Axe Group Combines Innovative Startup Culture and Rigorous Security Practices with CrowdStrike

The Axe Group ("Axe") is a leading insurance software solution specialist headquartered in Sydney with staff Australia-wide. Axe provides the latest InsureTech solutions to its clients in Australia and New Zealand so they can stay ahead of the competition. Its core product is Axelerator — an innovative, modular, and fully flexible SaaS platform designed specifically for the needs of insurers and reinsurers, processing over AU$7 billion in policies and claims every year.

With its solution delivered from AWS cloud infrastructure, Axe's main security concerns are the availability of the service for clients, maintaining data sovereignty, and protecting sensitive client information and personal and financial data residing on the platform. Axe also has to ensure it is meeting its clients' stringent regulatory compliance obligations.

Originally a startup that has developed its software platform over the last two decades, Axe has maintained a lean and agile team focused on innovation and the strategic direction of the business and its products. However, prior to CrowdStrike, Axe had a limited security environment relying on basic endpoint protection and native AWS and GCP tools. Axe's security team had no visibility on known vulnerabilities in its environment, nor any ability to identify any existing or emerging threats.

"This led to a notable influx of false positive alerts, and we encountered a lack of contextual information or guidance to prioritize and address the relevant alerts," said Gaurav Verma, Head of IT Risk and Security, Axe Group.

Axe completed proofs of concept with a number of endpoint detection and response (EDR) solutions and chose CrowdStrike for its anti-tampering protection and on the basis of its superior detection and blocking capabilities, which are based on behavioral analysis augmented by AI and machine learning.

"In the initial year, we exclusively deployed CrowdStrike on our endpoint systems. The positive experience prompted us to extend this protective measure to encompass our cloud infrastructure," said Verma.

"In the event that we require assistance from CrowdStrike, their accessibility is consistently reliable, addressing both technical and non-technical issues. The caliber of their support is truly exceptional."

Gaurav Verma, Head of IT Risk and Security, Axe Group

INDUSTRY

Insurance/Software

LOCATION/HQ

Sydney, Australia

CHALLENGES

- Meeting clients' stringent security compliance requirements with a small in-house team
- Balancing robust security practices and controls with an agile, innovative startup culture
- Managing rapid growth and scale on public cloud production and test and development environments

SOLUTION

Initially engaging CrowdStrike's managed endpoint detection and response (MDR) services, Axe Group extended the Falcon Complete team's remit to include cloud workload protection to help ensure the availability and security of its core SaaS platform running on AWS. This enables Axe to maintain a lean and agile in-house team that can focus on strategic issues, and helps ensure Axe is meeting the stringent security and regulatory compliance requirements expected from its insurance clients.

Maintaining a Lean In-house Security Team

Axe expanded its relationship with CrowdStrike, using the CrowdStrike Falcon® Complete managed detection and response (MDR) service, which also extends to managing cloud security. That enables Axe to offset Levels 1 and 2 security operations to CrowdStrike, allowing Axe to keep a lean and agile startup team that can focus on Level 3 and strategic aspects of security.

Axe has integrated CrowdStrike Falcon with Slack so the entire team sees every alert received. That's made it very easy for the Axe security team to take immediate action.

“The Falcon Complete team has played a pivotal role in minimizing our endpoint alerts to a monthly occurrence and cloud alerts to once or twice a week," said Verma. "This has resulted in significant time savings, enabling us to redirect our focus towards governance, risk and compliance processes, as well as exploring new solutions and technologies. As an example, we are currently deliberating on our AI usage policy.”

At the same time, Axe is also able to meet the stringent security and compliance requirements from its insurance clients.

As part of its regular compliance and audit processes, Axe has conducted regular internal penetration tests with the Red Team typically able to compromise and take control of endpoints in the environment. However, after engaging Falcon Complete, it was a different story.

