SECTIGO®

An Introduction to Private PKI

Table of contents

Introduction: The case for private PKI

The rising complexity of modern networks

As businesses embrace digital transformation, their internal networks are becoming increasingly complex. Modern IT ecosystems now span on-premises data centers, cloud services, and edge devices, creating a vast landscape where secure communication is paramount. The need to authenticate systems, protect data in transit, and verify identities is a cornerstone of security. Yet, many organizations struggle to keep up with the growing number of endpoints, applications, and services that require digital certificates for encryption and authentication.

The role of PKI in a connected world

Public Key Infrastructure (PKI) provides the cryptographic foundation for trusted communication across networks. It enables the issuance and management of digital certificates, ensuring confidentiality, integrity, and authenticity in digital transactions. By establishing trust through cryptographic keys and certificates, PKI addresses critical challenges such as secure communication, user and device authentication, and compliance with regulatory requirements.

Why private CAs matter

While public Certificate Authorities (CAs) play a vital role in securing internet-facing applications, they fall short when it comes to internal operations and specific organizational needs. Private CAs offer a tailored solution, enabling organizations to issue, manage, and revoke digital certificates internally. This approach allows businesses to enforce strict security policies and ensure that only authorized devices and users can access critical resources.

Private PKI provides the backbone for secure authentication, encryption, and integrity within an organization. Certificates issued by a private CA can authenticate users, devices, and applications, secure data in transit, and establish trust across internal systems. This level of control is crucial for organizations managing sensitive operations, where public CAs may not offer the flexibility or specificity required.

Overcoming the challenges of private CA management

Despite their advantages, many organizations grapple with the complexity and management overhead associated with private CAs. Transitioning from legacy systems such as Microsoft Active Directory Certificate Services (AD CS) can add to the challenge. However, by understanding the role of private CAs, assessing organizational needs, and selecting the right solution, organizations and businesses can overcome these obstacles. This approach not only enhances security but also builds a scalable, compliant, and resilient digital infrastructure.

Additionally, the proliferation of digital certificates compounds the challenges businesses face. Certificates must be issued, tracked, renewed, and revoked, often across siloed teams and tools. Without a cohesive strategy, organizations risk operational inefficiencies, compliance gaps, and vulnerabilities like expired certificates that can disrupt critical services.

Chapter 1: Fundamentals of PKI

Safeguarding each organization’s internal operations is not just a necessity - it’s a strategy for survival. Private CAs are a secret weapon in this battle, providing the security and control needed to protect communications, authenticate devices, and ensure that every application runs as intended.

Public vs. Private CAs

Public CAs are widely used for securing external resources, but private CAs are essential for managing certificates tailored for internal use. They provide granular control over certificate policies and lifecycle management, aligning directly with an organization's specific security requirements. As cybersecurity challenges evolve, private CAs help organizations bridge the gap between external-facing services and internal operations, ensuring only authorized users and devices have access to sensitive resources.

Public CAs are trusted globally and issue certificates for external-facing services such as websites, emails, and applications accessible to the general internet.

Private CAs manage certificates for internal resources, offering tailored security for networks, applications, and systems that do not require or benefit from external validation.

The business impact of private CAs

Private CAs have a far-reaching impact on organizational operations, and this influence extends across critical areas, driving both operational resilience and strategic outcomes.

Enhanced security:

Direct management of certificate issuance and lifecycle allows you to mitigate risks associated with expired or misconfigured certificates, ensuring continuous protection for your systems.

Operational efficiency:

Automating the issuance and renewal of certificates streamlines operations, cuts down on manual tasks, and reduces human error, thereby enhancing the overall efficiency of your IT operations.

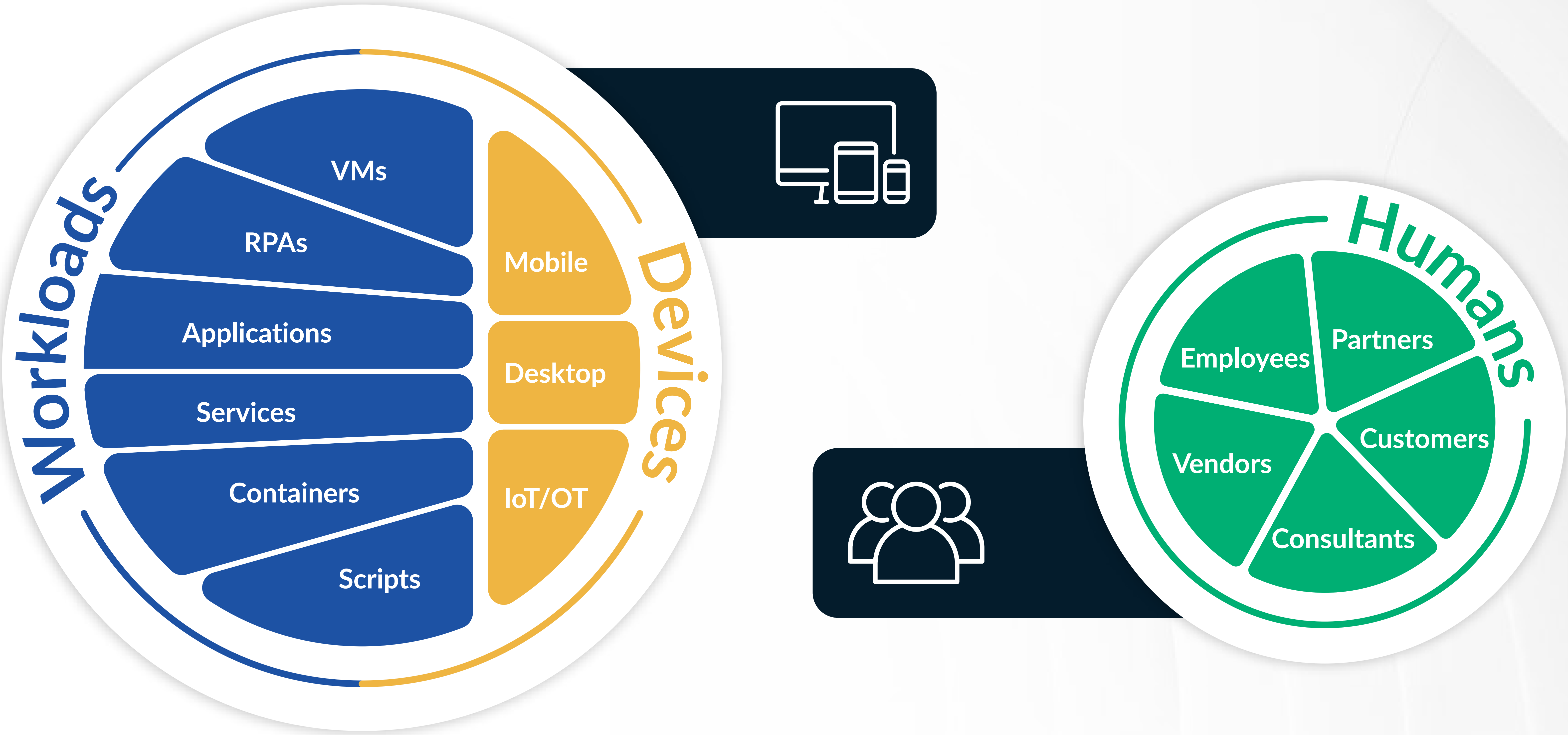
Regulatory compliance:

Many sectors face stringent compliance demands that dictate rigorous data security measures. Private CAs enable you to customize and control how certificates are managed, helping you meet these regulatory requirements more effectively.

