appviewx

APPVIEWX.COM

The CISO's Guide to Machine Identity Management

Contents

01

Introduction

The digital tipping point

> The knock-on effect of a data breach can be devastating for a company. When customers start taking their business - and their money - elsewhere, that can be a real body blow.
>
> - Christopher Graham

According to the Clark School study at the University of Maryland, "A hacker attack happens every 39 seconds."

The enterprise IT landscape is experiencing phenomenal disruption. Digital transformation, cloud migration, and the work from anywhere model are opening up a world of possibilities for organizations, pushing them to reinvent core business models and unlock new revenue streams. From BFSI to healthcare to energy and utilities—all industries are now catching up to digital transformation and embracing workplace modernization with a renewed sense of urgency.

On the other hand, these sweeping changes are permanently resetting the rules of the cybersecurity game. The attack landscape is responding to these changes with increased frequency and sophistication. From SolarWinds to the recent Colonial Pipeline attack, it has been raining cyberattacks, making it increasingly clear that no industry is insulated from the risk of cybercrime.

In the wake of rampant cyberattacks, data privacy regulatory bodies such as GDPR (EU General Data Protection Regulation) and CCPA (California Consumer Privacy Act) are also tightening the noose by continuously amending and updating the existing regulations. Biden's recent cybersecurity executive order, the latest in a slew of regulatory changes, called for strong measures in modernizing federal cybersecurity systems to fight modern threats.

This new reality, although daunting, has provided CISOs with an opportunity to reinvent security for the digital and turn it into an enabler of digital transformation and a champion for business growth.

Machine identity management - A better way to build digital trust

As organizations evaluate new and alternative approaches to securing a growing, cloud-driven, distributed environment, machine identity management has emerged as a top priority. Digitization proliferating deeply has led to massive growth in the number of physical machines and digital assets, opening up a huge attack surface. Securing these distributed assets and their communication is critical for data security. However, with network perimeter fast disappearing, digital security has become a significant challenge for organizations. This has led to security leaders recognizing the importance of machine identity management.

Through strong authentication and authorization mechanisms, machine identities help verify all devices, applications, and workloads regardless of where they are, ensuring secure machine-to-machine communication. In doing so, they help build a cybersecurity model that is multi-layered, transparent, location-independent, and, more importantly, based on zero-trust, the bedrock of digital security.

> "As the number of devices increases — and continues to grow — establishing an enterprise-wide strategy for managing machine identities, certificates and secrets will enable the organization to better secure digital transformation."
>
> **Gartner Top Security and Risk Trends for 2021**

The key question is - how do you build a strong machine identity management system? Well, it isn't necessarily complex unless you pick the key pieces, understand the challenges that come in the way of piecing them together, and choose the right approach to resolving them.

This guide is designed to provide CISOs with an insight into three of the key pieces of machine identity management and the role automation plays in an organization's cybersecurity strategy.

- Simplifying certificate ownership and approval for efficient certificate management
- Seamless integration of certificate management with other enterprise solutions
- Real-time discovery, visibility and monitoring of certificates

Simplifying certificate ownership and approval for efficient certificate management

One of the crucial aspects of certificate lifecycle management is delegating the management responsibility of certificates and keys, in other words, assigning certificate owners and approvers. The underlying intent of establishing an ownership and approval process is to ensure that only authorized personnel are allowed to make changes to the certificate infrastructure. This process eliminates the existence of undocumented or unapproved certificates with weak security standards, thereby mitigating the risk of a data breach.

Properly assigning certificate owners and escalations, designing an approval workflow, and creating a simplified certificate enrollment process are pivotal to successfully implementing a standardized certificate management system.

However, organizations employing manual processes store certificate ownership information in excel spreadsheets and databases along with other certificates and key-related information. These cursory approaches make establishing ownership and enforcing accountability for certificate actions a significant challenge. As the organization's digital footprint increases, the number of digital certificates to be managed can run into thousands. Manually tracking assigned owners and approvers for thousands of interlinked certificates via spreadsheets becomes plain unreasonable and, not to mention, highly error-prone.

