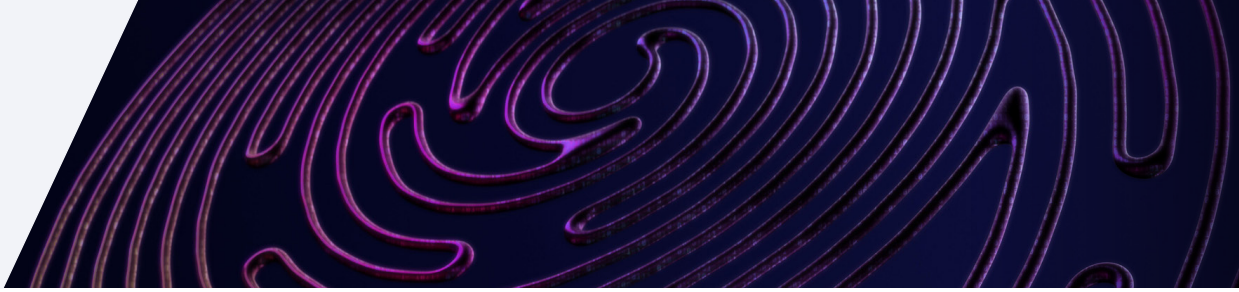
Venafi



CASE STUDY

TLS Protect Drastically Cuts F5 Certificate Renewal Times

Challenge: F5 TLS certificates took months to update

An F5 lead administrator at a large government agency faced an onerous task at the start of each fiscal year. He needed to update the TLS machine identities for about 100 F5 BIG-IP load balancers. To attempt to simplify the process, he used three wildcard certificates—each one for around 33 F5 systems. But the process proved to be more complex than he had imagined. The certificate renewal wasn't simply a matter of updating each group of load balancers, most of which were in HA (high availability) mode. He also had to do so without bringing down all the applications that were dependent on each of these devices.

To minimize the risk of inadvertently bringing down any of the many applications that relied on these load balancers, the administrator faced a long process requiring a great deal of coordination. The high-touch tasks he needed to perform before updating each of the three wildcard certificates involved multiple manual steps, including:

- Get a list of all the apps currently running on each group of F5 devices
- Find the current owner of each app
- Schedule when the wildcard certificate would be pushed out to each app manually
- Ask app owners to generate a certificate request for their apps
- Ensure that each certificate request had the correct corresponding private key before it was installed
- Inform each app owner when their app would be updated so they could test the app to make sure it still worked and prevent any traffic interruptions

And rarely did things go as planned. "A lot of the time the app owners either send me the wrong private key or one that isn't formatted properly," said the F5 lead. "If I'm lucky I 'only' need three months to get everything done—but usually, it takes a bit longer."

Then the agency announced a mandate to discover, report and inventory all TLS certificates. Moreover, the agency wanted to phase out wildcard certificates because of the risks they posed, including unexpected certificate-related outages and potential security compromises caused by lost or stolen private keys.

Said the F5 lead: "I was looking at spending most of my job renewing certificate after certificate, like a machine. There was no way I could do that on my own," especially when he lacked visibility into these 100 F5s, as well as the apps associated with them. Fortunately, the agency had recently purchased an enterprisewide machine identity management solution. And the F5 lead's situation proved to be an ideal pilot project to test the solution before migrating it to other business units.

Solution: Venafi TLS Protect automated the renewal process

The machine identity management solution, Venafi TLS Protect, offered the ability to streamline and automate most of the steps that previously had to be done manually. The F5 lead was skeptical and more than a little apprehensive about the approach. The idea of migrating each app from one of the three wildcard certificates to its own TLS certificate—even though this needed to happen for security and compliance reasons—meant so many things could go wrong.

On the other hand, the potential to automate so many steps and limit human error was enticing. If Venafi worked as advertised, the F5 lead would be able to transform his labor-intensive process and make his area of responsibility safer to boot. The Venafi team explained that this would require more configurations up front but reassured the F5 lead that they would work with him to make this happen using best practices developed over Venafi's decades of being the machine identity management leader. This included helping him create new TLS profiles for applications and then migrate them from the wildcard certificates to their own individual ones. The end result would be that the lead would have visibility into all these certificates and could control them separately, without having to worry about any of them potentially affecting other applications.

Cutting F5 TLS renewals while providing individual certificate profiles

Thanks to TLS Protect, the F5 lead automated multiple steps in procuring and renewing TLS certificates for F5 apps. TLS Protect created the TLS keys and certificates inside the Venafi Platform, ending the need for him to hunt down app owners or worry about being given the wrong private key. Now he could automatically renew certificates outside of business hours so that they would have no impact on application availability, removing the need to coordinate with app owners to get it done.

And because separate TLS profiles now existed for each app, TLS Protect handled the rest of the process, so that all he needed to do was "press a button." Moreover, TLS Protect performed regular discovery of TLS certificates so that if a certificate needed to be revoked or renewed, he could trigger a workflow to get that done.

By automating all these previously manual steps, the F5 lead cut the time renewing his F5 TLS certificates from three months or more for the three wildcard certificates to about eight days for hundreds of certificates. "It would have been even faster if we didn't need our PKI team to do final approvals. In that case, it would have taken a few hours, maybe a day at most," said the F5 lead in wonderment.

Improving TLS certificate management speed and security

In addition, TLS Protect performed "exactly as described," said the F5 lead. By enabling him to provide individual TLS certificates for each app, his F5s were in compliance with the agency's security mandate ahead of schedule. Also, TLS Protect scales up so that as more apps are created—either in the data center or increasingly, the cloud—every single app would be secured and operational in record time, facilitating greater security, better availability and faster performance.

Perhaps most exciting, now that the F5 lead cut the yearly update processes from several months to around a week, he's been able to reclaim time to work on other projects that help the agency. By automating the work he had found so repetitive and frustrating, he can even "take a vacation without worrying that something is going to fail," he said with a laugh. "I'm actively encouraging other business units to follow suit and offload these repetitive machine identity management tasks to TLS Protect."

Trusted by

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks