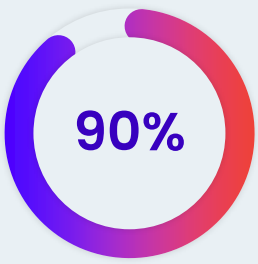
appviewx

3 reasons your business can't ignore certificate management

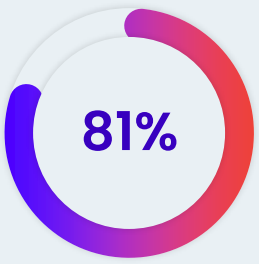
Achieve visibility and control of your certificate ecosystem with AppViewX CERT+

Do you have the right solution in place to manage your certificate ecosystem? Ineffective certificate management can affect your security posture and your bottom line. Without the right governance or enforced policies for public key infrastructure (PKI), digital certificates can expire, create outages, and lead to compliance violations.



of emails sent in 2022 were phishing emails, which can be caused by expired certificates.[1]

certificates are issued internally in IT organizations, on average.[2]



of organizations have experienced outages caused by expired certificates.[2]

1. Spam E-Mail Traffic Share 2022, n.d.
2. State of Machine Identity Management. HubSpot User Content. 2022.

Prevent certificate outages and minimize security risks

Leverage the right certificate lifecycle management (CLM) to:

- Prevent security blind spots.
- Eliminate certificate-related outages.
- Promote process efficiencies.
- Ensure best practices and maintain compliance.
- Build up-to-date certificate inventories.
- Automate the entire process of certificate lifecycle management.

AppViewX CERT+ with Amazon Web Services (AWS) Certificate Manager helps enterprises overcome operational and security challenges.

CERT+ on AWS

aws