Here’s how certificate ownership dilemmas can kill your security posture and affect your bottom line revenue

- In a typical enterprise public key infrastructure (PKI) setup, there are many stakeholders involved in the development, deployment, and management of a single application. Based on the different stages of the application lifecycle, multiple certificate groups are created and allowed to manage certificates independently. When multiple stakeholders are involved, poor collaboration and ambiguous ownership mapping lead to unknown or undocumented certificates being provisioned.

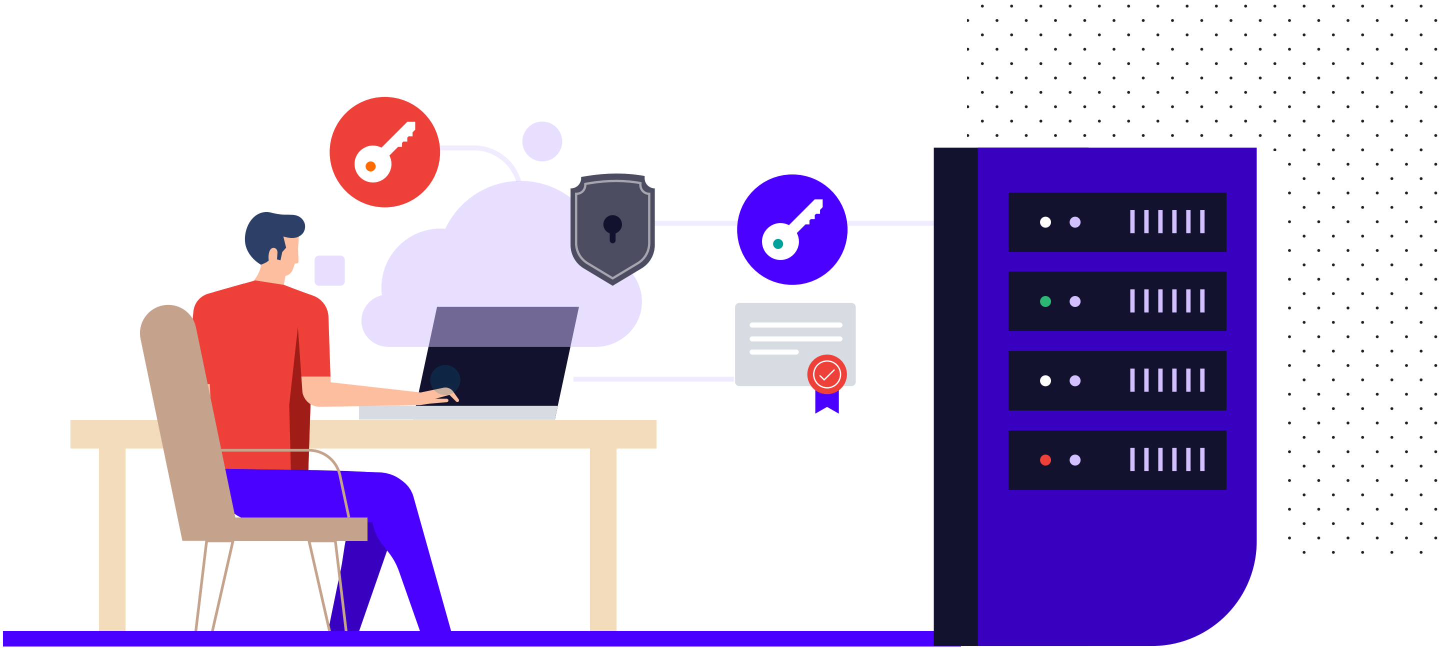
  When working with manual processes, tracking and monitoring these multiple groups and their actions becomes a huge challenge. The inability to regulate the access and prevent unauthorized actions inadvertently creates auditing issues, certificate expirations, outages, and security vulnerabilities.

- Digital certificates must be continuously monitored for renewals to avoid expiry and application outages. In a manual management premise, when a certificate is due for renewal, renewal requests are raised via email, and more often than not, these requests are buried among other service inquiries in an owner’s inbox. Missed requests often lead to certificate expiry and result in unnecessary outages that not only impact business revenue but leave the security door ajar for bad actors.

  In the event of a certificate owner changing position or quitting the company, certificate ownership is not updated and left to linger in ambiguity. When this orphaned certificate expires or is compromised, certificate teams struggle to ascertain the rightful owner to initiate renewals and revocations. Not having this critical piece of information delays incident response, risks data exposure and leads to unplanned application downtime.

  Another reason for worry is change in root ownership. Change in root ownership happens when one company sells off its CA division to another company, mostly due to a shift in focus. The impact is relatively less for CAs with root and intermediate certificates already available in the trust stores. But, for enterprises with pinned intermediate or root certificates, there’ll be huge service disruptions due to certificate trust. There’ll be an even higher impact for CAs that’ve spun off as a separate entity and are trying to change the root CA abruptly. Apart from just certificate expiries, enterprises using certificates from deprecated roots or intermediates can also suffer severe disruptions.

How should you respond?



- Assess the certificates within the discovered inventory. Group and prioritize them according to the organization's requirements. For example, replace weak certificates on mission-critical and public-facing applications before updating certificates on internal servers.

- Establish well-defined roles in the PKI management team with an ownership hierarchy. Each level in the hierarchy should be a part of an approval chain that allows the delegation and validation of ownership.

  Develop a management process that helps enforce role-based access control. For example, a super administrator will be able to request, enroll, and push certificates to their endpoints, while an administrator will only be able to request certificates – they would have to require the super admin's approval before taking any further actions on it. Restricting the level of access for users and groups based on requirements helps prevent unauthorized certificate actions, bolstering the security posture.

- Enforce strict policies for use and generation of certificates and keys - such as recommended cryptographic techniques, hashing algorithms, key lengths, CAs, and workflows – consistently across the infrastructure to validate and eliminate non-compliant certificates. Mandate network-level changes to be approved by authorized personnel only.

- Simplify the process of adding new certificate owners. This can be achieved by assigning ownership for the entire certificate group or by allowing existing owners to transfer the ownership before changing positions or moving out of the company.

- Create an audit trail system that logs every action taken by stakeholders in the hierarchy, along with a timestamp. Make sure critical events are automatically reported back to the respective certificate teams. Audit logs are immensely useful for determining the cause of certificate-related issues and for detecting policy violations.

- Set up an automated alerting and reporting mechanism that sends periodic reports and notifications on expiry, validity, and compliance status of certificates to the corresponding owners. This helps with in-time renewals and proactive resolution of certificate issues.

Seamless integration of certificate management with other enterprise solutions

In a typical IT operations premise, enterprises use various solutions for authentication, authorization, monitoring, ITSM (IT Service Management), and SIEM (Security Information and Event Management). A certificate management solution is required to integrate with these enterprise solutions to simplify and secure operations.

Also, the true power of automation can only be realized when a certificate lifecycle management (CLM) system tightly integrates with other existing enterprise solutions.

