

Cyberark Zero Touch PKI

Eliminate costs and headaches with fast, easy modern SaaS PKI

DATA SHEET

Recent changes in technology and society have stressed the first-generation PKI (public key infrastructure) systems that maintain and distribute internal TLS certificates to their breaking points.

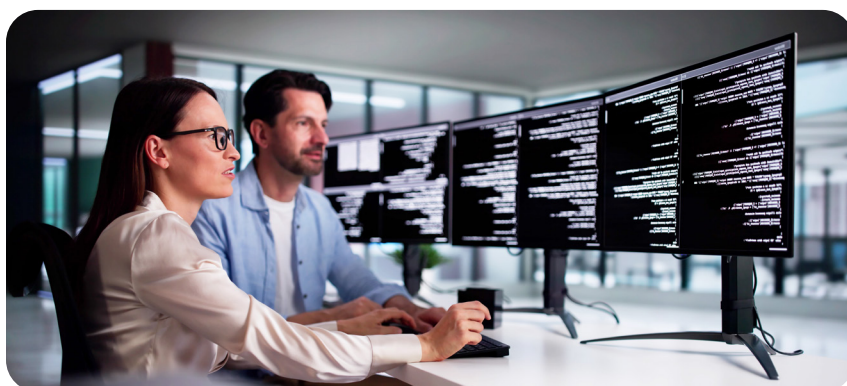
As a result, established PKIs are expiring when security teams are overburdened with more work than ever before. PKI software designed over 20 years ago is no longer able to keep up with modern requirements and costs too much.

Many PKI teams are already working with brittle, hard-to-maintain internal PKI systems that require constant care and immediate updates. Demands on PKIs have doubled or tripled, requiring even more attention from already strapped teams. In many cases, this has created a painful three-way collision: Internal teams have less time, but they are also responding to exponentially more requests that carry an even higher level of urgency.

CyberArk is the inventor and creator of the machine identity security category. With over 20 years of innovation in PKI, CyberArk is the trusted partner who delivers a state-of-the-art internal PKI service that's the most cost-effective. The power of CyberArk Zero Touch PKI meets the scalability and residency needs of businesses with global data center operations.

Challenges

PKI has always been hard. It's a complex system that demands a level of expertise that is difficult to find and retain, especially as the number of machine identities that organizations need to remain secure skyrockets. But recently, several emerging challenges have transformed what has been a difficult task into an almost impossible one.



ZERO TOUCH PKI AT A GLANCE

CyberArk Zero Touch PKI is the preferred modern, SaaS-based solution that breaks free from legacy cost and hassle of creating, issuing and maintaining privately trusted X.509 digital certificates for your network systems, devices and users.

- Delivers complete modern PKI with ready-made digital certificate issuing profiles for mobile and network devices
- Deploys flexible root and intermediate issuing CA hierarchies to fit business needs
- Autoenrollment and automated issuance for Microsoft desktops and laptops
- Rotate, replace or revoke any group of certificates in real time
- Includes instant scaling, hardware security module (HSM), 24x7 monitoring to protect your business

Maintaining your own private PKI is expensive and hard. Refreshing, or migrating to a new PKI requires expertise and knowledge you may not have. Zero Touch PKI frees your team to focus on the ever-increasing demands of machine identity security.

BENEFITS

- Simplify your private PKI through a hassle-free, SaaS-based service
- Replace brittle, outdated systems with modern, fast PKI architecture
- Focus scarce resources on high-benefit projects while CyberArk maintains your internal PKI

Updating Windows PKI. Many organizations have built their private PKI on Microsoft Active Directory Certificate Service (ADCS), the Windows server role that allows them to provide public key cryptography, digital certificates and digital signature capabilities to their organization. Now they find themselves unable to keep up with the steady stream of patches, updates, hot fixes and vulnerabilities Microsoft requires with AD and SQL Server. These Microsoft PKIs are expiring and must be refreshed on unforgiving deadlines.

Modernizing PKI. Many internal PKI systems were built on older processes and standards that are over 20 years old, but PKI requirements in these standards are evolving rapidly. As recently as September 2020, the multinational Internet Engineering Task Force (IETF) updated RFC-8894, the specification standard for Simple Certificate Enrollment Protocol (SCEP). In addition to SCEP, modern PKI solutions also support other enrollment standards such as Enrollment over Secure Transport (EST, RFC 9148) for more secure certificate provisioning and Automatic Certificate Management Environment (ACME, RFC 8555) for automating certificate issuance and renewal, ensuring seamless integration across diverse environments. For most organizations, keeping up with these new recommendations and best practices is arduous and time-consuming. Unfortunately, cybercriminals are increasingly targeting machine identities — so updates are no longer optional.

