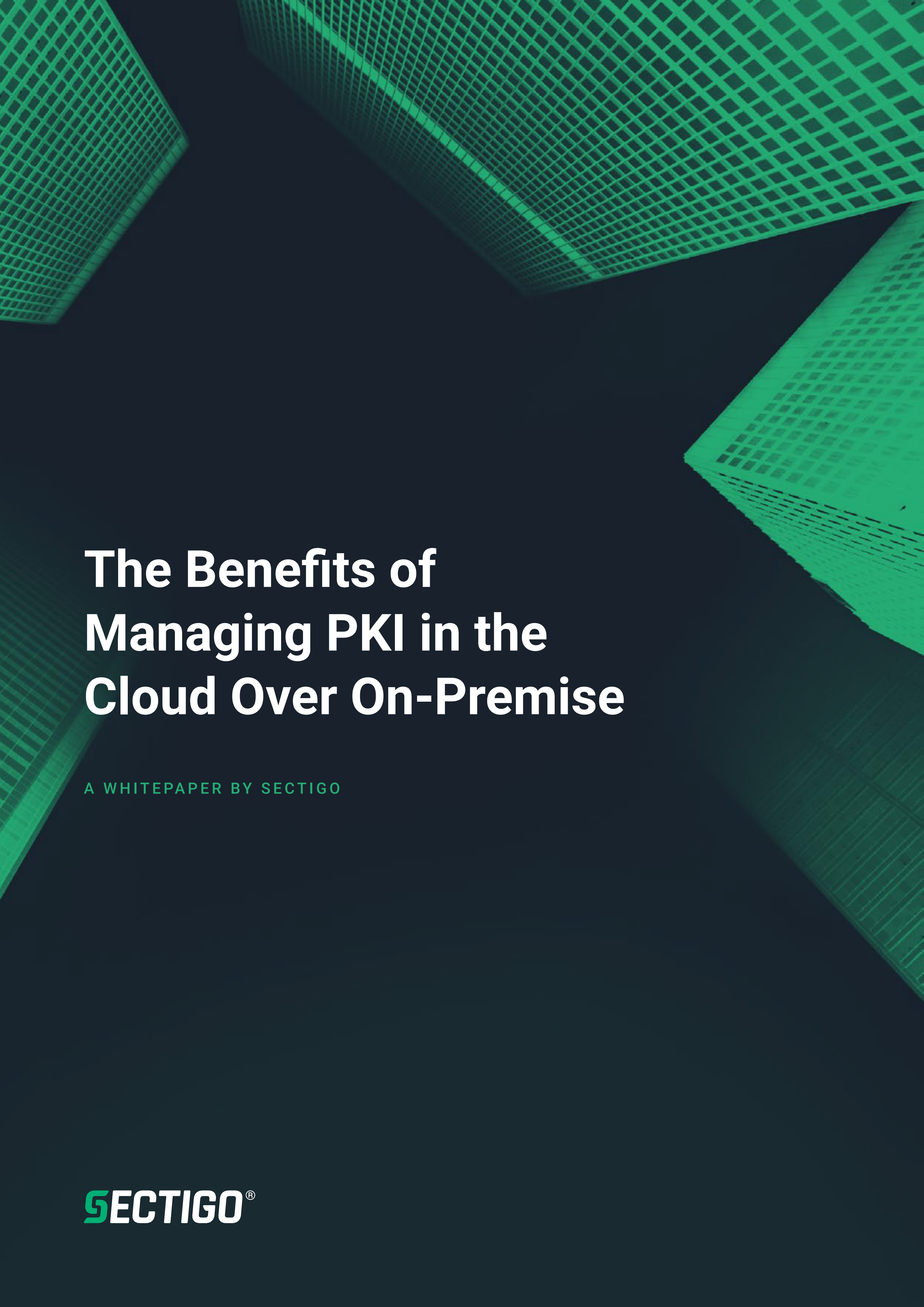


The Benefits of Managing PKI in the Cloud Over On-Premise

A WHITEPAPER BY SECTIGO

SECTIGO®

The Benefits of Cloud-based PKI Management for the Modern Enterprise

Today's threat landscape has raised the cross-industry debate on the security of on-premise versus cloud deployments to new levels. While the conversation is certainly not new, several high-profile on-premise breaches, despite firewalls and other roadblocks, give pause to the belief that data center proximity equals impenetrable protection.

