M&T Bank achieves secure agility with certificate lifecycle automation

Company Overview

M&T Bank is a Fortune 500 Americn bank based in Buffalo, New York, with more than 155 billion in assets. Founded in 1856, M&T Bank has been a community-driven company from its roots, originally serving manufacturers and trades and now operating more than 780 branches across the eastern United States. In 2021, the bank unveiled M&T Tech Hub, a new initiative to drive collaboration and innovation with the people and businesses they serve.

Challenges

Embracing agility and transformation without disruption

As a community-driven bank, M&T is focused on transforming its digital footprint and embracing agility to meet constantly evolving customer needs. However, with digital transformation comes the need for digital trust and security.

“Our goal is to become more agile with our approach to security. We want to foster a new way of thinking — be more efficient, drive automation wherever possible, and educate our people on good security principles,” says Joshua Nash, Technology Manager for Security Engineering at M&T Bank.

Industry

Banking & Financial Services

Location

Buffalo, New York

Pain Points

Poor visibility led to unexpected outages caused by untracked and unknown certificates

Developers and system admins used self-signed and wildcard certificates that did not comply with internal policy

Manual processes for certificate requests, renewals, and revocation created bottlenecks

Solution

M&T Bank uses Keyfactor Command to gain complete visibility over it’s rapidly expanding certificate footprint and to automate processes for end-users to move faster without friction.

Public key infrastructure (PKI) lays the foundation for trust and authentication, and the importance of agility is no exception. M&T Bank relies on PKI and digital certificates to securely connect devices and applications across its digital footprint. But over the years, both technology and cryptography have evolved significantly, creating new challenges.

M&T initially partnered with Keyfactor in 2010 — then a PKI consulting service known as Certified Security Solutions (CSS) — to help with the momentous task of migrating from SHA-1 to SHA-2 and re-building their entire PKI from the ground up.

“We decided to grow up at M&T about how we handled PKI,” says Nash. “Keyfactor helped us to re-build our PKI the right way, including a proper CA hierarchy with separation of duties. We also reduced three roots of trust down to just a single root and connected it to our issuing CAs, which was far easier to manage and maintain.”

However, as the number of devices and workloads expanded rapidly, so did the number of certificates required across their environment. The increasing volume and speed at which certificates were issued made it difficult to keep track of them. Nash says, “setting the foundation for our PKI was a step in the right direction, but as we grew, it became much harder to maintain visibility and control over certificates issued from our PKI and other CAs. We didn’t really have a good handle on what certificates we had out there.”

Solution

One platform for certificate visibility and automation

The M&T team knew they needed a certificate management solution, and Keyfactor came to their attention because of how effortlessly they were able to re-build their PKI. When the team reached out to Keyfactor, they had just the right solution.

Results

Simplified and consolidated their PKI infrastructure

Eliminated 50% of non-compliant self-signed certificates

Educated end-users on best practices for certificate issuance and management

Scaled from 2,000 to 350,000 active certificates with complete visibility

Products

Keyfactor Command

“Before Keyfactor, we were using Command Line and native tools to manage certificates. Now we’re using APIs and automation that can scale.”

Joshua Nash

Technology Manager and SVP, Security Engineering, M&T Bank

Certificate discovery and inventory were priority number one. "We can't manage what we can't see," says Nash. The second was continuous visibility of certificates across their multiple platforms and CA solutions, not just auto-enrolled certificates from their internal PKI. Finally, the team needed a solution that would scale. "It had to scale with our demands, and we have a lot of certificates…a lot," says Nash.

In 2014, M&T rolled out Keyfactor Command to get better visibility of their certificate inventory and set basic alerts to remind users to renew certificates at a set schedule before expiration. As the product evolved, M&T continued to rollout new capabilities, which now include network discovery, self-service enrollment, APIs and automated workflows for certificate renewal and provisioning.

"We've been a customer of Keyfactor for more than 10 years now," he says. "As Keyfactor evolved from their roots in PKI consulting to a full-stack platform for PKI and certificate management, we've evolved too. From rebuilding our PKI to getting complete visibility and automation for all our certificates, Keyfactor is a critical component in our security infrastructure."

> "We went from 2,000 certificates to more than 350,000 certificates. That's a lot to keep track of, but Keyfactor helps us keep everything in view and it's allowed us to scale massively."
>
> **Joshua Nash**
>
> Technology Manager and SVP, Security Engineering, M&T Bank

Business Impact

Certificate management drives effiency and scale

Eliminated certificate blindpots

Initially, Keyfactor integrated directly with M&T Banks' Microsoft CAs to provide visibility and real-time monitoring for all certificates issued from their internal PKI. This initial discovery provided them with a much more efficient way to inventory and audit their certificate landscape.

"Before Keyfactor, we had to export an Excel spreadsheet from our CA manualy, then search through a massive inventory of auto-enrolled certificates to find any anomalies," says Nash. "Now we can see all our certificates in one place and easily search and identify a single certificate out of hundreds of thousands within seconds.

After integrating with Microsoft CA, the Keyfactor team helped M&T discover unknown certificates in their network. Using network scanning capabilities built into the Keyfactor Orchestrator, the team quickly got an in-depth look into all of their certificates, including details like ownership, expiration, and all the locations they were installed.

Nash explains, “Right off the bat, we were able to identify and eliminate 50% of the self-signed certificates across our environment. Now we’re not chasing ghosts and we’ve been able to proactively educate users on why they should opt for CA-issued versus self-signed certificates. It’s reduced our rate of error significantly.”

Streamlined processes for cybersecurity and developers

Like many companies, at M&T Bank, the team responsible for managing publicly-trusted SSL/TLS certificates is different from the internal PKI team. Keyfactor bridged the gap by integrating with Entrust CA to provide the cybersecurity team with the same seamless experience for certificate enrollment and lifecycle management.

Now the cybersecurity team can tag certificates with unique metadata, organize them efficiently, and notify application owners before their certificates expire. According to Nash, “the metadata feature in Keyfactor Command is incredibly powerful. Now we can tag certificates with relevant data like emails for certificate owners and approvers, so we can track them with much better accuracy.”

About Keyfactor

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human.

Contact Us

- www.keyfactor.com
- +1.216.785.2946

At the same time, Nash worked with M&T’s developers and operations teams to reduce manual processes related to requesting and provisioning certificates. “Our developers can just leverage the Keyfactor Swagger API interface to provision certificates much faster and without any friction. They’re using more certificates than ever because the process is now much faster and more efficient.”

Rather than chasing developers and system admins using wildcard certificates, which do not comply with internal policy, they can provide an easy alternative for short-lived certificates that still fit within their policy guardrails.

Scaled to 350,000+ certificates without skipping a beat

Today, M&T Bank has more than 350,000 active certificates across the enterprise, which includes auto-enrollment, as well as certificates for mobile devices, web servers, network and cloud infrastructure. To achieve certificate management at this scale, Nash says the performance and scalability of the Keyfactor Command platform has been instrumental.

“We weren’t out to cut costs; although we did, our objective was to scale. And that’s exactly what Keyfactor has allowed us to do,” explains Nash. “It’s giving us scale and efficiency to use more certificates to better secure devices and workloads. There really is no limit to what we can accomplish with the platform.”