Venafi

RESEARCH REPORT

Organizations Largely Unprepared for the Advent of 90-Day TLS Certificates

Is your organization ready to move to 90-day certificates? Most are not.

There's been a lot of talk about Google's recommendation to reduce certificate lifespans from 398 to 90 days. In March of 2023, Google formally announced its intention to move to 90-day certificates. With Google Chrome having over two-thirds of the global browser market, this effectively guarantees that the CA/B Forum will put forward a Ballot Proposal to ratify 90-day certificate lifespans.

This is a radical change. The new proposal from Google would reduce certificate lifespans by 75%. And while that number is extreme, the reduction itself is in line with the frequency of previous reductions. Since 2011, the group has consistently reduced lifespans every two to three years. However, while shorter certificate lifespans reduce the risk of compromise, handling a higher volume of certificates, and more rapid renewals, also heightens the risk of outages and gaps in security.

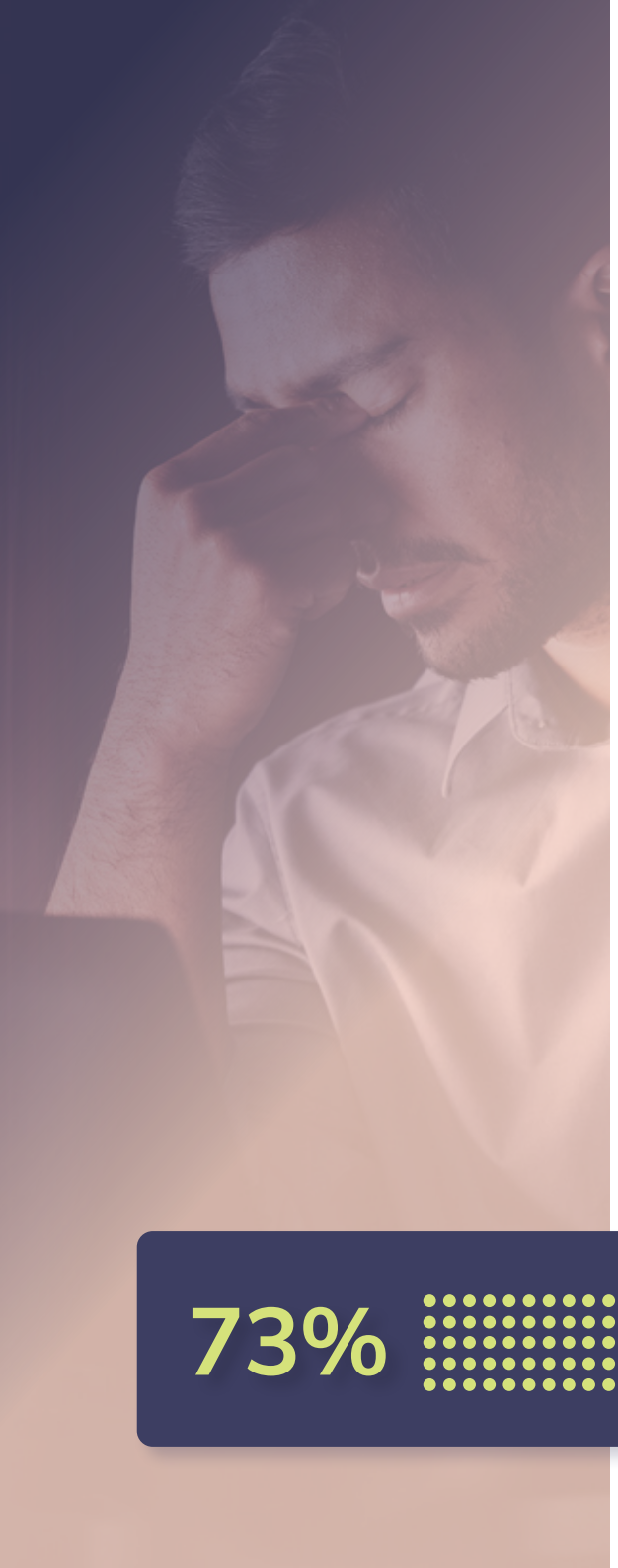
But this increase in certificate management complexity is not driven by certificate lifespan alone. The challenges of managing shorter certificate lifecycles are compounded by factors such as growing certificate populations, certificate authority (CA) revocations and quantum migration.

In particular, uncertainty about the future of TLS certificates has fueled a surprising level of debate about the impending risks of post-quantum cryptography.

To understand how these factors are impacting organizations, we surveyed 800 security leaders across the U.S., U.K., France and Germany. The goal of this research was to discover how prepared organizations would be for the upcoming 90-day TLS certificate standard, where they were most challenged to comply and how concerned they were by this bold move. The results indicated that, by and large, organizations are not only unprepared, but they are also worried that this new standard for shorter certificate lifespans would break their businesses in many ways.

> “At any point in time, we are 24 hours away from a mandated revocation, similar to a Heartbleed-type event.”

Ryan Hurst
Former Head of Product for Google's Core Security Foundation team



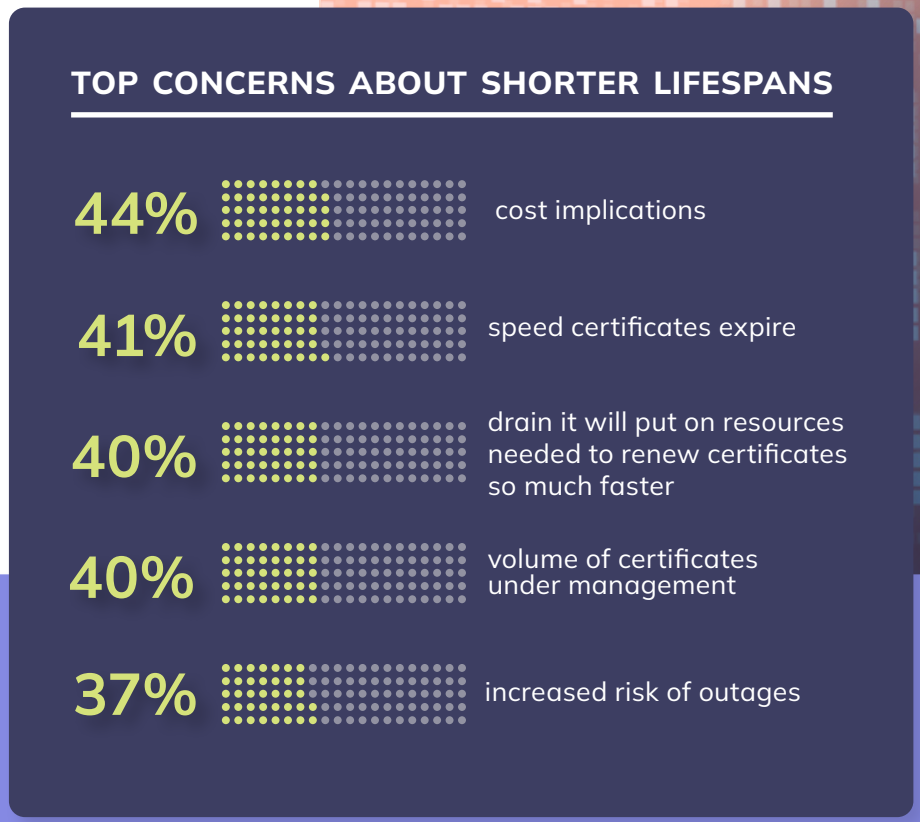
Widespread anxiety about managing the migration to 90-day certificates

As the industry transitions to 90-day certificate lifespans, the burden will predominantly fall on organizations rather than CAs or browsers. With shorter certificate lifespans, organizations will need to renew their digital certificates more often—at least five times a year instead of once. That means organizations must be prepared to quickly identify expiring certificates, request that new ones are issued and revoke the expiring certificates several times a year. As a result, 73% of security professionals believe the Google proposal to shorten TLS certificate lifespans from 398 days to 90 days will cause chaos, leaving many companies blindsided.

73% Believe shortening TLS certificate lifespans from 398 days to 90 days will cause chaos

Given that a separate Venafi study found that 83% of organizations still suffered at least one certificate-related outage a year, it's fairly obvious that organizations already struggle to manage certificates with a one-year validity period. Perhaps that's why 94% of respondents expressed concerns about Google's proposal to reduce certificate lifespans.

94% Expressed concerns about reduced certificate lifespans



Do the security benefits outweigh the operational risks for 90-day certificates?

As certificate lifespans perennially decrease to bolster security—the shorter a certificate's lifespan, the shorter an attacker's timeframe of attack—on-time renewals become imperative. In fact, 76% of security professionals recognize the need to shorten certificate lifecycles to improve security.

On the one hand, shorter certificate lifespans do limit the window of opportunity for compromise, but it also forces security and operations teams to renew expired certificates at an ever-increasing rate, which is often too much for some organizations. This scenario also statistically increases the chances for human error. That could explain why 75% of security professionals think that shorter certificate lifespans could actually make them less secure. And 77% of security leaders think more outages are "inevitable" with 90-day certificate lifespans.

76%
Recognize the need to shorten certificate lifecycles to improve security

75%
Believe shorter certificate lifespans could actually make them less secure

77%
Think more outages are "inevitable" with 90-day certificate lifespans

90-day certificates impact all aspects of the lifecycle

Certificates are not a “fire and forget” solution. These machine identities have their own lifecycles, which need to be managed effectively. Once a certificate is installed, it must be continuously monitored for security issues that could break its validity, revoked and replaced with a new one when necessary, or simply renewed before it expires to prevent an application outage.

But full certificate lifecycle management is not a small task. Machine identities currently outpace human identities 45:1—a gap that’s only going to widen as digital transformation accelerates. With shorter 90-day TLS certificate lifespans, organizations will face even more mind-boggling levels of complexity in managing the full certificate lifecycle. And security professionals agree, with 81% of those surveyed stating that 90-day certificates will amplify existing challenges they have around managing certificates.

81%

Believe 90-day certificates will amplify existing certificate management challenges

Managing certificates throughout their entire lifecycle is critical to their continued operation and security. Without proper management, certificates can fail at any point from issuance to provisioning, deployment, discovery, inventory, securing, monitoring, renewal and revocation. But this process becomes even more complex as certificate lifespans continue to shrink and certificates require more frequent maintenance.

Accelerated growth of certificates exacerbates management challenges

CIOs know their organizations are using a lot of machine identities, including TLS certificates. Widespread digital transformation efforts have resulted in tremendous growth in the number of these machine identities, with 95% of organizations saying digital transformation initiatives have increased their use of SSL/TLS in the past year. And the number of certificates they use has increased by an average of 36%. Looking forward, these certificate populations will continue to grow at a faster rate over time. 92% of security leaders expect this number to increase by 39% within the next two years.

95% Say digital transformation has increased their use of SSL/TLS in the past year

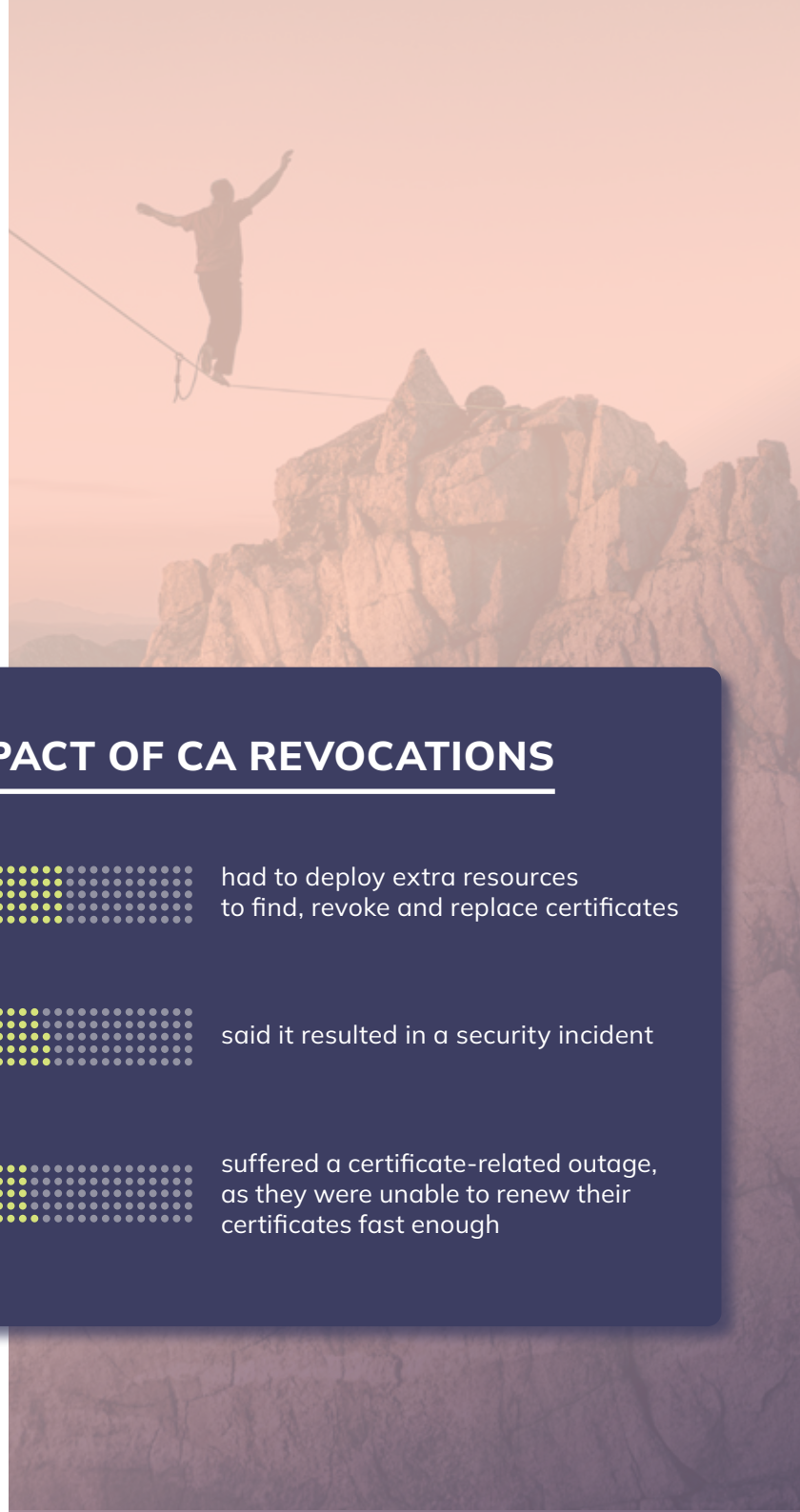
WHY FIVE TIMES A YEAR?

Certificate management best practices recommend that a certificate be renewed 30 days before its expiration, equating to renewals every 60 days for 90-day TLS certificates.

There's no avoiding it. Impending 90-day certificate lifespans will place an increased burden on security teams to rotate TLS certificates five times a year instead of just once. So, the sheer numbers of certificates alone are a looming issue, but the frequency of renewals with them compounds the challenges exponentially.

Volatile CA landscape creates additional risk

A growing number of certificates could result in heavier reliance on CAs. But that may not be the best strategic approach for organizations. Over the past decade, we've seen a variety of CA errors: most recently when Google announced that it would distrust certificates for major CA Entrust. After the CA experienced a series of compliance failures and unmet improvement commitments, many organizations were left scrambling to find and replace thousands of Entrust certificates.

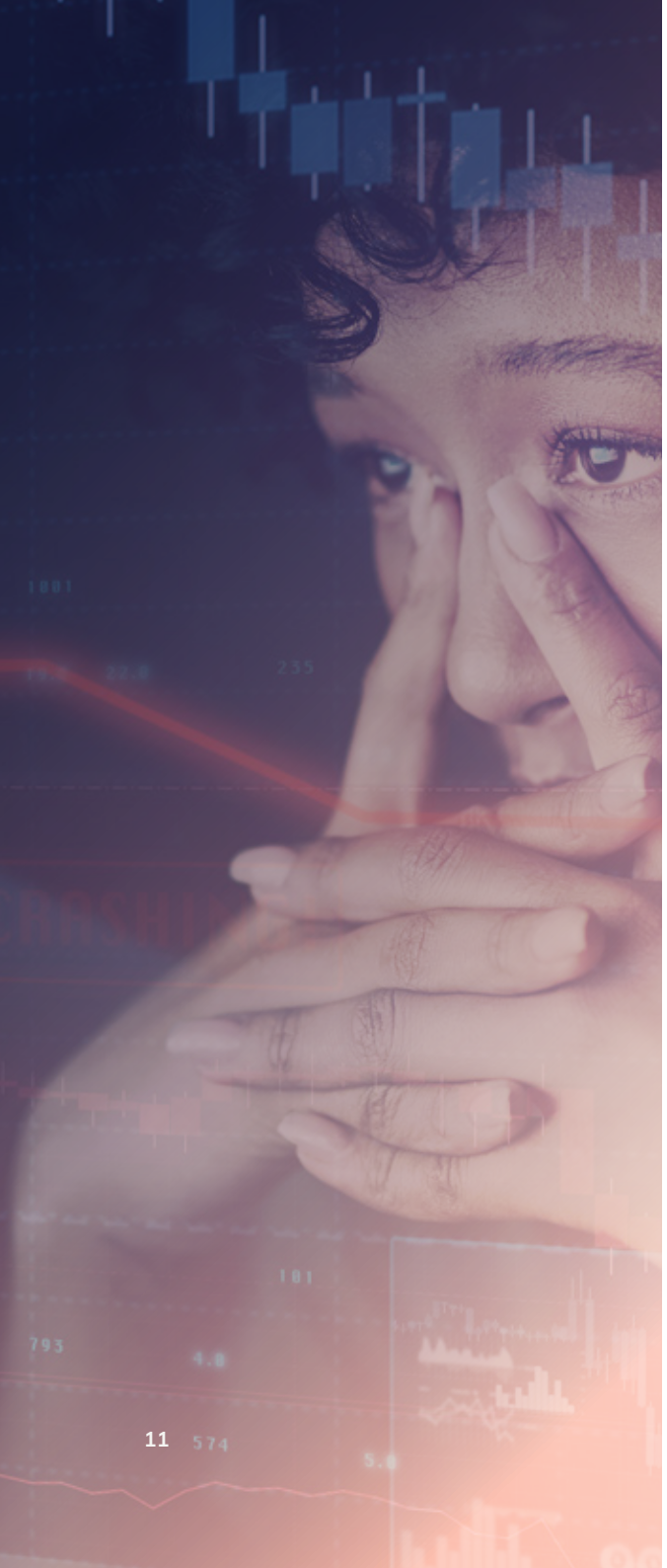


IMPACT OF CA REVOCATIONS

45% had to deploy extra resources to find, revoke and replace certificates

38% said it resulted in a security incident

31% suffered a certificate-related outage, as they were unable to renew their certificates fast enough



When your CA commits an error or suffers from a compromise, you need to protect your business against potential fallout. To minimize your exposure, you must be agile enough to change CAs and replace impacted certificates quickly. What types of CA errors can cause a certificate to be revoked? There are many, including a lack of internal controls, human error, hacker compromise, technology malfunction and abuse of trust.

88% Have been impacted by CA revocations

With 88% of companies surveyed having been impacted by CA revocations, it's a serious factor impacting the strength and reliability of machine identities within organizations. Of those reporting an impact from CA revocations, the fallout was relatively severe.

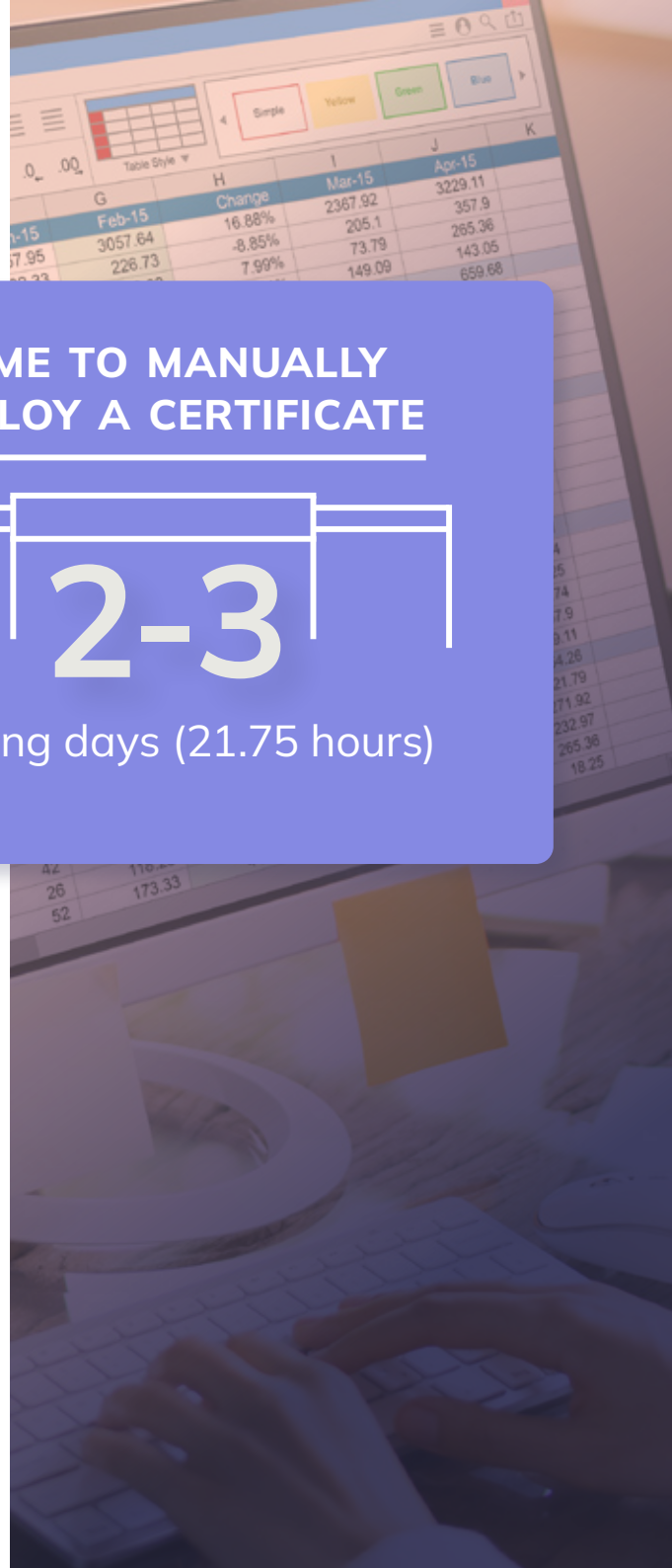
It is crucial for organizations to recognize that their certificate management should not be tied to any single CA. They must maintain CA agility to futureproof their organizations against certificate mis-issuance and errors that can result in distrust of the CA.

In fact, automating TLS certificate lifecycle management and identifying TLS certificate owners are the biggest TLS challenges faced by businesses, according to security leaders. Surprisingly, 29% still rely on their own software and spreadsheets to manage certificates. As a result, organizations take two to three working days (21.75 hours) to manually deploy a certificate. This resource drain alone would make manually managing 90-day certificates untenable.

TIME TO MANUALLY DEPLOY A CERTIFICATE

2-3

working days (21.75 hours)



29%

Rely on their own software and spreadsheets to manage certificates

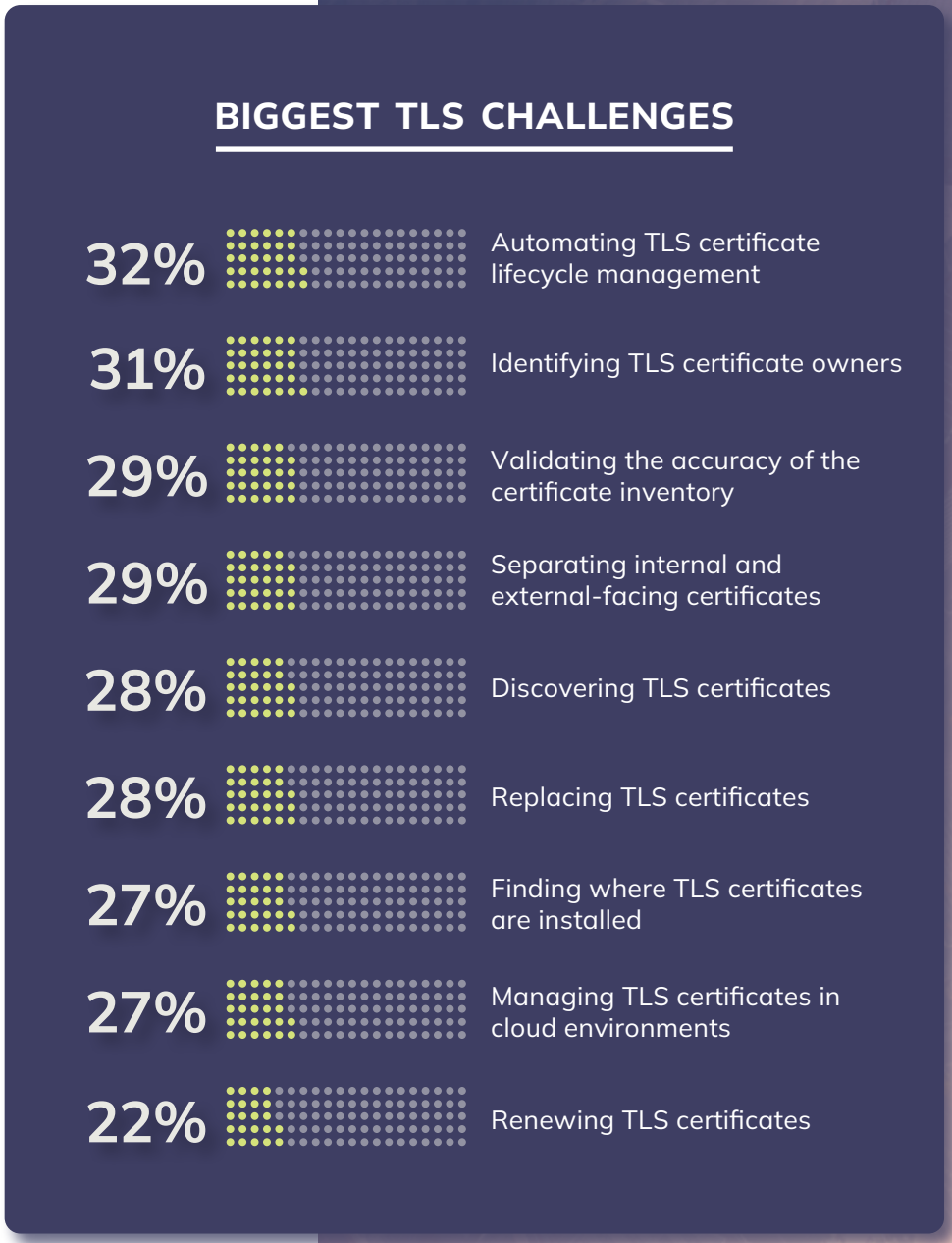
Organizations lack the automation needed to manage 90-day certificates

Even with 13-month lifespans, many certificate management programs are still carried out manually. And with mixed results. A 90-day certificate lifespan would necessitate automation, and that is why Google is championing it.

Employing manual processes to manage the certificate lifecycle creates many painful areas, especially if we consider the expanding number of certificates required for reliable and secure operations.

Forcing everyone away from time-consuming and error-prone manual issuance processes is one of the desired outcomes of Google's recommendation to reduce certificate lifespans.

Because many organizations lack the automation capabilities to replace certificates with short lifespans at machine scale and speed, they are likely to see sharp increases in outages caused by unexpected certificate expirations. These problems are exacerbated by the fact that most organizations have certificate renewal processes that are prone to human error. In a nutshell, manual management will challenge your organization in several ways. Not only is it time-consuming, but it's also fundamentally unreliable, suffers from inefficient policy enforcement and it blurs visibility of certificates across your enterprise.



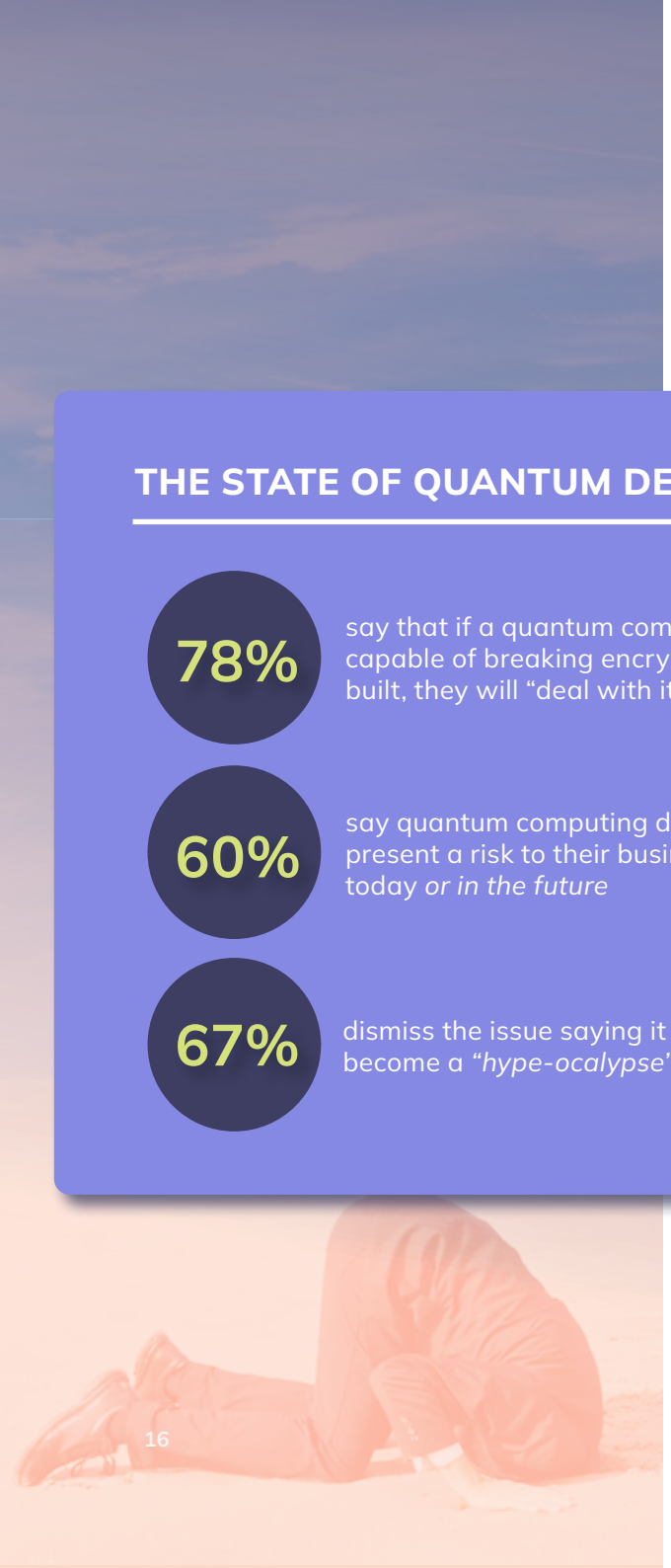
Organizations unprepared for 90-day will not be prepared for quantum

The automation your organization needs to migrate to 90-day certificates is the same automation you'll need to migrate to post-quantum algorithms. Indeed, 86% of security leaders validated that taking control of the management of keys and certificates is the best way to prepare for future quantum risks. But that may be easier said than done.

Sixty-seven percent of security professionals think shifting to post-quantum cryptography will be a nightmare, as they don't know where all their keys and certificates are located. But this is the same problem they'll face when they migrate to 90-day certificates. Only it will impact them much sooner

86% See taking control of certificate management is the best way to prepare for future quantum risks

67% Think shifting to post-quantum cryptography will be a nightmare



THE STATE OF QUANTUM DENIAL

78% say that if a quantum computer capable of breaking encryption is built, they will "deal with it then"

60% say quantum computing doesn't present a risk to their business today *or in the future*

67% dismiss the issue saying it has become a *"hype-ocalypse"*

But there are still those who would prefer to keep their head in the sand, even though they recognize that post-quantum cryptography will catch up to them sooner or later. Sixty-seven percent say they dread the day the board asks about their post-quantum cryptography migration plan. At the same time, many are postponing any action at all for now.

67% Dread the day the board asks about their post-quantum cryptography migration plan

The good news is that the automation you put in place today for 90-day certificates will make your job significantly easier when the time comes to migrate to post-quantum cryptography.

5 immediate actions you can take to prepare for 90-day certificates

Automation empowers you to seize control of your renewals and ensure no certificate is neglected, sparing you unnecessary pain and toil. Here are five ways automation can simplify your current operations and future-proof your TLS certificate lifecycle management.

1

Implement continuous discovery and inventory. Create and maintain a complete inventory of your TLS/SSL certificates, including who owns each certificate, where it is installed and when it expires. Once that is complete, continuously automate discovery to ensure business continuity and best practice security.

2

Automate renewal processes. By automating renewals, you'll not only save time—you'll make sure your certificates stay up to date, avoiding downtime caused by expired certificates. It's important to use a certificate lifecycle management solution that allows you to automate with ACME, APIs, SDKs, agents and more.

3

Configure global policies and workflows. To ensure your certificates use the most stringent attributes, you must adopt global policies and workflows. Automating these safeguards through self-service prevents business units from going rogue with unauthorized or non-compliant certificates.

4

Integrate with DevOps tools. Make life simple for your developers by integrating your certificate lifecycle management solution with their existing tools. Turnkey, API-driven integrations enable automated provisioning of certificates in continuous deployment environments, maintaining strict adherence to the validity periods for certificates used in both new and existing applications.

5

Set up real-time monitoring and reporting. By setting up continuous monitoring and reporting, you can ensure all certificates comply with the new, shortened lifespans and organizational policies. Regular, real-time audits help identify and rectify deviations, reducing the risk of security breaches or non-compliance penalties.

Conclusion: Automate certificates now to prepare for 90-day TLS certificate standards

It's clear that most organizations are simply not prepared to migrate to 90-day TLS certificates, especially if that move is mandated in a relatively short timeframe. Given the exponential growth of machines and their shortening lifespans, IT and security teams are discovering that their current tools and strategies are no match for managing millions of certificates many times a year. The potential speed, scale and cost of the migration, along with a lack of internal skills and knowledge, also raise major concerns.

A comprehensive certificate lifecycle management program must leverage automation to orchestrate the actions necessary to secure certificates throughout their lifecycles. Adopting shorter certificate validities with automation not only aligns with current security best practices but also prepares organizations for future challenges. It promotes agility, enhances security and supports continuous compliance with evolving web standards. The simple fact is that your ability to successfully transition to the 90-Day TLS standard depends on your ability to closely coordinate people, processes and technology.

Change management takes time. So now is the time to begin.

Learn how Venafi can help your organization assess your readiness for 90-day certificates.

Visit venafi.com/90-day-tls-readiness today.

Venafi

Venafi is the cybersecurity market leader in machine identity security, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. To learn more, **visit venafi.com**