Moving PKI to the Cloud. Cloud platforms offer a similar set of benefits across many different technology areas: the ability to scale up and down rapidly as business demands change; manageable and forecastable costs; and the flexibility needed to rapidly support new initiatives. PKI is no exception. Real SaaS PKI provides both the ease and simplicity of a service and the agility required respond quickly to shifting business needs.

PKI at Enterprise Scale. Microservices architecture, containerization and DevOps toolchains all increase the number of TLS connections that need to be managed by an internal PKI. The deployment of millions of IoT devices has added many more. Using TLS to secure worker endpoints, mobile phones and network devices have added even more. Together, all these changes have dramatically increased the scale of challenges PKI teams must solve. PKI that was designed and deployed 10 years ago just can't keep up anymore. A new approach is needed.

Demonstrating Security, Proving Compliance. The list of regulatory standards, security frameworks and compliance mandates that verify the robustness and integrity of internal encryption processes continues to grow. PCI DSS, NIST and ISO all have added requirements for stronger cryptography and updated protocols in recent releases. In addition, industryspecific mandates, like NERC CIP requirements for energy providers and FFIEC for banking, are likely to respond to the increase in remote working with new machine-to-machinerequirements soon.

The Solution: Zero Touch PKI

The best way to take the pain and risk out of internal PKI is to hire experts to do the job for you. The CyberArk Zero Touch PKI solution is a robust, flexible and highly secure solution that addresses your pressing private PKI needs — while requiring almost no time or effort from your own InfoSec staff. It also does not require an army of consultants and a hefty services budget.

Powerful PKI SaaS. CyberArk Zero Touch PKI is a SaaS-based service with effortless onboarding provided by CyberArk experts. Your modern PKI is built to your specifications, leveraging the CAs, roots and intermediaries needed by your business. Each customized PKI is designed with current best practices for design, deployment and security in mind, ensuring your PKI leverages the latest capabilities and protocols. Your team has complete REST-API, standard protocols and GUI-based access to Zero Touch PKI. But unlike your old PKI and other approaches, you do not need to set up your own servers, configure requests, validate functions, upgrade databases and monitor connections or set up HSMs and other key management systems.

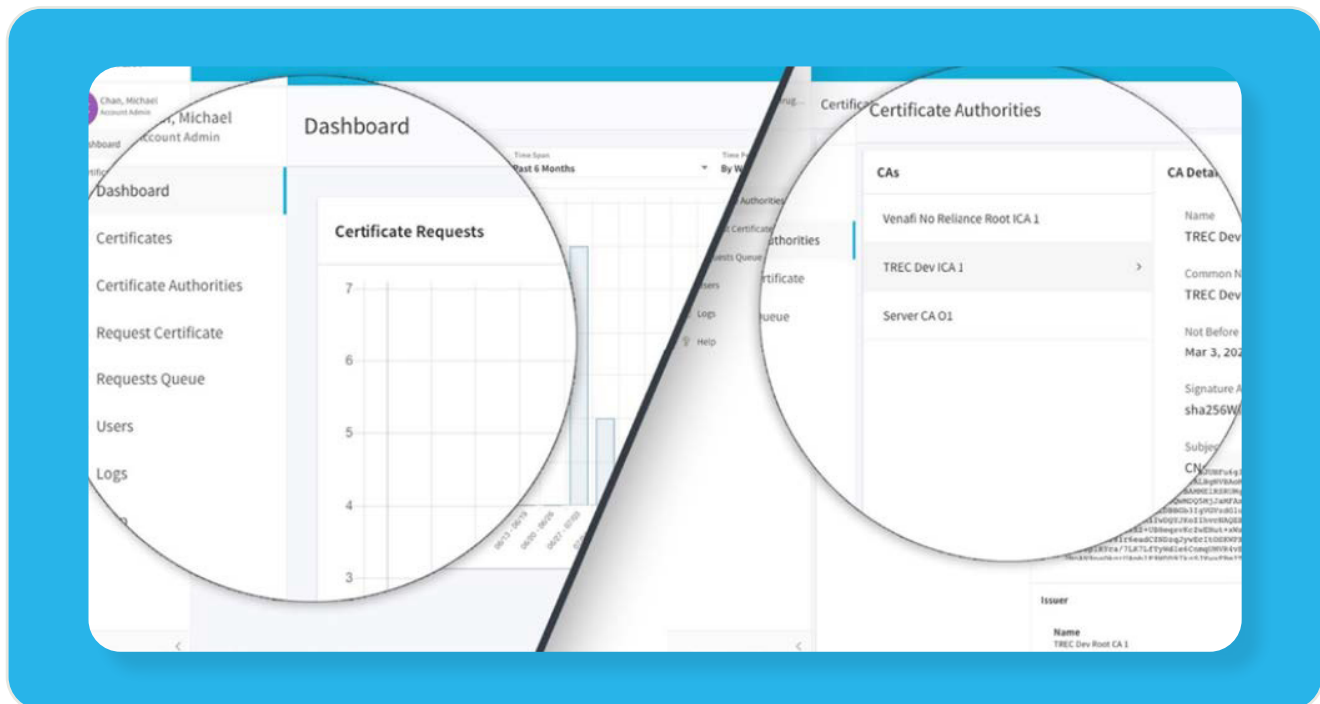
CyberArk Zero Touch PKI gives your business a modern, powerful PKI service, offering the agility and speed you need to succeed today while preparing to meet tomorrow's machine identity security challenges. Designed for cloud-native security, Zero Touch PKI automates certificate issuance for microservices, Kubernetes, and DevOps pipelines via REST API, ACME, and EST.