Here's how a siloed CLM can cripple your IT operations efficiency

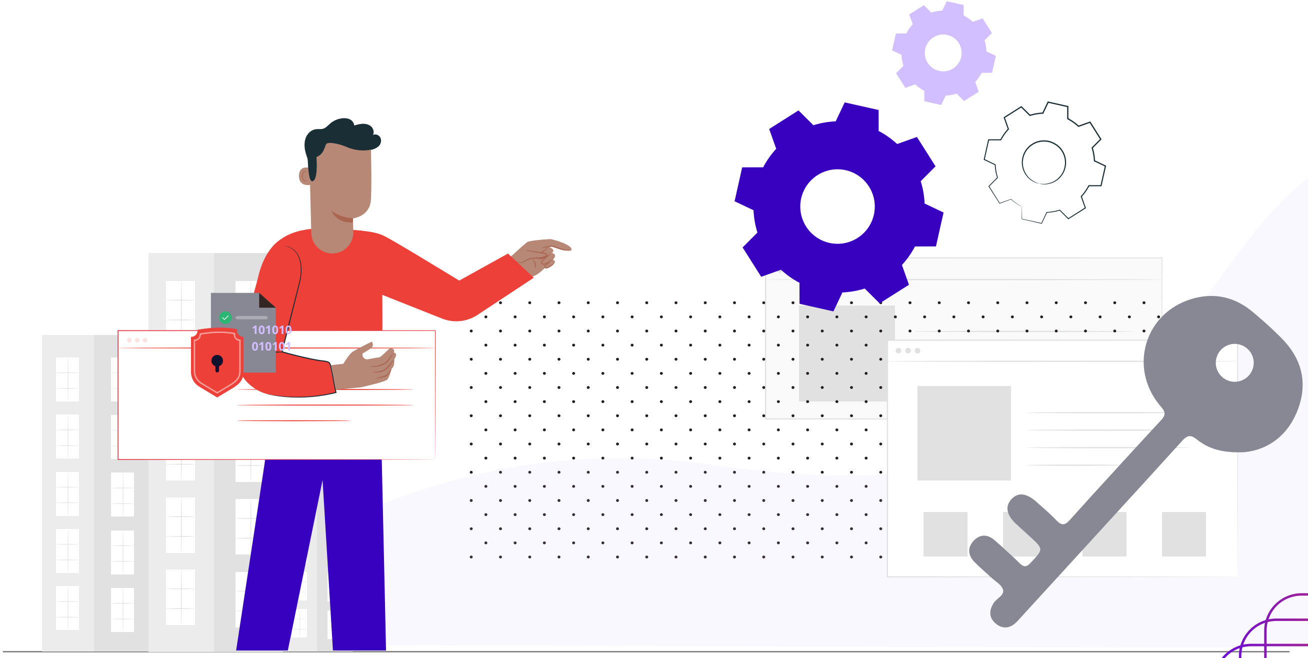
- When certificate management operates in silos, IT operations face the challenge of a grinding long-drawn process that involves manually raising certificate requests, procuring them from CAs, and pushing them to the devices using another IT solution. The disconnect stemming from the lack of integration creates serious delays in the certificate lifecycle process. Also, too many pit stops in the lifecycle increase operational complexity, thereby introducing security vulnerabilities in the IT operations systems.

Siloed CLM
can cripple your IT operations efficiency

Managing certificates in distributed cloud environments starts with holistic visibility and discovery of all certificates installed across various endpoints in the network. Visibility is the cornerstone of any protection mechanism. Yet, most enterprises still have little to no visibility into their certificate infrastructure. Most of the information that ensures full visibility (such as the number of certificates in use, their locations, their expiration dates, and their ownership details) are either improperly documented or not documented at all when managed manually in spreadsheets. Even when they are documented, the high risk of human error affects the accuracy of the inventory.

Discovering certificates that are installed across various endpoints in an organization's network is key to achieving holistic visibility. The process of discovery involves scanning the entire network and recording key details of certificates such as their locations, health, types, days to expiry, their positions in the chain of trust, etc. They provide insights into the security map of a network infrastructure and help detect major flaws. However, legacy tools often fail to discover certificates in distributed cloud environments, as they don't integrate with enterprise network scanners, which leads to certificates going undocumented and unmonitored.

- As far as control and visibility are concerned, mobile devices still pose a serious threat to enterprise security. Since mobile devices leverage digital certificates for authentication and security, it is essential to closely monitor and manage these certificates. This requires CLM platforms to integrate with mobile device managers (MDM). Lack of integration in manual processes makes monitoring certificates for expiry, issuing new certificates, and updating weak certificates across mobile devices extremely challenging.



