Singtel Business

Product Brochure
Managed Defense Services

Outwit The Adversary. Elevate Your Defense.

The security landscape changes every day, as attackers devise new ways to circumvent traditional security defences. Technology alone is not enough. You need a new approach that relies on experts with front-line intelligence about changing adversarial tactics. With Singtel Managed Defense Services powered by FireEye™, detect and respond to cyber-threats in minutes, not months. You focus on your business. Let Singtel take care of security.

Singtel
Let's make everyday better

Managed Defense Services

A Security Approach that Works

The headlines are real. Companies all over the world are routinely hacked by professional attack groups using new malware, social engineering tricks, and zero-day exploit tactics. Sophisticated and elusive, these groups know how to cover their tracks and hide inside your network for months, leaving your organizational assets and reputation exposed and vulnerable.

Now is the time to establish a security posture that proactively defends against both traditional and advanced threats to accelerate incident response in minutes – not months. This requires a proactive defense with experts, intelligence, and technology to identify signs of compromise early, resolve security incidents quickly, and learn from the experience to prevent a recurrence.

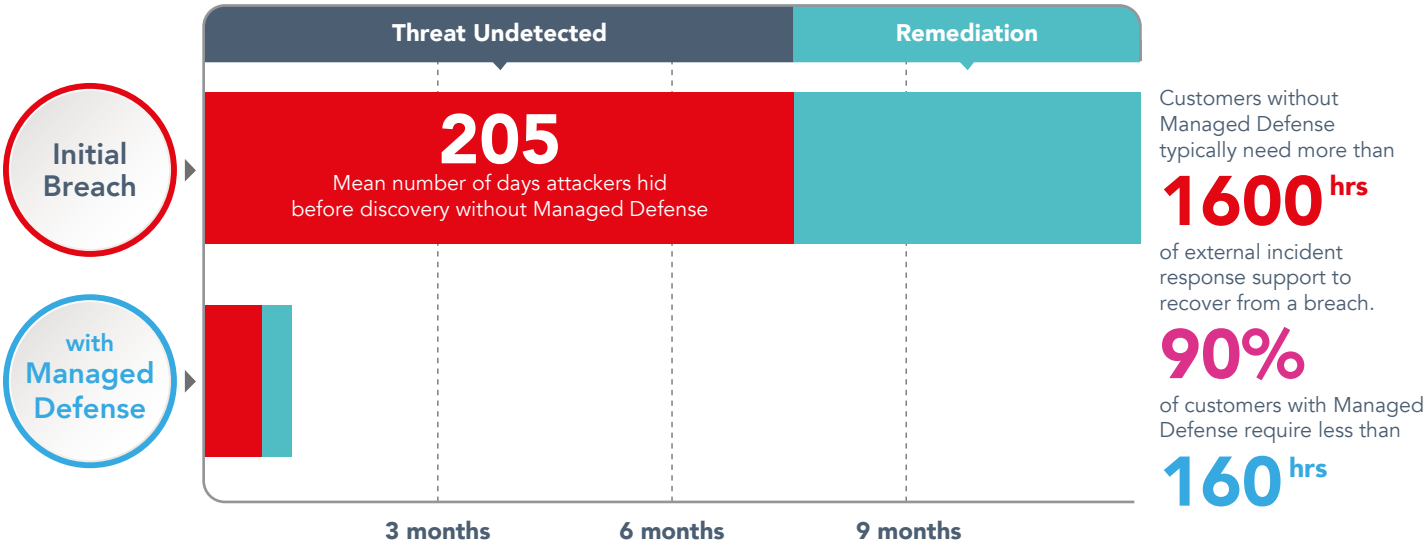
Benefits of a proactive security approach:

- Less business disruption
- Less risk of data and intellectual property theft
- Intact corporate credibility
- Avoidance of costs associated with a security incident

The result? Less business disruption, less risk of data theft, ongoing credibility without reputation damage, and avoidance of costs associated with a breach.

Elevate Your Defense

In 2014, advanced persistent threats went undetected for a mean of 205[1] days, before being discovered.



Source: Mandiant M-Trends Report

To defend yourself against these stealthy, persistent attackers, you need a comprehensive approach that enhances technology defences with expertise and threat intelligence to:

- Reduce the time between initial breach and detection from months to minutes
- Reduce the time and cost of incident response significantly

Singtel Managed Defense Services powered by FireEye™

Singtel Managed Defense Services, powered by FireEye™, is a subscription-based service offering proactive round-the-clock monitoring by security analysts applying the latest threat intelligence and an advanced security platform to quickly detect and contain incidents and help you respond effectively and efficiently.

Protect against both traditional and advanced threats Including known, un-known, zero-day, behavioral and targeted threats.	**Accelerate detection and response to minutes** With 24 x 7 x 365 monitoring and analysis, contextual compromise reports, and one-click containment.
Answers, not alerts By correlating and prioritising alerts with advanced threat intelligence, you have the context you need to take effective action.	**Continuous improvement of security posture** Deep insights, extensive intelligence and wide-ranging incident response experience enable you to stay ahead of evolving threats.