Security Controls and Best Practices Built-In. Industry best practices for PKI and Trust infrastructure are constantly evolving. Every CyberArk Zero Touch PKI is implemented with modern best practices for security and control including HSMs, 24x7 monitoring and full redundancy. Nothing extra. And there is nothing extra to learn, manage and maintain.

Ready-Made Certificate Issuing Profiles. Certificate issuing profiles are critical tools that can make or break your private PKI. These profiles configure the content for TLS certificates, establish security constraints, and define input and output forms for certificate enrollment. CyberArk Zero Touch PKI includes profiles for cloud-native processes as well as for mobile, telephony and network devices. These templates dramatically simplify your private PKI solution without sacrificing security or functionality.

Auto-Enrollment Ready. In today's threat landscape, all systems are critical systems, not just web servers and app servers. Microsoft Active Directory Certificate Service (ADCS) allows Microsoft servers and devices in your organization to automatically enroll for TLS certificate coverage. Auto-enrollment automates a labor-intensive process, and by integrating with it, CyberArk Zero Touch PKI makes sure the largest portion of your IT estate does not go without the protection TLS certificates provide.

Instant Integration with CyberArk. CyberArk customers rely on visibility, intelligence, and automation for TLS certificates all the way down to specific hardware, application, and workload levels. CyberArk Zero Touch PKI comes with out-of-the-box integration, providing an end-to-end solution that automates the machine identities your business relies on.



How It Works

CyberArk Zero Touch PKI is the modern SaaS service that frees teams from legacy PKI software and approaches. CyberArk brings the deepest experience in PKI best practices to set up and run Zero Touch PKI without you needing PKI experts or PKI consultants. And CyberArk delivers world-class availability and scalability that only true SaaS can deliver.

Zero Touch PKI

PKI Features	• Flexible root and intermediate CA hierarchy configuration • RSA and ECDSA CA and certificate issuance • Offline root key custody management • Management of online issuing CA(s) signing, operations and documentation • Offline and online key material BCP and disaster recovery process • Management of all certificate validation processes, including HA implementation and highly scalable OCSP responders and CRL servers • HSM operations and HA model for continuous operations • Web-based certificate management portal • Ongoing secure operations of all online issuing CAs in FIPS 140-2 level 3 hardware • Automation for MS autoenrollment and other standards-based certificate management protocols such as SCEP, EST and ACME, as well as API support • Design and implementation of private trust hierarchy architecture(s) • Turnkey root key generation ceremony processes and documentation
Service and Support Features	• Guidance and support for current PKI migration to CyberArk Zero Touch PKI as well as guidance and recommendations for migration of CA key material obtained in acquisitions • Instant scalability and geographic redundancy without extra configuration or setup • 99.9% availability and uptime SLA with 100% historical uptime over multiple years • U.S. and European operations • 24x7x365 availability, support, security monitoring
Integrations and Services	• Mobile Device Management: Microsoft Intune, Workspace ONE by VMWare, MobileIron, Citrix XenMobile, Jamf Now, Jamf Pro and more • Microsoft Auto-Enrollment: Windows desktops, servers and laptops • Network and IoT Enrollment: SCEP (Simple Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport) • Applications and Developers: ACME2 for cert-bot and more integrations; complete REST API

Next Steps

Does your organization need to replace outdated systems, expand your PKI to meet new security needs or support new sites and services for remote workers? CyberArk Zero Touch PKI can help. Get a consultation with a PKI expert or visit <https://www.cyberark.com/try-buy/zero-touch-pki-consultation/>



© Copyright 2025 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. U.S., 11.24