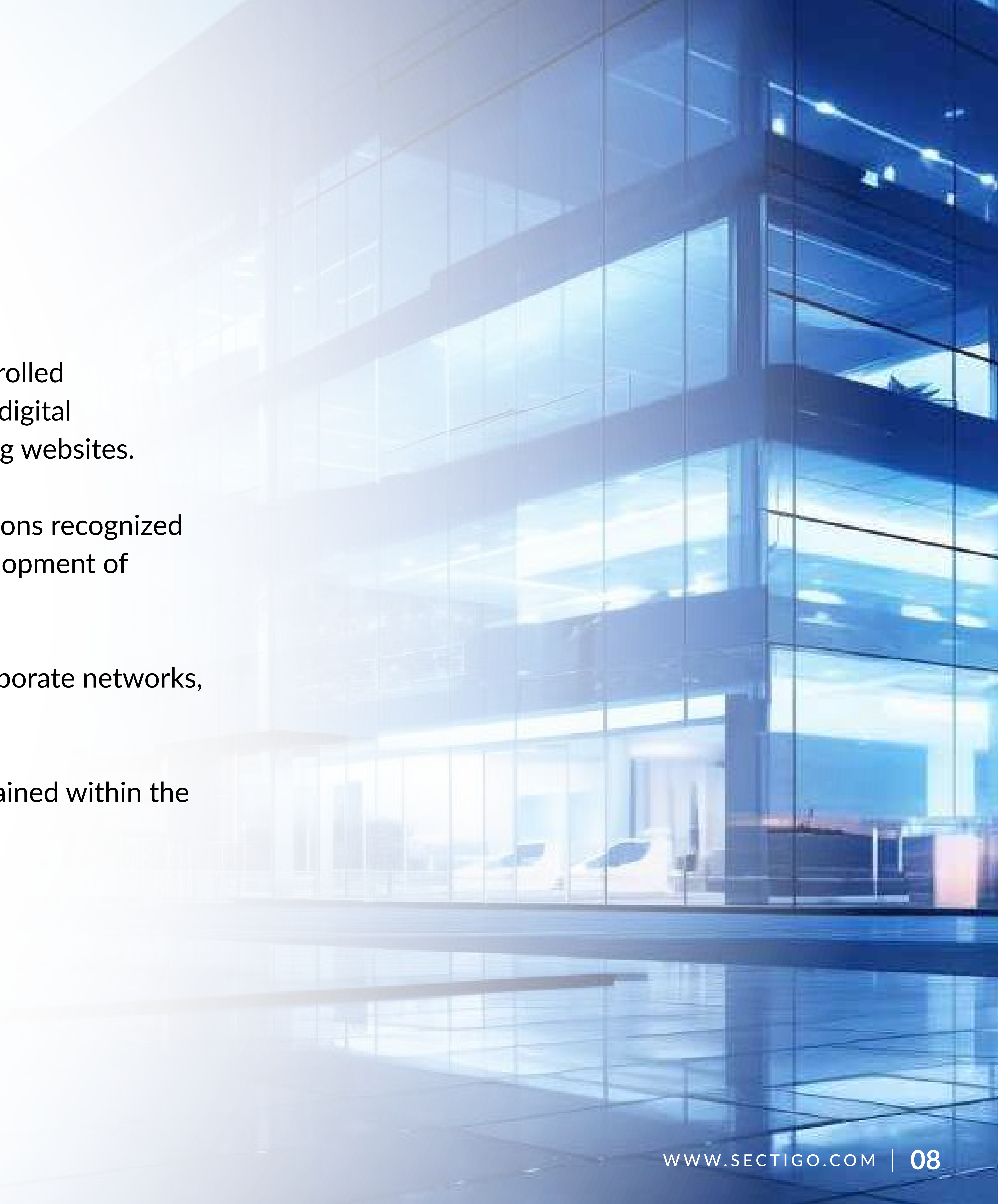
Managing and securing human and machine identities

The interaction between human, device and workload identities underpins digital operations in modern organizations. Ensuring the integrity and trust of internal systems requires robust authentication and secure communication, which PKI, supported by private CAs, provides as the foundation of this security framework. By managing certificates across these diverse identity types, PKI creates a unified and scalable solution.

Private CAs play a key role by issuing and managing certificates to authenticate users, validate workloads, and secure device communication. Integrated seamlessly with organizational systems, they ensure trusted entities access critical resources while keeping data exchanges secure. This framework supports scalable identity management and safeguards the integrity of interactions across the organization.



Chapter 2: The history of Private CAs



The evolution of private CAs began as a response to the growing need for secure, controlled internal communications and operations within organizations. During the early days of digital technologies, public CAs primarily supported external communications, such as securing websites.

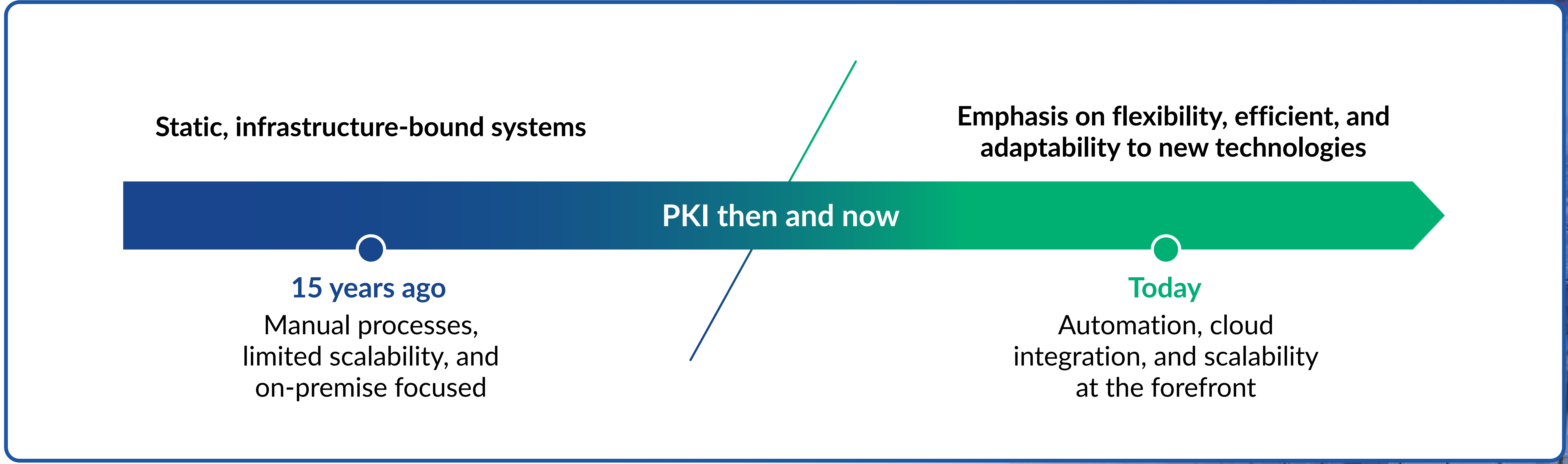
However, as enterprises expanded and internal systems grew more complex, organizations recognized the need for internal trust frameworks independent of public CAs. This led to the development of Private CAs, allowing organizations to issue, manage, and revoke certificates internally.

