Insignia Financial Contains Risk, Simplifies Security, and Strengthens Compliance

How one of Australia's leading wealth management companies improves visibility, reduces complexity, and limits the impact of cyber incidents.

Building resilience in a complex, regulated environment

Insignia Financial manages more than AU$320 billion in assets and serves more than two million Australians. As part of the country's critical infrastructure, the company faces high expectations for cybersecurity.

After merging three large organizations, Insignia Financial had a fragmented IT environment and needed to uplift that environment quickly to protect financial systems and meet high regulatory requirements.

"We're considered critical infrastructure in Australia," said James Ng, GM Cyber Security and Chief Information Security Officer (CISO) at Insignia Financial. "That comes with a responsibility to our customers and to the financial system as a whole."

Recent breaches across the country in a variety of industries raised the stakes. With regulators increasing focus and attackers growing more aggressive, Insignia Financial knew it needed more than firewalls; it needed an ability to contain threats before they could spread.

Insignia™ Financial

Industry
Financial services

Environment
Hybrid: private data centers and cloud

Challenge
Integrate and extend security across three merged organizations with the objective of reducing complexity and improving resilience against cyber threats.

Use Cases
- Asset mapping & visibility
- Compromised asset containment
- Critical asset protection

Benefits
Rapid visibility into risky traffic and legacy behaviors; reduced time and impact of active incidents; faster return on investment with macro to micro segmentation; tool consolidation and reduced operational burden.

Too many vendors, too little visibility

Post acquisitions, Insignia Financial was managing more than 40 different security vendors. "We had three of everything — it was operationally unmanageable."

The team started with macro segmentation — creating broad zones to separate major systems and reduce cross-network risk. This provided the foundations to progressively achieve incremental benefit whilst maturing towards microsegmentation for fine-grained visibility to ringfence and contain assets. Legacy systems made that harder — some couldn't support endpoint agents, which left inconsistencies.

"We needed a way to reduce risk without waiting until every tool and every asset was perfect," said Ng. "We couldn't afford to let perfect be the enemy of progress."

From prevention to containment — and everything in between

Insignia Financial leveraged Illumio to take better control. Its host-based segmentation gave the team immediate visibility and insights. "From the moment we deployed in passive mode, we were able to identify risk behaviors," said Ng. "RDP where it shouldn't be, SSH in unexpected places — it was all there."

"The team used this visibility to route network traffic to internally approved solutions. This visibility and control was also valuable when we identified suspicious network traffic. We were able to leverage Illumio to ring-fence assets in real time," said Ng. "It bought us the time we needed to investigate without impacting the business. That was a big win."

Results

Real-time visibility across a complex environment
Insignia Financial has immediate insight into traffic across its data centre workloads — identifying risky behaviors and legacy practices before they become incidents.

Active containment to minimize business disruption
Insignia Financial leveraged Illumio Segmentation capability to isolate and contain identified suspicious assets to allow internal investigations to be completed without impacting business operations.

Support for Zero Trust across merged organizations
Illumio helps enforce segmentation across disparate environments, streamlining operations and strengthening Insignia Financial's Zero Trust posture.

Tool consolidation reducing complexity
By eliminating duplicative vendors and surfacing actionable telemetry, Insignia Financial reduced complexity and improved control.

About Illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.