How should you respond?

- Choose a certificate lifecycle automation solution that has pre-built integrations with third-party systems. This integration allows IT operations teams to access simple automation workflows from third-party systems for self-servicing certificate requests, therefore standardizing certificate management. For example, integration with ITSM tools such as ServiceNow and BMC Remedy, allows teams to design manual ITSM tasks, such as creating a ticket, pushing a configuration, and closing a ticket, directly into an automation workflow, which dramatically accelerates the entire process.

- Choose a certificate management solution that can seamlessly integrate with existing enterprise scanners in the network. This integration allows the CLM solution to penetrate deeply into the enterprise network and discover all certificates in hybrid network infrastructures, procured from multiple vendors and on an on-demand basis. The integration also eliminates the complexity of running multiple scanners for certificate discovery. Brownie points if the solution allows enterprises to customize the intensity of scans for uninterrupted discovery. The ability to discover all certificates provides enterprises a holistic view of the chain of trust and installation location.

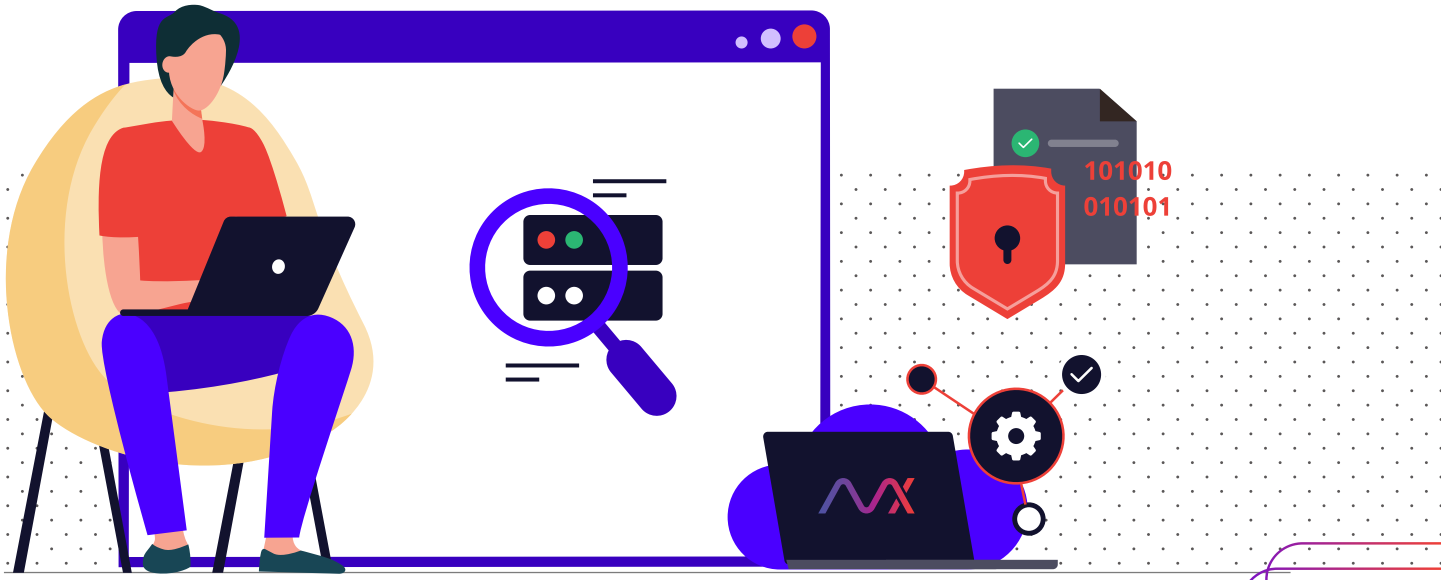
- Choose a certificate lifecycle automation solution that integrates with MDMs and enterprise mobility management (EMM) systems for simplified and secure certificate management. It helps discover certificates from each device group within the MDM, monitor them for expiry, leverage both internal and external CA for issuing new certificates, and push these certificates back to the device group efficiently.