Early use cases included securing internal email systems, authenticating devices on corporate networks, and protecting client-server communications in custom applications.

These systems provided tailored security solutions, ensuring sensitive information remained within the organization's control.

Modern private CAs: Not your grandfather’s PKI

Today’s private CAs represent the culmination of this evolution. These systems offer high scalability, flexibility, and seamless integration with other security frameworks. They automate the entire lifecycle of certificates - from issuance to renewal and revocation - reducing administrative overhead and bolstering security. Additionally, modern private CAs are highly customizable, enabling organizations to tailor security settings to meet specific operational and security needs.



PKI then and now

Static, infrastructure-bound systems

15 years ago

Manual processes, limited scalability, and on-premise focused

Emphasis on flexibility, efficient, and adaptability to new technologies

Today

Automation, cloud integration, and scalability at the forefront

Chapter 3: Use cases of private PKI

In a world where digital threats lurk at every corner, safeguarding your organization’s internal operations is not just a necessity—it’s a strategy for survival. Private Certificate Authorities (CAs) are your secret weapons in this battle, providing the security and control needed to protect your communications, authenticate your devices, and ensure that every application runs as intended. With Private CAs, you wield the power to fortify your network, shield your data, and stay two steps ahead of potential security breaches. Let's explore how deploying Private CAs can turn your security measures from a routine protocol into a dynamic shield that guards the lifeblood of your organization.

User authentication and access control

User authentication and access control play a critical role in modern digital security by leveraging Private PKI to issue certificates tied to user identities, ensuring that only authorized individuals gain access to sensitive systems. Integrated with identity providers (IdPs) like Microsoft Active Directory, Okta, or Ping Identity, PKI supports certificate-based authentication for single sign-on (SSO) strategies, enabling seamless yet secure access. It enhances security further through multi-factor authentication (MFA), combining certificates with tokens or biometrics, and privileged access management (PAM), which uses certificates to authenticate high-privilege accounts with traceability. Network access control (NAC) solutions like Cisco ISE and Aruba ClearPass rely on PKI to verify users before granting access, while automation protocols like SCEP, EST, OAuth, and OpenID Connect streamline certificate issuance and federated identity management across devices and systems.

Leading technologies:

- Microsoft Active Directory Certificate Services (AD CS)
- Okta Identity Cloud
- Cisco Identity Services Engine (ISE)
- Aruba ClearPass Policy Manager

Device authentication

Device authentication ensures robust security by leveraging Private PKI to issue certificates to laptops, mobile phones, IoT sensors, and servers, allowing only trusted devices to access the network. This approach strengthens IoT and endpoint security, supporting zero-trust architecture where every device must validate its identity before gaining access. PKI also secures machine-to-machine (M2M) communication, ensuring data integrity and confidentiality. Unified Endpoint Management (UEM) tools like Microsoft Intune, VMware Workspace ONE, SOTI, and Jamf facilitate PKI certificate management for enrolled devices, while IoT gateways use PKI to authenticate edge devices and ensure secure communication with central systems. Authentication protocols such as 802.1X and EAP-TLS, and automation protocols such as ACME, SCEP, and EST streamline certificate issuance for network access and lifecycle management, bolstering device security across diverse environments.

Leading technologies:

- Microsoft Intune and Azure IoT Hub
- VMware Workspace ONE for device management
- JAMF
- AWS IoT Core for secure IoT operations
- Palo Alto Networks for secure VPN communication

Secure web applications

Secure Web Applications benefit from robust data protection and secure communication through Private PKI, which encrypts sensitive information both in transit and at rest. It safeguards data across internal and external systems, ensuring only authorized access. With PKI-issued certificates, you can enable encryption to prevent unauthorized access, while TLS/SSL certificates secure internal web applications, APIs, and services. PKI also strengthens VPN authentication by verifying users and devices for secure remote access. It extends protection to database security, encrypting communications between databases and applications. Leveraging automation protocols like ACME simplifies TLS/SSL certificate management, while configuration management tools such as Ansible, Terraform, and Puppet seamlessly integrate PKI into system setups, enhancing encryption and security across the organizational ecosystem.