Singtel Managed Defense provides three critical components:

Expertise

Proactive hunting for signs of compromise, backed by 24x7 security operations center, deep malware analysis, incident response and threat assessment. Analysts have years of experience with advanced attackers and have developed profiles of threat actor groups. They will tell you what is happening and how to respond.

Intelligence

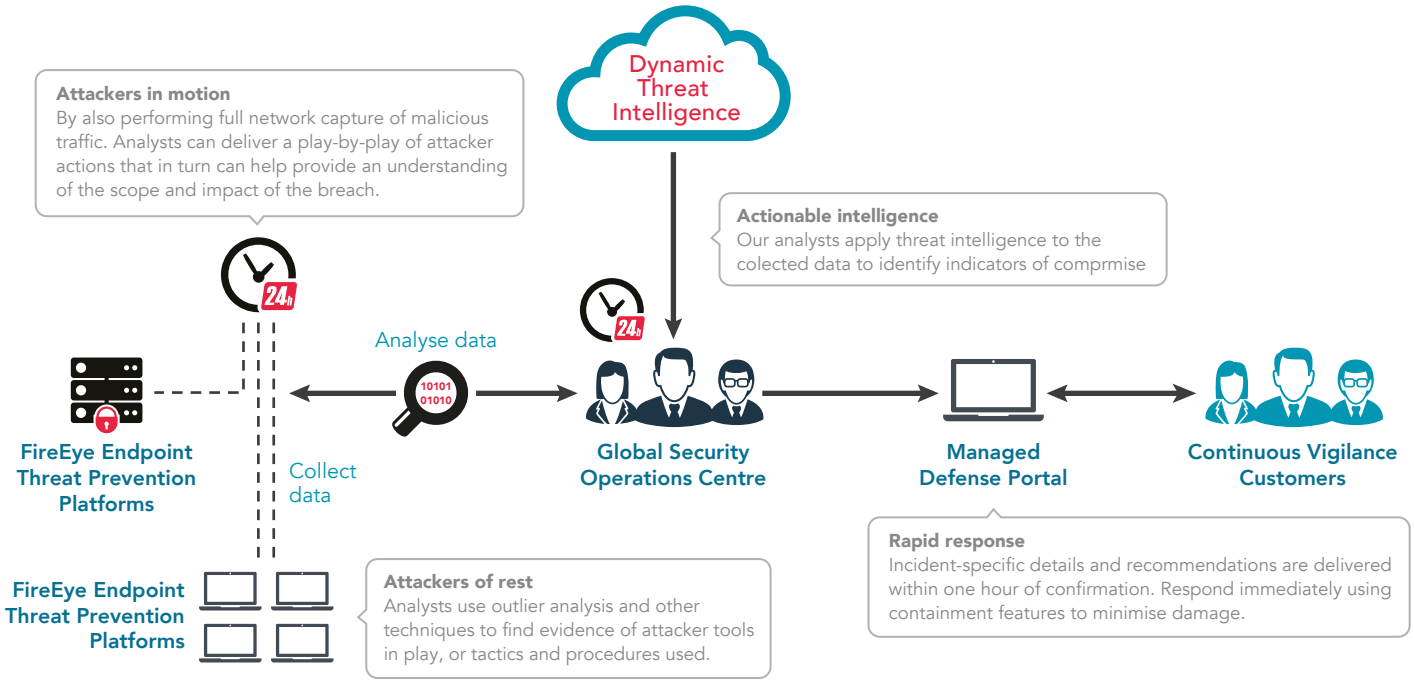
Know the enemy with access to strategic intelligence, threat actor profiles, and indicators of compromise.

Technology

The service is enabled by an advanced technology platform that monitors network, email, and endpoints to detect and block known and new threat tactics. Additional forensic tools enable our experts to investigate even deeper, hunting for signs of compromise that might circumvent technology defenses.

How It Works

Our experts monitor your system using FireEye technologies and apply their own investigative techniques and intelligence to hunt for attackers in your environment. When our analysts validate a compromise, they will provide you a report with the context you need to respond. With our service, there are no false positives. When you hear from us, it's a legitimate incident.