This concern also applies to reliance upon an on-premise architecture for public key infrastructure (PKI) environments. Organizations who think PKI architecture is more secure because the root key and certificate management server are in their data center, and not in the cloud, may be putting themselves at risk.

Consider the Headlines:

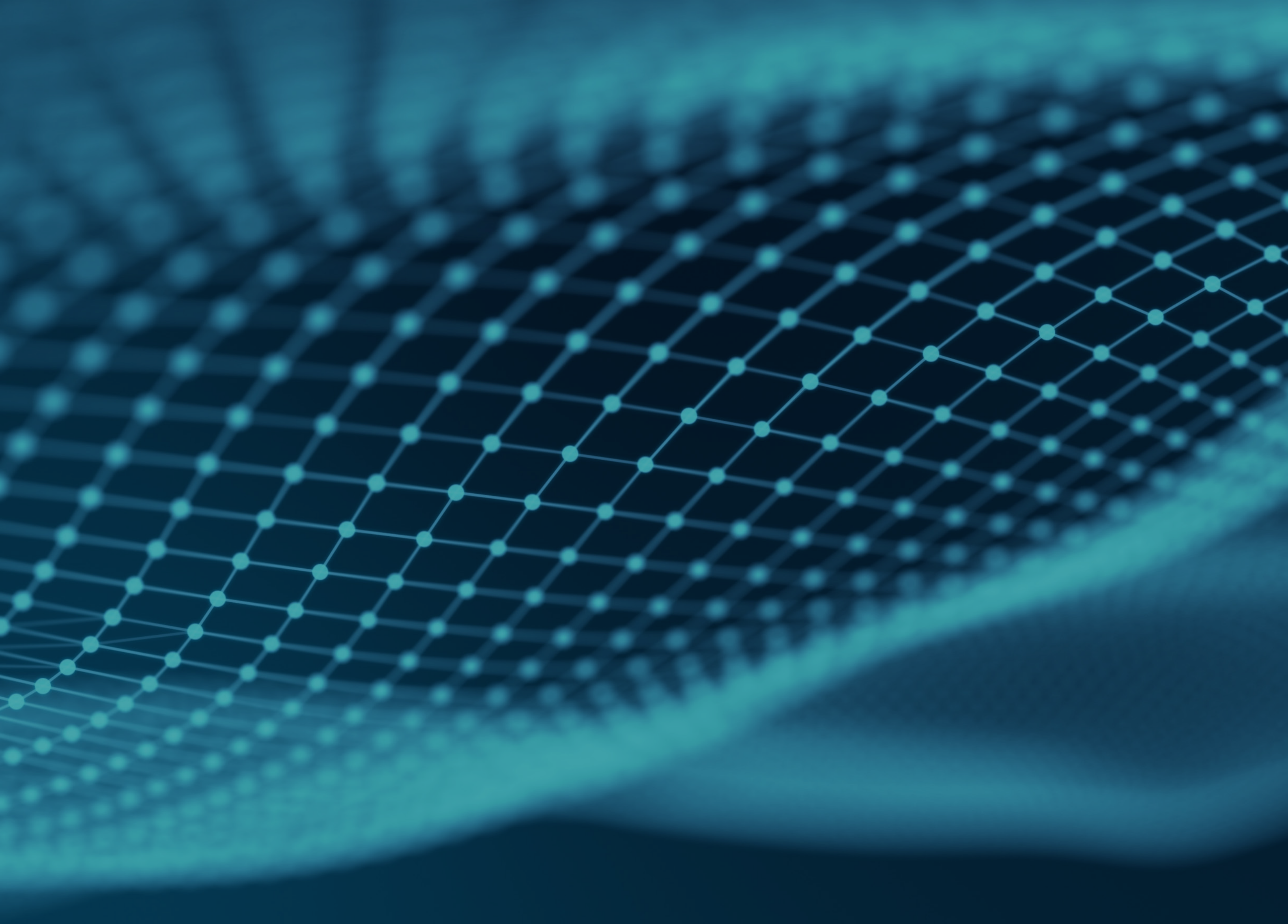
- The on-premise attack on network management company Solarwinds enabled cybercriminals to infiltrate customer networks, providing access to sensitive data from clients including Microsoft, Cisco, and U.S. government agencies, including the US Treasury and departments of Homeland Security, State, Defense, and Commerce. A supply chain attack that inserted malicious code into a signed software version went undetected for months. Compromised updates were shipped to 18,000 customers in March, 2020. The backdoor created by the breach enabled lateral movement to other systems, allowing hackers to install even more malware to spy on additional Fortune 500 companies and government agencies.

- In January 2021, the impact of a global, on-premise breach of Microsoft Exchange servers began to emerge. By March, 250,000 servers were affected across 30,000 U.S. organizations and 7,000 servers in the United Kingdom. The massive attack gave cybercriminals full access to emails, passwords, administrator privileges, and lateral access to connected devices on the same network. Hackers grabbed data, stole credentials or explored inside networks and left backdoors at universities, defense contractors, law firms and infectious-disease research centers.

Today's cybercriminals take whatever approach provides the most lucrative gain for the lowest risk. According to the 2020 Trustwave Global Security Report, that means corporate and internal networks are priority targets, representing 54% of environments breached in 2019. Both the Solarwinds and Microsoft Exchange Server on-premise infiltrations provided hackers with a massive payoff, enabled in part by lateral movement and backdoor approaches to affect tens of thousands of each organization's customers.

Violators with the "keys to the castle" impersonate trust to access critical business systems, making it difficult to avoid detection by covering their trail. CISOs shudder at the thought that an on-premise breach could reach an internal PKI implementation. And well they should. Breached access plus lateral movement can wreak havoc.

If it includes on-premise PKI management, your private keys, digital identities, and digital certificates could become compromised and insecure, bringing business to a halt.



Impact of Digitalization

The time is now to re-assess on-premise vulnerabilities, including the reliability and anticipated scalability of your approach to cybersecurity. A strategic response must take into account the impact of digitalization and the ever-changing corporate perimeter. The pace of digital transformation has dissolved traditional network boundaries, changing the effectiveness of legacy security strategies and processes. We couldn't agree more with Gartner's assessment that, "In a world of cloud-based users and devices accessing public cloud-based services, the relevance of the legacy enterprise perimeter declines."

Cloud computing has become integral to enterprise digitalization efforts, increasing the need for digital authentication processes to secure ecosystem infrastructure. In fact, an interesting trend has emerged with respect to 2020 enterprise investment in cloud versus on-premise data centers. Synergy Research Group reports that cloud infrastructure spending grew by 35% to reach almost $130 billion. Meanwhile enterprise spending on data center hardware and software dropped by 6% to under $90 billion. Expected benefits, realized by peers and cross-industry implementations, include scalability, lower costs and greater resilience.

As a result of digitalization, 53 percent of corporate data is now stored in the cloud, yet the 2021 Hiscox Cyber Readiness Report reveals that 73 percent of organizations say they're not prepared for a cyberattack. The oxymoron begs the question, "how will an on-premise PKI implementation accommodate this transformation to hybrid data access models?" Is certificate automation in place? Is a dedicated PKI IT team available to proactively monitor for increasing threats and attacks in a hybrid environment? Does a DIY PKI provide centralized and complete visibility into the threat landscape to respond in minutes rather than hours or days?

If the answers are unsettling, you are not alone. According to IBM, the average time to identify and contain a data breach, or the "breach lifecycle," was 280 days in 2020. Companies that contain a breach in less than 30 days save more than $1 million in comparison to those who take longer.

> "The average time to identify and contain a data breach, or the "breach lifecycle," was 280 days in 2020, according to IBM."

