


What's the best mobile security for the staff of a financial services provider? 

The one its workforce will use.

Any defences an organisation puts into place for authentication are rendered moot if they're too cumbersome for users to adopt.

So when a Financial Services Provider was looking to upgrade its security for a new Bring Your Own Device (BYOD) policy, its technical services department turned to the one authority that could advise them on which characteristics would be easily adopted by everyone on the staff: the users themselves.

Challenge

For the Financial Services Provider, mobilising its workforce would have significant benefits for productivity and communications, while at the same time acknowledging the burgeoning use of and preference for personal devices.

Additionally, as the organisation looked towards the future of technology and the new generation of workers, it was clear this initiative would fit within the organisation's ongoing strategy to make its systems and data more available at any time from any device.

This momentum led the business to roll out BYOD and CYOD (Choose Your Own Device) initiatives, and mandated that the technical team find a way to allow sensitive data and networks to be accessed by the mobile devices in a secure manner – and only by authorised users.

How could the technical team find a solution that met the legal and regulatory obligations to adhere to internal security policies, while fitting in with the objectives of a mobilised workforce?

Exploration

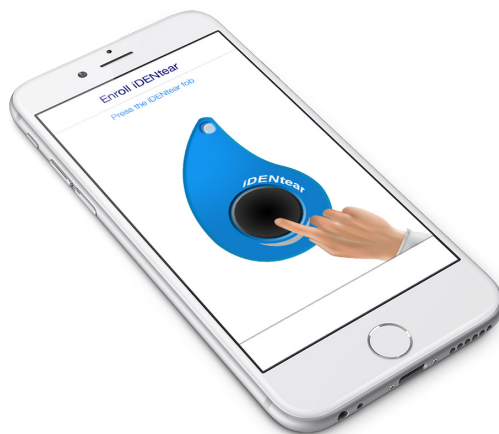
With the challenge in place to provide the highest levels of security, the Financial Services Provider conducted internal surveys to determine what their users expected from their mobile device and how they perceived their way of working would change in the future.

The results of the questionnaire were clear: user experience and simplicity featured highly as requirements.

Long complex passwords, cumbersome or bulky hardware, and excessive authentication processes – typically associated with security initiatives – would not be well adopted by users.

At the same time, strong security needed to be guaranteed so that the mobile strategy could be executed – for instance, how would data be protected if a mobile device was accidentally misplaced or stolen?

Traditional security methods were becoming outdated and weren't considered strong enough to ensure protection against today's technology threats – such as sophisticated malware, phishing and cyber attacks – so simple software-based solutions would not be sufficient. Only physically segregated, true multi-factor authentication would ensure the highest level of security, or sensitive data would be at risk.



Solution

With its simple “click and forget” functionality, Apply Mobile's iDENTtear® became the solution of choice for the Financial Services Provider. iDENTtear provided the seamless experience that was best aligned to the expectations of the user base, together with superior authentication and data security compared to other products the organisation tested.

At the user level, iDENTtear simplified the experience just as employees demanded; it's a simple one-button press that requires no juggling of devices or reading codes from the screen of one device and inputting those codes into a second device.

End users would prefer using their mobile devices when sending and receiving secure emails – this can be a problem in regards to security on mobile as secure email requires both a decryption key and a digital signature key to be used along with a strong and secure way of managing those keys. With iDENTtear, users can now use their mobile devices to interact with secure email and maintain the expected level of security and trust for these confidential transactions, directly from their mobile devices.

From an administrative perspective, integration with existing technologies such as RADIUS and Active Directory – and leading Mobile Application Management (MAM) and Mobile Device Management (MDM) platforms – provides ease of use for overall administration of infrastructure.

Most importantly, iDENTtear is aligned to FIPS 140-2 Level 3 and meets the requirements for strong authentication (NIST LOA4) to achieve the strictest security goals of the Financial Services Provider for strong data protection.

The Result

iDENTtear is a strong and secure solution that provides a great user experience, consolidates existing fragmented - and outdated - toolsets, brings significant cost savings and provides a strong security success factor for any financial services provider's mobile strategy.

With traditional security technologies being incapable of providing the required protection, iDENTtear gives users who are the first line of defence against modern malicious attacks, the tools to ensure data remains safe. Our multi-layered approach keeps the workforce well-armed to protect against unauthorised access to sensitive and valuable information, the most valuable asset to any of today's modern businesses.