Singtel Managed Defense Services offer two subscription levels: **Continuous Monitoring®** and **Continuous Vigilance®**

	Continuous Monitoring®	Continuous Vigilance®
What it does	Augment your IT security team with 24 x 7 system health monitoring. We deliver proactive critical alerts that are prioritized for quick follow-up and periodic intelligence reports to stay informed about the changing threat landscape.	The most comprehensive service to investigate alerts and provide detailed compromise reports for each confirmed threat. Leverages proprietary analytical techniques to proactively hunt and contain attackers hiding in your network.
Key capabilities	• **Proactive notification**: We notify you right away when an APT or zero-day attack is identified, with advice on how to respond. • **Threat intelligence**: A private, secure portal provides the APT Encyclopedia and Intelligence Center for current information on specific APT actors and their tactics, techniques and procedures. Access periodic reports on emerging industry-specific threats, along with ratings on risk severity and heightened industry- or region-specific risks. • **System health monitoring**: Provide proactive notifications on potential issues that could compromise the health and detection efficiency of subscribed systems. Offer access to private, secure portal to review periodic system health reports anytime, anywhere.	• **Analyst investigation**: Team of analysts monitor for signs of intrusion 24x7. They conduct in-depth malware and forensic analysis of systems suspected to be compromised to confirm attack. They provide detailed reporting with actionable recommendations for remediation, which helps to prioritize incident response efforts. • **On-demand "Live Response"**: Our team performs real-time risk investigation, classification and analysis of live systems, backed by system and network forensics. They provide immediate information on what exactly happened and recommendations on threat containment. • **Incident response and containment**: Automatically quarantine with a single click any compromised systems on or off your network to impede any potential lateral movement within your network. Compromise reports provide contextual intelligence and technical advice. We will also provide sustained investigation of infected systems after containment, to uncover attack vectors and strategize remediation. • **Proactive hunting for enemies**: We leverage our latest intelligence on attacker tactics, techniques and procedures to proactively hunt for potential new threats that will compromise your systems. If we see it at one customer site, we look for it everywhere. A few of our tactics include full-packet capture, netflow analysis and reverse-engineering of malware to detect suspicious activities on your network and correlate them with behaviors of known attackers. • **Personalized intelligence reports**: We provide periodic intelligence reports with specific insights, key findings and recommendations crafted for your business. Reports include attacker context and risk assessment information including: identified attackers targeting your industry, key business indicators that motivate these attacks, and attack methodologies. • **Incident response**: We ensure a smooth pivot to incident response, when necessary, where our consultants arrive on-site to protect your business across all phases of the attack lifecycle. • **Threat Assessment Managers (TAMs)**: A single point of contact serves as your trusted advisor for information security, providing guidance on managed defense strategies. This helps us deliver a seamless, streamlined service experience.

Why Singtel?

Singtel Managed Defense Services complements Singtel Managed Security Services to deliver a comprehensive, end-to-end and integrated Enterprise Security Services suite, ranging from: managing security devices, security monitoring, to breach detection and managed defense.

Increase threat detection and cut response time: Early threat detection, contextual intelligence reports, and analysis and validation of compromises cuts incident response from months to minutes.

Peace of mind: 24x7x365 monitoring with Singtel Network Operations Centre and Security Operations Centre provides end-to-end visibility across corporate networks and Internet traffic – backed by Singtel's highly-experienced team of security experts, with domain knowledge and skills in security in:

- IT security incident management, response handling and investigation
- Vulnerability assessment and penetration testing
- IT security governance, risk assessment and compliance

Deeper insights and remediation recommendations with Singtel Security Threat Intelligence: Network and endpoint sensors within your networks combined with real experience on the front-lines of incident response give us exceptional visibility to stay informed of changing attacker tactics.

Ensure regulatory compliance: We centralise log and event collection, correlation and monitoring and ensure monitor your security devices, with configuration management, ongoing event aggregation, and correlation and alert monitoring.

Entrust your security to Singtel Managed Defense Services. Armed with leading security expertise, deep threat intelligence, and an innovative, proven technology platform, Singtel Managed Defense Services will help you navigate the fast-evolving security landscape.

Footnotes:
1. Based on investigations in 2013 from FireEye's Mandiant incident response unit.
2. Mandiant M-Trends 2014

About Singtel

Singtel is Asia's leading communications group providing a portfolio of services including voice and data solutions over fixed, wireless and Internet platforms as well as infocomm technology and pay TV. The Group has presence in Asia, Australia and Africa with over 610 million mobile customers in 24 countries, including Bangladesh, India, Indonesia, the Philippines and Thailand. It also has a vast network of offices throughout Asia Pacific, Europe and the United States.

Awards

Frost & Sullivan Singapore Excellence Awards 2016
Managed Security Service Provider of the Year

Frost & Sullivan's Asia Pacific ICT Awards 2016
Telco Cloud Service Provider of the Year

NetworkWorld Asia Info Mgmt Awards
Security-as-a-Service (2012 - 2016)

NetworkWorld Asia Readers' Choice Awards
Managed Infrastructure Services (2012 - 2015)
Managed Security Services (2014 - 2015)

NetworkWorld Asia Info Mgmt Awards
Disaster Recovery & Business Continuity (2014 - 2016)

Telco Cloud Forum Awards 2016
Telco Cloud of the Year

October 2016

For more information www.singtel.com/security g-security@singtel.com Contact your Account Manager