FACTSHEET

INCLUSION OF PRE-APPROVED CYBERSECURITY SOLUTIONS UNDER THE SMES GO DIGITAL PROGRAMME

Many Small and Medium Enterprises (SMEs) are going digital to seize the exciting business opportunities available. However, cybersecurity remains a challenge. Business risks arising from cyber incidents are wide-ranging and can impact the business itself. It is therefore critical for SMEs to invest in cybersecurity to ensure that their assets and systems are protected from malicious cyber activities.

2. The Government recognises that SMEs may face resource constraints when it comes to improving their cybersecurity posture. To assist SMEs, Cyber Security Agency of Singapore (CSA), Infocomm Media Development Agency (IMDA) and Enterprise Singapore (ESG), have expanded the range of pre-approved digital solutions under the SMEs Go Digital programme to include cybersecurity solutions.

3. With this expansion, SMEs can receive funding support under the Productivity Solutions Grant (PSG) of up to 70% of the qualifying cost (e.g. subscription, license, and installation fees), to cover part of the cost of pre-approved cybersecurity products and services. There are four supported categories: Unified Threat Management (UTM), Endpoint Protection Platform (EPP), Managed Detection and Response (MDR) and Data Loss Prevention (DLP) (refer to details in Annex A).

4. To date, we have received more than 10 applications for pre-approval. Details of the pre-approved cybersecurity solutions will be progressively listed on the Tech Depot website (www.smeportal.sg/content/tech-depot/en/home.html). We will continue to work with the industry to expand the list of pre-approved cybersecurity solutions, to better support the needs of different businesses.

5. SMEs can approach SME Centres for general guidance on identifying suitable pre-approved cybersecurity solutions and implementing these measures. SMEs which require more support will be referred to the SME Digital Tech Hub for one-to-one consultation on the ways to improve their cybersecurity posture.

6. While adopting technology is important, people and processes are also key to addressing cybersecurity challenges. CSA has published a “Be Safe Online” handbook, which identifies 13 integrated cybersecurity measures that companies can adopt. These measures

can help SMEs enhance their cyber defence capabilities and digital risk management to better protect themselves against the increasing frequency and sophistication of cyber-attacks.

7. More information on the expansion of the range of pre-approved digital solutions under the SMEs Go Digital programme is available on IMDA's website (https://www.imda.gov.sg/SMEsGoDigital).

-END-

Annex A

The four supported categories of cybersecurity solutions under the SMEs Go Digital programme as defined[1] are as follows:

1. Unified Threat Management (UTM) is a converged platform of point security products, particularly suited to small and middle-sized businesses. Typical feature sets fall into three main subsets: (a) firewall/intrusion prevention system (IPS)/virtual private network; (b) secure Web gateway security (URL filtering, Web antivirus [AV]); and (c) messaging security (anti-spam, mail AV).

2. Endpoint Protection Platform (EPP) is deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts.

3. Managed Detection and Response (MDR) solutions deliver 24/7 threat monitoring, detection and lightweight response services to customers leveraging a combination of technologies deployed at the host and network layers, advanced analytics, threat intelligence, and human expertise in incident investigation and response. MDR providers undertake incident validation, and can offer remote response services, such as threat containment and support in bringing a customer's environment back to some form of "known good".

4. Data Loss Prevention (DLP) describes a set of technologies and inspection techniques used to classify information content contained within an object — such as a file, email, packet, application or data store — while at rest (in storage), in use (during an operation) or in transit (across a network). DLP tools also have the ability to dynamically apply a policy — such as log, report, classify, relocate, tag and encrypt — and/or apply enterprise data rights management protections.

[1] Definitions of the cybersecurity solutions are referenced from Gartner's IT Glossary, www.gartner.com/it-glossary

Media Contacts:

Name: Goh Jing Xian
Designation: Assistant Director (Comms & Engagement)
Email: Goh_Jing_Xian@csa.gov.sg

Name: Chloe Choong
Designation: Assistant Director (Comms & Marketing)
Email: Chloe_Choong@imda.gov.sg