The 2024 PKI & Digital Trust Report

Top Trends and Threats Impacting Digital Trust in 2024

Attention CISOs:

Welcome to the Year of Digital Disruption!

Here are key highlights from Keyfactor's new global study that uncovers what's really impacting digital trust — mismanaged public key infrastructure (PKI), a proliferation of digital certificates, and impending changes to modern cryptography.

PKI is the foundation of digital trust for organizations — providing authentication and encryption for everything from their websites and applications to IoT devices and cloud workloads. But increasing usage of PKI is pushing teams and tools to their breaking point.

What security leaders can do...

It's time to evaluate your PKI infrastructure and assess whether it can support current use cases, and more importantly, is ready to adapt to significant changes on the horizon.

98% say they need to modernize their PKI

PKI is critical infrastructure, but it's getting complex

5+ Hrs to identify and remediate a certificate outage

Outages are diminishing revenue (and trust)

KEYFACTOR

Organizations are deploying more keys, certificates, and machine identities than ever — 91% compared to 74% in 2023 and 61% in 2021. Security teams must constantly worry whether application and operations teams might make mistakes or ignore policy, which leads to disruptive outages. The report shows that, on average, it takes teams more than 5 hours to identify and remediate a certificate outage. It's time to invest in visibility and automation. Fortunately, respondents indicated this is a top priority for the year ahead.

What security leaders can do...

Outages caused by expired certificates take a serious hit on customer trust, revenue, and employee productivity, especially when they impact external-facing systems. Security leaders must understand the severity and frequency of outages and prioritize their team's ability to prevent and respond to these incidents.

95% face obstacles preparing for post-quantum cryptography

Quantum looms on the horizon

Ready or not, quantum is coming, and organizations must prepare by adopting post-quantum cryptography (PQC). Threat actors have already begun harvesting and storing encrypted data now with the aim of decrypting it when a quantum computer powerful enough to break modern encryption becomes available.

What security leaders can do...

It's time to begin planning your roadmap to quantum-safe security — that starts with getting visibility of your data and cryptographic assets.

Want to learn even more about top trends and threats?

Download Keyfactor's 2024 PKI and Digital Trust Report and get fresh ideas to improve the security, reliability, and integrity of your organization's digital interactions.

Download now ↗