puppet

SOLUTION BRIEF

Why CIS Benchmark Compliance Matters for APAC Organizations + How Puppet Can Help

- Why CIS Benchmark Compliance is Important Across Private + Public Sectors
- Examples of Organizations Who Failed to Meet Compliance
- How Puppet Helped DBS Bank Build Secure, Scalable Compliance

Introduction

Your organization's infrastructure is unique. So is your compliance.

For most organizations, IT compliance is a necessary step that takes up an unnecessary amount of time. It's more than configuring or enforcing controls; it's the time spent gathering documentation, proving compliance, working with auditors, and remediating drift when you're found to be noncompliant.

This document outlines the use case for CIS Benchmarks in the infrastructure and IT systems of APAC organizations, as well as why they're specifically well-suited for helping organizations in Singapore establish, meet, and prove an appropriate degree of compliance across public and private sectors. It also elaborates on how the right choice of compliance assessment and enforcement solution helps you establish a compliance strategy that enables your organization to innovate without compromising system security.

What Are CIS Benchmarks?

CIS Benchmarks are a set of internationally recognized cybersecurity standards for imposing and evaluating security controls in an IT system. CIS Benchmarks are utilized by both public and private sector entities to strengthen their cybersecurity defenses.

CIS Benchmarks are created to ensure cybersecurity in critical systems, but they're developed by a global community of cybersecurity experts. Their industry-agnostic, international acceptance makes them a lucrative standard for meeting a wide array of regulatory expectations for cybersecurity.

CIS Benchmarks help strengthen cybersecurity and prevent breaches by:

- Outlining security configuration standards
- Proposing hardening guidelines
- Offering vulnerability mitigation strategies
- Facilitating in compliance and auditing

The hundreds of controls outlined in the CIS Benchmarks apply to software, mobile devices, servers, operating systems, and network devices. Additionally, CIS Benchmarks are organized into three distinct levels that allow organizations to choose the security hardening standards that align with their security objectives and risk tolerance. Virtually every organization in the world with any kind of IT infrastructure uses some kind of technology mentioned in the CIS Benchmarks.

Why Do CIS Benchmarks Matter in APAC?

In addition to a growing threat landscape, organizations in Singapore, both in the public and private sectors, are subject to strict cybersecurity regulations.

CIS Benchmarks Help Meet Regulatory Compliance

The Singapore government has established stringent cybersecurity regulations and guidelines (like the Singapore Cybersecurity Act of 2018) to protect critical infrastructure and sensitive data. These regulations require organizations doing business in Singapore to implement cybersecurity measures to secure their networks, data, and systems.

For example, the Singapore Personal Data Protection Act of 2012 (PDPA) is focused on protecting Singaporeans' personal data. Enforced by the Personal Data Protection Commission (PDPC), the PDPA outlines rules and regulations on how organizations can collect, use, store, and disclose the personal information of Singaporean citizens. Among many other measures, the PDPA requires specific measures be

put in place to protect Singaporeans' individual data as it's transferred to other countries. Non-compliance with the PDPA can result in penalties, millions of SGD in fines, and significant reputational damage.

System Security Acceptance Testing (SSAT), created by the Cyber Security Agency of Singapore (CSA), evaluates the effectiveness of an organization's security controls and their ability to mitigate vulnerabilities in their critical infrastructure. Among other metrics, the SSAT tests the effectiveness of security hardening controls like the ones outlined in the CIS Benchmarks. While there are no stated fines for failing the SSAT, all public sector IT projects in Singapore are subject to testing prior to project commissioning.

In 2019, the Monetary Authority of Singapore (MAS), the central bank of Singapore, issued the Notice on Cyber Hygiene. It outlines cyber hygiene requirements for financial institutions, including securing admin accounts, security patches, configuration standards , network defenses, malware protection, multi-factor authentication, and more. The Notice applies to all banks in Singapore, and failure to comply can cost a bank up to $100,000 – with an additional $10,000 fine per day of continued non-compliance.

CIS Benchmarks provide detailed configuration standards that align with best practices and meet many of the obligations of the Singapore Cybersecurity Act, the PDPA, Cyber Hygiene, the SSAT, and other relevant regulations for organizations in Singapore.

CIS Benchmarks Help Address the Singapore Cyber Threat Landscape

As a global financial hub and a digitally connected nation, organizations in Singapore face numerous mass-scale cybersecurity threats. Data, networks, and systems integrity all feature vectors for cyberattacks, both internal and external. Even a single accidental or non-malicious act can cripple system security.

The 2018 SingHealth Data Breach is one such incident that highlighted the importance of robust cybersecurity measures in Singapore. Singapore's largest healthcare group experienced a major cyberattack resulting in a data breach, which compromised the personal and medical records of about 1.5 million patients – including the Prime Minister of Singapore.

Cyberattacks in Singapore's other business sectors have had similar effects. The Ministry of Defence (MINDEF) breach in 2017 exposed the personal data of soldiers and staff. The attack targeted the internet-facing systems of the Singaporean government, underscoring the vulnerability of even the highest offices. In 2018, StarHub, a telecom provider in Singapore, faced DDoS attacks that disrupted internet services to its customers – costing the company revenue in the form of downtime, customer service, and work to bring systems back online.

Adhering to CIS Benchmarks gives organizations a framework for addressing common vulnerabilities and threats (like breaches, leaks, and DDoS attacks) before they become incidents. Because CIS Benchmarks outline specific guidelines for operating systems, device security, software, and more, they help fortify defenses against known and unknown attack vectors.

How Puppet Helps Organizations Enforce CIS Benchmarks

DBS Bank, a leading Asian financial services group headquartered in Singapore, built their proprietary system security framework (SecureSys) with Puppet. Moving from manual configuration management to automated compliance helped them reduce dedicated compliance staff from 13 members to just three. That lets them reallocate valuable human resources from mandatory compliance to IT projects that drive real value for their business. With Puppet, all drift in DBS Bank's configurations is automatically healed, and reports are automatically generated every 30 minutes from within Puppet.

Using Puppet, DBS Bank also handled complex RBAC and built SecureSys for long-term scalability.

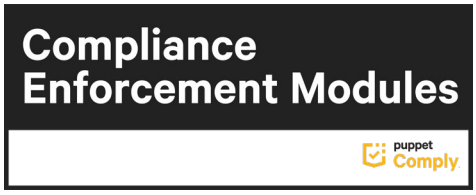
Read the full case study here >>

Puppet Comply continually reviews your infrastructure for compliance with CIS Benchmarks and other cybersecurity standards to give you instant insights into your compliance state. In fact, Puppet Comply

integrates the Center for Internet Security's own CIS-CAT Pro Assessor to evaluate compliance with CIS Benchmarks automatically.

In-depth charts, graphs, and trends in Puppet Comply give you unprecedented visibility into your compliance state over time. With provable compliance and a detailed record of what changes were made, when, and by whom, weeks of burdensome audit prep is reduced to hours.

Puppet Comply also allows you to define your desired compliance so you can comply with multiple cybersecurity standards and frameworks simultaneously – down to the node level, including on individual machines.



Puppet Comply detects and reports on noncompliance in your network. Compliance Enforcement Modules (CEM) automatically remediate drift and bring your systems back into compliance. CEM are modules for Puppet Enterprise that are aligned with CIS Benchmarks, saving IT operations and security teams the time of manual configuration and enforcement. CEM are a truly plug-and-play solution for continuously enforcing CIS Benchmark compliance in any infrastructure.