Leading technologies:

- Apache and NGINX for web server security

Code signing

Code signing ensures that applications, scripts, and updates originate from a trusted source and remain untampered, safeguarding software integrity. By signing software artifacts, organizations can verify their authenticity and protect against malicious alterations. It can seamlessly integrate with CI/CD tools like Jenkins, GitHub Actions, and GitLab to streamline secure development workflows. Signing tools such as Microsoft SignTool, OpenSSL, and Java Keytool facilitate the code-signing process, while PKCS standards, including PKCS #7 and #12, support the signing and distribution of verified code. This comprehensive approach bolsters trust and security in software development and deployment.

Leading technologies:

- Microsoft SignTool for Windows application signing
- Docker Content Trust for securing container images
- Jenkins for PKI-integrated CI/CD

Document signing

Private document signing with PKI ensures the integrity and authenticity of contracts, approvals, and other sensitive documents, providing a secure foundation for trust and accountability. Unlike public document signing certificates commonly associated with Adobe Document Signing, private certificates are versatile and can be used to sign any document, regardless of platform. By digitally signing documents, organizations enhance security, prevent unauthorized alterations, and streamline workflows with automated approvals. PKI integrates seamlessly with tools like Adobe Acrobat, DocuSign, and HelloSign, as well as document management systems such as SharePoint and Alfresco, making it an essential component of secure and efficient document management.

Leading technologies:

- Adobe Acrobat for secure document workflow
- Microsoft SharePoint for internal document collaboration
- DocuSign for enterprise signing solutions

Compliance and governance

Compliance and governance are supported through the use of Private PKI, which enables organizations to meet regulations such as GDPR, HIPAA, and PCI DSS by enhancing security and traceability for sensitive operations. Certificates provide detailed auditing and logging, ensuring actions and access can be tracked to meet regulatory requirements. Managing PKI infrastructure internally helps maintain data sovereignty by retaining control over cryptographic keys and certificates to comply with local or industry-specific rules. PKI integrates with SIEM tools like Splunk or Azure Sentinel for audit logs and enforces policies like certificate expiration and automated revocation.

Leading technologies:

- Splunk and Azure Sentinel for monitoring PKI usage
- Microsoft Certificate Lifecycle Manager for compliance workflows
- IBM QRadar for SIEM integration

Security for emerging technologies

Security for emerging technologies is ensured through Private PKI, which plays a pivotal role in securing innovations like IoT, edge computing, and AI by providing robust authentication and encryption mechanisms. It ensures trusted interactions and data integrity as these technologies evolve, requiring scalable and automated PKI systems for security and reliability. PKI authenticates IoT devices, secures distributed edge nodes, and protects AI models and datasets through certificates for mutual authentication and encrypted communication. Blockchain environments leverage PKI for securing identities and transactions. Technical implementations, such as MQTT over TLS for IoT, over-the-air updates for firmware, and secure boot protocols for embedded systems, underline PKI's critical role in enabling secure innovation in new and complex technology landscapes.

Leading technologies:

- AWS IoT Core and Azure IoT Hub for IoT device management and PKI integration
- NVIDIA AI platforms for securing AI model exchange
- Hyperledger Fabric for blockchain identity and transaction security

Chapter 4: Choosing your path

Choosing between on-premise and cloud-based PKI is a critical decision for businesses, as it directly impacts security, scalability, and operational efficiency. The right approach ensures seamless management of certificates while aligning with an organization's specific infrastructure needs and security goals. This decision ultimately influences how effectively a private CA supports the organization’s broader digital ecosystem, enabling secure and agile operations.

