Resolution Life

CASE STUDY

Security exemplified for Resolution Life Australasia

Resolution Life Australasia turned to Palo Alto Networks for a unified cybersecurity platform upholding the trust placed in them by their customers.

paloalto NETWORKS

IN BRIEF

Customer

Resolution Life Australasia

Product and Services

Acquisition and management of portfolios of life insurance policies

Industry

Insurance

Organization Size

1,000+ employees

Country

Australia

Website

www.resolutionlife.com.au

Challenges

Resolution Life acquired the AMP Life insurance business in 2020 (now Resolution Life Australasia) and as a result needed to ensure the smooth separation and set up of a new platform for secure sensitive customer information to meet stringent regulatory requirements.

Requirements

+ Secure by design
+ Security platform consolidation
+ Data-driven outcomes and metrics
+ Cloud-native security
+ Trusted cybersecurity partner

Solution

+ Resolution Life Australasia selected the Palo Alto Networks platform, comprising of VM-Series Virtual Next-Generation Firewalls (NGFWs), Panorama, Prisma Access, Prisma Cloud, Cortex XDR, Cortex XSOAR, Cortex Data Lake and Cloud-Delivered Security Services (CDSS), such as Threat Prevention, URL Filtering, GlobalProtect, and WildFire.

In 2018, Resolution Life, a well-known market leader in the global life insurance group, acquired AMP's life insurance business. Owned by Resolution Life, Resolution Life Australasia is one the largest life insurers in Australasia, serving 1.1 million customers and managing ~A$27billion in assets.

CHALLENGE

Building a best-in-breed infrastructure from scratch

After the acquisition and separation of AMP Life from AMP, the Resolution Life Australasia team was presented with the freedom to create something of their own design and direction, which they harnessed into best-in-breed cybersecurity services. Their task's uniqueness was not just characterised by the fact that it had to secure services that were being built in a greenfield environment. Resolution Life is an in-force specialist life insurer dedicated to servicing their existing customers, providing them with competitive premiums, quality investment management, excellent customer service, and efficient claims management. Instead of selling new life insurance products to new customers, its growth comes from the strategic acquisition of complementary life insurance businesses and portfolios.

"Our business effectively operates as a cycle of growth, consolidation, and optimisation from an IT standpoint, with somewhat predictable moves up and down. We needed to ensure smooth transitions in scale both up and down with consistent levels of security," says Rob Jillson, Head of Cyber Security at Resolution Life Australasia, and the project's architect. The team was on a tight schedule and looked to minimise the number of vendors and products in order to maximise efficiency.

A delicate balance of securing sensitive personal information and adhering to regulatory compliance

Adding to the complexity of building a new environment in a short period of time was the collection and protection of sensitive personal and health information which posed a unique challenge.

The type of information—personally identifiable information (PII)—that organisations like Resolution Life hold, is extremely valuable to cybercriminals. Jillson elaborates further, "When thinking about cybercrime, people often think credit card fraud is the worst thing that can happen. However, identity theft, which can come from cybercriminals exploiting the kind of information we are managing, may only be discovered years later and can follow you for life. Legal bills can pile up, identities used for illegal immigration, and doctors can even be targeted for falsified prescriptions."

"We needed to ensure that we safeguarded our clients confidential personal and health information while adhering to a strict regulatory environment. Being compliant does not guarantee that information is secure and being secure does not guarantee compliance with regulatory obligations. We took the time to ensure we not only meet the letter of the regulatory obligations, we also meet the spirit of the obligations. We needed a partner whose expertise could help us think through the requirements, avoid decision fatigue, and help create a best practice model—which we did through Palo Alto Networks," explains Jillson.

All organisations that collect personally identifiable information are required to be compliant with the Privacy Act 1988 and the Notifiable Data Breaches (NDB) scheme. For organisations that fail to comply with the Privacy Act 1988, there would be both financial and reputational risks. Beyond the regulatory requirements, Resolution Life Australasia is committed to upholding the trust placed in them by their customers through a security-first approach.

REQUIREMENTS

Prioritising security and automation

Resolution Life Australasia had to fulfill a number of requirements to help them build the cybersecurity infrastructure required to support business growth, safeguard their customers' sensitive personal and health information, trust, and adhere to regulatory requirements:

- **Secure by design**
- **Security platform consolidation:** Minimise hardware, software, and cloud vendors to a single vendor for efficiency and ease of management.
- **Data-driven outcomes and metrics:** Ensure that all cyber services were measurable and quantifiable security benefits.
- **Cloud-native security:** For effortless change in scale and adoption of evergreen principles.

- **Trusted cybersecurity partner:** To upload strong cyber governance and provide assurance that chosen solutions will continue to operate at desired expectations.

These requirements go hand-in-hand to ensure that the chosen solution can integrate with Resolution Life Australasia's cybersecurity infrastructure and prioritize automation for future-proofing.

SOLUTION

Security simplified and exemplified

The three pillars of cybersecurity—people, process, and technology—is something that Jillson strongly believes in. On the technology front, Palo Alto Networks was the partner of choice for Resolution Life Australasia due to the completeness of its platform and the ability to integrate, customise, and automate. In fact, there is a large number of technical controls based on the technology that Palo Alto Networks provides.