“When we did the same internal exercise last year, the attacker was not able to get a C&C [command and control] connection out of the machine, which was blocked on the fly by Falcon,” said Verma. “CrowdStrike was not aware that we were doing an internal pen test at the time but in less than 10 minutes I got a call. The experience from the Falcon Complete team was incredible — I was not expecting them to take action that quickly.”

Managing Shadow IT

As with many software development companies with easy access to cloud infrastructure, Axe had struggled in managing shadow IT infrastructure. In the past, Axe's security team was not always aware of developers running up servers and applications on AWS instances, which meant these applications and workloads were missing AWS protections and were outside normal security controls.

The addition of CrowdStrike Falcon® Cloud Security has ensured better protection and control to support Axe's expansion of its cloud footprint with AWS and GCP. The CrowdStrike Falcon solution automatically scales to immediately manage and protect new instances when they are created.

“We have very good visibility now into containers, and we can see exactly what services are running in Kubernetes. If it is malicious, then it is blocked by CrowdStrike on the fly. I've seen some of the alerts which were triggered by the Falcon Complete team, but 90% of them are resolved by CrowdStrike — we don't even need to look at them,” said Verma.

The CrowdStrike Falcon cloud security posture management (CSPM) dashboard enables Axe to generate reports on compliance with either Center for Internet Security (CIS) or National Institute of Standards and Technology (NIST) benchmarks, and helps during the audit process for Axe to maintain its PCI DSS and SOC 2 Type II certifications.

RESULTS

- Helps meet the security and regulatory compliance obligations required by the insurance industry
- Manages core security 24/7/365, which has allowed Axe Group's in-house team to focus on strategic issues
- Provides visibility for Axe across the entire cloud environment and ensures DevSecOps while working toward a Zero Trust model

ENDPOINTS

300 endpoints, workstations and AWS workloads

PRODUCTS

CrowdStrike Falcon® Prevent

CrowdStrike Falcon® Insight XDR

CrowdStrike® Falcon OverWatch™

CrowdStrike Falcon® Discover

CrowdStrike Falcon® Cloud Security

CrowdStrike Falcon® Premium Support

“It is saving us time because we don't need to reach out to DevOps or any other team to look at whether or not our systems are compliant with CIS benchmarks. With a single click on the Falcon CSPM dashboard, I can see everything.”

Axe is also using the CrowdStrike Security for Jenkins plugin for its development team to use the automated assessment to find vulnerabilities in container images early in the development process (i.e., “shift left”) and then block them per predefined policies within the Falcon platform. The process requires the developer to attach a screenshot from Falcon showing the assessment as part of the approval workflow.

Verma cites a couple of scenarios where this can make a big difference. “If one of the DevOps team members makes a mistake in a test environment by leaving an S3 bucket public, CrowdStrike would send us an alert. Similarly, we get an alert from CrowdStrike when an EC2 security group is publicly accessible. I can check internally with the DevOps team to confirm if it’s a business requirement to make it public.”

Supporting Future Growth

Axe has seen exponential growth over the past few years and is set for continued expansion, with infrastructure set to scale up by 40% to 50% in the coming years. CrowdStrike has already demonstrated its ability to scale with the technology, and Falcon Complete offers Axe a much more cost-effective alternative to expanding its in-house team.

“Falcon Complete represents extremely good value because the security resource cost in Australia is very high,” said Verma. “The Falcon Complete team is working 24/7/365 doing end-to-end monitoring, blocking, and then alerting us 24 hours a day. If I had to hire a team to run my own SOC, it would be ten times the cost.”

Axe is also moving to a Zero Trust model and putting a lot of effort and technology in the Zero Trust framework.

“We are focusing on “POLP” — the principle of least privilege — and CrowdStrike is helping with the implementation of that framework. In the event that we require assistance from CrowdStrike, their accessibility is consistently reliable, addressing both technical and non-technical issues. The caliber of their support is truly exceptional,” concluded Verma.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world’s most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Start Free Trial →

Learn more **www.crowdstrike.com**