Real-time discovery, visibility, and monitoring of certificates

From a load balancer to a cloud application to mobile devices, every non-human entity on the network requires digital certificates. In a typical IT environment, multiple teams such as security, networking, and DevOps are involved in the development, governance, and maintenance of the network infrastructure. These teams have the flexibility of procuring and provisioning certificates independently to facilitate uninterrupted operations.

When multiple teams manage certificates, enforcing a uniform PKI policy becomes challenging. Ad-hoc processes are error-prone and non-compliant, and often lead to variations in cryptographic standards. The security risk is amplified when PKI teams rely on manual processes for discovering and monitoring certificates. Spreadsheets and legacy monitoring tools do not offer real-time, top-down visibility of certificates distributed in multi-cloud environments. This increases the probability of orphaned certificates becoming weak links.

The problem of discovery, visibility, and monitoring of certificates is more pronounced when it comes to DevOps and containerized environments. The fast-changing nature of these environments has reduced the validity of digital certificates from years to a few hours. This means certificates are now renewed and provisioned more frequently, and therefore must be closely governed to avoid security lapses. If encrypted communication is not properly orchestrated and managed—the very advantages of DevOps and containers such as agility and ease of deployment—can become the greatest vulnerabilities.



Certificate Management in DevOps and containerized environments

As organizations move towards infrastructure-as-a-code culture that is rife with rapid release cycles and continuous integration/ continuous delivery (CI/CD) practices, speed is always the top priority. This need for speed has inadvertently made it difficult for security teams to shift left and bake security right into the DevOps lifecycle. As DevOps grows increasingly multi-faceted with cloud deployments, containers, microservices, and several other open-source management tools—the risk of a cyberattack increases multifold. Mitigating this risk requires DevOps to align with cybersecurity.

One of the pivotal and time-tested security measures enforced to secure the CI/CD pipeline is digital certificates. These certificates add a much-needed layer of security for DevOps by authenticating and securing all digital communication. Implementing a well-documented, policy-based, compliant certificate infrastructure for applications used in DevOps toolchains and containerized environments is key to making the most out of speed and agility, without compromising on application security. However, many organizations employ manual processes for certificate management. The inefficiency and complexity of these processes create a host of challenges for the DevOps teams as they try to balance rapid development timelines with secure certificate management practices.

Here’s how manual certificate management can hurt your DevOps agility and your security posture

- The DevOps environments today are overrun with new web servers, virtual machines, and containers that are constantly being spun up and down in a matter of hours. This has substantially increased the use of digital certificates. In a conventional development pipeline, procuring trusted certificates can take days. Ticketing systems that are required to move the request from one point to another are typically scattered, which further delays the certificate issuance process. Given the fleeting lifespans of virtual machines and containers, issuing certificates cannot be a delayed process as it breaks the application delivery speed.

  Because speed is critical, DevOps teams often tend to steer clear of speed breakers. This means taking shortcuts to certificate generation and provisioning. One of the most commonly used hacks by DevOps in this context is to procure certificates from CAs of their choice or issuing self-signed certificates, which causes inconsistencies in certificate management and puts security at high risk.

- With the number of digital certificates increasing substantially, the manual process of monitoring, allocation, expiration, and binding of thousands of certificates across the organization can become a dreaded chore for DevOps. The burgeoning volume and chaos of manual requests clouds visibility. Tracking and monitoring certificates for expiry becomes difficult and are neglected. The problem is further exacerbated by the lack of consistent communication with the CA. Together, this leads to frequent certificate expirations and DevOps outages—the consequences of which can greatly damage the enterprise reputation.

How should you respond?

