digicert® + Omdia by Informa TechTarget

Certificate Blind Spots Are an Outage Waiting to Happen

Only 34% of enterprises have a complete certificate inventory, according to the DigiCert 2026 Global PKI Research Report.

Organizations aren't as prepared as they think. New findings from Omdia and DigiCert reveal why.

Organizations operate PKI environments they can't fully see, **yet remain responsible for outages, breaches, and compliance failures.**

PKI is no longer a system. It is a full ecosystem that has fragmented too quickly for organizations to keep up.

PKI modernization can't wait. AI and quantum are accelerating the need to move from awareness to action.

You can't manage what you can't see

PKI risk starts with visibility gaps. Many enterprises are operating certificate environments they cannot fully account for, creating systemic exposure.

Almost 2 out of 3 enterprises don't have a complete, up-to-date inventory of their digital certificates.

What best describes your organization's current state for tracking digital certificates?

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

50% Partial inventory, some certificates may be unknown

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

PKI risk is understood. It is not controlled.

There is a clear gap between awareness and execution. Organizations recognize the risk, but their operating models have not caught up.

Enterprises extremely / very concerned by:

73% Risk of outages or service disruptions due to expired certificates

74% Certificate sprawl as the number of systems or identities grow

PKI Has Evolved. Management Hasn't.

Manual tracking and spreadsheets remain the most widely used certificate management method.

Complexity is the enemy of modern PKI

PKI has become structurally complex, not just technically complex. Integration and organizational friction are now the primary blockers to progress.

Current certificate management and verification challenges:

- Lack of visibility
- Siloed solutions

Expected PKI modernization implementation challenges:

- System complexity
- Coordination across teams

The identity explosion is both a challenge and an opportunity for PKI

The shift to non-human identities (NHIs) at scale is overwhelming legacy PKI approaches—especially where Agentic AI is concerned. Organizations need to work hard to meet coverage needs.

Current PKI coverage

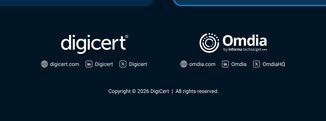
Highest Machine identities (**64%**)

Lowest Agentic AI (19%)

Everyone uses PKI. No one owns PKI.

Diffuse ownership is slowing progress. PKI modernization isn't just a technical challenge, it's a governance and accountability issue.

What level of involvement does each stakeholder have in PKI decision making at your organization?



Overwhelmingly CISOs, at **40%, are the key decision makers for PKI.**

There is help from CIOs, CTOs, and security teams, but the rest of the CXO team **need to instill valuable, additional support.**

Only 9% of PKI decision making is through the Board.

The future of trust is already here. Organizations aren't ready.

The next wave of demand, driven by AI, quantum risk, and Zero Trust, is accelerating faster than organizational readiness.

Current understanding of PKI modernization:

70%

Low

Combines 'basic knowledge', 'beginning to learn', and 'no understanding'

Plans to fully modernize PKI infrastructure:

68%

Within next 24 months

Organizations cannot do this alone. The expertise and support of digital trust providers and partners will help organizations achieve this shift.

Organizations that have introduced PKI modernization experience a higher than **60% reduction in outages.**

Download the full report

digicert®

digicert.com | Digicert | Digicert

Omdia by Informa TechTarget

omdia.com | Omdia | OmdiaHQ