Singtel Business

Product Brochure
Managed Endpoint Threat Detection and Response (ETDR)

Get Armoured Against Endpoint Attacks.

Singtel Managed Endpoint Threat Detection and Response Service, delivered through our Managed Security Services, helps you regain control over your endpoint security via effective malware hunting, continuous monitoring and forensic reverse engineering.

CounterTack®

Singtel

Managed Endpoint Threat Detection and Response (ETDR)

Get Armoured Against Endpoint Attacks

Traditional and current advanced endpoint protection offers a preventive security approach in which threats are identified through known Indicators of Compromises (IOCs), signatures, exploits and sandboxing technologies.

Enterprises need to reinforce their existing preventive endpoint protection solution with predictive measures. With the ability to perform behavioural analysis coupled with the capabilities to continuously monitor the endpoints, new generation endpoint security such as the Singtel Managed Endpoint Threat Detection and Response (ETDR) provides visibility into endpoint behaviours, allowing enterprises to pro-actively respond to potential threats. Unlike traditional and advanced endpoint security solutions, where malware hunting requires node-based scans which can potentially affect performance, Singtel Managed ETDR combines efficient threat detection, data collection and correlation with big data technology to scale ETDR and counter threats based on unprecedented endpoint intelligence.

Building a Business Case: Advanced Endpoint Security

Advanced endpoint threat detection and response is required to protect against today's zero-day threats. A renewed focus on endpoints can strengthen your overall security defence because:

- Endpoints act as security sensors to determine if you have been or are being compromised[1]
- Monitoring endpoints increases the success of early detection of malware when it is at its most immature state, to enable swift remediation[2]

61% 61% of respondents told Ponemon that endpoint security is becoming a more important part of their overall IT security strate[3]

95% 95% of respondents also revealed that they will evolve towards a more 'detect and respond' approach from one focused on prevention[4]

Singtel Managed Endpoint Threat Detection and Response (ETDR) Service

To help your business regain control of endpoint security, we offer comprehensive Managed Endpoint Threat Detection and Response (ETDR) Service, built on **big data architecture**. This service redefines ETDR by hunting down and exposing attacker behaviours **via enhanced threat detection, continuous monitoring, timely remediation and forensic reverse engineering** expertise.

Powered by unique **operating system (OS) surveillance**, Singtel Managed ETDR service delivers predictive binary analysis, coupled with **real-time, multi-faceted behavioural capture and analysis**, to deliver more accuracy in predicting malicious activity and heighten overall security defence. Most importantly, this is offered as a managed service to help your business establish a proactive and integrated security system approach - **Detect, Analyse and Respond** - for optimal threat mitigation.

Managed ETDR Service delivers:

Detect	Performs behavioural analysis of both known and unknown malware based on real-time capture of advanced attacks. Capability extends to post-incident detection and analysis.
Analyse	Correlates OS-level behavioural analysis with threat intelligence for real-time, advanced forensics. On-demand reverse engineering determines the extent of the threat's impact, if it has been executed.
Respond	Generates IOCs for detected threat activity. Quarantines affected endpoints to prevent further threat infiltration and remediates threats based on attack data collected from OS and memory levels. Hunts for legacy threats across the enterprise via API-based automated threat response.

Service Offerings

Malware hunting: on-demand malware detection and analysis

What it is	Scheduled behaviour-based malware detection and analysis that enable rapid discovery of compromised endpoints and deliver deep visibility into the extent of the malware attack.
What it does:	• Pinpoint compromised systems quickly and easily • Determine scope of breach and contain malware • Generate threat intelligence to harden endpoints against future attacks • Enable scaling of investigative efforts across the enterprise via streamlined incident response lifecycle processes
How it works:	**Scan and identify:** On-demand scanning of endpoints down to the physical memory-level with user-defined or built-in scan policies to target any aspect of physical memory, operating system or connected drives. **Sweep:** Sweep OS, memory and disk-levels to reveal zero-days, rootkits and other malicious threats. **Classify and analyse:** After threats are identified, threat data is collected and analysed against the Malware Genome database for classification as good, bad or neutral. Rules and weightage are applied to each threat to compute its overall security score. This enables easy recognition of breach indicators and detection of new malware in the future. **Contain:** Identify initial points of infection; isolate lingering malicious files/system changes, and generate threat intelligence to harden endpoints against future attacks.

Continuous monitoring: real-time, continuous endpoint threat detection and response

What it is	Real-time, continuous threat monitoring, detection and response built on big data architecture. Embedded in OS-level for tamper-resistant monitoring of system behaviour with full visibility.
What it does:	• See attacker behaviour in real-time • Capture all malicious events and processes during attack • Identify and prioritise threats for optimal threat response • Automate prescriptive threat analysis with built-in indicator profiles • Determine threat impact with full threat contextual analysis from infection to remediation • Remediate both known and unknown threats, backed by built-in and learned knowledge base established over time
How it works:	**Identify and capture:** Endpoint sensors use real-time OS-level surveillance to identify attacker behaviour and capture all system-level events and processes as the malware attack unfolds. **Collect and report:** Endpoint attack data is collected and sent to collector nodes. This will trigger an incident report with the Security Information and Event Management (SIEM) platform. **Characterise and correlate:** All endpoint attack data are deduplicated, compressed and encrypted across all collector nodes before sending to the Endpoint Analysis Cluster for real-time threat characterisation and correlation via big data analytics. **Search:** Powerful search capabilities based on reported host IP address are used to hunt down all hosts across the enterprise that has communicated with that IP address. This will reveal critical information on affected host, communication time stamp, process details and more. **Contain:** Quarantine and remediate affected endpoints by deleting files, terminating processes on-demand, denying network access by affected endpoints, and configuring alert messages when an endpoint has been quarantined. **Understand:** Build intelligence knowledge base by understanding how malicious programme gained entry into endpoints, to determine the attack source and preserve evidence for future reference.

Business Applications

Forensic reverse engineering: memory forensics and reverse engineering

What it is	Live physical memory forensics and behavioural analysis with automatic reverse engineering capabilities for effective incident response, data compliance and electronic discovery. Supports Windows and Linux.
What it does:	• Search, uncover, identify and report critical digital artifacts • Capture and analyse both Windows and Linux physical and virtual memory images for memory forensics on endpoints • Provide interactive views on the elements of a malware and linkages (who, what, when, where, why and how). • Offer drill-down trait profile on preferred combinations of tools and techniques employed by individual hackers and organised groups
How it works:	**Capture:** Use live memory acquisition tool for full capture and memory imaging of Windows and Linux physical and virtual memory. **Reverse engineer:** Automatically reverse engineer and analyse captured memory for hard-to-detect threats such as zero-day malware, rootkits and more. **Understand:** Generate actionable intelligence on malware attacks including: methods of infection employed; which files and registry keys were accessed; and more.

Benefits

More accurate in predicting malicious activities: Employs state-of-the-art endpoint threat protection technologies including: kernel-level data collection, enterprise-scale data analysis and correlation, and a combination of predictive binary and events analysis – backed by behavioural intelligence, to transform the way IT/security teams predict attacks.

End-to-end endpoint security assurance: Benefit from the industry's only 'complete attack capture' tracking of advanced threats throughout the entire threat lifecycle from detect, analyse, response to remediation.

Save time: Lesser time taken from infection to remediation with full threat context and impact analysis. Gain further efficiencies with repeatable workflows.

Scale investigation efforts easily: Scale investigative efforts enterprise-wide with streamlined incident response lifecycle.

Prioritise threat response with big data analytics: Easily correlate massive amount of data collected from the continuous monitoring of endpoints across the enterprise. Prioritise remediation efforts based on threat severity scores for timely remediation of accurately-identified threats and cut time troubleshooting false positives.

