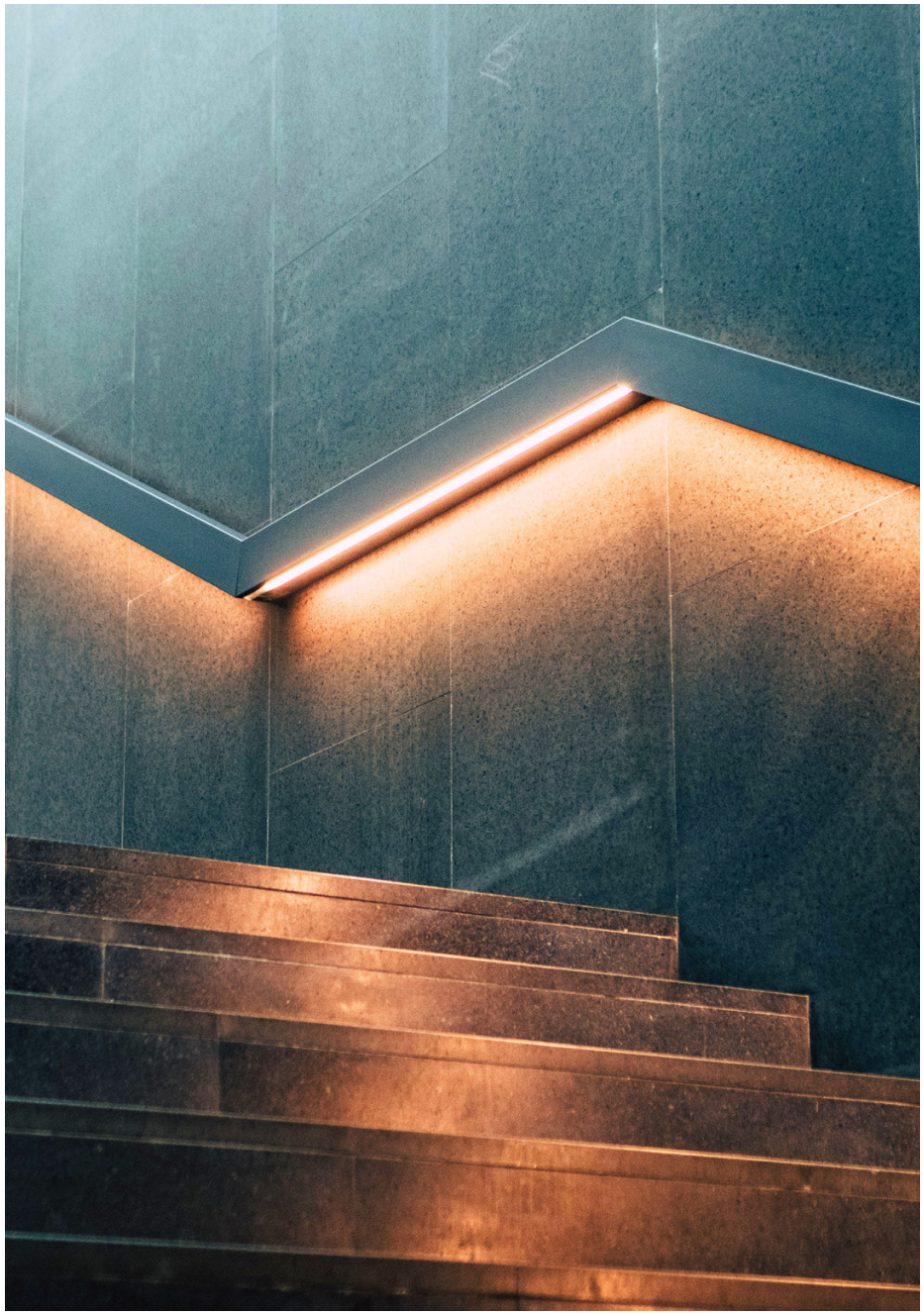
These blind spots include connections among applications and between applications and the Internet — the very paths ransomware and attackers use to move through your network and coordinate their activity.

