digicert®

Certificate lifecycle management, PKI and software supply chain security in financial services

Key findings from Ponemon's global study

DigiCert partnered with Ponemon Institute to gain insights into the effectiveness of certificate lifecycle management, PKI, and software supply chain security across the financial services industry.

Big picture

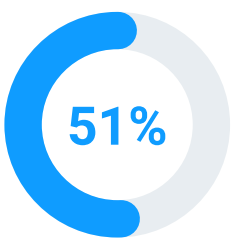
2,546 Ponemon surveyed **2,546** IT and IT security practitioners across the globe

62%
of respondents' organizations had one or more digital certificate-related outages or security incidents

48%
of respondents' organizations have been impacted by one or more attacks on the software supply chain

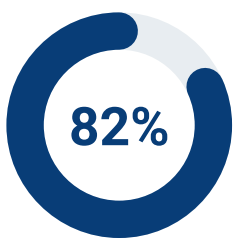
51%
of respondents have seen their staff's operational burden increase due to the increasing use of digital certificates

The state of PKI and certificate lifecycle management



Centralized visibility is a must.

51% of respondents don't know how many certificates they have, and they can't manage what they can't see.



82% of organizations

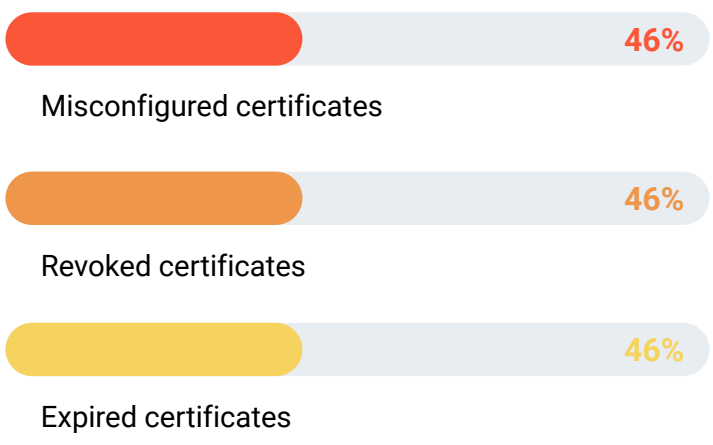
lack an optimal solution

for certificate lifecycle management.

Causes of

security incidents

due to an issue with digital certificates.



The state of software supply chains

27%
of organizations have policies for verifying published software, but lack centralized governance

44%
Policy and workflow enforcement are the most important code-signing solution features for 44% of respondents

55%
Malware, vulnerabilities, or other open-source software threats were behind 55% of supply chain attacks

Where to go from here

The path to modernizing your PKI starts with

Discovery & ownership

Software supply chain security ***requires*** strategies like governing code signing, understanding the third-party components within your software, and scanning builds for malware and vulnerabilities.

Want to learn more about how to safeguard your environment?

Read the report