illumio

CASE STUDY

How an Australian School Built Enterprise-Grade Security for Ransomware Protection

St. Mary MacKillop College in Canberra, Australia turns to Illumio to safeguard against cyberattacks, secure student records and reassure parents

Industry: Education

Location: Canberra, Australian Capital Territory, Australia

Environment: On-premises data center with Linux and Windows servers; cloud platform (AWS); hypervisors

Challenge: Build out Zero Trust Segmentation cost-effectively with limited resources and staff

Solution: Illumio Core

Benefits: Preventing the lateral movement of cyberattacks and malware; full visibility into application traffic flows; boosting digital safety for students and their families

Business Goals

Parents want to know their children's school records are safe and secure. Yet cybercriminals find schools easy targets.

But St. Mary MacKillop College is changing that. By partnering with Illumio, the school is bringing state-of-the-art Zero Trust security to its organization, its students and their parents.

St. Mary MacKillop College is a private Catholic school in southeastern Australia that offers classes in grades 7 through 12. Founded in 1998 and named for Australia's first saint, the school operates under the governance of the local Catholic Education Office.

Protecting students — and their digital records — is a top issue for St. Mary MacKillop College. That's because it is a private school, meaning its parents pay annual tuition and other fees. If a school can't protect its data, parents can choose to enroll their children somewhere else.

Technology Challenges

Luke Bell, the college's network and security engineer, knew that Zero Trust Segmentation was a necessity for his organization, what he calls "the obvious way to go."

To implement foundational access control mechanisms required by Zero Trust security, Bell considered hypervisor solutions. But he found them too complex and limited.

Complexity, in particular, was a key consideration. St. Mary MacKillop's IT department — just four people in all — supports some 70 virtual servers and roughly 4,000 users including staff, students and parents.

Also, the school runs three IT environments: on-premises, cloud (AWS), and two hypervisors.

> "With Illumio, we went from nothing to basically full enforcement across our entire server infrastructure in just three weeks."

Luke Bell
Network and Security Engineer
St. Mary MacKillop College

Bell realized a traditional approach to micro-segmentation would be too complex for the small IT staff. He sought a Zero Trust approach would be viable for his small organization.

How Illumio Helped

Bell discovered Illumio at a conference. "With the first demo, I was wowed," he says. "Illumio seemed so elegant and simple."

That first impression led Bell to do further research. And he liked what he found.

Unlike hypervisor solutions that use network-level firewalls, Illumio uses the native firewalls on workloads or devices? That's a lightweight solution that doesn't interfere with ongoing operations or slow traffic.

Illumio's clever use of existing OS and network firewalls also makes Illumio highly scalable.

"It can go at least 100 times bigger than our installation," Bell says. "Whether we have 65 servers or 65,000, Illumio is totally capable."

Plus, Bell found that Illumio's pricing was competitive with that of the hypervisor solutions. And, unlike those options, Illumio can handle the school's mix of on-premises servers, infrastructure-as-a-service (IaaS) and hypervisor environments.

> "The fact that we're small made very little difference to Illumio as a product. Whether we have 65 servers or 65,000, Illumio is totally capable."
>
> **Luke Bell**
> **Network and Security Engineer**
> **St. Mary MacKillop College**

"Otherwise," Bell says, "we would have needed three micro-segmentation solutions."

Results

St. Mary MacKillop College rolled out Illumio in about three weeks. Then Bell started building rules for a few noncritical applications. Once he tested those and got a feel for how Illumio worked, he moved on to methodically expanding micro-segmentation protection for the school's core applications that house student records and financial information.

Now that he has used Illumio for several months, he says its application dependency map has been a revelation. With it, he and his staff have also gained full visibility into the school's IT assets.

That has helped Bell discover — and remediate — unencrypted applications (including one database), several incorrectly set up servers, and dangerously open ports on unmanaged endpoints such as printers, copiers and IoT devices.

Importantly, Illumio is now in place to halt the lateral movement of any ransomware attack.

"I sleep easier now," Bell says. "And we can tell our parents that we're one of the few schools with Zero Trust security in place. Some people have actually enrolled their children here because they know we take security more seriously than other schools."

Help for Zero Trust

Contact us today to learn more about how Illumio quickly and easily pinpoints systems at risk and isolates breaches to keep your organization safe.

About Illumio

illumio

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit https://www.illumio.com/what-we-do and engage us on LinkedIn and Twitter.