How Illumio Lowers ACH Group's Cyber Risk — With Nearly Zero Overhead

Illumio helps Australian aged care provider build its cyber resilience with Zero Trust Segmentation

Industry: Aged Care (nonprofit)

Location: Adelaide, Australia

Challenge: Protect against ransomware and lower cyber risk with limited staff and budget

Solution: Illumio Core supported a "pragmatic" Zero Trust security strategy

Benefits:

- Greater visibility into workloads

- Easy 'pragmatic' Zero Trust Segmentation

- Simple creation and management of deny lists

- Almost zero management overhead

Business Goals

When you're a not-for-profit organization, a cyberattack isn't just a business problem. It's also a threat to your societal mission.

Take ACH Group. Its 1,800 employees provide housing and other related services for some 20,000 older people in South Australia.

ACH's tagline is "good lives for older people." But if the organization's IT systems are breached by ransomware, its ability to support those good lives could be compromised.

"For us, cybersecurity is less about getting hacked and more about the availability and integrity of our services," says Jason Loveday, information security manager for ACH Group. "So when we commit funding to technology, it needs to clearly help us serve our customers more effectively."

Technology Challenges

To lower ACH's cyber risk, Loveday set out to establish an efficient, central way to manage segmentation and firewalling policies. He wanted to be able to tag a workload, then have a security policy automatically assigned to it, instantly protecting that workload and blocking unnecessary communications.

Because ACH uses a hyper-converged infrastructure, it was challenging to segment development, test and production environments, Loveday says.

"They all run on the same server chassis," he explains. "We didn't have a way to segment that chassis by environment."

"With Illumio, we just set it and forget it. It's ridiculously simple."

Jason Loveday
Information Security Manager
ACH Group

This represents a big change from ACH's previous technology policy, which focused on network firewalls. Further complicating matters, the organization operates an array of legacy hardware applications, due for retirement.

With limited budget and a small operations team, Loveday needed a technology that added key defensive capabilities while still being simple to learn and easy to manage.

How Illumio Helped

To reduce the cyber risk from an attack or malware that could impair ACH's ability to serve its customers, Loveday focused on "pragmatic" Zero Trust security that embodies a "sometimes trust, always verify" approach.

To implement this pared-back Zero Trust strategy, Loveday still needed a platform that made it easy to implement microsegmentation down to the workload level. All roads led to Illumio.

"Once we decided this was the problem to solve, choosing Illumio was a no-brainer," he says. "There's really no other product that can do what Illumio does."

By using Illumio Core, Loveday says ACH Group can now easily enforce segmentation access policies down to the workload, across the entire IT infrastructure. Loveday simply tags a given workload, then Illumio automatically assigns the right policy to each workload.

"With Illumio, we just set it and forget it," Loveday says. "It's ridiculously simple."

Results

Loveday says the visibility Illumio provides into application communications has been revolutionary and the key to its effectiveness.

"In one view, we can see everything that is going on," Loveday says. "We know exactly what is talking to what. And that has been eye-opening."

With Illumio, Loveday can map application dependencies, then use that information to set policy. Previously, he had to reference scattershot documentation that was incomplete at best.

Illumio also helps ACH define polices for blocking all but essential traffic, creating "deny lists."

By switching on enforcement one application at a time, Loveday can easily segment ACH Group's development, testing and production environments, something that was impossible previously.

But for Loveday, the best part about Illumio is how it is supporting his organization's mission to focus resources on its customers. Maintaining segmentation policies with Illumio only requires about 2 hours of staff time a week.

"Our overhead has been nearly zero," Loveday says.

> "Once we decided this was the problem we were going to solve, choosing Illumio was a no-brainer. There's really no other product that can do what Illumio does."
>
> **Jason Loveday**
> **Information Security Manager**
> **ACH Group**

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.