Hap Seng Consolidated Berhad chose SecureKi to secure their access to corporate resources with centralized credential management and security policies, improving device visibility, and more.

> “Having a manual system for password management these days just won't cut it anymore.
>
> **Chia Nam Liang**
>
> *Hap Seng Group CIO*

The Company

Hap Seng Consolidated Berhad ("HSCB") is a public company listed on the Main Market of Bursa Malaysia Securities Berhad, with over RM21.03 billion in market cap and 1,500 employees. HSCB is a diversified group with six core businesses, namely plantation, property investment & development, credit financing, automotive, trading, and building materials

Zero Trust for a Remote Workforce

Companies today find themselves dealing with a growing number of contractors and other third-party vendors accessing their crucial data and applications. Often, these vendors never set foot on company property and instead work from various locations around the nation. Lack of visibility and control over devices as well can potentially put critical resources at risk. A vital component of any zero-trust strategy is to enforce controls so only approved users can access the resources for which they are approved. A solid workforce security strategy can enable organizations the flexibility to work with third parties remotely while ensuring critical applications and data are safe. Hap Seng implemented such a strategy with SecureKi and secured all their third-party access from all their servers and sensitive network devices in Malaysia.

The Challenges

Cybercriminals frequently consider conglomerate companies such as Hap Seng a target-rich environment to infiltrate. With an extensive network of third parties such as vendors and contractors, it only adds complexity when enforcing access control policies. When third parties share credentials while accessing company resources, it increases the risk of credentials being compromised. To prevent these bad security practices, the team at Hap Seng looked for a multifactor authentication (MFA) solution that gave administrators the visibility they needed to track the number of devices registered and access requests.

The company also sought to have a Privileged Access Management (PAM) solution to enforce and automate role-based privileged access control to secure accounts and mitigate password vulnerabilities.

The Solution

The IT security team at Hap Seng evaluated several MFA and PAM solutions and narrowed them down to two at the proof-of-concept (POC) stages. "Two rounds of POC wasn't easy, as my IT team at Hap Seng was not only demanding but meticulous to ensure all issues are ironed out smoothly, having SecureKi's solutions tested on every server and device in each location!" says Chia, Hap Seng Group CIO.

The IT security team at Hap Seng evaluated several MFA and PAM solutions and narrowed them down to two at the proof-of-concept (POC) stages. "Two rounds of POC wasn't easy, as my IT team at Hap Seng was not only demanding but meticulous to ensure all issues are ironed out smoothly, having SecureKi's solutions tested on every server and device in each location!" says Chia, Hap Seng Group CIO.

Securing Access to Critical Business Applications

Hap Seng requires its vendors and contractors to use VPN to access their business's applications. SecureKi's MFA & PAM worked seamlessly with the company's existing VPN solutions and was able to enforce end-to-end zero-trust policy adoption for all employees and third-party VPN access across their devices platforms.

With SecureKi in place, Hap Seng can report on any user activity and has a single dashboard that provides visibility on users accessing their protected resources and the devices that have access. The team can make security decisions and establish access policies that protect their environment without interrupting their day-to-day activities.

In addition, Hap Seng has established security best practices across their environment with SecureKi's PAM – Automating password change policies based on pre-defined rules to meet their security compliance, providing their IT admins with personalized workflow for quicker access, and improving usability with a centralized credential management solution. "It's tedious and time-consuming to change all local network devices and systems' privileged accounts and passwords to meet compliance requirements. Having a manual system for password management these days just won't cut it anymore," states Chia.