

You Must Prioritize Post-Quantum Cryptography (PQC) and Shorter TLS Validity Readiness: **Here's Why**

PKI is evolving faster than ever before and to keep up with the changes you must evolve your processes or risk falling behind. There are now aggressive timelines for shifting to shorter TLS lifespans and migrating to Post-Quantum Cryptography (PQC) to be prepared for quantum threats against current encryption algorithms.



Recent PKI Changes and Developments

● NEWS □ ×

Shorter TLS Lifespans

LIVE ● NEWS

The CA/Browser Forum has officially passed Apple's proposal to gradually reduce the maximum lifespan of public TLS certificates from 398 days to just 47 days by 2029

TECH NEWS

Let's Encrypt issues first 6-Day TLS certificate

Post-Quantum Cryptography (PQC)

URGENT!

Recent quantum advancements (i.e. Google's Willow, Microsoft's Majorana 1, AWS's prototype processor Ocelot) show that quantum computers are advancing quickly, threatening to break today's cryptography

BIG NEWS

NIST announced three finalized PQC encryption and digital signature algorithms, signaling the race toward PQC adoption







LIVE NEWS

NIST set an aggressive timeline to deprecate algorithms like RSA by 2030 and fully phase them out by 2035 ("disallowed")



What Are the Risks of Not Being Prepared?

If you're not preparing for these massive industry shifts today, you're already behind. By not being ready with crypto-agile processes, the time, resources and costs will continue to escalate and the success of the projects will be jeopardy. **Here are the top risks:**

Shorter TLS Lifespans	Post-Quantum Cryptography (PQC)
<div>Increased Team Workload</div> <p>Renewing and provisioning certificates up to 12 times a year will put tremendous pressure and stress on resource-limited teams.</p>	<div>PQC Migration Complexity</div> <p>Migrating to PQC will be the most complex cryptographic transition yet, as there are no drop-in replacements for existing algorithms. New infrastructure, redesigned protocols, and careful integration with current systems are required.</p>
<div>Greater Risk of Outages</div> <p>Shorter certificate validity increases certificate lifecycle management (CLM) complexity, raising the risk of missed renewals or misconfigurations causing outages of critical applications and services.</p>	<div>The "Harvest Now, Decrypt Later" Threat</div> <p>Attackers are collecting data now to decrypt once quantum computers are capable of breaking current encryption algorithms.</p>
<div>Rising Operational Costs</div> <p>Frequent renewals and managing more certificates will drive up administrative costs.</p>	<div>Legacy System Vulnerabilities</div> <p>Legacy systems that are often more difficult to update may become exposed, threatening critical infrastructure.</p>

Shorter TLS Lifespans



Security Gaps

Manual certificate management increases the likelihood of human error, vulnerabilities, and cyberattacks.



Compliance Risks

Poor certificate management can lead to non-compliance and regulatory penalties.

Post-Quantum Cryptography (PQC)



Cost of Delayed Adoption

Delayed adoption and migration plans could lead to costly retrofitting and security gaps.



The Unknown with Rapid Quantum Advancements

Quantum computing could advance faster than expected, leaving you vulnerable to cyberattacks and compliance failures.

Consequences



Cyberattacks:

Compromised communications, data theft, and exposed private keys open up critical attack vectors



Financial Loss:

Penalties, fines, legal liabilities, and costly retrofitting



Operational Disruption and Outages:

Application outages, insecure services, broken automation, and slow remediation



Legal and Compliance Risk:

Invalid contracts, intellectual property theft, and privacy / compliance violations



Technology and Security Risk:

