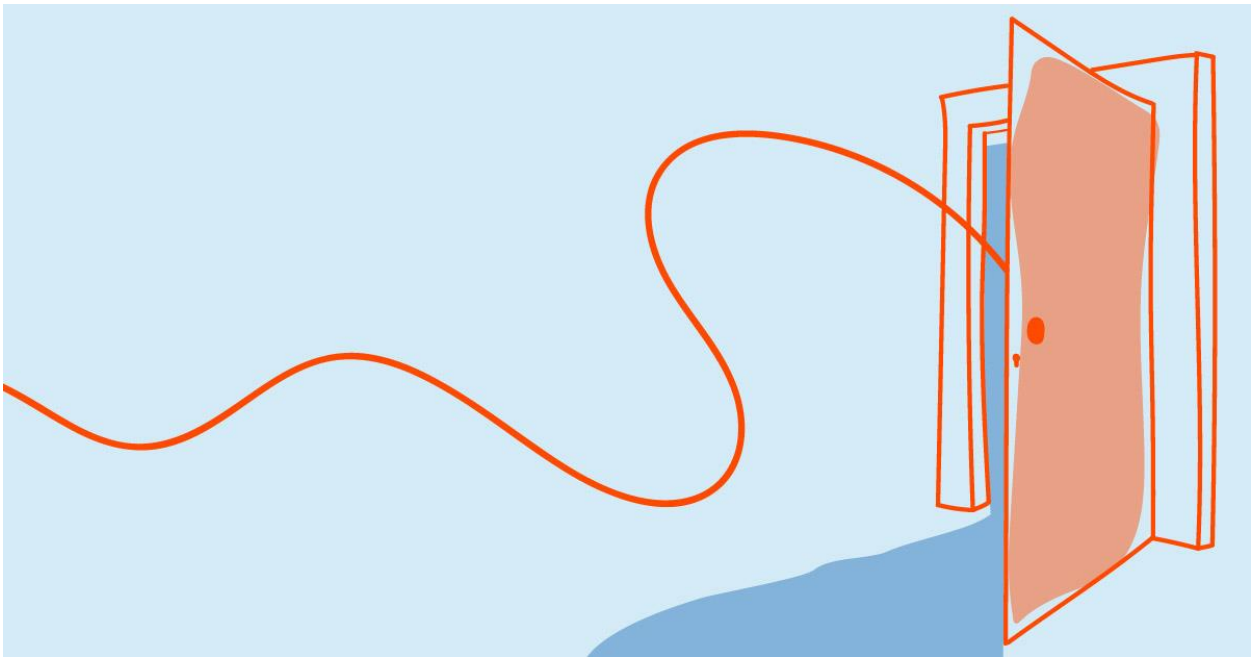

Resolve to Automate Your Certificate Management in 2024

January 2024

New Year's resolutions. Some of us love making them. Others cringe and skip it. And then there are gyms across the world that can't imagine a world without resolutions, and the major revenue boost each January ushers in.

There's no denying how hard it is to keep those dark 6:00 am dates with the treadmill. As a result, some of us may find that we once again put our personal health goals on the backburner, and sometimes even before January has come to a close (no judgement).

Organizations, though, can't take their eye off the health and wellbeing of their business continuity. It's a 24/7, 365-day requirement. Still, the start of a new year is often when organizations re-evaluate and recommit to priorities, strategies, and the overall health of the business that will carry them through the following twelve months.

A New Year Reset

One critically important area that should top a company's resolution list each new year is a well-defined and executed digital certificate management process. Most websites and all major browsers now require SSL/TLS certificates to verify website ownership and establish user trust.

But managing your digital certificates can be difficult and labor intensive. It involves tracking the Certificate Authority (CA) of each certificate, along with where it was installed, the expiration date, the cryptosystem used, key length, and algorithm.

Expired certificates can trigger alarm warnings in browsers, which in turn erodes trust and can lead users to abandon your website, damaging your brand which impacts revenue. Meanwhile, internal expirations can disrupt critical business processes.

Organizations can—and absolutely should—make it a practice at the start of each new year to inventory, reevaluate, and when needed, reinstall SSL/TLS certificates. Doing so can help your company stay on top of:

- Operational efficiency, as you budget for and renew certificates before they expire and disrupt service
- Compliance requirements, helping you avoid penalties or fines for outdated or expired certificates
- Security threats, by routinely updating certificates that are optimized against constantly evolving cyber risks

Automation: The Key to Seamless and Secure Certificate Management

Each new year ushers in a fresh opportunity to improve on the previous year's practices and results. And though you may—or may not—stick with being on that treadmill by 6:00 am for 60 minutes six days a week (hey, everyone deserves one day of rest), you can make this the year you simplify your company's certificate deployment and management process.

It starts with automation that allows you to quickly find and securely control all the certificates you need to manage, across your organization.