



The Economic Impact of PKI Modernization

Turning the PKI management challenge into a business opportunity



Security teams prioritize in terms of risk. That language is familiar, but when it comes to PKI, it can make the issue sound theoretical. For most organizations, PKI-related outages are already happening. If the probability of an incident is 100%, it is the cost of doing business, not a risk. This, in turn, means the payoff of PKI modernization is not theoretical.

In Forrester's Total Economic Impact™ study, commissioned by DigiCert, the composite organization experienced **24 certificate-related incidents a year** before implementing DigiCert's PKI platform, DigiCert® ONE. After implementation, Forrester modeled that incident count falling to one per year, producing a **three-year present value of \$2.8M from reduced incident costs**.

PKI modernization value drivers

Modernizing PKI delivers quantitative benefits to the business:

Fewer incidents	• Increased revenue from avoiding outages • Fewer penalties paid for missed service level guarantees • Cost savings from decreased incident response and post-mortems
Increase efficiency	• Decreased administrative overhead of manual processes • Increased reliability from automation of repetitive administrative tasks • Improved quality of services (e.g., faster provisioning)
Tool consolidation	• Decreased scope of required product knowledge • Simplified licensing and maintenance costs • Increased reliability of product integrations

There are qualitative benefits, too. Compliance audits are easier. Entering new markets is faster. New technologies will be easier to secure.

Forrester modeled \$7.9M in three years present value from reduced labor costs for renewing existing certificates, plus \$993K from deprecated legacy tools and \$1.3M from revenue growth tied to meeting partners' or customers' strict security standards.

The cost of doing nothing

Many enterprise PKI environments work because talented teams have made them work. Scripts, spreadsheets, calendar reminders, and behind-the-scenes heroics keep certificates up to date, so critical systems stay available.

That effort should be applauded but not mistaken for an optimized operating model.

That siloed approach to PKI won't keep up as certificate lifecycles shrink, machine identities grow, AI creates new trust requirements, and quantum readiness moves toward execution.

The modernization fixes for each of these pressures are connected. The automation needed for 47-day certificates helps to scale machine identity management. Stronger machine identity practices help establish trust for AI agents. The visibility, policy, and lifecycle discipline required across all of it creates the agility needed for post-quantum cryptography.

The status quo may seem to work now, but it will become more brittle and expensive soon enough. The good news is that CIOs and CISOs can modernize incrementally based on what's best for their business and incrementally realize the benefits in-kind.

DigiCert ONE unifies certificate lifecycle management, PKI, and DNS under a single governance and automation layer. It empowers organizations to replace fragmented tools and siloed PKI environments with one scalable platform.

312%

Return on investment

\$10.1M

Net present value

<6 months

Payback

Data source: [The Total Economic Impact™ of DigiCert ONE](#)

Read next: Practical Lessons for PKI Modernization

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.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.