Password-less protection

Kloudynet

Aim

To enable easy and secure access to corporate owned devices and apps by eliminating the user of passwords.

System Objectives

- ➢ Users should be able to sign in directly via biometric recognition—such as fingerprint scan or facial recognition.
- ➢ Enabling single sign-on across enterprise applications to provide a superior log in experience for existing users and reducing or eliminating log on prompts.
- ➢ Manage end user device configuration, Windows update and ensure compliance, create an optimal device experience for users.

Challenge

Our customer is one of the leading telecommunications groups in Asia

With needing to key in a complicated password just to gain access to the device and then on top of it forgetting the right login credentials was naturally a major setback, for IT department and it costs more than just password support and maintenance.

- Even employing stronger password with complexity and demanding more frequent password changes isn't enough for current cybersecurity threats and lead to poor user experience related to password reset requirements.
- Passwords are increasingly become predictable and leave users vulnerable to theft. Even the strongest passwords are easily phishable and is a major cause of concern.
- Managing the end user corporate owned devices in this modern complex environment and keeping the devices up-to date and secure, with the workforce connecting from anywhere round the clock is a difficult task.
- With increasing number of corporate applications, users must remember application-specific passwords and sign-ins for each application. Users need to remember their passwords, plus spend the time to sign into each application.
- Given the complexity in managing the current needs of managing the end user devices, complex user passwords and providing easy access to corporate applications, customer was looking at a easier, reliable and secure solution, which can help IT control and manage devices, including settings, features, and security from anywhere.

81% of hacking related breaches used either stolen or weak password

Technologies Used

- The Azure Active Directory (Azure AD) enterprise identity service provides single sign-on and multi-factor authentication to help protect your users from 99.9 percent of cybersecurity attacks.
- Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM). It integrates with other services, including Microsoft 365 and Azure Active Directory (Azure AD) to control who has access, and what they have access to, and Azure Information Protection for data protection.
- Windows Hello for Business lets you use your face, iris scan, fingerprint, or a PIN to unlock your Windows PC quickly, without using a password and lets you authenticate to an Active Directory or Azure Active Directory account.

Why kloudynet

- Microsoft Silver partner with expertise in M365, Business Process Automation & Azure
- Certified M365 and Security consultants with experience in consultation and deployments at large enterprises
- Managed SLA backed support including out of hours support and 24/7 monitoring
- Azure expertise areas
    - Migration – Architecting & Designing Cloud landscape
    - Security, Governance & Compliance – Auditing security & governance of Cloud landscape
    - Managed Services for Azure and M365 Managing & Optimizing Cloud Landscape

For more info, or a demo:
Mail – sales@kloudynet.com
Call - +60107122130

Solution/Action Taken

- Customer decided adopting Microsoft password-less strategy to eradicate the use of passwords, the authentication requires two or more verification factors to sign in that are secured with a cryptographic key pair. Windows Hello for Business replaces passwords and enables the user to authenticate to enterprise applications, content, and resources without a password being stored on your device or in a network at all.
- Setup Single Sign-On (SSO) for all corporate applications with Azure Active Directory so that all employees could quickly access the corporate applications without multiple prompts, or the need to manage multiple passwords.
- Enroll the corporate owned windows devices to Intune, move from Configuration manager to modern approach of managing the devices settings, security and updates and push applications with Microsoft Intune without the need to maintain hardware infrastructure.
- Customer is also looking to manage the end user devices with Intune Mobile application management capabilities to protect the company information and prevent information

Benefits

- Windows Hello for Business replaces passwords in every common situation except for the initial one-time provisioning of its strong credentials, meaning IT doesn't have to sink so much time into resetting users' passwords and verifying their identities and IT can devote time to more strategic projects.
- Users can sign in faster to use applications and services, since Windows Hello for Business also has support for SSO with Azure AD, users can sign into multiple applications with a common set of credentials and not have to reenter them on a per-application basis once logged in onto the system.
- Microsoft Intune gives the capability to set and define policies via a single admin portal that allows rules configuration and device management, scan computers for malicious software, define whether to require enrolled devices to have TPM chips onboard, push applications and manage update policies and incase the device is stolen or lost a full wipe can be initiated remotely that will keep the companies confidential information safe.