Technical debt, security gaps, and vulnerabilities



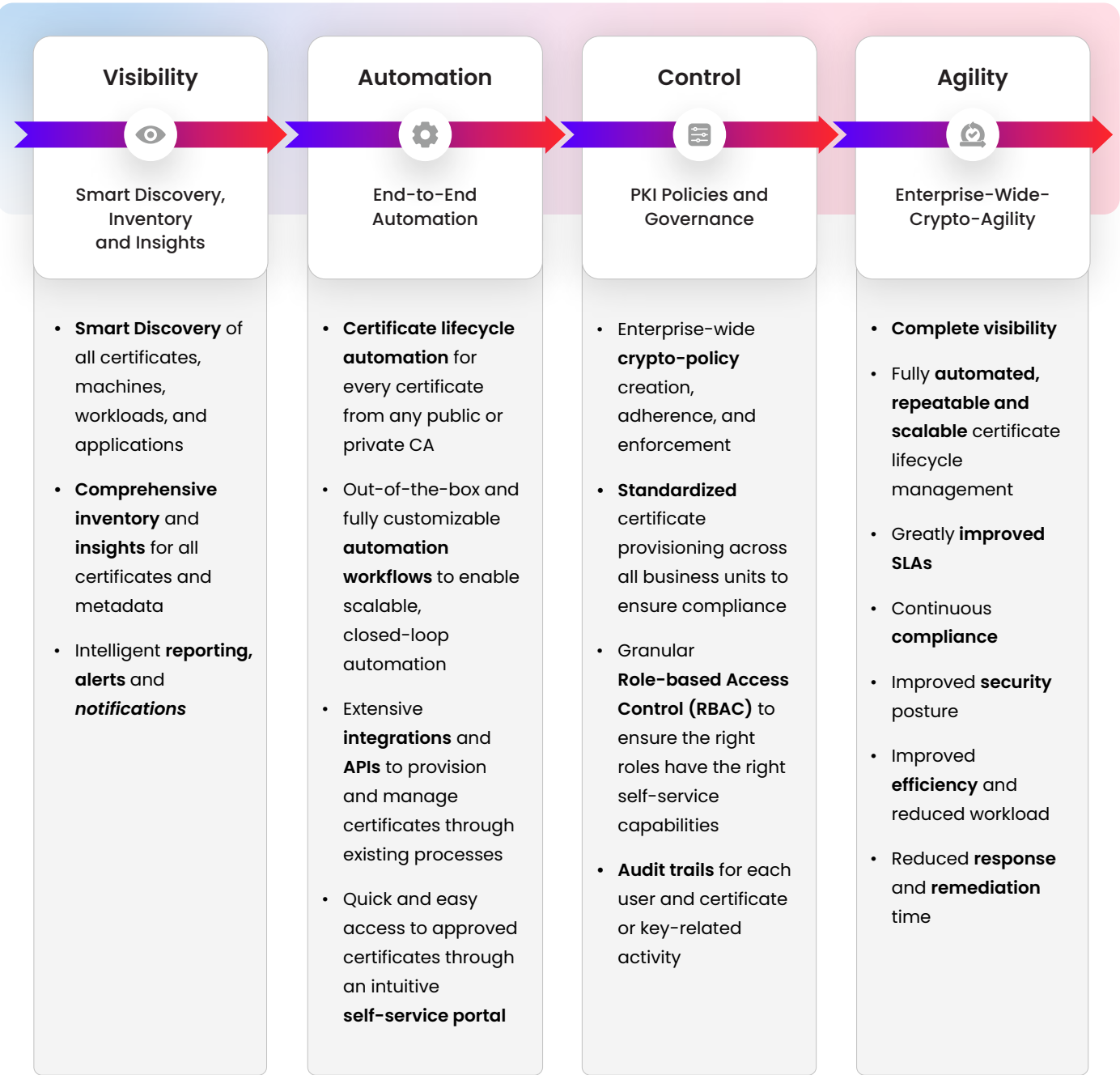
Reputational Damage:

Public incidents, service disruptions, and brand damage

Accelerate Your Readiness with Crypto-Agility from AppViewX AVX ONE

Cryptographic algorithms like RSA have been the cornerstone of cryptography for over three decades, and TLS certificates once had lifespans of 8 to 10 years. Transitioning to shorter-lived certificates and adopting PQC as a completely new cryptographic foundation is easier said than done. AppViewX can help you accelerate your readiness right now.

The AppViewX AVX ONE CLM and PKI platform enables crypto-agility through visibility, automation and control, ensuring you're prepared to seamlessly transition from old to new before disaster strikes or deadlines come due.





**To learn more about how AppViewX AVX ONE
accelerates your readiness planning for
shorter validity TLS and PQC, schedule a demo today.**

AppViewX Inc.,

AppViewX provides digital identity protection solutions that simplify PKI and certificate lifecycle management for modern enterprises. The AVX ONE CLM solution is the most advanced SaaS certificate lifecycle management (CLM) platform for enterprise PKI, IAM, security, DevOps, cloud, platform and application teams. With visibility, automation and control of certificates and keys, AVX ONE enables crypto-agility to rapidly respond to cryptographic changes, mitigate threats, prevent outages, achieve Zero Trust, and prepare for Post-Quantum Cryptography.



City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226