digicert®

2026 Global PKI Research Report

PKI Under Pressure: The Tipping Point for Modernization

Research Report | 2026

Table of Contents

Foreword

Lakshmi Hanspal
Chief Trust Officer | DigiCert

PKI modernization and post-quantum readiness are no longer future problems. They're today's operational realities.

Security and infrastructure leaders are navigating a collision of forces. Organizations deal with more machine identities, more connected systems, more AI-driven uncertainty, and shrinking windows to act before cryptographic vulnerabilities become business liabilities. All this leads to complexity challenges at a time when certificate-related outages and trust failures are becoming an increasingly common source of business disruption. Cryptographic agility isn't nice to have. It's quickly becoming essential to everyday operations at every level.

To understand where organizations stand, we surveyed more than 400 senior IT and security decision-makers, including CISOs, CIOs, and leaders across cybersecurity, IT operations, GRC, and product organizations worldwide. What they told us was both clarifying and sobering.

Most organizations understand the stakes. Far fewer have turned that understanding into action.

At DigiCert, we didn't just study this problem, we lived it. As our own environments expanded, we faced the same hard truths. Our teams had limited visibility into cryptographic assets, while dealing with fragmented certificate ownership and the very real pressure of modernizing infrastructure without disrupting the business running on top of it. Post-quantum readiness added urgency we couldn't ignore.

So, we became our own Customer Zero. We inventoried our cryptographic assets, surfaced unmanaged certificates, automated lifecycle management, and began hardening critical systems for quantum-ready cryptography. It was necessary, and it gave us a firsthand, real-world understanding of what organizations will face at every stage of this journey.

Here's what I know to be true: you don't need a perfect budget, a flawless roadmap, or a big-bang transformation to make real progress. What you need is a clear starting point, the right visibility, and a commitment to taking the next step.

This report gives you the data, the benchmarks, and the honest picture of where the industry stands. I invite you to use it, start the conversation, build the case, and move forward.

The organizations that act now will be the best positioned to keep up with today's challenges while navigating tomorrow's constantly evolving cryptographic landscape.

Executive summary

This research shows a growing shift among enterprise organizations, from recognizing PKI challenges to actively addressing them for improved operational resilience.

PKI is becoming more important at the exact moment it is becoming harder to manage. The gap between important and operating readiness is now wide enough to command executive attention. Leaders understand the risk. What many organizations are still building is the visibility, governance, and automation needed to manage PKI as an enterprise system rather than a collection of point solutions.

PKI risk is well understood but not well controlled

Adam Strange, Principal Analyst, Data Security, Omdia.

Today's 3 PKI challenges

1

The amount of visibility dictates the risk exposure.

A lack of visibility into the full certificate landscape is the biggest challenge enterprises face. Only 34% of organizations report having a complete, up-to-date inventory of all digital certificates.

There is a clear connection between visibility and risk. 73% of organizations are very or extremely concerned about outages caused by expired certificates.

2

Complexity and PKI maturity stand in the way of addressing growing business needs.

74% of organizations are concerned about certificate sprawl, and 52% expect PKI investment to increase in the next three years.

Yet, even while IT and security professionals recognize threats and the need for PKI modernization, many struggle to elevate conversations about resources and PKI risks to decision-makers.

3

Adapting to rapid AI change and the increasing quantum threat require agility and planning.

More than 73% of organizations say PKI will play a critical role in establishing trust for AI use cases.

Quantum preparedness lags with only 22% fully assessing cryptographic systems for future quantum-related vulnerabilities.

PKI modernization offers solutions to these challenges

The operational necessity of modernizing PKI is increasingly self-evident, but many organizations are still in the early stages of execution. Because modernizing can be complex, most enterprises take a phased approach. These organizations find that success depends on reducing manual processes, improving visibility, and inviting the right expertise and operational support needed.

The PKI Modernizing impact

Organizations that have modernized their PKI report a 60% reduction in outages.

Introduction

PKI under pressure

PKI is under pressure because the operating environment that shaped yesterday's operating model no longer holds.

Certificate volumes are rising, non-human identities are proliferating, certificate lifecycles are shrinking, and the number of systems that depend on cryptographic trust keeps expanding. At the same time, regulatory and industry compliance are pulling PKI into scope, holding leaders accountable for outcomes like uptime, resilience, and AI governance.

This combination is changing PKI from background infrastructure into a strategic capability that lands squarely on IT and security leadership for implementation, monitoring, and management.

How to use this report

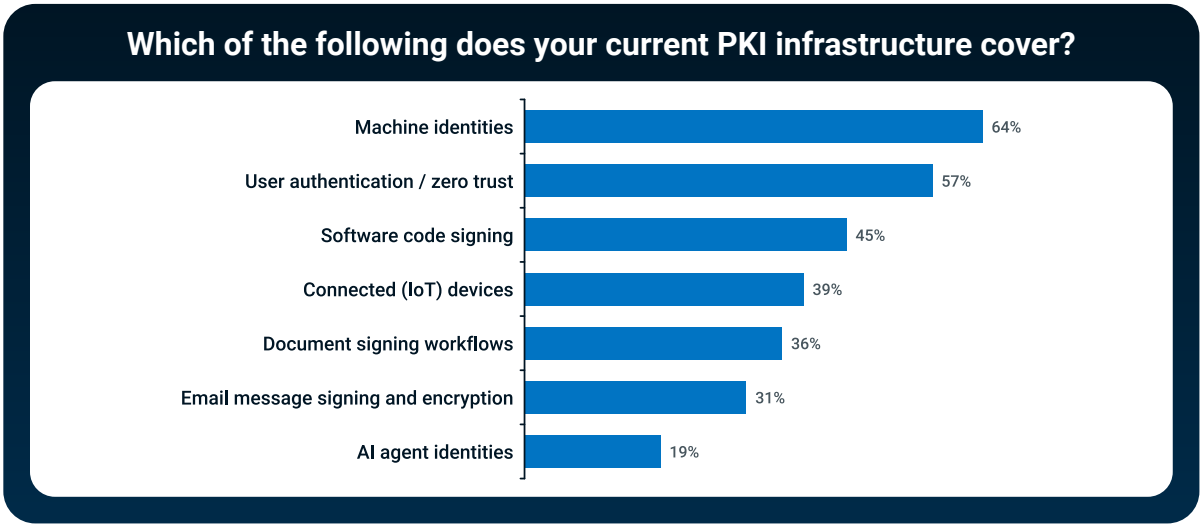
The data in this report focuses on leadership over day-to-day PKI operations. By surveying the senior leaders who operationalize PKI in their enterprises, we examine where PKI stands now and what it must do to continue to function moving forward.

The following results will help you see the current state of PKI operations, help you assess how your organization compares to averages, and give you data and considerations for your own planning—both internally and with decision-makers throughout your organization.

Understanding today's enterprise PKI

Before looking at PKI through the lens of the three most prominent challenges, we first look at how PKI exists in today's organizations. The data shows that PKI has expanded well beyond public web certificates. Machine identities, user authentication and Zero Trust initiatives are major components of PKI in over half the respondents, with significant coverage in other non-web use cases like software code signing, IoT, and content.

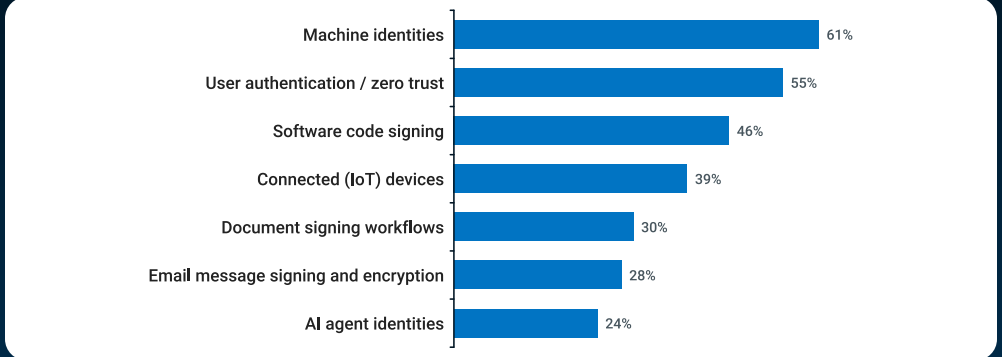
These findings show why organizations are extremely concerned about outages, with PKI providing encryption, identity, authentication, and more to a wide range of critical enterprise infrastructure, well beyond public-facing web servers.



Priorities for PKI modernization

Not surprisingly, we find a correlation between infrastructure use and PKI modernization priorities. Nearly three-quarters of respondents are very concerned about outages caused by expired certificates and certificate sprawl. Professionals understand the consequences of failure, and they set modernization phases that correspond to the areas of greatest need and highest risk.

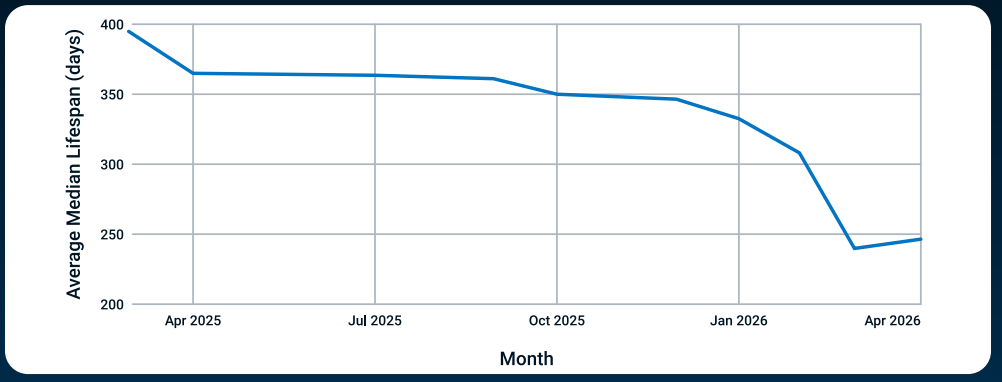
Which areas has your organization prioritized for PKI modernization?



Shrinking lifecycles increase the pressure

Even as complexity and the number of connections, identities, and use cases grows, the public certificate lifecycle is shortening. The industry is on a path toward a 47-day maximum validity period for public TLS certificates in March 2029. This leaves even less room for teams still relying on manual installation, unclear ownership, or spreadsheets as the system of record. In many organizations, PKI has become an ecosystem that is fragmenting faster than teams can integrate and govern it.

Monthly median certificate lifespan (2025-2026)



AI and quantum further complicate a complex system

AI raises the demand for stronger identity, integrity, provenance, and policy enforcement across content, models, and agents. The transition to quantum-safe cryptography raises the stakes on visibility and agility across the environment. Together, they make the case that PKI modernization is a natural response to a looming trust problem.

Takeaway

The pressure on PKI is not coming from one source. It is the cumulative effect of machine identity growth, shrinking certificate lifecycles, the need for AI governance, and quantum readiness arriving at once—especially when Gartner's prediction for Q-Day[1] coincides with the start of the 47-day certificate lifecycle mandate in 2029.

1 Gartner Insights Abstract, How to Mitigate the Cryptography Risks Posed by Quantum Computing

Visibility and risk

When organizations increase visibility, risk decreases

Only a complete inventory over the deployment and status of every certificate in the enterprise gives the insight needed to avoid gaps, lapses, and failures.

Visibility prevents outages and attacks

The study makes one issue clear: organization cannot effectively manage certificate risk without visibility. The results show that only 34% of organizations say they have a complete, up-to-date inventory of all digital certificates. That means two-thirds of organizations have only a partial inventory, no inventory, or no certainty as to their certificate landscape. Most enterprises operate thousands of certificates. The fact that only one expired certificate can bring down an entire business application explains why the risk is so high when inventories are incomplete.

What best describes your organization's understanding/tracking of digital certificates currently in use?

16%
Not sure how many certificates we have or where they're used

50%
Partial inventory. Some certificates may be unknown

34%
Complete, up-to-date inventory of all digital certificates

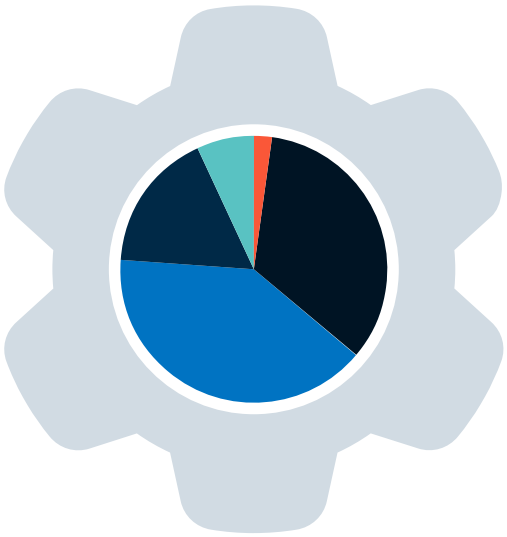
This concern is not lost on leadership. Nearly three-quarters of respondents are very or extremely concerned about outages due to expired certificates, and nearly the same proportion are very or extremely concerned about certificate sprawl. Together, these findings describe a familiar enterprise tension: organizations understand the consequence of certificate failure, but many still lack the visibility needed to prevent it consistently.

In addition, about half of those surveyed also cite siloed solutions that are difficult to manage, and 47% point to error-prone spreadsheet tracking. In other words, the visibility gap is not just about incomplete discovery. It is also the result of fragmented tools, fragmented ownership, and fragmented processes.

How concerned are you about the risk of outages/service disruptions due to expired certificates?

41%	Extremely concerned
32%	Very concerned
19%	Moderately concerned
6%	Slightly concerned
2%	Not at all concerned

How concerned are you about certificate sprawl in your organization as the number of systems/identities grow?



40%	Extremely concerned
34%	Very concerned
17%	Moderately concerned
6%	Slightly concerned
2%	Not at all concerned

4.1 billion

public certificates issued in 2025

This is a 55% increase over the previous year, when 2.6 billion certificates were issued globally throughout 2024, according to public transparency logs. Internal certificates are being issued at a far greater rate.

The right tools and processes increase visibility while lowering risk

Despite variability in the implementation of modernization, survey respondents were clear about what constitutes better PKI. Enhanced monitoring and stronger control over certificates, centralized visibility, time savings, and fewer outages all lead to easier, stronger management with lower risk. We see centralized visibility and a single-pane-of-glass approach continuing to emerge as top priorities for organizations managing PKI complexity.

This is why discovery should be treated as the first step in modernization. A reliable inventory is how organizations move from assumptions to evidence. It allows teams to assign ownership, identify renewal dependencies, prioritize automation, and understand where cryptographic agility will be hardest to achieve. Without that visibility, every other modernization effort is working with partial information.

Takeaway

Visibility helps address the risks of certificate-related outages and provides the foundation for modernizing PKI.

Complexity and maturity

Complexity and low maturity are at the root of visibility and risk

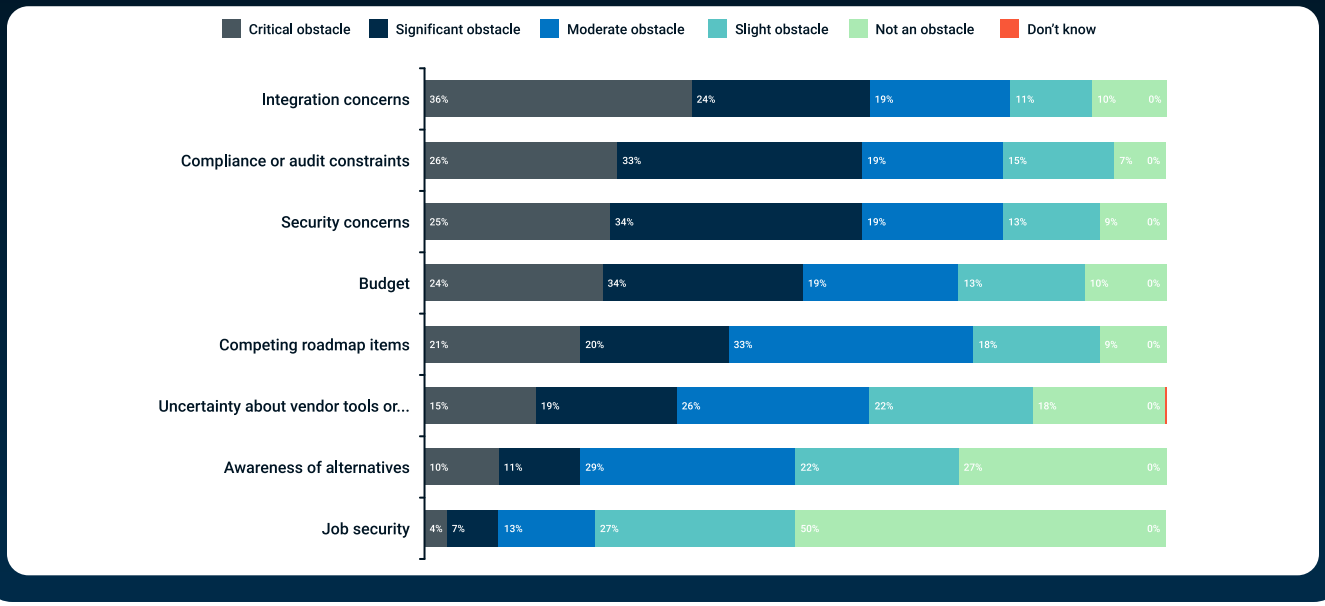
Fragmented PKI and fragmented PKI management make it increasingly difficult to control certificate sprawl

Complexity is both a structural and a technical challenge

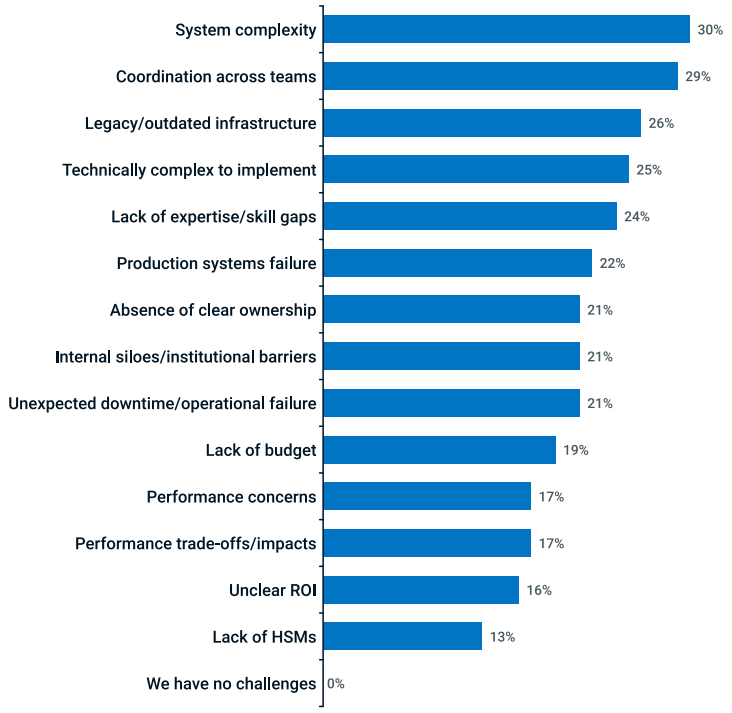
Complexity is the reason behind persistent visibility challenges. PKI has become structurally complex, not just technically complex. The issue is not merely that one integration is hard, or one workflow is clunky. It is that digital trust has expanded across public and private PKI, cloud services, legacy certificate authorities, machine identities, code signing, connected devices, and specialized platforms faster than most organizations have been able to integrate and govern it.

Survey respondents report concerns across a variety of issues, spanning all forms of complexity. Integration concerns rank among the top roadblocks to operational progress, but professionals also cited security- and compliance-related issues, along with budget, planning, and others. Here, we see that organizations are not struggling with a single obstacle. Implementing and operating better PKI is challenged by a web of dependencies: architectural, procedural, and organizational.

To what degree are the following an obstacle in your organization's adoption of automated certificate management?



What challenges have you experienced, or expect to experience, with implementing PKI modernization?

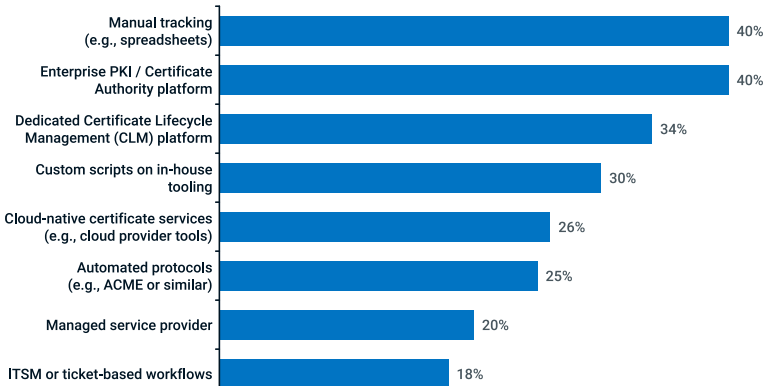


Multiple certificate management processes fall short of enterprise needs

Many enterprises are not operating from one unified certificate management model. They are using multiple methods simultaneously, with manual tracking often co-existing alongside enterprise PKI (Private CA) solutions, certificate lifecycle management platforms, custom scripts, and IT workflow software (ITSM).

On average, enterprises are using two to three different methods at the same time. This means that many organizations are in a transitional state from no automation to partial automation to full automation. In practice, partial automation means automatically renewing the certificate but not the installation of it. While this is an improvement over fully manual processes, without end-to-end automation, outage risk remains high.

Which methods/platforms does your organization currently use for certificate management?



Manual methods cannot solve for sprawl—especially spreadsheets

Spreadsheets have served as the basis for PKI inventory and status management for decades. They are convenient, familiar, and often the fastest way to keep a team moving. The problem is that they are being asked to do a job they were never designed for. As certificate volumes rise and renewal windows shrink, spreadsheets stop being a management tool and start becoming a risk multiplier.

Before reliable automated tools existed, spreadsheets were necessary. Today, though, mature certificate lifecycle management platforms, interoperability standards, policy controls, and automated installation can reduce a meaningful amount of the burden associated with spreadsheets and other manual processes. The key is sequencing: rationalize, integrate, and automate the highest-value certificate use cases first rather than trying to bring the entire enterprise PKI ecosystem under one automation platform all at once.

Takeaway

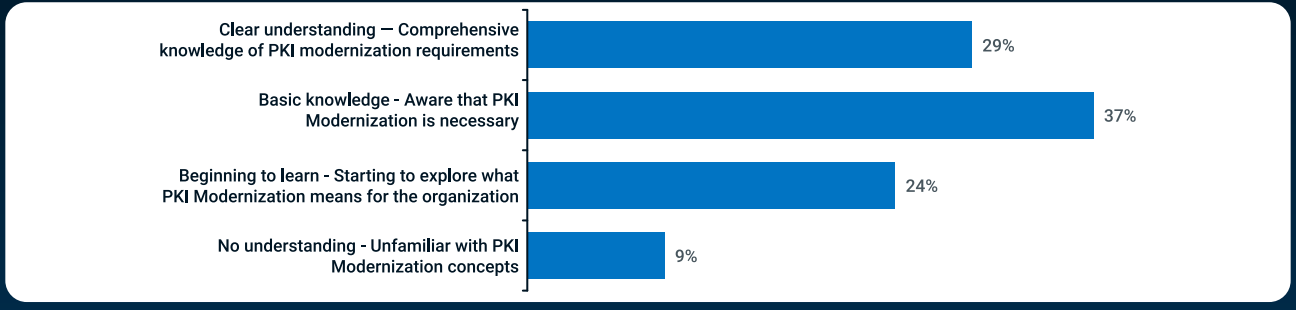
Complexity is a challenge, but it is manageable. It is evidence that PKI needs a unified operating model, with phased consolidation, reliable integrations, and automation first applied to where the risk is highest.

Maturity means operationalizing PKI best practices

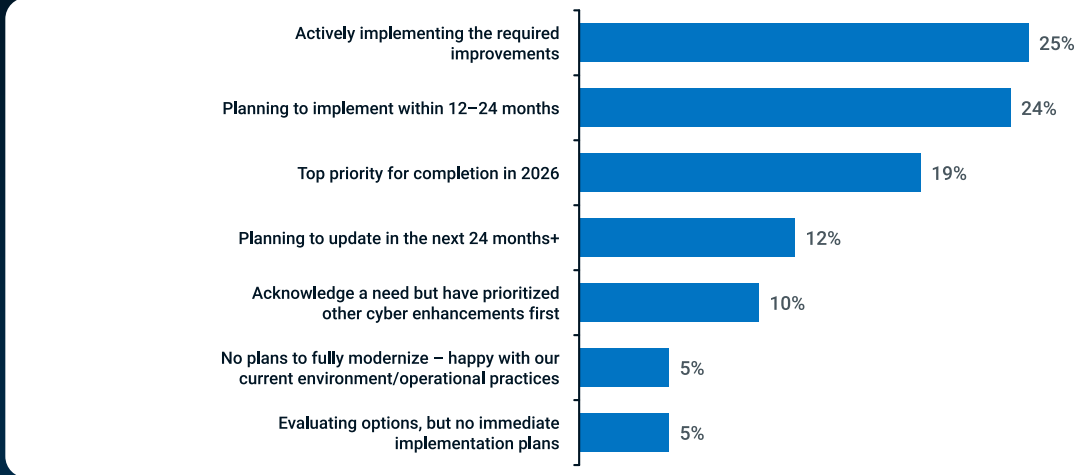
Maturity is where PKI stops being a set of good intentions and starts becoming an operating model for enabling the business to scale and accelerate, safely. It is about building the visibility, ownership, governance, and repeatable processes required to run PKI as an intelligent system. By that standard, modernization efforts are early but not nascent. This looks misaligned: awareness, urgency, and execution are not moving at the same pace.

That misalignment is clear in the survey. Nearly three in ten respondents say their organization has a clear understanding of PKI modernization, and one in four say they are already implementing the required improvements. At the same time, roughly 80% are either acting or planning to act across the next one to three years. There is mainstream intent, even if execution remains uneven.

Faced with the growing need to reduce certificate lifespans and the forthcoming influence of PQC around the corner, organizations are needing to update their PKI estates. What describes your organization's understanding of PKI modernization?

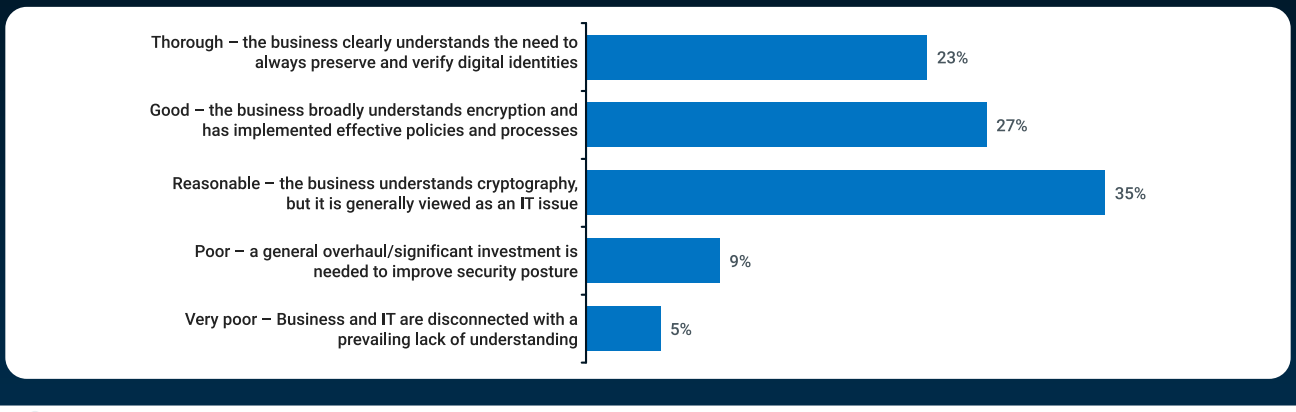


What are your organization's plans to fully modernize PKI infrastructure?



There are also signs that conversation is improving within organizations. Just over half of respondents describe their business understanding of digital identity and cryptographic integrity as thorough or good, while another 35% say the business understands cryptography but still tends to view it primarily as an IT issue. In other words, PKI is moving up in executive relevance, but many organizations are still in the process of translating that awareness into process discipline and governance.

In your view, what is the overall understanding within the business of the criticality of an effective and modern PKI?

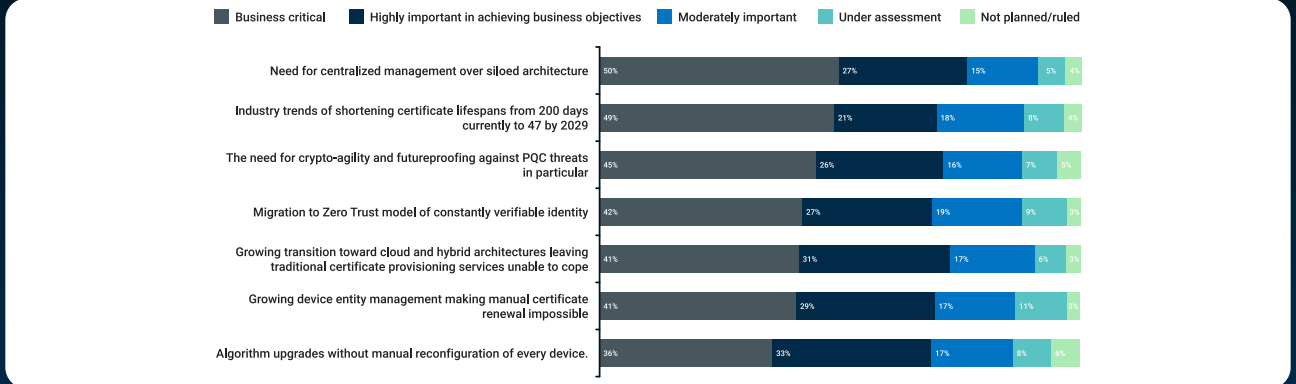


Mature organizations prioritize centralization

Siloed environments make it more difficult to maintain complete visibility, avoid risks associated with certificate sprawl, and manage all certificates. We see mature organizations opting for centralized PKI management, with 76% identifying it as business critical or highly important.

Along with unified management, concerns surrounding shortening certificate lifespans and preparing for post-quantum threats describe a mature operating model in plain terms: centralize critical PKI infrastructure, automate what repeats, and build for change, rather than treating PKI as static.

How important are the following factors that are driving/would drive your organization's need to modernize/update your PKI environment?



Improved outcomes for modernized organizations

Results from the survey indicate notable improvements in areas of concern, after introducing modernized PKI. Among modernized respondents, 64% report automated lifecycle management, 60% cite reduced outages, 44% point to better support for regulatory compliance, and 43% say they have gained increased visibility and control. When done well, modernization reduces outages, lowers administrative overhead, and streamlines compliance.

PKI maturity is not defined by how many certificate authorities an organization owns or how many tools it has purchased. It is defined by whether the organization can reliably answer a practical set of operational questions: what do we have, who owns it, when will it renew, what service depends on it, what policy applies, and can we make changes without disruption?

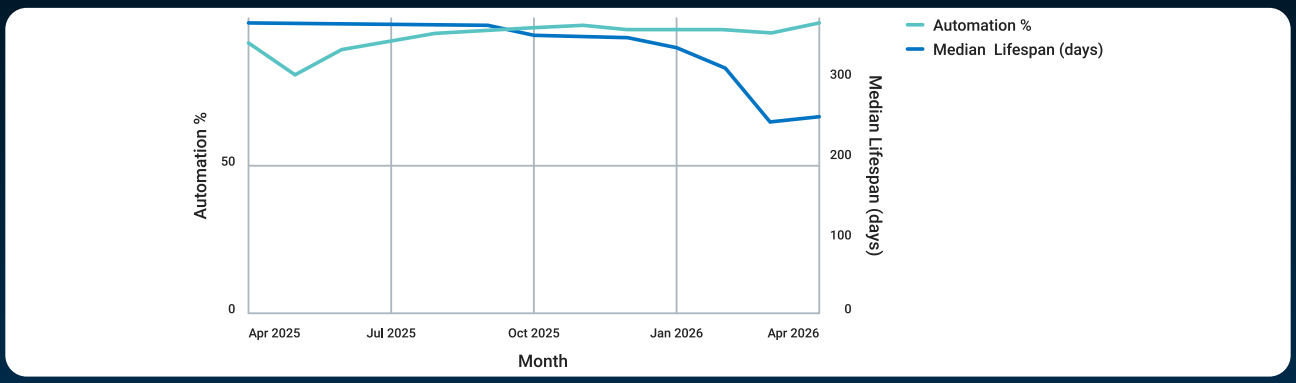
Takeaway

Organizations appreciate the problem and are beginning to understand what they need to do. Those that are furthest down the implementation road are seeing the benefits.

47-day mandate and automation

Certificate management data from DigiCert ONE customers shows they began shortening public TLS certificate lifespans following the CA/B Forum's approval of a phased reduction to 47-day certificate validity periods. This phased reduction does not necessarily increase the number of certificates an organization has to manage. It increases the number of times their security teams have to perform certificate lifecycle tasks.

Automation % vs Median Public Certificate Lifespan



AI and Quantum

AI and quantum signal both an acceleration and a paradigm shift

These emerging technologies offer the greatest challenge—and perhaps the only truly foundation transformation—to PKI in decades.

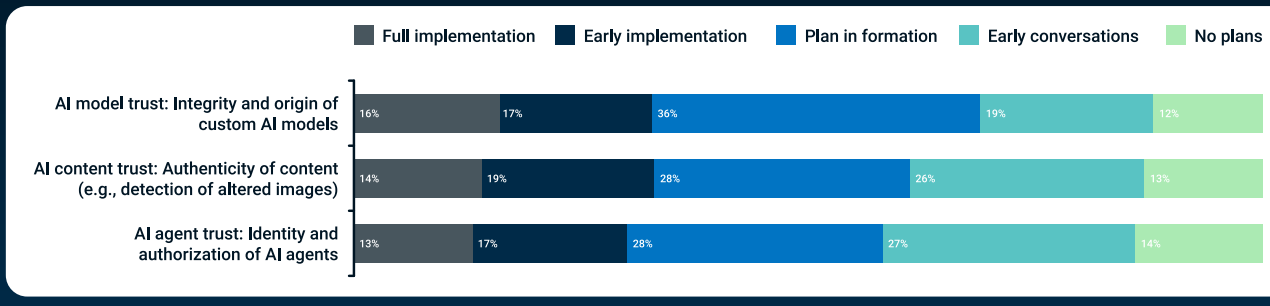
AI content, model, and agent trust require special PKI considerations

AI raises the bar for digital trust by forcing organizations to answer harder questions about identity, provenance, and authorization at machine speed. As enterprises introduce autonomous agents, deploy models, and generate content, they need stronger ways to prove what is authentic, what is trusted, and what is allowed to act. These are familiar problems to solve with PKI, but AI makes them more visible.

The survey shows that leaders already recognize the strong connection between the AI challenge and PKI. Roughly three-quarters of respondents say PKI will play a large role in AI use.

What is not yet present is readiness. Survey respondents suggest that, while organizations increasingly recognize the relevance of PKI to AI-related security and governance, most are still in the early stages of planning and implementation. The dominant pattern is not broad adoption of mature processes, but a mix of early exploration, developing plans, and initial projects.

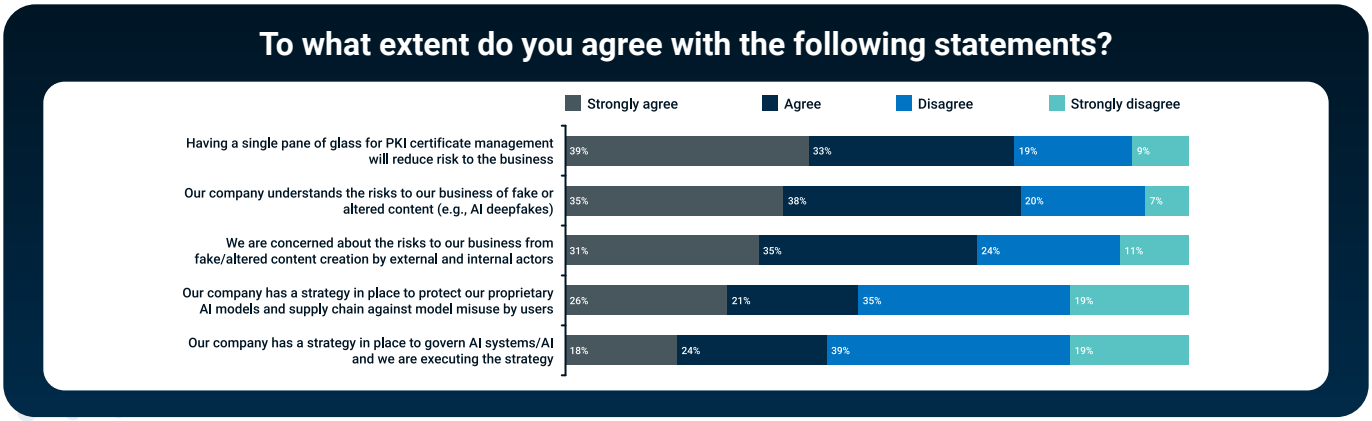
What best describes your current level of planning around these specific aspects of AI trust?



Bridging from risk awareness to an operational AI trust strategy

Governance is where that readiness gap becomes most visible. The majority of respondents disagree that their company has a strategy in place to govern agentic AI and execute it. More than half also disagree that they have a strategy to protect proprietary AI models and secure the supply chain of external models they may use. At the same time, 73% say their company understands the risks of fake or altered content, 66% say they remain concerned despite the actions they are taking, and 72% say centralized visibility for PKI certificate management will be critical in the AI era.

That is why AI should be treated as a forcing function for PKI modernization rather than a separate trust program. Organizations that cannot see and govern their use of certificates today will struggle to trust AI agents, models, and content tomorrow.



Takeaway

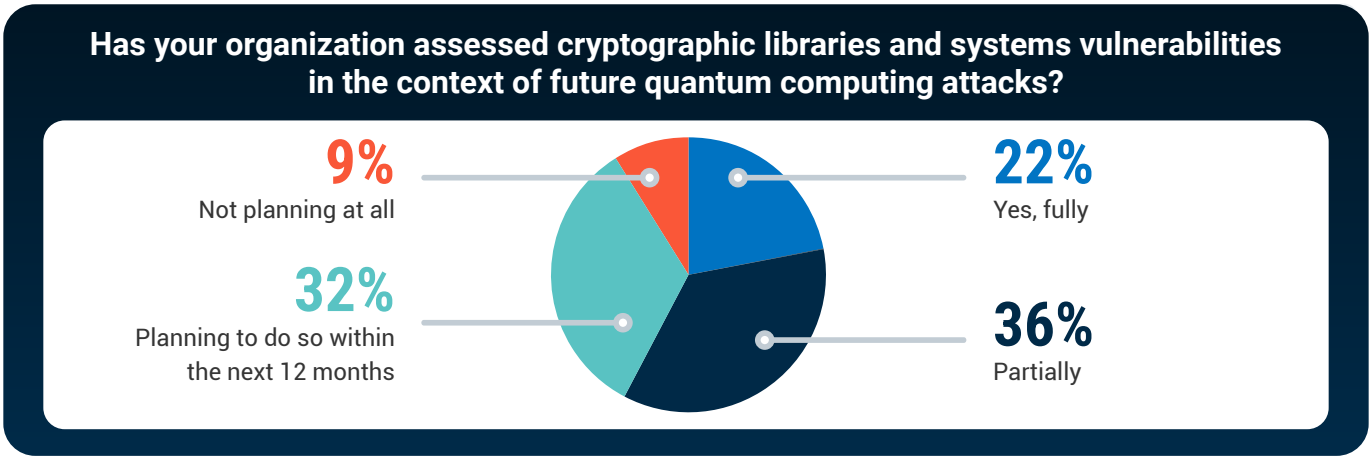
AI trust is not a separate discipline from PKI modernization. It is one of the most visible reasons organizations need stronger governance now.

Quantum is approaching quickly. Planning takes time.

While AI is the immediate trust challenge, quantum computing is not far behind. The shift to post-quantum cryptography will not be a routine refresh or a one-time activity. It will require that organizations understand where cryptography lives, what systems depend on it, how those dependencies are connected, and how to transition with as little disruption as possible.

The survey results shows both awareness and unfinished work. Only 22% of respondents say they have fully assessed cryptographic libraries and systems for vulnerabilities in the context of future quantum attacks. Another 36% say they have partially assessed them, and 32% say they plan to do so within the next 12 months. Full readiness is still rare, yet most organizations are moving in the right direction.

This aligns with how respondents describe modernization drivers. More than 71% say the need for cryptographic agility and future-proofing against quantum threats is business critical or highly important. Leaders understand the strategic importance of quantum readiness even if the underlying discovery and migration work is still early.



The important point is that quantum readiness depends on the same operational foundations discussed throughout this report. An organization cannot become cryptographically agile if it does not know where certificates, keys, algorithms, and cryptographic libraries are deployed. It cannot plan coordinated change if ownership is fragmented or if lifecycle processes remain manual. Quantum readiness therefore begins long before an organization rolls out a new algorithm.

Takeaway

Quantum readiness is not a separate effort. The certificate inventory and lifecycle automation required for other initiatives help achieve the agility necessary for migrating to post-quantum cryptography.

Modernizing PKI

PKI modernization solves for visibility, complexity, maturity, AI, and quantum

The central message of this research is not that organizations are failing at PKI. It is that PKI has outgrown the approaches many organizations still use to manage it. The problem is more solvable than it first appears. Leaders recognize the need to modernize, they are budgeting for it, and most organizations are already planning to do so. The goal is to turn that momentum into repeatable operational control.

For IT and security leaders, that means treating PKI modernization as a core capability. PKI affects uptime, operational efficiency, AI governance, and cryptographic agility. Organizations that effectively modernize will not only reduce certificate-related outages or improve operational efficiency. They will put in place an intelligent and scalable trust system for the next wave of machine identity, AI adoption, and quantum security.

PKI modernization can sound broad because it is broad. But it is not vague. Start where the operational value is immediate and the business case is easy to explain.

Run Discovery and Inventory

Solve for risks due to a lack of visibility

Build a reliable inventory of certificates and related cryptographic assets across public and private environments. Then add the context like ownership and business impact that turns raw discovery into actionable information. This is the foundation for everything that follows. Discovery is how teams move from “we think” to “we know."

Automate critical certificates

Solve for lapses and gaps to manage complexity and increase maturity

Public TLS/SSL is the most universal modernization use case because every internet-facing organization is affected by shorter certificate lifetimes. The cadence is only going one direction. Automating issuance and installation for public TLS is therefore one of the fastest ways to reduce outage risk while building repeatable lifecycle capability. It also helps teams create operational patterns they will need to extend automation into internal PKI, code signing, device identity, and other trust domains.

Standardize internal PKI

Reduce fragmentation and prepare for future cryptographic change

Internal PKI is often where complexity accumulates fastest and where outdated practices persist the longest. As certificate volumes grow and cryptographic requirements evolve, inconsistent practices increase operational risk and make change harder to coordinate.

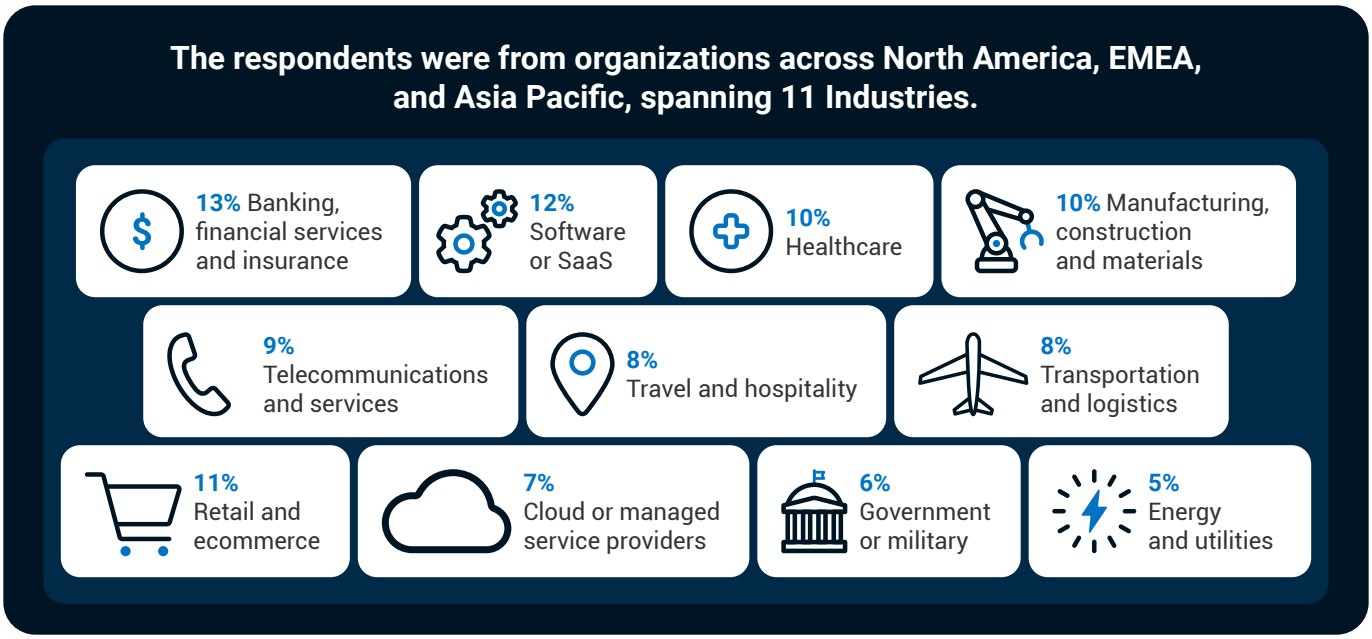
Organizations should establish centralized governance by defining policies for internal PKI environments. Policies can specify factors such as approved certificate authorities, business criticality and ownership, certificate and cryptographic configuration standards, and compliance needs. Consistent policies improve visibility, reduce operational friction, simplify compliance efforts, and create a stronger foundation for future initiatives such as AI governance and post-quantum cryptography.

Policies enable organizations to consolidate unnecessary or overlapping certificate authorities, retire legacy platforms, and bring siloed internal PKI environments under a more consistent governance model. Remediate high impact policy violations first. The goal is not to rebuild everything at once, but to systematically reduce risk across both current and emerging uses of PKI.

Methodology

This report is based on primary research independently conducted by Omdia in April 2026. The survey covered PKI evolution, modernization drivers, operational challenges and future considerations.

The research included 423 senior decision-makers, including CISOs, CIOs, and senior IT/security leaders, responsible for cybersecurity, PKI, and digital infrastructure. Respondents represented Product and Research & Development, IT and Technical Operations, Cybersecurity, and Governance Risk and Compliance functions.



All participating organizations had at least 1,000 employees:

39%
had 1,000 – 4,999 employees

24%
had 5,000 – 9,999 employees

37%
had 10,000 or more employees

Survey questions were designed to measure operational realities and strategic priorities related to PKI modernization, digital trust, and cryptographic readiness. Analysis and conclusions are based on the data collected, Omdia's research methodology, and a proprietary dataset. Some questions allowed multiple responses; therefore, totals may exceed 100%.

Supplemental analysis used data from DigiCert's managed PKI and public certificate authority operations from January 2025 through March 2026. The data included summary statistics from a selection of 757 enterprise customers. Public certificate authority operations data was from certificate transparency logs.

Authors and contributors

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through a global base of analysts, offer expert analysis and strategic insight across the IT, telecoms, and media industries. Omdia's unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making. Omdia is part of Informa TechTarget, the Informa group is listed on the London Stock Exchange.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com