

Lion Hops from a Ransomware Attack to a Resilient Security Infrastructure with Illumio

Beverage manufacturer reduces risk and accelerates their bottom line with Illumio Zero Trust Segmentation

Business Goals

Picture this: just as the hospitality industry is facing uncertainty during the height of the COVID-19 pandemic, a ransomware attack strikes, forcing your beverage company to shut down key systems and operations as a precaution. That's exactly what happened to Lion in June of 2020.

Lion is on a mission to bring people together responsibly for a good time with alcoholic and non-alcoholic drinks. With a wide range of infrastructure including IT and OT across different continents, Lion knew it needed a different approach to security – a proactive approach to minimize the impact of inevitable breaches before they impact operations and critical data.

“After a ransomware attack, you become obsessed with building a more resilient organization. Your top priority is getting ahead of the problem and proactively stopping attackers before they impact your operations or your customers,” said Jamie Rossato, Chief Information Security Officer at Lion. “It’s clear that today breaches happen, so to have a strong security posture, you have no choice but to assume breach. Once we knew our goal was to reduce risk from the outset, implementing Illumio Zero Trust Segmentation (ZTS) was a no-brainer. With Illumio ZTS, only the essential connections are happening in our environment, giving us the confidence to move and scale quickly as a business.”

Technology Challenge

Understanding how workloads and applications

Industry: Manufacturing/hospitality

Challenge: Minimize risk by visualizing network communications and automatically stopping attackers

Solution: [Illumio Core](#)

Use cases: Ransomware containment, network visibility

Benefits:

- **Comprehensive view of network communications**
Visibility into communications across environments helps Lion better collaborate to identify and reduce risk.
- **Resilience to cyberattacks**
Illumio allows Lion to be proactive in combatting breaches.
- **Trusted security supports the bottom line**
Confidence that granular security controls will not break critical production applications

“

“Technology is the life blood of every organization, and Illumio allows us to show up as strategic and trusted advisors with our colleagues. Because we’re partners to the business and our security posture is resilient, we can all move faster and more confidently, ultimately supporting the bottom line.”

–Jamie Rossato
Chief Information Security Officer
Lion

interact across a global network is a major hurdle for security teams.

“At Lion, we’re working with a sprawling network, with IT and OT across a host of locations and continents. It can be difficult to understand and keep track of all the communications happening and, therefore, tough to identify risk and prioritize what to lock down. We need to be able to support our teams with technology that scales securely and reliably alongside them. It’s crucial for us to have visibility into our network and to prevent breaches from spreading automatically to keep our promise as a security team to our colleagues and customers.”

In addition to gaining visibility, Lion needed a way to automatically shut down unauthorized access to servers to stop breaches in their tracks. When attacks can spread, they often reach critical applications and data that limits or completely shuts down business operations – this is exactly what Lion needed to prevent.

“

“Regardless of which industry you’re in, technology is essential to business growth. And to grow quickly and responsibly, leadership must be able to trust that the organization’s technology and data is secure. Illumio makes not only our technology team, but also our entire business confident that our operations are secure and resilient to inevitable cyberattacks now and as we scale.”

–Jamie Rossato
Chief Information Security Officer
Lion

How Illumio Helped

Lion’s security team identified Illumio Core as the perfect fit for their needs. Illumio illustrates network communications in an easy-to-read map, giving the entire team (including applications owners, architects, project managers, those responsible for incident response, and more) the visibility and confidence they need to plan the most impactful security strategy.

Illumio Core also makes segmentation simple, so Lion could implement dynamic segmentation controls that stop breaches from reaching their most important assets. In the face of attacks, Illumio allows Lion to keep the lights on by isolating attackers while leaving business operations up and running.

Together, this not only protects the business, but it allows them to better collaborate and scale more quickly.

Results & Benefits

Lion continues to see benefits from Illumio Core including:

Technology cost savings.

With the visibility and insights Illumio provides, Lion identifies inefficiencies in its network, allowing them to reallocate and save resources.

Reduced risk and increased business resilience.

Breaches happen at most organizations. With Illumio, Lion can contain attacks proactively so their impact on operations and the business is negligible.

An accelerated business and bottom line.

Today, organizations run and get ahead with technology. Illumio gives Lion the data and confidence to run faster, accelerating the bottom line.

About Illumio



Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.