- Choose a certificate lifecycle automation solution that tightly and seamlessly integrates with your DevOps tool such as Puppet, Chef, Ansible, Terraform, and Saltstack. This way, you can rest assured that every new application or update is secured with an X.509 certificate. As DevOps requires certificates to be deployed rapidly for uninterrupted operations, an integrated CLM will allow DevOps teams to request and install certificates right from the CI/CD pipeline.

- Automate certificate lifecycle operations in the DevOps environment. This allows teams to order certificates from any supported CA, push issued certificates to associated applications, renew and revoke existing certificates, and delete unused certificates—all from their preferred DevOps tool.

- Use automated workflows to enable self-servicing for certificate generation and enrollment. These predefined workflows allow DevOps teams to procure and provision certificates without any manual intervention. An automated solution automatically provisions newly issued certificates and associates them with necessary SSL profiles on end-servers, wherever they may reside. This process accelerates certificate enrollments while also ensuring strict policy compliance.

  Adopting automation also helps DevOps gain complete and holistic visibility of the certificate infrastructure. This gives them the ability to identify the entire chain of trust, including the issuing CA and the endpoint where the certificate resides.

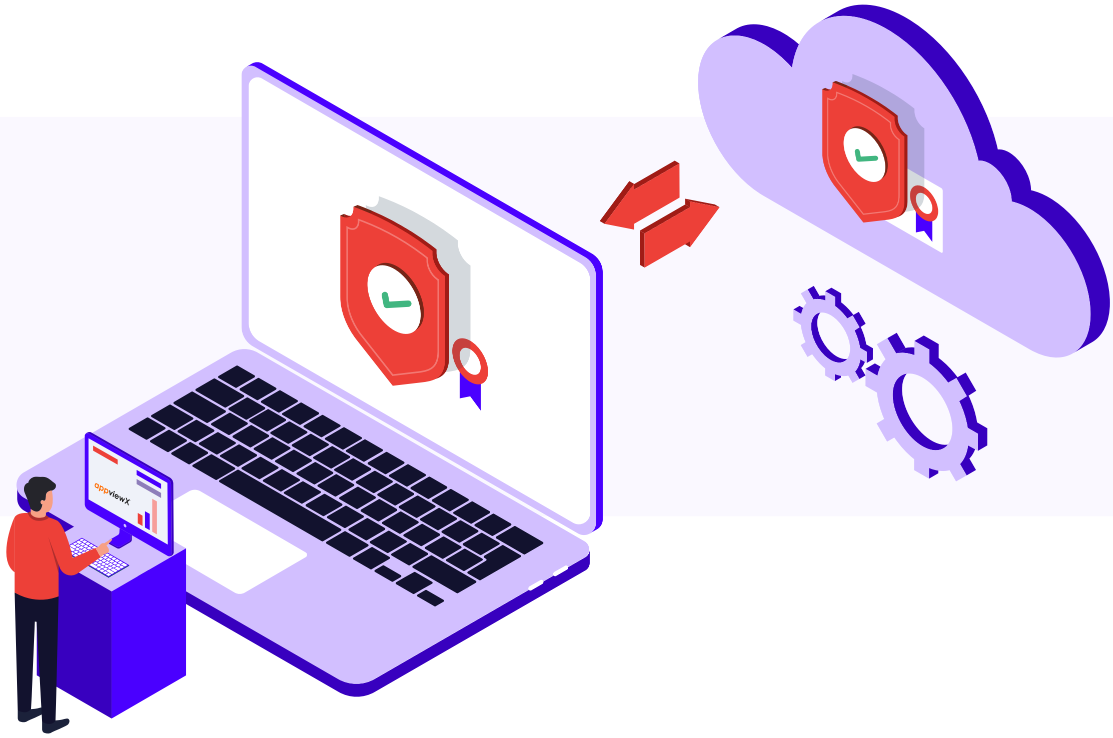
- Employ a CLM solution that supports container-based platforms and integrates with dedicated container management tools. Containerized applications and workloads sometimes use certificates with a lifespan of a few hours. Having an integrated CLM provides an efficient and reliable mechanism for deploying certificates and keys for applications hosted in a container infrastructure.

