cpl.thalesgroup.com

THALES
Building a future we can all trust

Healthcare Organization Addresses Cloud Access Management Solutions with the OneWelcome Identity Platform

Summary

A recruitment firm-cum-clinical process outsourcing (CPO) company based in Philippines requires an access management system to centrally manage and secure access to cloud applications like Microsoft Azure administrator portal and Microsoft Office 365 users, as well as the ability to secure on-premises systems like Windows devices by introducing modern authentication based on contextual attributes and utilizing policy based Single Sign-On for ease of use and user convenience.

The Organization

The healthcare organization operates as a nurse recruitment and deployment agency for healthcare business process outsourcing (BPO) services to deliver clinical and administrative services on a global scale.

They focus on clinical workflows provide premium services for the following:

- Hospitals and Health Systems
- Health Plans
- Managed Care Organizations and Third Party Administrators (TPA)
- Healthcare Service Companies

The healthcare organization provides dedicated teams of over 3,000 remote and onsite clinicians who solve medical and administrative problems on a daily basis.

The company is based in the United States and the Philippines.

Business Need

The healthcare organisation required an access management system to centrally manage and secure access to cloud applications like Microsoft Azure administrator portal and Microsoft Office 365 users, as well as the ability to secure on-premises systems like Windows devices by introducing modern authentication based on contextual attributes and utilizing policy based Single Sign-On for ease of use and user convenience.

Additionally, to further enhance their overall security posture, the organisation required the ability to enforce policies on a real-time basis at the individual user, group or application level.

The State of Security in Asia-Pacific Organisations

Insights from the 2020 Thales Asia-Pacific (APAC) Data Threat Report reveal that nearly half (45%) of all data from APAC organisations is stored in the cloud, and with under half of that data (42%) in the cloud is described as sensitive.

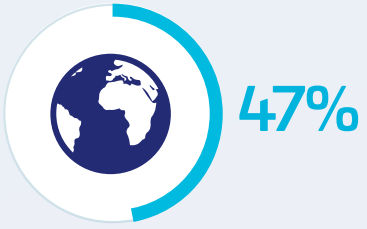
The study further reveals that APAC businesses are increasingly vulnerable to cybersecurity threats, with two-thirds of the surveyed executives in APAC seeing themselves as vulnerable to internal data security threats.

Security Risks from Working from Home

Working from home has become the new norm due to the Covid-19 pandemic, leaving most employees in Asia-Pacific, including the Philippines, to use their own personal devices to perform work-related tasks.

Unsecured devices for employees are among one of the difficulties that organisations may face as they may result in security risks for organisations. A recent Asia-Pacific study polled that 45% said their organisation did not provide employees with "additional training on dealing with cybersecurity risks associated with working from home."

of Asia-Pacific organisations admitted to having been breached in the past year.



of Asia-Pacific organisations have experienced a breach at some point in their history.

of Asia-Pacific respondents' focus is on data security, yet data security averages just 14.5% of overall IT security budget.

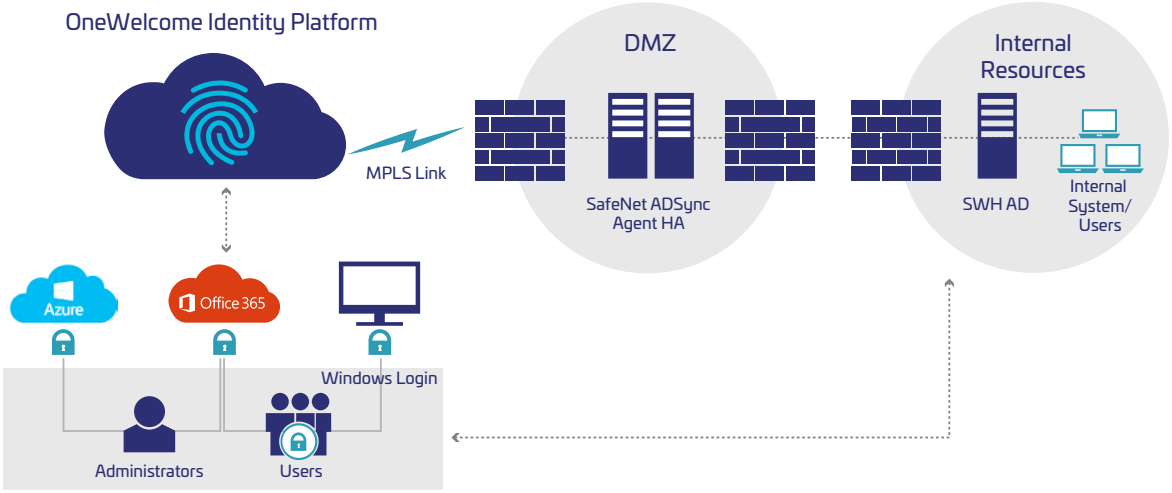
Key findings from the 2020 Data Threat Report – Asia-Pacific Edition show that 47% of APAC organisations have experienced a breach at some point.