Digitalization increases requirements for sophisticated encryption and authentication that supports business continuity for the digital era. As the corporate ecosystem continues to evolve in complexity and hybrid architectures, so too does the risk of emerging vulnerabilities that are gateways to on-premise attacks. The CISO mandate? How to add security at the speed of digital transformation.

LESSONS LEARNED

THE ZERO TRUST REMINDER

Investments in digital transformation can be pointless if they can't protect the business, its customers and vital assets, and the ecosystem of partners and vendors. Applications and data running across cloud, hybrid, and multi-cloud environments, distributed workforces, and innovative connected devices are all intersecting in ways that demand a modern cybersecurity approach that protects against persistent and emerging threats. Enter Zero Trust, where trust is never granted implicitly and must be continually evaluated. As defined by NIST, a Zero Trust architecture treats all users as potential threats and prevents access to data and resources until the users can be properly authenticated and their access authorized.

Today's technology interpretation of Zero Trust is readily accessible through a managed cloud-based enterprise PKI implementation – without giving up control and flexibility. Eliminating the possibility that your on-premise PKI server or worse, domain controller, becomes another attack vector during an on-premise attack is the ultimate goal. Combining it with the opportunity to apply consolidated and proactive authentication, authorization, and encryption through collaboration with dedicated security experts is a strategic advantage toward addressing the threat landscape.

The benefit to strained IT resources using a reactive approach to identify hidden vulnerabilities will be immediate via the automation of the installation, revocation, and renewal of all digital certificates, including SSL/TLS, device and user identity certificates, digital signatures, email certificates, and more. Yet you avoid the abundant risk, sky-rocketing costs, and daily headaches of managing an on-premise PKI infrastructure by yourself.

IMPLEMENTATION STRATEGIES

ADVANTAGE: CLOUD

As we discussed earlier, the Solarwinds and Microsoft Exchange Server on-premise breaches resurfaces the longstanding core debate on the safety of cloud versus on-premise deployments. For CISOs, the core question is how to establish, strengthen, and scale PKI infrastructure to protect identities and access to critical business systems no matter where they reside. As a pillar of an enterprise cybersecurity program and endorsed by NIST as an essential foundational component of Zero Trust architecture, we know that PKI solutions are the gold standard for highly secure and trusted authentication, digital signatures and encryption.

The urgency to prevent your PKI server from becoming an easy target has never been greater. It is clear that brazen on-premise attacks are not likely to go away anytime soon. In fact, once the Microsoft Exchange Server breach came to light, additional hackers worked to take advantage of exposed vulnerabilities while IT and security teams scrambled to patch as part of damage control. Check Point Research reported a tenfold increase in attempted worldwide organization attacks once the breach became global news, noting the rise in exploitation attempts from 700 on March 11 to over 7,200 on March 15. Unfortunately, time is not on your side.

And let's not forget about the risk of malicious insider attacks on on-premise servers. Insider threats are on the rise according to a 2020 report from The Ponemon Institute, who reports that the number of insider-caused cybersecurity incidents increased by a whopping 47% since 2018. The average annual cost has also skyrocketed in only two years, rising 31% to $11.45 million. An interesting takeaway from these stats is that insider incidents are even more likely to be caused by negligent employees or contractors. In terms of PKI management, negligence is a strong word to describe human-driven errors such as failing to manually identify expired certificates, but compliance audits that measure exposure and time to response may beg to differ.

The time for proactive prevention is now. Managed cloud-based PKI delivers the digital identity management solution that today's enterprise needs to implement a Zero Trust strategy without the loss of control or flexibility. Interoperability, high uptime, and governance are key benefits. And bolstering security at the speed of digital transformation is attainable through automated certificate lifecycle management for issuance, management, and revocation. From a total cost of ownership (TCO) perspective, scaling an on-premise infrastructure to meet tomorrow's inevitable threats is simply not cost-effective in terms of specialized labor and additional hardware and software investments.

Let's dive into the details.

Foundational Cloud Advantages

Cloud computing is fundamentally designed for enterprise cost-savings. Key drivers for migration include the ability to decrease TCO by:

- Decreasing organizational reliance on expensive IT specialists
- Reducing capital expenses by eliminating up-front and ongoing hardware and software costs
- Reducing operating expenses through lower services, support and maintenance costs
- Eliminating indirect costs such as unplanned downtime

Accessing on-demand, high availability of systems, ensuring upward and downward scalability, and the ability to meet demanding compliance requirements round out the foundational advantages of cloud computing.

