PULSE | KEYFACTOR

FinServ Identity and Access Management Trends and Strategies

IT leaders and teams in financial services are responsible for ensuring the security of payment-related data and financial records. These important tasks are coming under increased focus after high profile data breaches in the financial services realm.

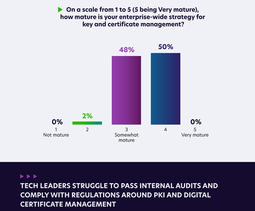
Pulse and Keyfactor surveyed 100 IT and security leaders in the financial sector to discover trends in identity and access management (IAM), and where machine identities fit into their overall IAM strategy.

Data collected: May 6 - June 22, 2021 Respondents: 100 IT and Security Leaders in Finance

100% OF TECH LEADERS IN FINANCE CONSIDER DIGITAL CERTIFICATES IMPORTANT TO IAM STRATEGY, BUT FINSERVS LACK MATURITY IN KEY AND CERTIFICATE MANAGEMENT

The majority of respondents (77%) believe the use of digital certificates is moderately to very important to their identity and access management (IAM) strategy.

How important is the use of digital certificates (e.g. TLS) in your Identity and Access Management (IAM) strategy?



But when it comes to their enterprise-wide strategy for key and certificate management, half of tech leaders in finance (50%) believe their strategy is not yet fully mature. None of these respondents would consider their key and certificate management strategy very mature.

On a scale from 1 to 5 (5 being Very mature), how mature is your enterprise-wide strategy for key and certificate management?

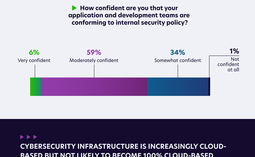
TECH LEADERS STRUGGLE TO PASS INTERNAL AUDITS AND COMPLY WITH REGULATIONS AROUND PKI AND DIGITAL CERTIFICATE MANAGEMENT

94% of respondents have failed one or more internal audits related to PKI and digital certificate management in the last two years, where nearly half (49%) experienced three or four failures.

In the last two years, how many failed internal audits have you experienced related to PKI and digital certificate management?

Tech leaders agree PCI DSS is the most difficult regulation to comply with.

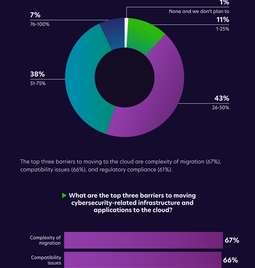
When it comes to key and certificate management, rank the regulations most difficult to comply with from highest (1 - most difficult) to lowest (4 - least difficult)



FINSERVS ARE RELYING ON TRADITIONAL AND EMERGING PKI USE CASES TO SECURE FUNCTIONS DESPITE A LACK OF CONFIDENCE IN TEAMS TO COMPLY WITH INTERNAL SECURITY POLICY

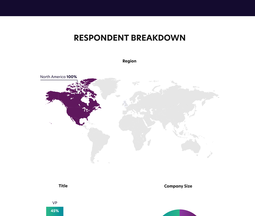
The majority of respondents consider financial transactions (77%) a potential use case for Public Key Infrastructure (PKI), followed by web server infrastructure (59%) and end-user smart card authentication (58%).

Which use cases will you consider using PKI to secure in the next 12 months?



Over half of respondents (55%) will use code signing to secure centralized server, container repo or end user package and update management in the next year, while 10% already do.

Will your organization use code signing to secure centralized server, container repo or end user package and update management in the next 12 months?



But the efficacy of security measures like PKI requires compliance with internal security policy. Currently, only 6% of tech leaders are very confident that their application and development teams are conforming to internal security policy.

How confident are you that your application and development teams are conforming to internal security policy?

CYBERSECURITY INFRASTRUCTURE IS INCREASINGLY CLOUD-BASED BUT NOT LIKELY TO BECOME 100% CLOUD-BASED FOR MOST

92% of respondents will move up to 75% of their cybersecurity infrastructure to the cloud in the next year.

In the next 12 months, how much of your cybersecurity infrastructure do you plan to move to the cloud?

The top three barriers to moving to the cloud are complexity of migration (67%), compatibility issues (66%), and regulatory compliance (61%).

What are the top three barriers to moving cybersecurity-related infrastructure and applications to the cloud?

RESPONDENT BREAKDOWN

Region

Title

Company Size

Insights powered by PULSE