CYBER TRUST

Overview of Cyber Trust

The Cyber Trust mark is a cybersecurity certification for organisations with more extensive digitalised business operations. It serves as a mark of distinction for your organisation to prove that you have put in place good cybersecurity practices and measures that are commensurate with your cybersecurity risk profile.

The products listed here help organisations to address the domains in the Cyber Trust mark[1]

Cybersecurity Preparedness Domains	How Palo Alto products enable organisations to address the Cyber Trust mark
Anti-virus/ Anti-malware	**Helping to address Cybersecurity Preparedness in Antivirus/Anti Malware, Asset Management and System Security with Cortex XDR (Prevent | Pro):**
	A market leader in the industry, Palo Alto Networks Cortex XDR is a Leader in The Forrester Wave: Endpoint Security Software as a Service, Q2 2021 report. In MITRE ATT&CK round 3 evaluation, Cortex XDR achieved excellent results – delivering 100% threat protection and 97%+ detection visibility.
Asset management	Cortex XDR provides a comprehensive endpoint agent for Advanced Threat Prevention. It covers Anti-Virus/Anti-Malware, EDR, Ransomware Protection, Exploit Prevention, Malicious Behavioral Prevention and Forensics solutions within the single agent.
System security	Singapore Hosted Cloud management model is suitable for today's business usage and addresses local data residency requirements. It provides ease of deployment with no extra server or software deployment costs. Leveraging on AI Analytics Engine, Cortex XDR provides laser accurate detection to pinpoint evasive threats and uses machine learning to profile behavior and detect anomalies indicative of attack.
	Cortex XDR is able to support multiple OS like Windows, MacOS, Linux or Android to provide detailed information about your host information and settings. This serves as a good Host Inventory system to keep track of the organisation's assets.
	In the event of a Security Incident, Cortex XDR automatically reveals the root cause, reputation, and sequence of events associated with each alert (including system logs), lowering the experience level needed to verify an attack.
	Find out more: www.paloaltonetworks.com/cortex/cortex-xdr

Network security	**Helping to address Cybersecurity Preparedness in Network Security with PA-400 Series Next Generation Firewall:**
	Palo Alto Networks is a Leader in 2021 Gartner Magic Quadrant for Network Firewalls for the Tenth Consecutive Time. Adopting the Zero Trust approach, PA-400 series secure the network by proactively identifying cyber threats so organisations can prevent the majority of zero-day sophisticated cyber attacks. It is lightweight, easy to deploy yet powerful thus making it suitable for organisations looking for a solution that has comprehensive security and small footprint.
	Powered by Machine Learning capabilities, PA-400 series is able to effectively prevent various sophisticated attacks such as Ransomware, Phishing Attack, Password Stealing, Advanced Persistent Threats (APT) and DNS attacks.
	With Zero Trust User based identity control, it ensures sensitive data is readable only between trusted entities, even for encrypted traffic via SSL decryption or Virtual Private Network (VPN) technology, across various device types such as Windows, MacOS, IOS or Android. In addition, identity base control can also strengthen the user/device security posture by preventing credential and data (PII) leakages and securing IoT devices within the organisations.
	Find out more: www.paloaltonetworks.com/network-security/next-generation-firewall

1 – Organisations seeking Cyber Trust certification should complement these products with additional measures to fully meet the certification requirements.

Organisations should refer to CSA's website for more information on Cyber Trust.

In collaboration with:

PARTNERSHIP PROGRAMME

This information sheet is developed in collaboration with Cyber Security Agency of Singapore (CSA) as part of its SG Cyber Safe Partnership Programme to generate awareness and raise the cybersecurity posture of local businesses, individuals and the community. Please note that CSA does not endorse or recommend any particular organisation, individual, product, process, or service that is linked to the SG Cyber Safe partnership programme. Neither can CSA assure the quality of the work of any organisation or individual linked to the SG Cyber Safe partnership programme.