Step into the agile world of cloud and containers with safe and secure machine identity management

The AppViewX Next-Gen Machine Identity Automation Platform is purpose-built for orchestrating and governing digital identities—digital certificates and keys—of machines—devices, workloads, applications, containers, and the Internet of Things. The AppViewX Platform quickly and easily translates business requirements into automation workflows that improve agility, enforce compliance, eliminate errors, and reduce cost.

Powered by AppViewX CERT+, the enhanced platform addresses security compliance driven by exponential growth in machine identities by eliminating manual management, securing storage and distribution, and ensuring end-to-end visibility.

AppViewX CERT+ is a turnkey solution for all enterprise PKI needs. CERT+ simplifies management of certificates and keys across various technologies in varied hybrid cloud and multicloud deployment environments. It makes certificate management streamlined and efficient, allowing for endless upward scalability and cryptographic agility. The solution also provides enterprises with advanced PKI self-service, private key protection and policy enforcement both, on and off the cloud via strong integrations with leading PKI, identity and access management (IAM), cybersecurity, and DevOps solutions.



Context-aware and state-aware

Automation in CERT+ is 'smart.' Before running an automation workflow, the solution first checks the device's state, performance, capacity, etc., and proceeds only after getting a green light. This way, it prevents the all-too-common problem of automation collisions—a scenario where a device gets more requests than it can handle from various other devices and tools and eventually crashes. CERT+ here acts as a master-orchestrator—it can regulate and forward requests from other tools as well, such as a vulnerability-scanning tool like Rapid7 or a configuration management tool like Ansible, through REST API integrations.

Policy-based orchestration

CERT+ automates certificate management based on policies laid down by the enterprise, the CA, and industry regulations. PKI administrators can group certificates based on their type, use-case, criticality, etc., and apply a different policy for each certificate group. Policy-based automation takes care of certificate lifecycle tasks such as time-bound certificate renewals, key rotation, access privileges, and compliance audits.

DevOps-friendly

DevOps requires certificate lifecycle management to be integrated into CI/CD pipelines so that every new application or update will be secured with an appropriate X.509 certificate. Another requirement for DevOps is speed—certificates need to be deployed almost instantaneously for testing and production. CERT+ integrates with popular DevOps tools, such as Jenkins, enabling DevOps teams to request and install certificates right from the CI/CD pipeline. CERT+ also ensures that obsolete certificates (such as internal certificates used for testing) are destroyed automatically to prevent their misuse.

Support for containers and multicloud

Containerized applications and workloads may have ephemeral certificates with a lifespan of a few hours. Many times container applications use self-signing CAs within the Kubernetes cluster for ease and speed of certificate enrollment. AppViewX provides a Kubernetes controller as an integration point between CERT+ and Kubernetes. Any application running in the Kubernetes cluster can leverage this external signer for routing certificate signing requests (CSR) to the corporate CA. Typically, the service mesh solutions like Istio are configured to use this signer as the service mesh takes care of SSL offload. CSRs flowing through AppViewX CERT+ go through the central control policies defined by PKI administrators and ensure high security standards.

The Next-Gen Machine Identity Automation Platform from AppViewX consolidates its security automation solutions for certificates, keys, IoT security and SSH access management across multicloud environments. The platform enables zero-trust, making the entire system more flexible, adaptable, efficient, and agile. It is available as a service and can be deployed in the public cloud, private cloud or on-prem environments. The platform works hand in glove with AppViewX CERT+, providing a more comprehensive approach for enterprises to scale their machine identity management.

Security simplified with AppViewX

Trusted by one out of every five Fortune 100 companies, AppViewX CERT+ powered by enterprise-grade automation, helps with smart discovery, visibility into security standards and centralized management of certificates and keys across hybrid multi-cloud environments.

Scan QR code to learn more about how AppViewX can be your partner of choice in your cybersecurity journey

https://www.appviewx.com/