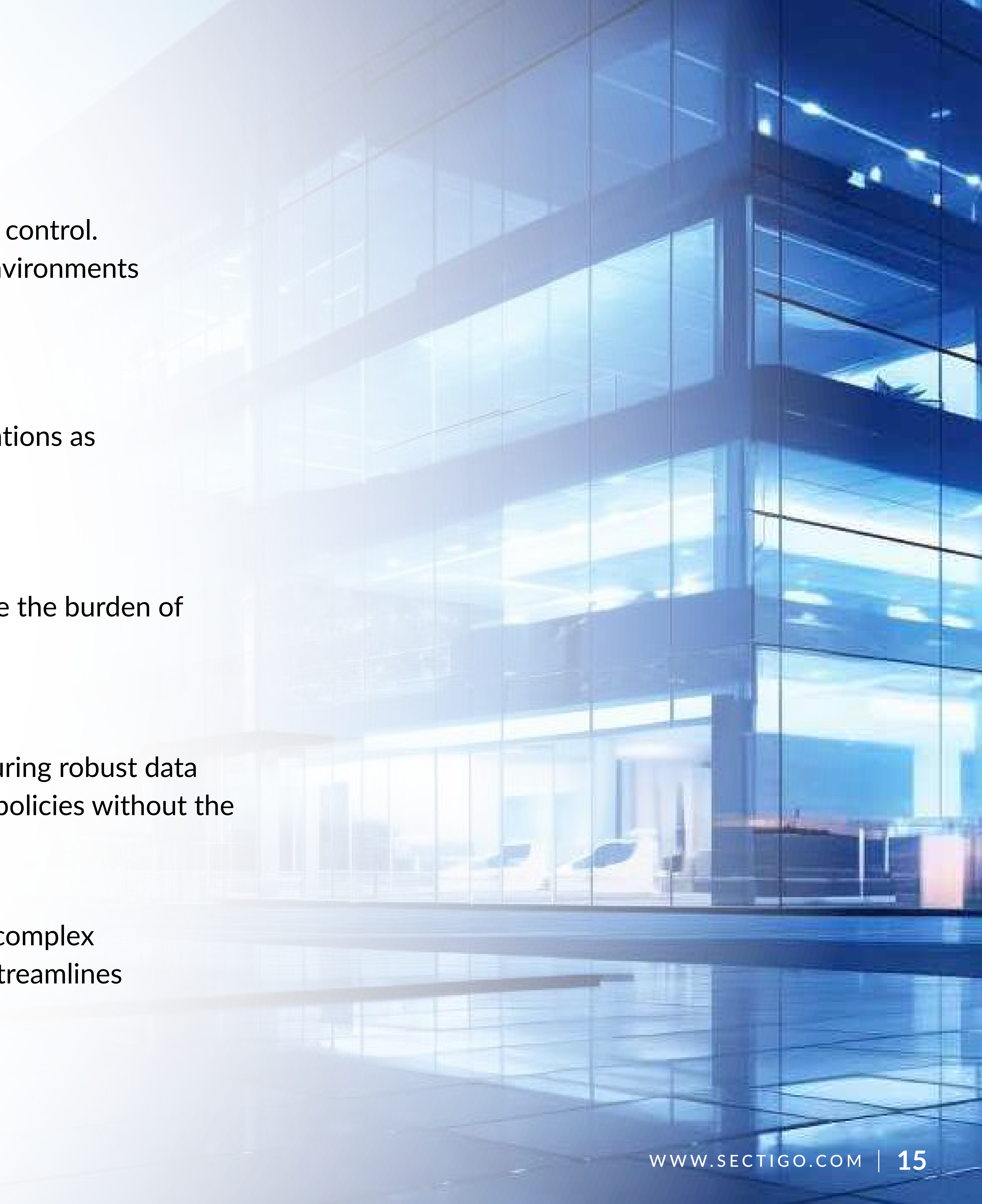
On-premise

On-premise PKI refers to a private, internal infrastructure where organizations manage their own CA and control every aspect of the certificate lifecycle, from issuance to revocation. This approach provides a high level of control and customization, ensuring strict adherence to security policies. However, it often requires significant resources in terms of hardware, maintenance, and management, which can be complex and extremely time-consuming and costly for large-scale deployments.

Cloud PKI

Cloud-based PKI, on the other hand, offers a more flexible and scalable approach to managing certificates. With cloud-based private CAs, organizations can leverage the infrastructure of trusted cloud service providers, eliminating the need for maintaining physical servers or internal hardware. This allows for seamless scalability, rapid deployment, and reduced operational overhead.

Making the right choice for your organization



Ease of management

Cloud PKI simplifies certificate management through automation and centralized control. Organizations can quickly issue, renew, and revoke certificates across multiple environments (e.g., hybrid cloud, multi-cloud).

Scalability

Cloud-based solutions scale dynamically with your needs, ensuring smooth operations as organizations grow or experience peak demand.

Reduced maintenance

By outsourcing infrastructure management to a cloud provider, businesses reduce the burden of hardware maintenance, software updates, and security patches.

Security and compliance

Cloud PKI leverages the latest security practices from established providers, ensuring robust data protection and regulatory compliance. Additionally, organizations can customize policies without the overhead of managing physical systems.

Cloud-based PKI is particularly beneficial for businesses with distributed workforces or complex environments that require flexibility, security, and ease of management. This approach streamlines certificate management while maintaining a high level of trust and control.

Chapter 5: Implementing private CAs effectively

Implementing private CAs is a key component in strengthening an organization's security posture. Whether establishing a new Private CA or transitioning from existing systems like Microsoft Active Directory Certificate Services, a strategic approach ensures smooth integration, efficiency, and comprehensive security. A well-designed private CA infrastructure should be scalable, capable of accommodating new devices, applications, and services as they evolve. By maintaining flexibility in managing various types of certificates, organizations can adapt their security strategies to meet the dynamic demands of both current operations and future growth, ensuring a responsive and agile security framework.

> **A thoughtfully implemented private CA becomes the foundation for a secure, scalable, and adaptable security ecosystem.**

Strategic deployment of private CAs

Integrating a private CA into your IT ecosystem requires thoughtful planning and execution. Organizations should begin by evaluating current security frameworks and identifying areas where a private CA can provide significant value - such as securing internal networks, specific device classes, or proprietary applications. Developing a phased deployment plan is encouraged as it allows for a gradual transition with minimal disruption to daily operations.

Navigating the Implementation Process

Setting up a private CA provides significant security benefits and can be a smooth process with thoughtful planning. Establishing a reliable and scalable infrastructure involves configuring systems that support future growth, and while this requires attention to detail, a well-structured approach helps streamline the process. Focusing on scalability early on ensures optimal performance as organizational needs expand.

Automation plays an important role in simplifying workflows for certificate issuance, renewal, and revocation, helping to reduce manual tasks and improve efficiency. Integrating with existing systems, including both legacy and cloud-based platforms, is achievable with careful planning and thorough testing to ensure seamless compatibility. Organizations can also benefit from leveraging internal expertise or working with experienced vendors to facilitate setup and ongoing management.

Finally, ensuring compliance with industry standards and regulatory requirements is key to maintaining security and alignment with best practices. By proactively addressing these considerations, organizations can establish a secure, efficient, and scalable private CA that supports their long-term goals with confidence.

Certificate management best practices

Effective management of certificate lifecycles is fundamental to maintaining a secure private CA environment. Automation plays a key role in simplifying certificate issuance, renewal, and revocation, reducing the risk of manual errors. Additionally, using a robust Certificate Lifecycle Management (CLM) solution ensures compliance with industry standards, scalability for future growth, and enhances overall digital trust. Establishing well-defined policies that align with your organization's security protocols ensures a streamlined and consistent approach to managing certificates.

Conclusion: Building a secure foundation with private CAs

A comprehensive understanding of private CAs empowers organizations to design and implement security frameworks that are resilient, scalable, and adaptable to future demands.

By evaluating unique security needs, identifying gaps in existing infrastructure, and selecting a private CA solution that aligns with both current operations and future growth trajectories, enterprises can establish a robust foundation for digital trust.

This process not only enhances the organization's immediate security posture but also positions it as a forward-thinking leader in digital asset protection.

The strategies and insights detailed throughout this guide serve as a roadmap for fortifying internal systems and ensuring sustained security in an ever-evolving technological environment.

What to consider when implementing a private CA

When selecting and deploying a private CA, organizations should focus on solutions that address their specific operational and security requirements while providing the flexibility to grow with technological advancements. Ease of integration with existing systems, robust automation capabilities to manage certificate lifecycles, and scalability to accommodate expanding infrastructure are critical factors.

Compliance support to meet industry standards and proactive vendor support for seamless implementation and ongoing management are equally essential. Additionally, organizations should prioritize solutions that offer strong interoperability, ensuring that the private CA can operate effectively in hybrid, cloud-native, or traditional on-premise environments.

The future of Private PKI

As technology evolves, private PKI is poised to adapt and grow, offering new possibilities for securing enterprise systems. Key trends shaping its future include:

Increased automation

Greater reliance on automation to handle certificate lifecycles, reduce human intervention, and enhance scalability.

Integration with cloud-native technologies

Enhanced support for containerized environments, microservices, and hybrid cloud setups.

Quantum-resistant cryptography

Preparation for the advent of quantum computing by adopting quantum-resistant algorithms.

PKI as a service (PKIaaS)

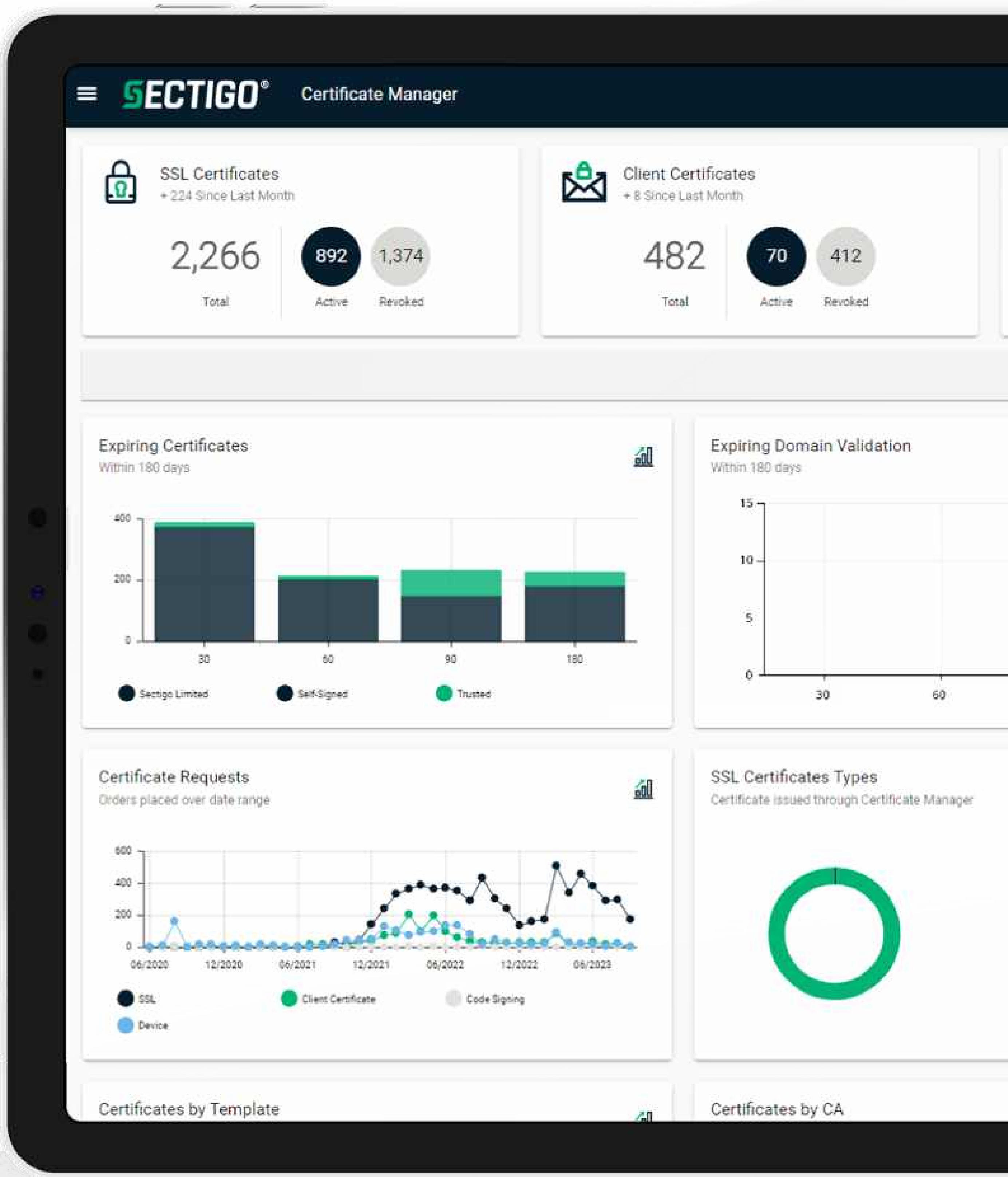
Growing demand for managed PKI solutions that offer flexibility, speed, and reduced overhead.

Decentralized identity systems

Using PKI to enable decentralized, user-controlled identities, particularly in blockchain and Web3 ecosystems.

Organizations will need to keep ahead of these developments and not only prepare for changes to technologies, but embrace these emerging technologies, as private CAs will continue to be essential in enabling secure and trusted digital interactions. They will not only address today's security challenges but also provide a foundation for tackling the unknown threats of tomorrow.

With the right tools, a clear roadmap, and a commitment to innovation, enterprises can confidently build a resilient security framework, ensuring that their digital assets remain protected in an increasingly complex digital landscape.



About SECTIGO®

Sectigo is a leader in certificate lifecycle management (CLM), providing innovative and comprehensive solutions to secure both human and machine identities for some of the world's most prominent brands. Its cloud-native, automated, and universal CLM platform simplifies and enhances enterprise security by issuing and managing digital certificates from all trusted certificate authorities (CAs). With over two decades of experience, Sectigo stands as one of the largest and most established CAs, serving more than 700,000 customers worldwide.

By delivering unparalleled digital trust, Sectigo continues to empower organizations to implement robust security protocols with efficiency and confidence.

Get in Touch