CASE STUDY

Texas Trust Credit Union Protects Its Employees and Members With Email Security and the Fortinet Security Fabric

Walk into any bank, credit union, or other financial institution, and you will see many obvious physical security deterrents, from cameras to the safe in the back room. However, one of the most important security measures is one you cannot see from the lobby: a secure email solution.

For Texas Trust Credit Union, that solution comes from Fortinet's FortiMail.

Texas Trust was established in 1936 and has been a fixture in the Dallas-Fort Worth area since 1948. After three mergers in the past 10 years, the credit union now has 23 branch locations and $1.7 billion in assets.

From a cybersecurity perspective, Texas Trust's biggest threat—and biggest attack vector—is email. "We have always been and will forever be a 'people company,' which means we focus on doing right by our members. Especially when it comes to protecting our members' information against security threats," says Blayne Henke, AVP of Cybersecurity for Texas Trust Credit Union.

The credit union gets a quarter of a million emails per month, and about 50,000 of those emails are spam. "Last month alone, we had 50 virus and malware attempts come through email," says Henke. "Those are pretty big numbers for a small credit union in Texas. We have had spear phishing, attempted spoofing of our CEO, and any other type of attacks through email. There are a lot of advanced persistent threats [APTs] out there that specifically target financial institutions like ours."

Ransomware: A Huge Concern

So far, Texas Trust has been fortunate enough to avoid ransomware attacks. But they are not taking any chances. In addition to implementing security awareness training and putting controls into place, they lock down and quarantine certain emails.

"If a user gets an email with loan documents to refinance a car, for example, those are the types of emails that get flagged for their quarantine, and it can be troublesome to review and release," says Henke. "We receive support requests stating to 'Please release, I need this for a loan.' We will then review the email before releasing, and it turns out to have nothing to do with the loan in question, and is either a scam or contains malware."

Previously, Texas Trust has had partnered vendors whose email account became compromised. "The bad actors sent an attachment that said, 'Invoice, with a URL to a web page,'" says Henke. "And requested users to 'Enter your Microsoft credentials to view the invoice.' The person on our side wrote back, 'Are you sure this is for me?' because they do not receive invoices. Since the email was compromised, the actors replied, 'Oh yeah, certainly, for you.' Those are the types of events that FortiMail catches. And the FortiMail console interface makes this a 100% easy process for us."

"It is very beneficial being able to have a full-service stack of integrated security tools, and utilize them easily, thanks to the Fortinet Security Fabric."

– Blayne Henke, AVP of Cybersecurity, Texas Trust Credit Union

Details

Customer: Texas Trust Credit Union

Industry: Financial Services

Location: Arlington, Texas

Business Impact

- Secured the email network, and safeguarded against threats and attacks
- Ensured compliance with government regulations for protecting customer data
- Gained single-pane-of glass view into network connectivity
- Improved network availability and reliability

Building on a Strong Fortinet Relationship

Texas Trust has relied on FortiMail for the past six years. The company uses an on-premises Microsoft Exchange Server, with FortiMail virtual machine specifically filtering emails for that ecosystem. But when Henke joined Texas Trust, he saw that it could be doing even more.

"A lot of my background was working with Fortinet, and I had great experiences with FortiMail," says Henke. "I saw that we could use it to set up blacklist and whitelist domains, and use DLP [data loss prevention] encryption. For example, if we did not set up a secure email solution, there could still be the potential to send out an email with a social security number in it, so we configured the DLP for that.

"FortiMail is so easy to use and implement. I think it was just a matter of having the proper training and support to get it deployed correctly." FortiMail is routinely positioned as best-in-class by independent testing firms.

Texas Trust is also taking advantage of the free Fortinet Network Security Expert (NSE) training and certification program, which Henke describes as helpful to the organization.

Greater Availability Through a Better Network

After Texas Trust migrated from a legacy multiprotocol label switching (MPLS) network to Fortinet's FortiGate Secure software-defined wide-area network (SD-WAN), all branch traffic has seen improved performance, lowered the overall complexity of its network, enabled redundancy, and cut costs exponentially.

Solutions

- FortiMail VM
- FortiGate Secure SD-WAN
- FortiAnalyzer
- FortiEDR
- FortiAuthenticator
- FortiAP

"A lot of my background was working with Fortinet, and I had great experiences with FortiMail. FortiMail is so easy to use and implement."

– Blayne Henke, AVP of Cybersecurity, Texas Trust Credit Union

"We get that single-pane-of-glass view over our internet connections," says Henke. "As well as managing our internal site links, we set the standard at our data center and HQ, with web filtering, application control, certificate inspection, and DNS filtering. The Fortinet Security Fabric basically supports every single security profile that we could use. It is very beneficial being able to have a full-service stack of integrated security tools, including FortiAnalyzer analytics and log management, and utilize them easily, thanks to the Fortinet Security Fabric."

To ensure high availability, the 23 branches have different, aggregated WAN links. "That way, if one internet connection goes down, we are still rocking, and the branch never loses connection," says Henke.

"Before, with our old MPLS, if we had a site go down, it could have been down for a week. That could happen multiple times a year. This has been a major pain point when servicing our members at our more remote branches. Now, with FortiGate Secure SD-WAN, if locations lose internet connectivity, even if it is the primary or secondary, the staff never knows an issue occurred and our members get the help they need to build brighter financial futures!"

The Security Fabric is also helping Henke with the limited resources he has. "Being able to correlate a security email event from our endpoints all the way up to the firewall saves a lot of time." This makes scaling operations manageable.

Meeting—and Raising—Compliance Standards

Financial institutions are highly regulated, and FortiMail helps Texas Trust ensure compliance with the Gramm-Leach-Bliley Act (GLBA) and other government regulations that require financial institutions to protect information. "The National Credit Union Administration [NCUA] is always reviewing and updating its cybersecurity standards, because, in general, cyberthreats and vulnerabilities continue to affect credit unions and the broader financial system," says Henke. "We follow the NIST CSF [National Institute of Standards and Technology Cybersecurity Framework], as well as the NCUA's ACET [Automated Cybersecurity Evaluation Toolbox], which is aligned with the Federal Financial Institutions Examination Council's [FFIEC] cybersecurity assessment tool. There is quite a bit of compliance on our end, but ultimately, it is all about protecting our members' data. And part of doing that is leveraging FortiMail's content-based IBE [identity-based] encryption, so we can send and receive secure email."

Texas Trust has also implemented FortiEDR (endpoint detection and response) for its board members. “They all have their own devices: MacBooks, Windows laptops, and more,” says Henke. “It is a wide array of devices, and we would prefer them not to be tied to our network in any way. So, we use FortiEDR for that.”

Continuing a Strong Partnership

Right now, Henke and his team are implementing FortiAP wireless access points. They also plan to utilize FortiAuthenticator for 802.11x wireless network secure access, and may deploy it on the wired network as well, as part of a single sign-on solution.

Next year, Texas Trust is planning to migrate to Microsoft 365 for email and plans to implement the cloud version of FortiMail—FortiMail Cloud. “We have to keep up with the times,” says Henke. “Credit unions are very much like smaller banks, and it is almost easier to keep everything on-premises. But the line starts to get blurred. Our perimeter is not just what is on our network anymore; all of our vendors are moving to cloud apps. And we are looking to do the same, so it is just a matter of making sure we do it securely.”

Henke was a believer in Fortinet solutions long before he came to Texas Trust, and his recent experiences have only strengthened his confidence. “I am a Fortinet fanboy,” says Henke. “I love Fortinet. I see it as a partnership with Texas Trust.”

March 11, 2022 2:15 AM

1506301-0-0-EN