

Defend against advanced security threats

Yes



Leverage the deep threat intelligence of Optus Managed Defense Powered By FireEye® to help proactively protect against both traditional and advanced security threats and help deliver a fast and effective response.

Highlights

Monitoring by experts.

Expert security analysts reviewing, investigating and prioritising alerts 24x7 from patented FireEye technology, aiming to reduce average threat detection and response time.

Applied intelligence.

Mobilises the latest tactical intelligence from across the FireEye global defence community to find threats in your environment faster.

Answers, not just alerts.

Validated compromise reports contain information about attackers, what we believe are their intentions, and guidance on how to respond.

Your adversaries create new malware, probe for vulnerabilities and vary tactics until they gain entry. Once inside, they blend in with their surroundings and may move across your organisation undetected, watching and learning about your employees and your network. They then formulate their plan of attack and wait patiently for the right moment to strike. When the time is right they can exfiltrate highly sensitive and confidential information about your business leaving behind very little trace that they were ever there.

Optus Managed Defense provides a last line of defence against advanced security threats that can evade traditional security solutions. We help protect against signatureless, zero day attacks, unknown threats and targeted threats that are increasingly complex and present significant risk to your business and your customers.

Our solution helps deliver continuous threat protection by monitoring your environment 24x7 with patented FireEye virtual-machine based technology augmented by expert security analysts.

Research has shown that on average sophisticated threats remain undetected for 146 days meaning that your organisation could be exposed to potential malicious activity for months without you knowing.

Our Managed Defense service helps to reduce the time it takes to detect threats.

Our team augments your in-house security teams' expertise to analyse data, undertake remediation, make configuration changes and respond to the threats that matter most. We assess the risk of each attack and assist you to rapidly contain compromised systems and devices, so you can resolve incidents more quickly and minimise damage to your reputation and business operations.

We help you to understand the behaviour of attacks by reconstructing the attack kill-chain – who is attacking you, what we believe their intention is, and how you should respond. Contextualising alerts in this way helps to improve incident response.

Rather than just sending details of alerts of known threats, Managed Defense is a proactive solution that sends you details of new and previously unknown threats. Alerts that can be acted on immediately. That's where our Managed Defense solution can make all the difference.

¹Mandiant Consulting M-Trends 2016 Report <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html/>

Intelligence

FireEye has discovered 28 out of 46 zero-day exploits since 2013

Front line Intel from incident response

Millions of network and endpoint sensors

Hundreds of Intel and malware experts

Hundreds of threat actor profiles

Expertise

Go-to responders for security incidents

Hundreds of consultants and analysts

Unmatched experience with advanced attackers

Technology

Identifies known and unknown threats – even those that do not use malware

Integrated to protect across all major attack vectors

Patented virtual machine technology



Optus Managed Defense supplements your traditional security posture with the technology, intelligence and expertise to properly secure against advanced attacks.

Continuous monitoring™

To help scale your security team, Managed Defense constantly monitors subscribed systems and informs you when alerts require follow up.

Proactive advanced threat prevention (ATP) and zero-day alerts—When we detect an ATP and/or a zero-day attack, our analysts provide a proactive notification with intelligence context so you can follow up on the attack as soon as possible.

Intelligence reporting—You receive monthly reports and alerts about emerging industry-specific threats. The report communicates the risk severity and alerts subscribers to heightened industry or region-specific risks.

System health monitoring—For continuous assurance, you receive proactive notifications of potential issues that could compromise detection efficacy for all subscribed systems.

Continuous protection™

Accelerate your response with expert analysts that investigate alerts and provide detailed compromise reports for each confirmed threat.

Analyst investigation—Our team of expert analysts evaluate detected attacks 24x7. When a potential compromise is detected, the team performs an in-depth analysis on

affected systems to confirm the attack and delivers detailed reporting with actionable recommendations to remediate the threat.

On-demand “live response”—Analysts leverage system and network forensics on live systems to investigate, classify, and analyse the risk in real time. They then provide information on what exactly happened and recommendations on how to contain the threat.

Incident response and containment—The service provides validated compromise reports with technical advice, contextual intelligence, and the ability to contain compromised devices and pivot to incident response and remediation support when necessary.

Continuous vigilance™

Actively pursue adversaries in your network with expert analysts that use advanced analytical techniques to find attackers hiding in remote corners of your network.

Proactive hunting for adversaries—Based on intelligence about attacker tactics, techniques, and procedures, expert analysts and forensics specialists proactively hunt for signs of compromise and investigate your systems for attackers on your network, whether they are active or not.

Advanced investigative techniques—Our expert analysts use proprietary technologies and methodologies to investigate system artifacts,

perform full-packet capture, conduct netflow analysis, and reverse-engineer malware to detect indicators of compromise (IOC).

Attacker context and risk assessment—Gain deeper insights by leveraging exceptional insight into threat actor tactics, modus operandi, and geo-political context gleaned from front-line incident response work, extensive intelligence research, and 100,000+ hours of incident response activity by FireEye every year.

Beyond technology

Today's advanced threats are targeted and persistent. They are also often devastatingly effective at breaching an organisation's systems and stealing sensitive data.

Technology alone will not defeat a determined attacker.

You need top security experts monitoring your network and systems around the clock with advanced technology and the latest curated intelligence from around the world.

As a telecommunications provider, security is in Optus' DNA. We provide protection from the network through to your content and endpoints, including mobile devices. Partnering with FireEye and embedding their expertise and technology allows us to extend our range of managed services to deliver a more comprehensive defence for our customers against the latest security threats.

OPTUS

1800 555 937

optus.com.au/enterprise

[@optusbusiness](https://twitter.com/optusbusiness)

yesopt.us/blog

bit.ly/OBLinkedIn