CLOUDFRONTS™
Dynamics 365 & Power Platform
MICROSOFT GOLD PARTNER

Case Study

Customer Success Story – Kloudify Technologies

CloudFronts collaborated with Sydney, Australia-based Microsoft partner Kloudify Technologies to deploy M365 to one of the NSW's leading boutique law firms specializing in liquor and gaming regulations.

About Kloudify

Being a Cloud Migration, Managed Services, and Security Specialist, Kloudify offers Microsoft Cloud Service and IT Solutions for SMBs in Australia to help run their business smoothly and securely. Please explore https://kloudify.com/

Business Challenges

The client's customer, a Sydney-based reputed law firm required stringent security and compliance policies in place to safeguard their organizational data as they were dealing with highly regulated gaming and liquor clients. Besides, they also required SPF and DKIM policy to be set up to mitigate any cyber attacks or risks.

Solution

Over the years, CloudFronts has been deploying Enterprise Mobility + Security (EMS) suite for its customers in the U.S. which is a mobility management and security platform that helps protect and secure your organization's data and empower your employees.

Microsoft discovered that on average, around 0.5% of all accounts get compromised each month, a number that in January 2020 was about 1.2 million. Of all the hacked enterprise highly sensitive accounts, only 11% had a multi-factor authentication (MFA) solution enabled, as of January 2020.

Considering the requirements in mind, Microsoft's Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) were configured on the customer's hardware. Simply speaking, Sender Policy Framework (SPF) is a security mechanism created to prevent the anti-social elements from sending emails on your behalf. DomainKeys Identified Mail (DKIM) is an email security standard designed to make sure messages aren't altered in transit between the sending and recipient servers. Mobile Device Management (MDM) solutions like Microsoft Intune have been deployed to protect the law advisory firm's highly sensitive organizational data by requiring users and devices to meet some requirements. In Intune, this feature is called compliance policies, and those were set up. Microsoft Multi-factor authentication (MFA) adds a layer of protection to the sign-in process. When accessing accounts or apps, users provide additional identity verification, such as scanning a fingerprint or entering a code received by phone.

> *"Your password doesn't matter, but MFA does." - Alex Weinert, Microsoft's Group Program Manager for Identity Security and Protection*

Key Technologies

1. Microsoft 365
2. Enterprise Mobility + Security (EMS)
3. Microsoft Intune

Post Go-live

Post-Go-live, the law firm was able to report the following benefits:

1. Microsoft MFA is helping the customer to protect itself by adding a layer of security, making it harder for attackers to log in.
2. As SPF is added as a TXT record that is used by DNS to identify which mail servers can send mail on behalf of your custom domain, DKIM and SPF are helping the firm to prevent spoofing and phishing.
3. Microsoft Intune is providing the client with the flexibility it needs to control their critical data regardless of the device. Due to its cloud-based feature, Intune can work to secure iOS, Windows, and Android devices from one single mobile solution.

Email us your requirements at ashah@cloudfronts.com or fill out the contact us form.