The use of cloud computing by organizations of all sizes continues to grow. Partly given the aftermath of the pandemic, Gartner predicts worldwide end-user spending on public cloud services will grow 18.4% in 2021 to total $304.9 billion, up from $257.5 billion in 2020.

Building on the Foundation: PKI Cloud Management Advantages

Managed cloud-based PKI delivers fundamental cloud advantages and then some. Automation as applied to the lifecycle management – the discovery, renewal, revocation, and replacement of all digital certificates and keys in your environment – delivers measurable and significant ROI. Additional core digital identity authentication benefits enable you to:

- Protect customers
- Safeguard enterprise intellectual property
- Strengthen compliance programs
- Prevent data breaches and increase the speed of discoverability
- Support a growing remote, distributed workforce
- Secure an increasing number of cloud applications and Internet of Things (IoT) devices

Cloud-based PKI also eliminates the hidden costs of on-premise deployments. In reality, traditional costs – software licensing, installation and hardware – are often only a small component of the overall on-premise TCO. Consider the following additional cost categories:

- Hardware and data center costs to maintain availability and redundancy
- Root key generation
- Backup software and failover technology to ensure continuous operation
- Regular security audits to maintain compliance and avoid fines
- Dedicated PKI experts to oversee it all and whose salaries are much higher than entry-level administrators

> “Cloud-based PKI reduces total cost of ownership by eliminating hardware costs, root key generation, backup and failover software, audit expenses, and high salaries of dedicated PKI experts.”

A word of caution however. As you explore the ability to utilize digital identity with stronger forms of authentication between people, devices, and applications, remember that all cloud-based solutions are not alike. Support for multiple use cases, Zero Trust principles, IT customization, interoperability and crypto-agility – all in an environment built for usability – are just some of the capabilities that characterize leading-edge deployments that address current and future threats.

The Ultimate Level of Enterprise Security Control—Without the Hassle

As a trusted public Certificate Authority (CA) that offers decades of impenetrable trust, yet vanguard new digital identity solutions, Sectigo has you covered. We protect private roots at the same level applied to the hundreds of millions of public digital certificates we've issued worldwide. And with direct connections with the Certification Authority Browser Forum and select government entities, Sectigo receives early alerts on any PKI security concerns, including concerns inherent to the evolution of quantum computing. Our legacy and tradition ensure that enterprise security programs remain at the leading edge of cryptography as your needs change and grow, providing cryptographic agility to adjust to advances in computing and cryptographic techniques.

The Sectigo platform is purpose-built in the cloud for identity information and data protection to secure your web servers, mobile devices, IoT devices, DevOps environments, and applications. Single pane of glass management enables you to automate the installation and full lifecycle of public and private digital certificates and keys across servers, devices, users, applications, cloud key vaults, SSL, SSH, IoT and DevOps, with full reporting capabilities. The entire platform is WebTrust certified and SOC3 compliant and subject to rigorous external Ernst and Young audits.

Enhanced security, stringent dual controls for physical access, sophisticated hardware security module (HSM) management for hardware availability and disaster recovery, and dedicated security experts combine to provide best-in-class cloud protection for organizational preparedness and cyber resilience. The power of the Sectigo platform eliminates the chaos of manual control while providing the visibility needed for IT teams to maintain control of configuration definitions and rules so that automation steps are performed correctly.

We invite you to cut costs, save time, better utilize your resources, and reduce the risks of attacks with the enhanced security you can only access by leveraging the cloud-based security strength of a public CA.

About Sectigo

Sectigo is a global cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As a leading Certificate Authority (CA) with more than 700,000 customers and over 20 years of online trust experience, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions to secure web servers and user access, connected devices, and applications. Recognized for its award-winning innovations and best-in-class global customer support, Sectigo has the proven performance needed to secure today's digital landscape and tomorrow.