SECTIGO®

On-Premise vs. Cloud What's Better for Managing PKI?

Cloud computing has become integral to any enterprise environment. Running PKI in a cloud/multi-cloud environment is now the new norm. But, how does the legacy on-premise approach stack up to the new modern cloud & multi-cloud model?

ON-PREMISE PKI VS CLOUD PKI

Security Concerns

High-profile breaches of trusted on-premise systems give pause to the belief that physical proximity behind a defined network perimeter equals security.

A More Secure Future

Today's enterprises require cloud-based digital identity authentication for all users, applications, systems, and devices to effectively secure the perimeterless enterprise.

Network Boundaries

Conventional on-premise security focuses on perimeter defense, where, once inside, users who are trusted are granted broad network access.

Perimeterless

Cloud PKI offers scalable provisioning to accommodate remote and distributed workforces of all sizes in which each touchpoint is identified individually and given only the privileges necessary.

"Gone are the days of a single firewall around the perimeter of the network with a relatively safe "green zone" inside."

Tim Callan, Chief Compliance Officer, Sectigo

READ THE INTERVIEW

Dependent on In-House Capabilities

Strained IT resources for PKI management, configuration, and maintenance.

Flexibility

A cloud-based platform supports flexibility for updates and operations requiring frequent and large numbers of certificates.

Risk of Misconfiguration

Mistakes are too easy to make. White hat research has taught us that extensive configuration analysis is required to eliminate security flaws.

Configuration Confidence

Utilize a security partner with depth of experience. Cloud offers isolation from legacy authentication directory technologies.

Expensive

Not only do you have to consider the substantial cost of the data center infrastructure, but on-premises PKI management and operation require specialized labor and additional hardware and software investments.

Lower Costs

Cloud-based PKI is more cost-effective, reduces the skills burden on the enterprise, and ensures greater scalability and availability.

Easy Targets and Attacks Go Unnoticed

It's challenging to detect attacks because bad actors impersonate trust, which covers their trail.

Prevents Data Breaches and Increases the Speed of Discoverability

Protect identities and access to critical business systems by automating the installation, revocation, and renewal of all digital certificates.

Lack of Control

Hidden vulnerabilities that cause an on-premise breach could reach an internal PKI implementation. Breached access plus lateral movement can wreak havoc.

Governance

Maintain control of configuration definitions and rules without the heavy lifting required to perform daily surveillance and anticipate certificate expiration.

Why Choose a Cloud-Based PKI Solution Over On-Prem?

- Decreases organizational reliance on expensive IT specialists
- Reduces capital expenses by eliminating up-front and ongoing hardware and software costs
- Reduces operating expenses through lower services, support, and maintenance costs
- Eliminates indirect costs such as unplanned downtime
- On-premise infiltrations provide hackers with a massive payoff, enabled in part by lateral movement and backdoor approaches

The Facts Are Clear

Cloud PKI exceeds the levels of security and control that on-premises can't achieve. Discover more in our eBook, The Benefits of Managing PKI in the Cloud Over On-Premise, today!

LEARN MORE