Prior to the COVID-19 pandemic, Resolution Life Australasia had already started migrating to cloud-delivered security with Prisma Access and had begun implementing security policies. This proved to be valuable during the pandemic. Jillson shares, "With Prisma Access, regardless of where our staff are working from—be it the home, office, or a Wi-Fi-enabled cafe—we can be assured of a consistent security and end-user experience."

The Palo Alto Networks platform, VM-Series Virtual Next-Generation Firewalls (NGFWs), Panorama, Prisma Access, and Prisma Cloud, is complemented by the suite of Cloud-Delivered Security Services (CDSS) including, Threat Prevention, URL Filtering, GlobalProtect, and WildFire. This reduced Resolution Life Australasia's security stack while ensuring the detection and prevention of advanced threats to their business.

> We needed a partner whose expertise could help us think through the requirements, avoid decision fatigue, and help create a best practice model—which we did through Palo Alto Networks.
>
> **— Rob Jillson, Head of Cyber Security, Resolution Life Australasia**

Cortex powerhouse of XDR and XSOAR

Using a traditional SIEM, the Resolution Life Australasia team had to manually pull the logs and write the correlation rules. With Cortex XDR and Data Lake, rich data is collected for behavioral analytics and AI while automatically correlating data to gain context for investigations, saving the operations engineers time on monitoring, investigation, and response. Instead, the team can now zone into the threat and take the necessary action.

Given the sheer speed and scale that cyberthreats are moving at, Jillson and his team opted for Cortex XSOAR to help optimise operations through a security orchestration, automation, and response (SOAR) strategy. Through the integration of threat intelligence with automation in a single pane of glass, Cortex XSOAR provides the security team with the ability to automate repetitive tasks instead of having to manually follow a set of actions to take. This enables the security team to scale and standardise incident response processes, speed up resolution time, and increase productivity.

Through the ingestion of alerts and IoCs via the SIEM and Cortex XDR, Cortex XSOAR is being leveraged for metrics and reporting. With over 900 out-of-the-box playbooks to automate and orchestrate any security use case, this aided Resolution Life in their security orchestration and automation capabilities. "80% of the modules and playbooks being utilised were out-of-the-box. The customisation process was extremely seamless as we often only had to make minor tweaks to tailor the available playbooks to our needs," shares Jillson. In summary, Jillson shares that he "can't say enough about Cortex XSOAR—we are thrilled with it. Two years in the journey a vast majority (69%) of all cyber incidents now have fully automated triage and resolution. Other events are deeply enriched with threat intelligence and consolidated event information for quick and decisive response by our Cyber Operations team, providing us with consistency and scale in our ability to respond to today's highly automated attack techniques used by cybercriminals."

"Cortex XDR, Data Lake, and Cortex XSOAR was a powerful combination—it allowed us to realise the benefits of automation to support a next-generation SOC. We wanted to build services with 'audit built-in' that would stand up to internal/external audit and regulatory scrutiny with defendable metrics. This would provide our senior leadership, risk, and audit teams, and myself with assurance that our security controls are effective and comply with our clients' expectations to safeguard their information, regulatory obligations, and control objectives with live dashboards," says Jillson. With Cortex XDR, Data Lake, and Cortex XSOAR, the unified platform strategy is now complete.

> Cortex XDR, Data Lake, and Cortex XSOAR was a powerful combination—it allowed us to realise the benefits of automation to support a next-generation SOC. We wanted to build services with 'audit built-in' that would stand up to internal/external audit and regulatory scrutiny with defendable metrics.
>
> **— Rob Jillson, Head of Cyber Security, Resolution Life Australasia**

BENEFITS

Resilient capabilities for adequate protection and actionable insights

The Palo Alto Networks platform has enabled Resolution Life Australasia to take automation to the next level. The integration of the suite of products has enabled actionable threat intelligence, helping to future-proof Resolution Life Australasia and safeguard their customers' trust, on top of their personal and health information.

A unified approach to cybersecurity that allows for at-scale security by design

Resolution Life Australasia found the deployment process smooth and relatively effortless, with a majority of the Palo Networks products being either turnkey or cloud based. This resulted in time savings for the team to focus on investigations and actionable threat intelligence.

With Palo Alto Networks, Resolution Life Australasia can safely say that they can scale, automate, integrate, and continually improve their capability maturity model. This capability is required to keep up with the fast-changing cyberthreats and increased regulatory compliance requirements.

CONCLUSION

In less than three years, the team built the entire capability from scratch, with approximately 38 cyber services commissioned. Jillson credits the trust built between teams and the shared ownership as the biggest drivers of the program—the success of which was immediate.

"Having a single partner to secure our entire environment was definitely an ambitious task. However, we were reassured of the outcomes as we have been able to deliver on time and on budget. We have been impressed by the constant innovation and creation of new features and integrations for the Palo Alto Networks platform. Palo Alto Networks plays an integral role in safeguarding the trust of our customer and we can't imagine a future without them," shares Jillson in conclusion.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com