Singtel Business

Product Brochure
Managed Advanced Threat Prevention

Outwit Cyber Criminals with Comprehensive Malware and Exploit Protection.

As cyber criminals outwit businesses by employing ever-new techniques and multi-vectors to gain a foothold in one's network, legacy approaches no longer work. Our Managed Advanced Threat Prevention Service helps you unify threat detection and prevention for network and endpoint defence against today's new enemies.

Singtel

Managed Advanced Threat Prevention

Outwit Cyber Criminals with Comprehensive Malware and Exploit Protection

Cyber criminals are as creative in their methods as they are relentless. They are more than a match for traditional network defences, which are too rigid and limited in the scope of their detection capabilities. What is needed is a new, proactive defence against modern cyber criminals: get inside their minds and anticipate their antics.

One possibility concerns the scripted nature of all cyber attacks, which adhere to the progression of the Cyber Kill Chain: the breach of the perimeter; the delivery of the malware; and, the lateral transport of malware across the network as well as the exfiltration of targeted data. Stopping a cyber attack at any of these stages will cripple the attack. Hence, businesses can effectively protect their networks and endpoints through a multi-layered, complete threat protection approach, utilising threat preventing next-generation firewalls, cloud-based malware analysis, advanced endpoint protection and cloud-based threat intelligence.

New Ways to Prevent a Perimeter Breach

- A threat prevention next-generation firewall defends a network from known threats by inspecting all traffic for commonly exploited file types and high-risk applications. By enforcing strict security policies, the lateral movement of malware within one's network can be prevented. Furthermore, ongoing monitoring and traffic inspection helps to block outbound command-and-control communications and prevents any data exfiltration.

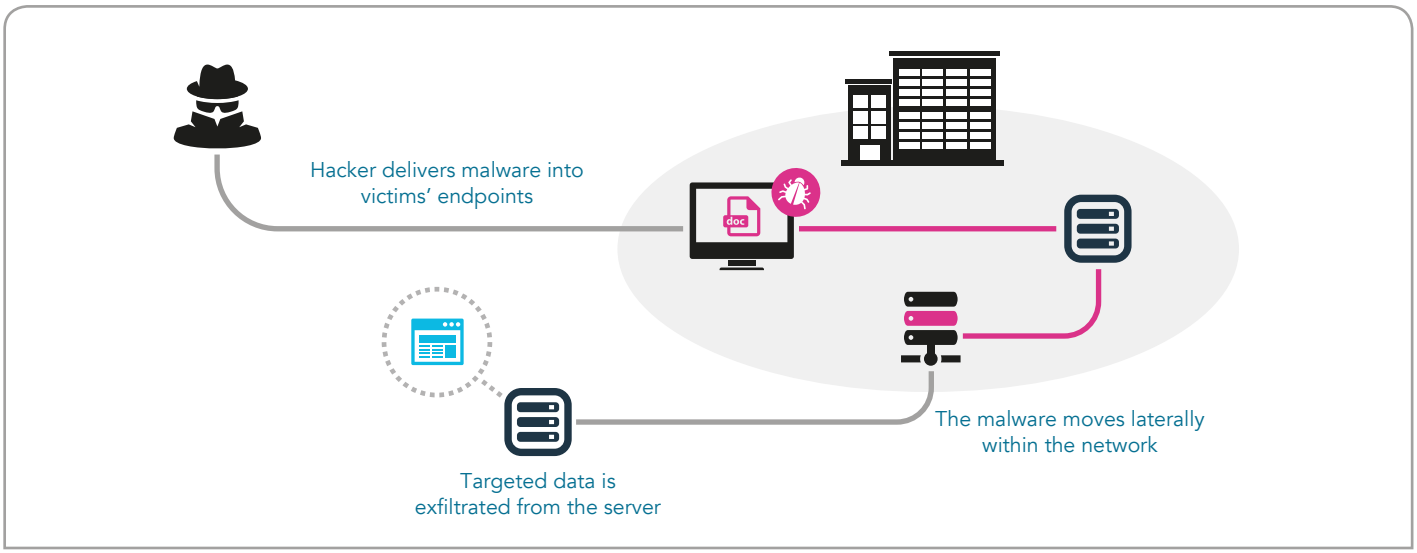
- Real-time cloud-based malware analysis protects a network from unknown threats by investigating unknown files or traffic patterns. Network security is thus guaranteed by automatically identifying 'unknown' threats and turning them into 'known' ones through the issuance of new signatures.

- Rich forensics and threat intelligence collates attack data and patterns, and then correlates the data with analysis and past trends to increase the risk posture of the network, improving protection against future threats.

Preventing Attacks at Every Stage of the Kill Chain

Breach the perimeter	Deliver the malware	Lateral movement	Exfiltrate data
Next-Generation Firewall	**Advanced Endpoint Protection /Cloud Based Malware Analysis**	**Next-Generation Firewall**	**Threat Prevention**
• Visibility into all traffic, including SSL • Enable business-critical applications • Block high-risk applications • Block commonly exploited file types	• Block known and unknown vulnerability exploits • Block known and unknown malware • Provide detailed forensics on attacks	• Establish secure zones with strictly enforced access control • Provide ongoing monitoring and inspection of all traffic between zones	• Block outbound command-and-control communications • Block file and data pattern uploads • DNS monitoring and sinkholing
Threat Prevention		**Cloud Based Malware Analysis**	**URL Filtering**
• Block known exploits, malware and inbound command-and-control communications		• Detecting unknown threats pervasively throughout the network	• Block outbound communication to known malicious URLs and IP addresses
URL Filtering			
• Prevent use of social engineering • Block known malicious URLs and IP addresses			
Cloud Based Malware Analysis			
• Send specific incoming files and email links from the internet to public or private cloud for inspection • Detect unknown threats • Automatically deliver protections globally			

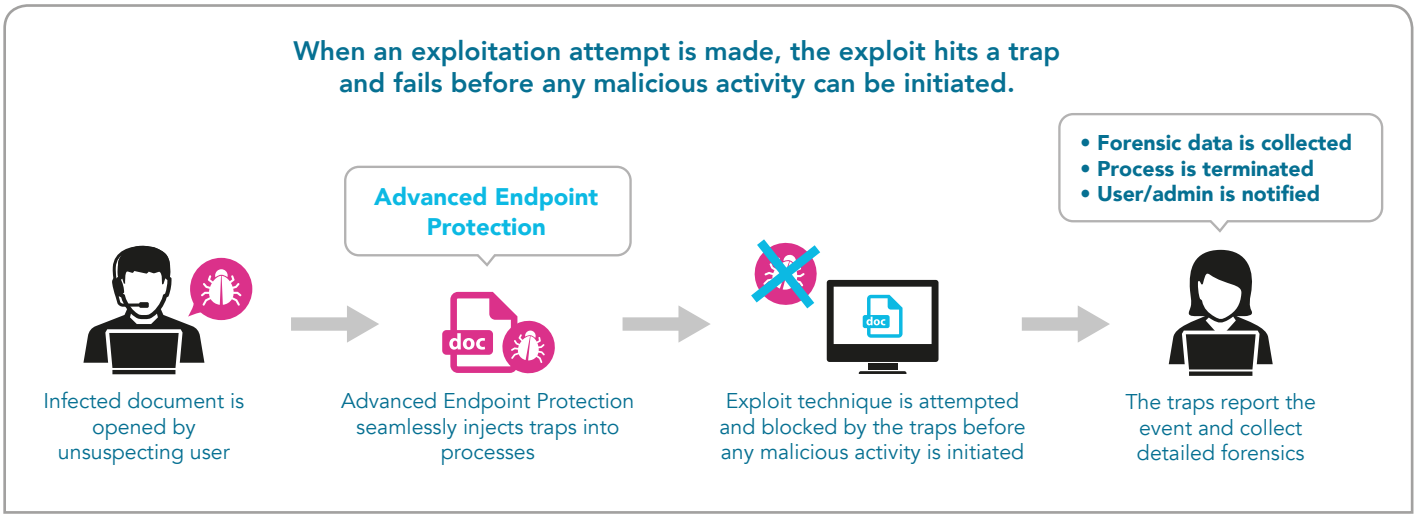
Preventing Attacks at Every Stage of the Kill Chain (continued)



New Ways to Prevent an Endpoint Exploit

- Protect against both known and unknown threats by injecting traps via advanced endpoint protection, allowing for the inspection of all processes/files and blocking of 'core techniques' before any malicious activity can be initiated
- Integrate with cloud-based threat intelligence to collect forensic data, which triggers alerts to security operations centres and correlates intelligence for sharing across security services

Exploit Prevention - User Experience



Time to Close the Security Gap

Cyber crimes are still widespread due to continued reliance on legacy approaches. It is time to close the security gap with these new approaches that:

- Prevent all known and unknown malware and zero-day exploits
- Are scalable and lightweight for deployment across all endpoints
- Offer closed-loop prevention and forensics to quickly share intelligence on new threats and report on potential infections
- Seamlessly protect network, endpoints and the cloud with unified detection, prevention and security policy for all users and devices.

Managed Advanced Threat Prevention (ATP) Service

Our Managed Advanced Threat Prevention (ATP) Service offers unified advanced threat detection and prevention for network and endpoint defence. It provides comprehensive exploit, malware, and command and control protection for your networks to prevent attacks at every stage of the cyber kill-chain.

Managed ATP Service, delivered via our Managed Security Services (MSS), offers multi-layered threat protection to stop advancing threats at every opportunity via four service offerings:
1. Threat Prevention Next-Generation Firewall
2. Advanced Endpoint Protection
3. Cloud-Based Malware Analysis
4. Cloud-Based Threat intelligence

Service Offerings

1. Threat Prevention Next-Generation Firewall

Our Threat Prevention Next-Generation Firewall performs a full-stack, single-pass inspection of all traffic across all ports — regardless of applications, threats and content. By taking an application-centric approach to inspect and classify all traffic, it helps to secure your network perimeter, while enabling full visibility and control over your business networks with policies that secure access to all applications located on them.

Features	Benefits
• Intrusion Prevention System (IPS): One-pass inspection, identification and mapping of applications and users to protect against known/unknown network and application-borne threats. • Anti-virus and anti-malware: Identifies and blocks malware variants and threats hidden in encrypted files and web traffic. • Command and Control (CnC) Protection: Blocks outbound requests to malicious domains/unknown CnC toolkits from infected devices. Prevents requests from leaving network to block possible exfiltration of data. Compiles reports on network hosts that are making these requests. • Content and URL filtering: Blocks access to undesirable websites via customisable URL filtering engine to enable granular web-browsing policies, whitelisting, blacklisting, custom categories, database customisation and more; while facilitating SSL decryption policies. • Global protect virtual private network (VPN): Enables IPsec compliant site-to-site and certificate-based remote user VPN for secure, encrypted access to corporate systems and remote offices. • Sandboxing: Integrates with cloud-based malware analysis platform for real-time protection from unknown threats.	• Ensures high throughput and eliminate redundant processes with a full-stack, single-pass inspection of all traffic (applications, threats, content) across all ports, protocol, evasive tactics, or SSL encryption. • Reduces network threat while allowing security-controlled access to applications via an application-focused approach. • Enables tight security policies focused on applications, users and content. • Enables fine-grained visibility and policy control over application access and functionality, with access to a complete context of applications, user identities and devices.

2. Advanced Endpoint Protection

Out of the thousands of new vulnerabilities and millions of malware 'introduced' each year, only 2 to 4 typically employ entirely new techniques. Several may devise new malware sub-techniques, but only as a minor permutation of the core techniques.[2]

Our Advanced Endpoint Protection focuses on 24 core techniques that are commonly used to protect endpoints against all exploits and malicious executables — without prior knowledge of threats and before any malicious activity can initiate. When a user tries to open an exploit document or executable, 'traps' are injected into processes to scan for any core techniques. Once identified, the processes in question are automatically blocked before any malicious activity can be initiated. In effect, the prevention of one technique blocks the entire attack.

