CASE STUDY

eSENTIRE

PKF Melbourne

Outsourcing 24/7 SOC-as-a-Service and threat detection and response enables PKF Melbourne to get around-the-clock monitoring, deep visibility, and minimise threat actor dwell time.

The Organization

PKF Melbourne is a full-service accounting firm that provides financial solutions to private businesses and individuals for personal and professional needs. Operating through a franchise model, PKF Melbourne is a member of the PKF international network that collaborates with 220+ firms across 150 countries.

- Serves national and international customers
- Supports 30+ different applications and large amount of sensitive data that needs to be protected to meet compliance requirements
- Needed a strategic partner who could provide expert-level 24/7 threat detection and response, help them consolidate their tools, and build a stronger cybersecurity strategy

Solutions and Results

The eSentire Managed Detection and Response (MDR) solution includes:

- **eSentire MDR for Network** for 24/7 network traffic monitoring across on-premises and cloud environment, automated threat blocking, and minimise threat actor dwell time.
- **eSentire MDR for Endpoint** to safeguard against cyberattacks with best-of-breed CrowdStrike endpoint technology and access to world-renowned threat intelligence expertise.
- **eSentire MDR for Log** for 24/7 active log monitoring to deliver critical multi-signal visibility, ensure compliance, offer a system of record across their environment, and expert guidance from the eSentire Blue Team.

Business and Security Outcomes

- Around-the-clock security event monitoring with 24/7 threat detection, investigation, and response with a 15-minute Mean Time to Contain by a team of SOC Cyber Analysts and Elite Threat Hunters
- Trusted expert-level guidance to analyse their security measures and rapidly deploy eSentire MDR services
- Unlimited threat hunting, original threat research, and regular updates to runbooks, detection rules and machine learning models from eSentire's Threat Response Unit (TRU) to help PKF stay ahead of the latest threats
- Reduced cyber risk by ensuring complete visibility and a consistent security posture across their environment
- Consolidated security tooling and unified cybersecurity strategy
- Outsourced and managed solution approach frees up IT staff to focus on core responsibilities

The Challenge

In recent years, there has been a significant uptick in threat actors targeting Australian organisations. This has led many businesses to take cybersecurity more seriously and outsource 24/7 Security Operations Center (SOC) as well as threat detection and response capabilities rather than handling them in-house. PKF Melbourne is no different.

One factor that complicates their approach to cybersecurity is adhering to the guidelines set by the PKF Global organisation and the PKF Australia member firm. Each member firm is required to meet certain requirements around their IT infrastructure to ensure their data and IT environment is secure.

Prior to working with Advanced Visions Technology (AVTech), a Managed Services Provider (MSP), PKF handled most of their security solutions in-house. As they scaled operations, managing too many point security solutions in-house became challenging and they needed to consolidate their security stack, leading them to consider a Managed Detection and Response (MDR) provider.

"As our infrastructure and office grew, we realised that there was a need to consolidate and have a better security strategy that provided better support and overall security," Oscar Ortiz, IT Manager at PKF Melbourne, said.

Plus, as a full-service accountancy firm, they have access to, and store, extremely sensitive financial data for their clients. They also needed to make sure that their staff have cybersecurity awareness training to mitigate the impact of the social engineering tactics, such as phishing, business email compromise, and search engine optimisation (SEO) poisoning attacks.

"Due to the sheer amount of valuable financial data accounting firms hold, we can be considered prime targets for cyberattacks. This was one of the reasons why we decided to obtain a MDR solution," Oscar said.

Additionally, PKF Melbourne had successfully transitioned to a hybrid working model so they needed a fully managed security solution that could protect their users whether they were in the office, working remotely, or at a client site. This would lift some burden off their IT staff and enable them to have 24/7 protection without needing to maintain 24/7 coverage themselves.

"We wanted to make sure that in the event of a threat, it was detected in the fastest time possible to minimise the impact of any security incident."

Since PKF Melbourne wanted to prioritise security tool consolidation while having access to 24/7 threat detection and response, they decided to outsource to an MDR provider that offered a cost-effective, all-in-one service with 24/7 SOC-as-a-Service.

Why PKF Melbourne Chose eSentire As Their Proven MDR Partner

Having an IT Security team build and manage their overall cybersecurity program in-house was incredibly challenging. While their IT staff had security solutions like anti-virus/malware applications, firewalls, email security, and security awareness training programs in place, the team was overwhelmed with balancing their day-to-day IT operations with cybersecurity.

Although the firm's operations were growing, it was difficult to hire skilled employees so they could get true around-the-clock coverage across their entire attack surface.

Moreover, PKF Melbourne had also partnered with AVTech, a leading MSP in the APAC region, to ensure their systems were secure and up-to-date through proactive monitoring and managed services. Seeing PKF's growing needs, AVTech identified that they wouldn't be able to provide 24/7 SOC coverage and threat detection and response capabilities.

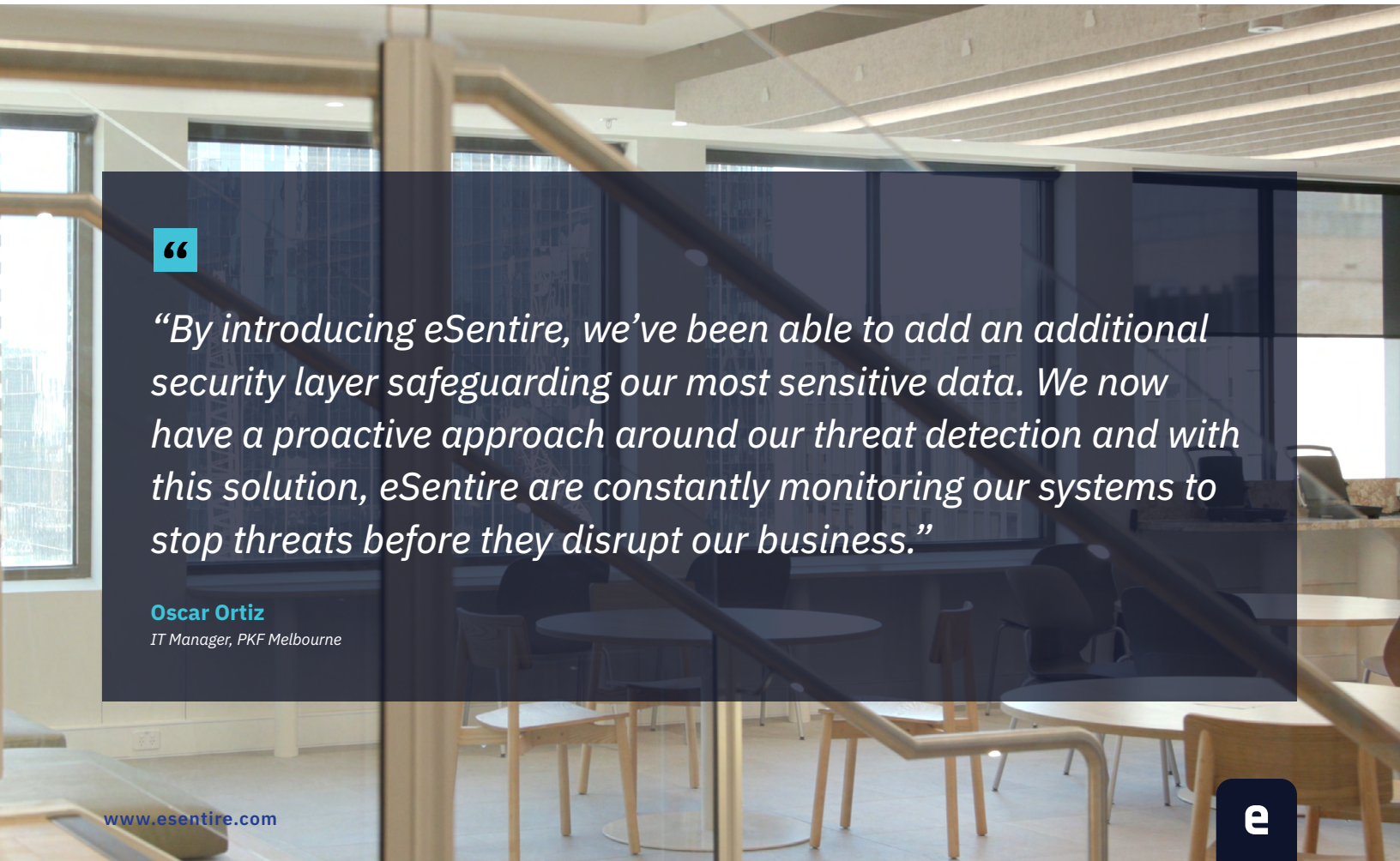
After researching different MDR providers, PKF Melbourne and AVTech chose eSentire MDR to fill this gap, largely due to the responsiveness of the SOC team, global reach, and access to highly skilled security experts.

"eSentire's SOC is known for its responsiveness. With a mean time to contain the most sophisticated threats in 15 minutes, they're available 24/7. Just pick up the phone and they will answer straight away," Oscar says. "We have eSentire's large pool of security experts monitoring and protecting our network 24/7, saving us the need to build and staff our own SOC."

To help PKF Melbourne get true 24/7 global coverage and complete visibility into their environment, we implemented eSentire MDR for Network and eSentire MDR for Endpoint, powered by CrowdStrike.

Two additional factors that were critical for both PKF Melbourne and AVTech were the onboarding experience, which had to be very low impact to PKF, and having multi-signal visibility while seamlessly integrating with the existing infrastructure.

Thanks to an average onboarding timeframe of 14 days and 300+ technology integrations that provide true muti-signal coverage, eSentire was able to differentiate itself on both counts.



> *"By introducing eSentire, we've been able to add an additional security layer safeguarding our most sensitive data. We now have a proactive approach around our threat detection and with this solution, eSentire are constantly monitoring our systems to stop threats before they disrupt our business."*

Oscar Ortiz
IT Manager, PKF Melbourne

Conclusion

Protecting sensitive data and defending against advanced cyber threats are core priorities of any financial services firm. Only a robust, multi-layered defense strategy can help financial firms safeguard against malicious threat actors and avoid business disruption.

By outsourcing their security monitoring and threat detection, investigation, and response to our 24/7 SOC Cyber Analysts and Elite Threat Hunters, PKF Melbourne was able to get around-the-clock security event monitoring, deep visibility across their entire attack surface, and minimise threat actor dwell time.

They can trust that eSentire will act on their behalf to contain and remediate the threat before notifying them of the activity and work with them to determine if any other steps need to be taken.

Plus, in an economy where every security leader is being asked to consolidate their spend and maximise their security investments, eSentire provides PKF Melbourne with an all-in-one solution with unlimited threat hunting and unlimited incident handling.

“With eSentire, we get unlimited threat hunting and continuous protection from the SOC for our local and global staff as well as clients who access our network. This gives PKF peace of mind and security and helps us sleep at night.”

Ready to get started?

To learn how eSentire MDR can help your organization reduce your cyber risks and build a resilient security operation, connect with an eSentire cybersecurity specialist today.

CONTACT US

IF YOU’RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSENTIRE