Singtel Business

Product Brochure
Cloud Protect - Managed Web Isolation Service

Protect Your Endpoints and End Users Against Web-Borne Attacks

Singtel Managed Web Isolation Service protects your endpoints and end users from Web-borne zero-day malware attacks and phishing threats. It executes all potentially harmful web browsing code, email content and attachments in a remote and safe environment, thus preventing cyber threats from reaching your endpoints and end users. This enables your end users to surf without fear, while minimising the administrative overhead of managing complex security policy exceptions.

Singtel

Cloud Protect - Managed Web Isolation Service

Your Web Browser Is Your Weakest Link

Gartner research has shown that over 90% of cyber-attacks originate from the Web and email[1]. With your web browser possibly the weakest link in your enterprise information security, your endpoints, devices and end users can be compromised — when connecting to the Internet to search for information or download a document for reference.

Traditionally, web proxies, gateways and sandboxes have been employed as the primary defence against web-borne attacks. However, they have become ineffective against today's evolving threat landscape and sophisticated malware evasion techniques, due to their use of web filtering techniques.

Cyber Realities

As long as Web-borne content is allowed to reach endpoints, infections are inevitable.

Existing defences such as web proxies usually provide effective security controls for 'known' or categorised websites. Even then, Symantec has reported that

78% of websites contain a critical vulnerability that poses security risks[2].

However, **when faced with 'unknown' or uncategorised websites, Web proxies are rendered 'helpless'** as web browser vulnerabilities are often exploited via compromised or malicious websites. The situation is further aggravated by:

- End users who tend to click on links without considering the risks of being compromised – making them easy prey to socially-engineered exploits.
- Web page addresses that mislead end users and redirect them to an unexpected site.
- Websites that require users to enable certain features or install more software, which expands the attack surface and places endpoints and devices at greater risks.

These risks are further compounded by **the increased interest in crypto-currency mining**.

Crypto-currency mining software has already infected at least 1.65 million endpoints for the first 8 months of 2017[3].

Cyber criminals are making a fast buck by drawing on significant computing power from unassuming businesses. This slows down business processes and can potentially cause denial-of-services to customers and users.

- **Symantec:** 78% of websites contain a critical vulnerability that poses security risks[2].
- **Gartner:** Over 90% of cyber-attacks originate from the Web and email. 50% of enterprises will leverage isolation to protect against cyber-attacks by 2021[1].

Recent Incidents

Since exploitation of JavaScript in cyber-attacks is not new, it is not surprising that web browsers are fast becoming a primary attack vector one needs to guard against. What's new is the increasing frequency of this attack vector. The key danger of such attacks is the ability of JavaScript codes to execute automatically once a webpage is loaded – without a user's interaction. Here are some recent incidents that should make one sit up, take notice and most importantly – take action, before it is too late:

Bad Rabbit[4]

New ransomware outbreak on 24 October 2017 has hit major infrastructure in Ukraine, including the Kiev metro. It is distributed via drive-by download where JavaScript has been injected in the HTML body or in one of the .js files of the websites.

Equifax[5]

A US-based credit bureau with global presence in 24 countries, Equifax had to take parts of its website offline on 12 October 2017. This is after discovering codes on its website which redirected users to a malicious URL and urged them to download malware.

KovCoreG[6]

A malvertising group KovCoreG has been tricking users to install the Kovter malware via fake browser and Flash updates. The downloadable files were JavaScript (Chrome, Firefox) or HTA (Internet Explorer, Edge) files.

Monero-mining malware[7]

Latest reports reveal that a monero-mining malware has been possibly active since May 2017. It targets older Windows servers, such as Windows Server 2003 via CVE-2017-7269, a known Buffer Overflow vulnerability in Microsoft Internet Information Services 6.0, to mine for crypto-currency.

A New Security Paradigm Web Isolation[8]

Gartner has affirmed that only browser isolation can completely protect against web-borne malware and phishing from uncategorised and risky websites. What is required is a new security paradigm — web isolation.

Cloud Protect - Managed Web Isolation Service

Singtel Managed Web Isolation Service provides an isolation layer or an 'air-gap' between the Web and your end users.

To give you complete malware protection, it assumes that all content can be malicious. As such, all potentially harmful web browsing code, email content and attachments — whether good or bad – are executed remotely in a safe, protected environment, before delivering a safe visual stream to users' devices. This completely eliminates web-borne threats by ensuring that no Web-borne zero-day malware attacks and phishing threats ever reach your endpoints and end users. With support for any operating system, browser or device, it delivers a seamless browsing experience. Your end users can now surf without fear, as they visit, click through and download documents from websites.

Singtel Managed Web Isolation Service is available as a virtual appliance or managed cloud service. An agent-free solution, it integrates easily with existing web proxies and firewalls, thus enabling rapid deployment.

Features	Capability	Outcome
Web isolation	Render web content remotely and return a safe visual stream to the end user's web browser	Prevent malicious code execution in the end user's web browser
Document isolation	Open online documents in a remote viewer and scan for malware when download is initiated	Block malicious download or allow end user to save document as PDF
URL filtering	Block access to web content based on pre-defined categories	Display a customised block page with an auto-generated ticket number to facilitate incident response
Anti-phishing	Disable all input fields when a website might be unsafe and prevent submission of sensitive data over an insecure (non-https) connection	Display an insecure webpage in read-only mode and auto-generate a pop-up message to warn and educate the end user
User action control	Log and control end user actions such as copy, paste, print, and save as	Limit certain user actions in the browser to prevent data leakage

Benefits

Ensure all traffic between Web browser and the Internet is risk free with protection against drive-by infection, malvertising and cross-site scripting attacks.

Optimise IT resources by reducing IT administrative overheads related to managing web access policy exceptions, support tickets, security alerts (false positives and false negatives) and forensic investigations.

Increase business productivity by granting end users safe access to uncategorised websites without risks.

Enable rapid deployment with no software or browser plug-in required on end user's devices; and seamless integration with existing security infrastructures and services.

Use Cases

Enable safe access to uncategorised websites
Redirect end user's browsing sessions of risky websites to the isolation platform for 'sandboxing', which creates an 'air-gap' between the Web and end users — similar to viewing a 'fire' behind a pane of glass.

Prevent email phishing attacks by restricting file uploads to uncategorised websites
Educate and prohibit users from uploading files, which may contain corporate credentials and other sensitive information, to potentially unsafe or uncategorised websites by rendering webpages in read-only mode — despite granting access.

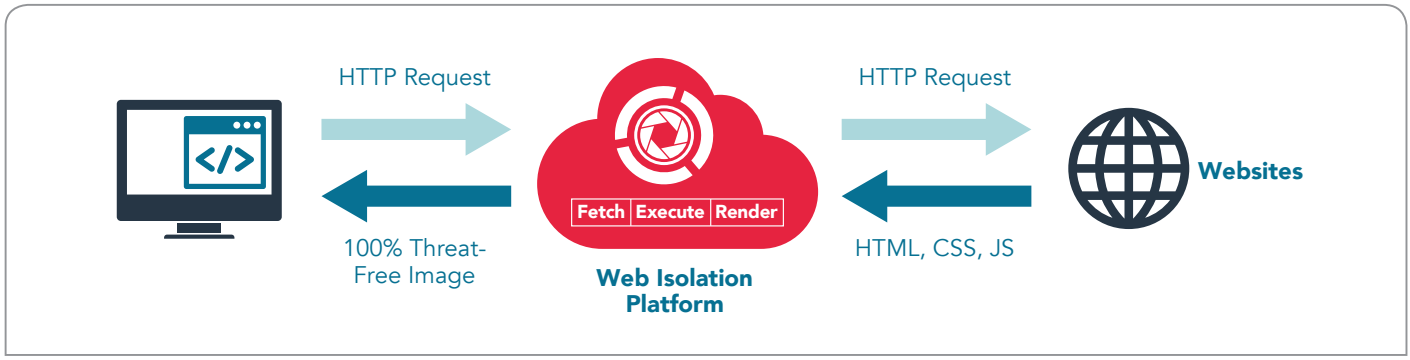
Mitigate web browser exploits
Execute original web content in a secure, containerised environment and return only a clean visual stream to the end user's browser for display. This prevents any malicious code from reaching the endpoint or end user devices directly, thus eliminating the web browser's attack vector.

Protect against malicious downloads
Download selected document types to the isolation platform for scanning and sanitising before activating the 'downloaded connection' on the end user's browser. For greater protection, end users can choose to download the documents in PDF format.

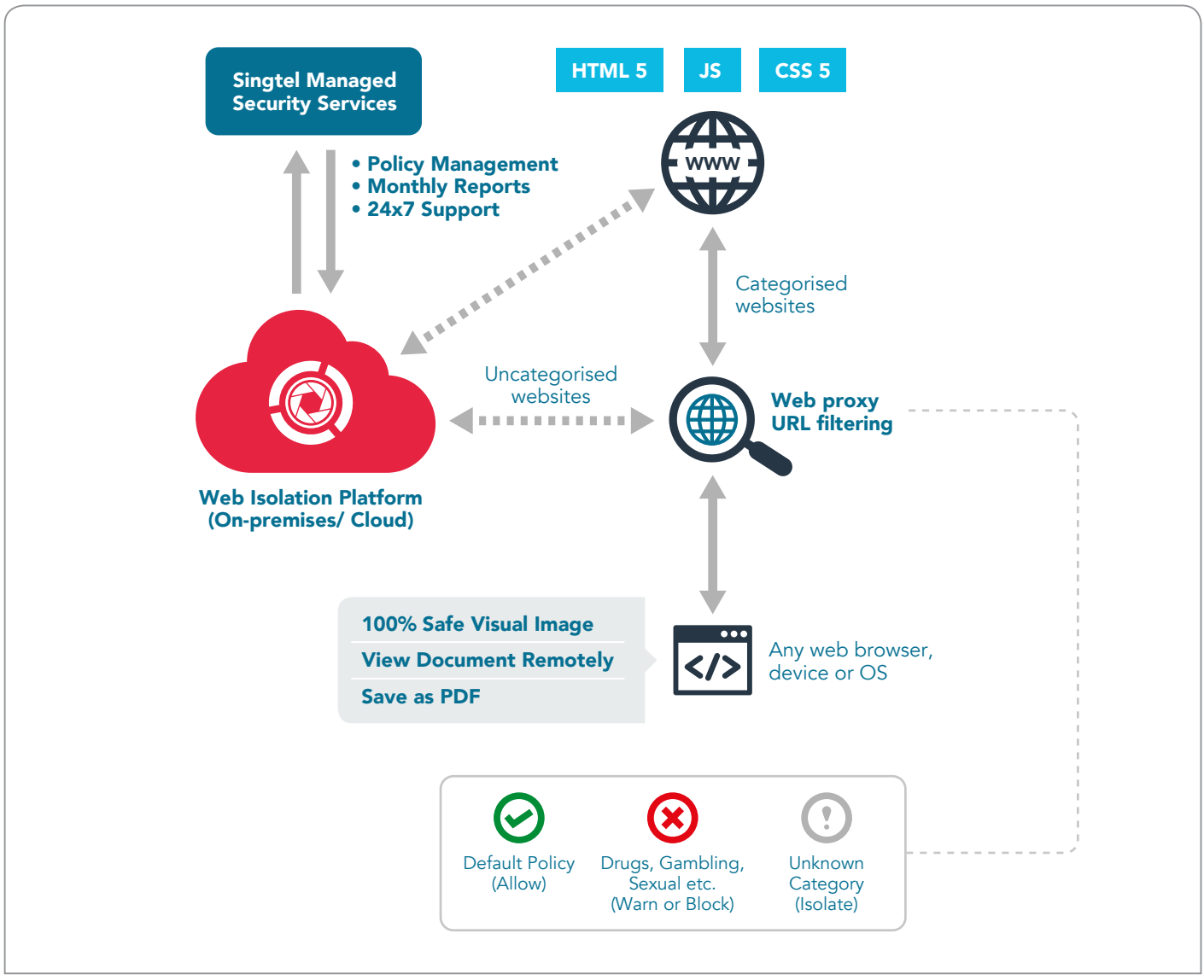
Service Offering

Offering	Managed Web Isolation
Subscription	Annual, per user license
Deliverables	Virtual appliance or as-a-service
Management	Self-service or via Singtel Managed Security Services
Compatibility	Any modern web browser, device, OS

How It Works



All web content are executed and rendered in a secure and remote environment. In this way, web isolation prevents malicious web codes from ever reaching your network and end user devices. For further protection, each end user's Web session is confined to a virtual browser that is disposed at the end of the session, thus eliminating malware persistency.



Why Singtel

For extra peace of mind, Singtel Managed Web Isolation Service is managed by Singtel's team of security experts who can help with policy change management and review of logs.

- Important to take a 360-degree approach to cyber security.
- Leverage Singtel's ecosystem of best-of-breed security technologies for your business.
- For complete protection against web-borne threats, web isolation should be seamlessly integrated with Singtel's Managed Endpoint Threat Detection and Response service, threat intelligence and advanced SOC capabilities.

A team of security-cleared and experienced professionals with over 30 years of deep domain knowledge and professional certification in CISSP, SABSA, CISM, CISA, GCIA, GCIH, GCFA, CEH, ECSA, CHFI, Mile2, HP ArcSight, Tipping Point, McAfee, Trustwave and more.

9 audit-ready Security Operations Centres (SOCs) –- 4 in North America, 4 in Asia Pacific and 1 in Europe, and together with SpiderLabs' global leading intelligence research team, we provide expert security and penetration testing services, incident readiness and data breach forensic investigations, innovative security research and major threat discoveries, and more.

End-to-end security capabilities as a solution provider in deploying enterprise-wide, mission-critical systems; trusted security advisors to help our customers identify, track, monitor and respond to security vulnerabilities; and independent security reviewer to determine compliance gaps and propose remediation measures.

Footnotes

1. Gartner, 30 September 2016: It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing
2. Symantec 2016 Threat Report
3. Kaspersky Lab, 12 September 2017: "Mining" Botnets are Back - Infecting Thousands of PCs, Generating Hundreds of Thousands of Dollars for Criminals
4. Welivesecurity, 24 October 2017: Bad Rabbit: Not-Petya is back with improved ransomware
5. LA Times, 12 October 2017: Equifax says code on its website 'was serving malicious content'
6. Bleepingcomputer.com, 9 October 2017: Malvertising Group Spreading Kovter Malware via Fake Browser Updates
7. Siliconangle, 29 September 2017: Cryptomining malware now targeting older Windows servers
8. Gartner, June 14, 2017: Gartner Identifies the Top Technologies for Security in 2017

About Singtel

Singtel is Asia's leading communications and ICT solutions group, providing a portfolio of services from next-generation communication, technology services to infotainment to both consumers and businesses. For consumers, Singtel delivers a complete and integrated suite of services, including mobile, broadband and TV. For businesses, Singtel offers a complementary array of workforce mobility solutions, data hosting, cloud, network infrastructure, analytics and cyber-security capabilities. The Group has presence in Asia, Australia and Africa and reaches about 640 million mobile customers in 22 countries. Its infrastructure and technology services for businesses span 21 countries, with more than 428 direct points of presence in 362 cities.

Awards

Frost & Sullivan APAC Best Practices Awards
Singapore Managed Security Service Provider of the Year (2016 - 2017)
Singapore Managed Cloud Service Provider of the Year (2017)

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

NetworkWorld Asia Information Management Awards
Security-as-a-Service (2012 - 2017)
Regional Security Operations Centre (2017)
Disaster Recovery & Business Continuity (2014 - 2017)

SC Awards 2017
Best Managed Security Service (Trustwave)

Telco Cloud Forum Awards
Telco Cloud of the Year – 2016
Best Telco Cloud SDN/NFV Project – 2017

February 2018

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