The increasingly complex, hybrid and distributed nature of digital environments makes visibility all the more crucial. Comprehensive, contextual visibility is now a prerequisite to keeping up with the pace of changes — and keeping your organization safe. IT teams need visibility that includes:

- Detailed application-centric mapping of traffic flows and dependencies
- A unified view of all flows across clouds, endpoints and on-premises environments
- Real-time, continuous and historical visualization of this flow data

Meeting these requirements will pave the way for your organization to make the right security decisions and shut down routes for ransomware and cyberattacks — leaving attackers with nowhere to hide.

This ebook walks through how Illumio makes it possible to achieve this level of visibility, block attack pathways, and reduce risk in three simple steps, then highlights success stories of organizations like yours.



illumio

3 Simple Steps to See Your Risks and Contain Cyberattacks

1. Automatically map all your traffic flows and dependencies in as little as an hour.
2. Capture critical insights to pinpoint the applications and systems that are most at risk.
3. Shut down the ports and pathways commonly used by ransomware and other cyberattacks.

The Power of Comprehensive Real-Time Visibility

Illumio's pioneering technology makes it possible to protect your organization against ransomware following these three steps.

Let's look at each step in more detail.

First, Illumio visualizes all communications between applications, workloads and devices — across any cloud, data center, container or endpoint — and their external communications with the Internet.

The result is a detailed real-time "application dependency map" of your entire IT environment. In an hour or less, you can gain a clear understanding of the pathways an attacker could use to move through your network.

Illumio makes it easy to pinpoint major sources of risk, including:

- Unpatched legacy systems and deprecated services that open a door into your environment.
- Commonly exploited ransomware attack vectors, such as Remote Desktop Protocol (RDP) and Server Message Block (SMB).
- Applications and systems that are communicating more than they need to with each other or the Internet.

With the ability to identify the most vulnerable systems, applications and workloads, Illumio equips organizations with actionable insights.

Next, it's time to take action to eliminate known security risks. You can now quickly:

- Close unnecessary pathways established by legacy protocols, such as FTP and Telnet.
- Shut down ransomware's favorite entry pathways for rapid spread, including RDP and SMB.
- Isolate core services, controlling inbound and outbound Internet traffic.

Now that you've addressed obvious risks, Illumio can help you establish robust protection against breaches. Using Illumio's unique testing capabilities, you can pre-build Zero Trust segmentation policies and safely activate them if a breach occurs. Automated policy creation and enforcement makes it easy to implement granular Zero Trust segmentation controls to protect your most critical applications and workloads.

On the following pages, learn how Illumio customers benefit from our real-time visibility and simplified approach to Zero Trust segmentation.

MANUFACTURING

Hi-Temp Insulation Launches Visibility and Segmentation in Just 30 Minutes

Key Challenges

Aerospace manufacturer Hi-Temp Insulation needed to respond to new security standards required of all contractors to the U.S. Department of Defense, added in the wake of recent breaches and ransomware attacks. For Hi-Temp, this meant addressing the lack of visibility into the traffic flowing across a hybrid data center and implementing a least privilege access model to tighten security controls and overcome the cumbersome task of writing Group Policy Objects (GPOs).

Key Results

Thanks to Illumio Core's real-time application dependency map, Hi-Temp gained complete visibility of its east-west traffic flows and application chatter. Now Hi-Temp can quickly identify risky traffic pathways and shut down unnecessary connections. The map is augmented by Illumio's historical traffic database, cutting Hi-Temp's troubleshooting time from hours to minutes.

With Illumio, Hi-Temp now protects its servers at a more granular level than GPOs allow. The team also reduced the number of rules from hundreds in Windows Group Policy to only 19 Illumio policies. What's more, Hi-Temp can deploy changes in minutes, down from hours using GPOs.

READ THE STORY >

"Illumio stood out from the crowd with its speed and ease. We were able to get it up and running in less than a half-hour. Instantly, we could see our traffic and set up policies to protect our network."

David Hanna,
IT Operations Specialist,
Hi-Temp Insulation

TRANSPORTATION

Cathay Pacific Reaches New Heights in Its Zero Trust Journey

Key Challenges

After being targeted by a cyberattack, the world-class airline Cathay Pacific redoubled its focus on Zero Trust security. With customer data and critical systems at stake, Cathay was met with a year-end deadline to shore up protection for its most critical applications — and eventually over 3,000 servers and 600 apps in all. The company needed an efficient solution that integrated visualization of application traffic across its hybrid, multi-cloud environment with Zero Trust policy enforcement.

Key Results

Cathay found exactly what it needed in Illumio. In less than three months, the implementation was complete, coming in well ahead of deadline. The team estimates it would have taken 12–18 months using a network-based solution.

Illumio's real-time application dependency map makes it easy to see connections between servers and applications, then to take immediate action to block or authorize flows. Thanks to Illumio, infrastructure and security teams are partnering better with application owners, working together to review communication flows and define access policies.

Illumio's efficiency and ease of use continue to fuel Cathay's Zero Trust security journey. The company also discovered that Illumio could help meet many PCI-DSS compliance requirements. As a result, Cathay has saved a considerable amount of time and an estimated $5 million that it would have cost to install data center firewalls for its PCI-DSS compliance initiative.

WATCH THE VIDEO > **READ THE STORY >**

"We were chasing down an attack and used Illumio to understand the attacker's behavior faster than some of our more traditional security tools because of the visibility and ease."

Kerry Peirse, General Manager
IT Infrastructure, Operations and Security,
Cathay Pacific

illumio

REAL ESTATE

Investa Builds Protection Against Breaches With Context-Rich Visibility

Key Challenges

Investa consistently delivers high-quality real estate services and outperforms for its investors. Protecting that reputation puts a spotlight on how the firm protects its IT environment, especially in light of growing cyber threats to the real estate industry. When the risk posed by legacy Windows servers with known but non-patchable vulnerabilities became too high, mitigating risk became a priority. Investa needed a new way to identify, visualize and control systems and servers at risk.

Key Results

With Illumio, Investa gained fast visibility into its data center traffic flows. Immediately it learned that its application environment was more complex than the company had realized. Now Illumio's real-time map displays how critical business applications work, with context down to individual workloads, and what unnecessary connections present risk. Plus, with cloud adoption on the horizon, Illumio delivers consistent visibility and control for any public cloud without introducing new network-based risks.

Having an accurate visual representation of Investa's application environment and security controls makes sharing updates with the executive team easy. The company is primed to limit an attacker's reach and minimize the impact of any potential breach.

READ THE STORY >

"With Illumio, we know exactly what is talking to what. No one wants to be the company that gets breached. But if that happens, we have peace of mind that the breach will be contained."

Nathan Powell,
IT Operations Manager,
Investa

illumio

Leading organizations worldwide rely on Illumio's unparalleled visibility to reduce risk and advance Zero Trust strategies.

More than
10%
of the Fortune 100 companies

Securing
6 of the **10**
largest global banks

Protecting
5
of the leading insurance companies

Safeguarding
3 of the **5**
largest enterprise SaaS companies

Principal℠ YAMAHA servicenow BNP PARIBAS

Morgan Stanley salesforce BlueCross BlueShield ORACLE + NETSUITE

“Given the complexity of a highly fragmented network, Illumio provides unparalleled and practical traffic transparency. This allows us to manage all traffic and to quickly discover misconfigurations and malicious activity.”

Thomas Vavra
Manager of Communication Networks
Mondi

READ THE STORY >

“Gaining live visibility into flows between workloads down to the paths of protocols provided immediate value. Illumio’s simple yet powerful graphical map gave us visibility that we never had before.”

Mikael Karlsson
Head of IT Infrastructure
AFA Försäkring

READ THE STORY >

“I sleep better at night knowing that Illumio closes the doors on potential attacks against our domain controllers. The demonstrable risk to our environment is noticeably lessened.”

Joel Duisman
Principal IT Security Architect
ServiceNow

READ THE STORY >

Visit illumio.com/customers to learn how other leading organizations use Illumio to see risk and protect critical data and applications.

Interested in a demo of Illumio’s visibility and ransomware containment capabilities?

Contact us today to make it happen!

illumio