THALES

Law Firm lifts the Fog over Cloud App Security with SafeNet Trusted Access

Overview

Lawyers typically have very specific IT needs and user experience is key. As a niche industry, security is critical to their business survival. The danger of cyber-attacks is real: The FBI has been warning about impending attacks for a few years. With the growing number of cloud applications, it's no longer enough to secure in-house, on-prem applications. Many law firms work remotely with both clients and regulatory bodies – using cloud and web-based applications or integrated cloud applications, such as (but not limited to) Salesforce, AWS and Citrix .

Apart from potential financial and reputation damage, the drivers for law firms to manage access to their applications, there are regulatory drivers as well. For example, GDPR and U.S. law may require firms to notify both clients that they represent and regulators if they suspect a data breach of personal data.

According to LOGICFORCE and an ABA Technology Survey, 22% of law firms were attacked in 2017, up 14% from the previous year. One of the reasons these firms are particularly vulnerable to breaches is because many do not invest the money to properly secure their data.

Challenge

In light of increasing regulations and the need to protect their growing number of cloud and web-based applications, a law firm approached Thales to inquire about their new Access Management solution – SafeNet Trusted Access. The law firm was an established customer and was already using Thales's SafeNet Authentication Service installed in on-premises. However, they wanted to extend protection to their cloud applications without increasing the login burden for their staff. The organization was looking for a solution that could offer flexible policies which could differentiate between trusted and risky networks.

> " Contextual logging in from within and outside the office was really important to us. With SafeNet Trusted Access, we enjoy great user experience with push authentication and SSO."
>
> – Security Officer, Law Firm

The Solution

Thales's SafeNet Trusted Access offered the law firm simplified cloud access with Single Sign On (SSO) secured by contextual access security. The Access Management Service provides privileged access policies for senior partners, financial officers or other executives. Policies can be set up per role, i.e. paralegal or clerk, who will not need access to sensitive applications.

Context-sensitive SSO

SafeNet Trusted Access combines the convenience of single sign-on with context-sensitive access security. By validating identities, the solution helped the law firm ensure secure, convenient access to all their cloud and web-based applications. Smart SSO let the law firm employees and contractors log in to all their cloud applications with a single identity, and only requires them to provide additional authentication in high risk login situations. Depending on their role or location, users are required to provide additional authentication or less restrictive steps, as required by the access policies. In this way, users may authenticate just once in order to access all their cloud applications, or provide additional authentication, as required by the policy.

Benefits

Thales's SafeNet Trusted Access provided the law firm with the level of security they required as well as flexible access management policies. These included different policies based on role, context or location. For example, it was very important for the law firm to mitigate high and low-risk cases, inside the office (trusted networks) and outside the office (higher risk networks).

SafeNet Trusted Access allowed the law firm to integrate with more cloud applications as the company expanded, and restrict or alleviate authentication as needed, to workers and contractors across the legal ecosystem.

About SafeNet Access Management and Authentication Solutions

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policybased SSO and universal authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.

To learn more about access management from Thales,

visit https://safenet.gemalto.com/access-management/ or join a livedemo webinar at https://www.brighttalk.com/webcast/2037/334449

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.

Policies in SafeNet Trusted Access for users working remotely or from trusted networks

REMOTE ACCESS ⓘ

Conditions ⓘ	Requirements ⓘ
When an access attempt occurs under all of the conditions	Then access is
	Granted
⧉ Network - Outside these networks ⌃	After authenticating with
Define IP addresses to be checked for within this condition. You can specify IP addresses in the following formats: - Single, example: 1.1.1.1 - Range, example: 1.1.1.1-1.1.1.255	**Password** ⓘ Every access attempt
1.1.1.1-1.1.1.10	**Token Based Authentication (OTP)** ⓘ Every access attempt

Trusted network access ⓘ

Conditions ⓘ	Requirements ⓘ
When an access attempt occurs under all of the conditions	Then access is
	Granted
⧉ Network - Inside these networks ⌃	After authenticating with
Define IP addresses to be checked for within this condition. You can specify IP addresses in the following formats: - Single, example: 1.1.1.1 - Range, example: 1.1.1.1-1.1.1.255	**Password** ⓘ Once per session
1.1.1.1-1.1.1.10	