Solutions

The healthcare organization choose Thales OneWelcome Identity Platform as their solution to centrally manage and secure access to cloud and on-premises applications. OneWelcome not only simplified their login experience for users but also reduced the overall security risk by applying flexible risk-based policies, smart Single Sign-on (SSO) and universal modern authentication methods.

As part of the solution, OneWelcome offered five core capabilities.

1. **Smart Single Sign-On (SSO).** Smart Single Sign-On (SSO) lets users log into all their cloud applications with a single identity, eliminating password fatigue, frustration, password resets and downtime. OneWelcome processes a user's login requests and ensures that SSO is applied intelligently, based on previous authentications in the same SSO session and the specific policy requirements applicable to each access attempt. In this way, users may authenticate just once in order to access all their cloud applications, or provide additional authentication as configured in the policy.



2. **Scenario-based Access Policies.** OneWelcome offers flexible access management through a simple to use policy engine that gives customers real-time control over the ability to enforce policies at the individual user, group or application level. The policy engine supports a broad range of authentication methods, including ones already deployed, allowing organizations to leverage their current investments and use them to secure cloud and web-based services.
3. **Data-driven Insights.** Data-driven insights into access events enable organizations to fine-tune their access policies, and ensure that they are neither too lax nor too stringent. Statistics and logs on access activity per app and per policy, along with the reason for failed or denied access attempts, facilitate audits and support inquiries, and allow identifying underutilized cloud app licenses.
4. **Universal Authentication.** OneWelcome supports numerous authentication methods and allows you to leverage authentication schemes already deployed in your organization. The broadest range of authentication methods and form factors supported combined with context-based authentication enhances user convenience and allows you to manage risk by elevating trust only when needed.
5. **Easy App Management**. A continuously expanding library of integration templates enables the easiest connectivity to leading cloud apps, such as Salesforce, AWS and Office 365. Just use the integration templates already built-in and defined for the apps you use today, or use the general-purpose custom integration template.

OneWelcome Identity Platform – Access Management as a Service

OneWelcome is a cloud-based access management service that combines the convenience of cloud and web single sign-on (SSO) with granular access security. By validating identities, enforcing access policies and applying Smart Single Sign-On (SSO), organizations can ensure secure, convenient access to numerous cloud applications from one easy-to-navigate console.

Benefits:

- Fast and easy cloud access through Smart Single Sign-On (SSO)
- A single pane of glass for centralized user access control
- Optimized security through fine-grained access policies
- Visibility into all access events for simplified compliance
- Secure access for partners and contractors
- Powerful and broad range of authentication methods

The Thales OneWelcome Identity Platform streamlines secure access, eliminates password hassles for IT and users, provides a single pane view of access events across your app estate and ensures that the right user has access to the right application at the right level of trust.

To learn more about Thales' the OneWelcome Identity Platform, click here.

Integration with Privileged Access Management Solutions (PAMs)

The healthcare organization will be using OneWelcome Identity Platform to integrate with Privileged Access Management Solutions (PAMs) to secure privileged accounts. A PAM solution can ensure the security of privileged accounts, only if the IT administrators accessing the solution have the right to do so.

To learn more about Privileged Access Management, click here.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.