Fortify Your Endpoint Security: Mitigate Risks Effectively with Singtel Managed ETDR Service

If you need endpoint protection for your Critical Information Infrastructure (CII), we recommend:

- Both Malware Hunting and Continuous Monitoring to proactively detect, analyse, respond and remediate malware threats
- Forensic Reverse Engineering for automated forensics investigations that reverse engineer threats to support potential law enforcement and other compliance requirements

Capabilities Highlight

Today's businesses are constantly confronted with choosing the 'right' security solutions and figuring out how to deploy them consistently enterprise-wide – all while keeping an eye on regulatory compliance. A managed security services (MSS) provider can help you devise a comprehensive, continuous, integrated and compliant security strategy to protect your business against today's cyber threats. Most importantly, outsourcing your security needs gives you cost efficiencies and the freedom to scale with your security needs – delivering valuable peace of mind.

Singtel Managed Security Services (MSS) delivers round-the-clock security protection for businesses of all sizes. Its comprehensive suite of services range from design, integration, access authentication, to change management, to 24x7 monitoring of security and network systems, and more. Our experienced team at Singtel Security Operations Centre ensures the effective detection, prevention and remediation of the damage caused by cyber-attacks, while minimising potential business interruptions. Singtel Managed ETDR Service is delivered by Singtel MSS.

24x7x365 Singtel global MSS, powered by Trustwave: Gain peace of mind with Singtel 24x7x365 security monitoring via our global network of federated Security Operation Centres, managed by the ITIL best practices certified SOC team armed with extensive certifications.

Incident and monthly reporting: Proactive monitoring and management of service platforms via Singtel SOC portal to maximise service availability.

Big data analytics at OPEX level: Advanced threat detection, continuous monitoring and response technology powered by big data analytics. Lower total cost of ownership with big data analytics available as an operating expense.

Cyber intelligence: Predictive analysis of potential threat through threat intelligence provided for by a global network of federated Security Operation Centres.

Regional coverage and deployment: Streamline security delivery with regional coverage and deployment, backed by in-country operations.

World-class data centres: Benefit from one of the most extensive points of presence in the Asia Pacific with our network of world-class data centres, which provide 24x7 facilities management, direct interconnectivity access, and a range of Information Communications Technology (ICT) Managed Services.

1. https://cdn2.hubspot.net/hubfs/150964/2016_State_of_Endpoint_Report.pdf
2. http://www.forbes.com/sites/frontline/2014/09/26/three-reasons-why-endpoints-cannot-remain-a-security-blind-spot/#f296e8a44734
3. https://cdn2.hubspot.net/hubfs/150964/2016_State_of_Endpoint_Report.pdf
4. Ibid.

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 595 million mobile customers in 25 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

Asia Communication Awards
Best Enterprise Service - Connectivity as a Service (2013)
Best Cloud Service (2011 & 2012)
Project of the Year - G-Cloud (2014)

Computerworld SG Readers' Choice Awards
Best Data Centre and Hosting Services Provider (2007 & 2009 - 2013)
Best Managed Connectivity Services Provider (2006 - 2013)

Computerworld Singapore Customer Care Award
Cloud Services (2012 - 2013)
Systems Integrations Services (2014)

NetworkWorld Asia Information Management Awards
Best in Security as a Service (2014-2015)

NetworkWorld Asia Readers' Choice Awards
Best in Managed Security Services (2014-2015)

Frost & Sullivan Asia Pacific ICT Awards
Telecom Cloud Service Provider of the Year (2012)

IDC MarketScape in Asia Pacific 2013
A Leader for Datacenter and Hosted Cloud Services

NetworkWorld Asia Readers' Choice Product Excellence Awards (2013)
Managed Infrastructure Services
Cloud Infrastructure Provider

Challenger in 2015 Gartner Magic Quadrant for Global Managed Security Service Providers, Worldwide
Gartner

Managed Security Services Leader (2014)
Forrester Wave™ Managed Security Services, North America

June 2016

For more information www.singtel.com/security g-security@singtel.com