White Paper

PKI Investments Help Organizations Improve Security and Modernize Business Processes, Study Finds

Sponsored by: DigiCert Inc.

Robert Westervelt
August 2019

EXECUTIVE SUMMARY

IT security professionals and operations teams are under increased pressure to manage the security and resiliency of mission-critical systems in support of rapidly evolving enterprise digital transformation (DX) initiatives. In a bid to alleviate that pressure and allocate resources more effectively amid the growing hybrid and multicloud environments, CIOs, chief information security officers (CISOs), and security architects are now addressing public key infrastructure (PKI) implementations that are often disjointed and poorly managed.

PKI is the backbone of many organizations that value cybersecurity resiliency because it enables organizations to automate the process of enforcing data security policies and procedures using digital certificates and public key encryption. PKI was designed to establish validated and trusted connections between systems and provide unhindered user access to sensitive resources. Over time, PKI grew to protect document, email, and code integrity through cryptographic signing certificates as well as protect assets and individuals with digital identities using device certificates.

Today, as security teams are under more pressure than ever before, PKI is being thoroughly tested and relied upon. Teams are using PKI to remediate risks as the business grows its use of cloud services, and attackers in turn seize on complexity and configuration issues caused by fragmented security infrastructure. CISOs are making it a priority to address this challenge, according to IDC's *Data Services for Hybrid Cloud Survey,* which reached more than 400 IT security and data management specialists in Europe and North America. In the survey, about 65% of organizations reported using digital certificates and PKI to support a variety of functions, including:

- **Secure BYOD:** To support unmanaged BYOD initiatives and maintain secure access to enterprise resources without sacrificing the mobile user experience
- **Secure authentication:** To strongly authenticate individuals to applications containing sensitive information
- **Secure remote access:** To strongly authenticate employees and partners to a wireless network or VPN for secure access
- **Secure email:** To enable email users to send encrypted and digitally signed emails across all corporate devices
- **Document signing integrity:** To validate the integrity and authenticity of digital signatures on critical documents
- **Secure Internet of Things (IoT) devices:** To provide device identity and establish root of trust and maintain the integrity of software and firmware on sensitive IoT devices