Features	Benefits
• Scalable and lightweight: Highly scalable, lightweight, and seamless, while offering minimal to no disruption. • Policy-based restrictions: Sets up security policies to restrict specific execution scenarios (e.g. prevent execution of certain file types from USB devices). • Advanced execution control: Enables granular control of global policies, applications, etc. • Malware techniques mitigation: Implements technique-based mitigations to prevent attacks using certain techniques like thread injection. • Forensics capabilities: Gathers detailed forensic information after an attack is blocked. Logs information with Endpoint Security Manager. • Sandboxing: Integrates with cloud-based malware analysis platform for real-time protection from unknown threats. • Close integration with security policies: Integrates closely with network and cloud security.	• Prevents all exploits including zero-day vulnerabilities. • Prevents all malicious executables without requiring prior knowledge. • Reduces surface area of attack with granular control of global policies, applications, etc. • Proactively defends other unprotected endpoints against possible attacks with detailed forensics against prevented attacks.

3. Cloud-Based Malware Analysis

Our Cloud-Based Malware Analysis offers revolutionary, real-time detection and protection against advanced, unknown threats. With granular malware detection across all protocols, it turns 'unknown' threats into known, preventable incidents by automatically creating protection against new threats within 5 minutes. Detailed forensic information is also collected to prioritise remedial action.

Features	Benefits
• Malware analysis: Real-time granular inspection and analysis of malware across more than 250 malicious indicators (e.g. host changes, outbound traffic, attempts to bypass analysis, etc.) • Automatic creation of new signatures: Creates protection against new threats by making them available across all globally, connected networks within 5 minutes. • Virtual malware verification in sandbox: Executes suspected malicious file in a virtual environment to determine if malicious or benign. • Dynamic whitelisting: Dynamically whitelists non-malicious URLs without manual intervention or maintenance. • Correlated forensics: Provides intelligence to easily investigate suspected infections.	• Offers comprehensive protection against unknown threats by turning unknown threats into known, preventable incursions within 5 minutes. • Shortens time between detection and mitigation with automatic protection against new threats. • Reduces costs with automatic protection without having to implement and manage separate devices for various security protection (e.g. web, email, etc.) • Ensures enterprise-wide protection with easy scaling of malware detection and protection via unique cloud-based architecture with no configuration required. • Hastens investigations with correlated forensics, and enables easy prioritisation and execution of security actions.

4. Cloud-Based Threat Intelligence

Our Cloud-Based Threat Intelligence provides actionable threat intelligence that highlights unique, targeted attacks to accelerate threat analysis and prioritise remediation action. Using powerful analytics, comprehensive information on the actor and his attack techniques are provided to expedite a timely response to the incursion. In addition, with intelligence gathered from our cloud-based malware analysis platform, together with third-party global intelligence feeds from both closed and open source intelligence, we can help you proactively prevent and respond to possible threats before a breach occurs.

Features	Benefits
• Statistical analysis engine: Offers artefact-level statistical analysis to correlate billions of artefacts across a global data set of indicators of compromise (IOCs). Applies unique weighting system to identify critical IOCs. • Actionable intelligence: Provides actionable intelligence and context around attacks, adversaries and campaigns, including targeted industries. Enables export of high-value IOCs into security devices to block malicious URLs, domains or IP addresses instantly. • Priority alerts: Triggers prioritised security alerts to distinguish most critical threats based on IOCs. • Security controls: Allows only authorised access to confidential security information with strict privacy and security controls.	• Increases threat understanding with contextual-based visibility into threats targeted at industry or global context to speed up decisive action to prevent future attacks. • Speeds up mitigation action with powerful analysis and correlation of threat intelligence to extract actionable intelligence for prioritised actions and alerts, without requiring additional specialised resources. • Ensures continuous protection against latest advanced threats by leveraging global threat intelligence. • Empowers entire IT security teams to become advanced threat hunters instead of relying on specific groups of highly-organised security operations professionals.

Why Singtel

Comprehensive prevention against both known and unknown threats
Comprehensive exploit, malware, command and control protection for your network and endpoints, backed by real-time, cloud-based malware analysis and cyber intelligence.

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

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

Monthly threat intelligence reporting
Leverage global threat intelligence platforms to deliver actionable intelligence.

Regional coverage and deployment
Streamline security delivery with regional coverage and deployment, backed by in-country operations in 42 cities across 22 countries.

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

Footnotes:
1. http://cyber.lockheedmartin.com/solutions/cyber-kill-chain
2. https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/white-papers/traps-pci-compliance.pdf

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