thalesgroup.com

THALES

Thales's SafeNet Trusted Access Helps Prevent Employee Identity Theft at VUMC

Plagued with phishing emails almost daily, this Nashville-based medical center at Vanderbilt University decided to add an extra layer of security by leveraging multifactor authentication within their organization. With the help of Thales (formerly Gemalto), VUMC can thwart cyber criminals' attempts at stealing sensitive data.

The Organization

Managing more than 2 million patient visits annually, Vanderbilt University Medical Center (VUMC) in Nashville, Tennessee, is one of the largest academic medical centers in the southeast U.S.A.

The Business Need

According to VUMC, cyber criminals had been targeting this healthcare institute to steal employee login credentials and then try to enter C2HR, the center's self-service human resources portal. Human resource departments are a favorite among thieves, because that is where a lot of the most delicate employee data is held. The most common tactic in this institute was email scams where imposters sent phishing emails, posing as VUMC employees. With employees' email login credentials, hackers can access the human resource departments and attempt to get ahold of their bank account information, automatic deposit of paychecks information, and social security numbers.

Challenge

- Vanderbilt University Medical Center sought an effective MFA solution that would prevent unauthorized access to employee credentials and thus minimize risk of manipulating these credentials to commit fraud, such as phishing attacks.

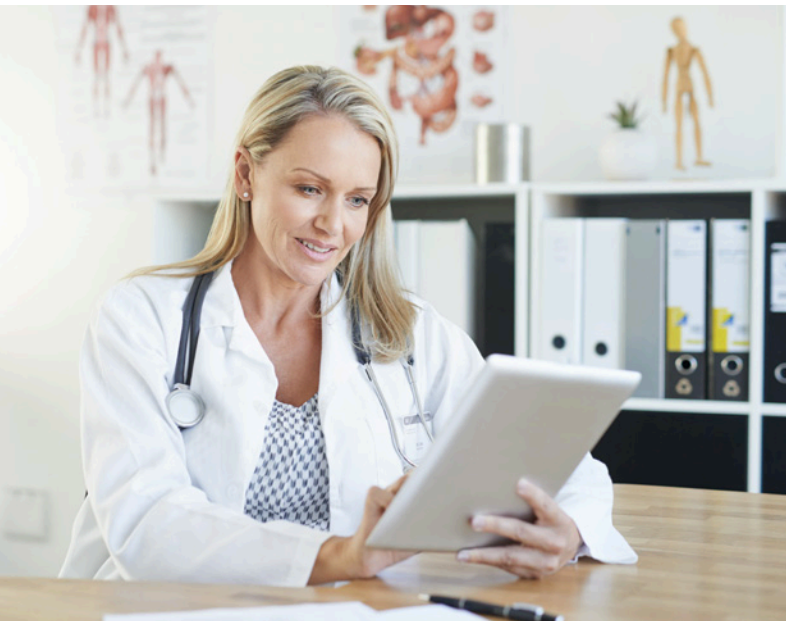
Solution

- SafeNet Trusted Access (formerly SAS Cloud), Thales's cloud-based Authentication Solution was chosen, along with SafeNet MobilePASS, to support both software and hardware options for their employees' varied network access devices.

Benefits

- Deploying the solution has enabled the medical institute to protect employee data integrity, enable stronger access to systems and resources, and prevent security breaches.

VANDERBILT UNIVERSITY
MEDICAL CENTER



" We're beginning the switch to broad use of multi-factor authentication as an important new safeguard for our employees and our enterprise. Security attacks are unrelenting, and we view MFA as a vital and necessary addition to VUMC's enterprise cybersecurity program."

– Andrew Hutchinson,
Executive Director, of Enterprise Cybersecurity, VUMCany

The enterprise cybersecurity unit of VUMC in Nashville detected phishing emails being sent using stolen or fake names of employees. VUMC noted that since 2016, the volume of phishing emails increased in the top five targeted industries, including healthcare, by about a third. These attacks coincide with figures reported by Gemalto's breach level index H1 2018 report – Healthcare companies experienced the greatest amount of security events in the first half of 2018, amongst all the industries. Thales also explains that the larger ramification of data breaches is often unknown, as hackers use stolen data to orchestrate other attacks.

With sensitive and confidential data being endangered on a daily basis, VUMC needed a method to add another layer of security to make sure that only authorized people accessed certain resources. The medical institute needed to put an end to the theft of employee credentials, as the first step to minimize security breaches. Preventing corporate identity theft also mitigates the risk of cyber criminals being able to these credentials to carry out phishing attacks and potential financial and reputational damage to the institute and its employees. Multi-factor authentication requires that users must provide something more than (or stronger than) a password to log into a system. Using a second factor or third factor of authentication, employee credentials are much harder to seize.

The Solution

VUMC now utilizes Thales's SafeNet Trusted Access, Thales's cloud-based Authentication Solution and SafeNet MobilePASS. As of November 19, 2018, VUMC requires multifactor authentication when users of the self-service portal of the university medical center's human resource center try to access their direct deposit details, tax information or personal profile. This capability was provided by an app called SafeNet MobilePASS, which can be downloaded to most mobile devices. Users without a smart phone can use a hard token with a digital readout for display of authentication codes.

Multifactor Medicine in Nashville: Thales's SafeNet Trusted Access

SafeNet Trusted Access leverages the authentication methods already employed in an organization's cyber security program. Switching to a broader practice of multi-factor authentication safeguards access to sensitive information. This is done by replacing a static password with a second factor of authentication that cannot be hacked or stolen. SafeNet Trusted Access supports a large variety of form factors and authentication methods to allow VUMC stronger authentication and more secure access to effectively manage risk.

The Benefits

Benefits for VUMC

- Prevent security breaches: SafeNet Trusted Access mitigates risk associated with identity thefts. With additional factors of authentication required when users access sensitive resources, the medical institute can reduce risk of compromised data records, protect the integrity of their systems and prevent potential threats and security breaches.
- Provides flexible form factors for diverse use cases: SafeNet Trusted Access supports both software and hardware authenticators. Thales offers VUMC whichever option their employees require, depending on the device they use to access their systems. System users with mobile phones can receive multi-factor authentication codes via a smartphone app or SMS text message. Users without a mobile phone can use a hard token that displays their authentication codes digitally.
- Leverage MFA throughout the enterprise: To comply with DEA rules for electronic prescribing of electronic prescribing of controlled substances, VUMC deployed MFA with a Thales SafeNet system in November, 2017. A year later, VUMC has implemented SafeNet Trusted Access for HR portal purposes. VUMC is leveraging the success of MFA for other areas. According to Andrew Hutchinson, executive director of Enterprise Cybersecurity at VUMC, 'additional VUMC systems will begin to require this form of user authentication'.

A more secure future

VUMC mission statement states that Vanderbilt aims to 'combine their transformative learning programs and compelling discoveries to provide distinctive personalized care'. Thales's SafeNet solutions assist Vanderbilt in managing, protecting and caring for the users involved in this mission, helping to ensure that their data remains in the hands of authorized users only.

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.

© Thales - November 2019 • RMv7

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com