IDC MarketScape

IDC MarketScape: Worldwide Certificate Lifecycle Management Software 2026 Vendor Assessment

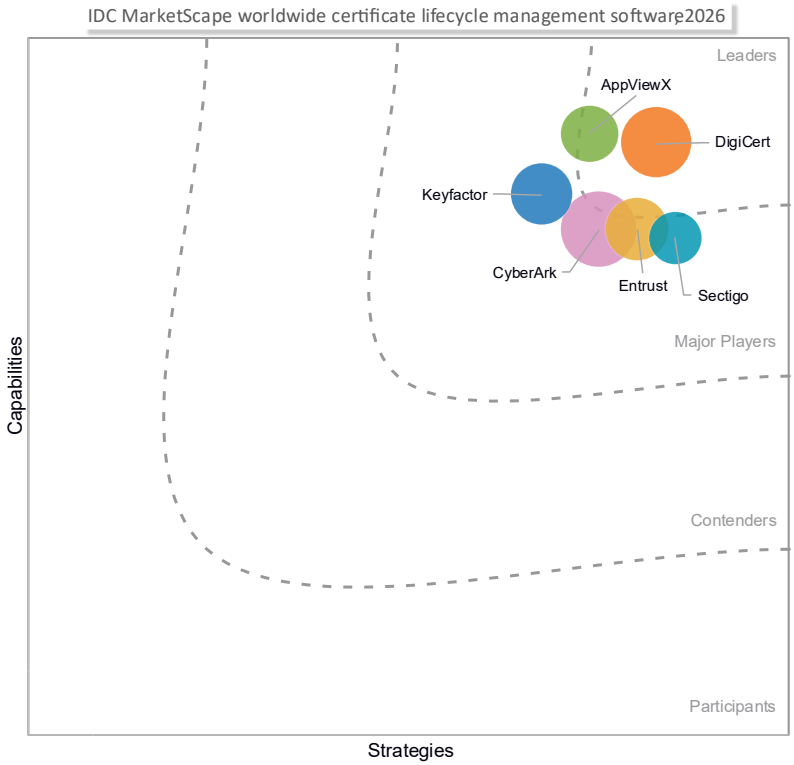
Jennifer Glenn

THIS EXCERPT FEATURES DIGICERT AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape worldwide certificate lifecycle management software vendor assessment



Source: IDC, 2026

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

January 2026, IDC #US52990725e

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Certificate Lifecycle Management Software 2026 Vendor Assessment (Doc # US52990725)

IDC OPINION

Certificates provide the backbone of secure computing. They offer the verification of authenticity for devices, websites, users, and organizations, enabling secure connections. To maintain security, these certificates must be issued, renewed in a timely manner, or revoked in the event of compromise. As businesses transitioned to digital, the number of certificates being used within these organizations exploded.

Certificate lifecycle management (CLM) offers a better way for organizations to manage high volumes of certificates from discovery to issuance and distribution to renewal and revocation. CLMs are also designed to identify compliance or security violations for individual certificates and offer options for remediation. Automated CLM tools offer the information, organization, and control that users need to address shortened certificate lifecycles and transition to post-quantum cryptography (PQC).

This 2026 IDC MarketScape for worldwide CLM software provides a quantitative and qualitative assessment of vendors in the CLM software market. The research assesses the strategies and capabilities of six CLM vendors that have qualified for inclusion in this study, based on annualized revenue and geographic presence. This study also includes a few "vendors to watch" that did not qualify as full participants but represent innovative players in the market.

Key trends and concerns in this market include:

- **Increased certificate volume and complexity:** Organizations now manage hundreds of thousands to millions of certificates across hybrid, multicloud, DevOps, and IoT environments, making manual or homegrown management unsustainable. Further, undiscovered or unmanaged certificates increase the risk of unexpected expirations, service downtime, and noncompliant cryptographic usage. Finally, dedicated CLM teams are typically small relative to other security staff and may not even exist in smaller organizations, further driving the need for automation.
- **Shortened TLS lifecycles:** In April 2025, the Certificate Authority/Browser (CA/B) Forum approved a standard that would reduce the life span of public TLS certificates on a phased schedule, starting with a reduction to 200 days in March 2026, then reduced to 100 days in March 2027, and finally to a maximum of 47 days in March 2029. This was a concern raised by every customer interviewed for this evaluation.

Meeting aggressive renewal windows without outages is viewed as unmanageable without high levels of automation and policy enforcement.

- **Preparation for post-quantum cryptography:** Quantum computing is quickly coming to fruition, and with that comes the concern for attackers using these tools to break encryption. Even now, we hear of threat actors exfiltrating encrypted data with the intent of using quantum computing to decrypt sensitive or confidential data when it becomes available. Buyers worry that today's cryptographic inventory and processes are not ready for quantum-safe migration, including algorithm changes, hybrid schemes, and staged cutovers.
- **Platform strategy and ecosystem integration:** A growing trend is to combine CLM with public key infrastructure (PKI), key and secrets management, code signing, SSH, and hardware security modules (HSMs) capabilities into unified platforms, sharing services, and offering tighter integration. Even when delivered as part of larger platforms, most CLM offerings emphasize CA-agnostic design and APIs so organizations can use multiple CAs and integrate with third-party ecosystem tools. This alleviates concerns about over-reliance on a single CA or tightly bound stack, particularly as certificate lifetimes shrink.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

The process for this IDC MarketScape on CLM software began in August 2025. IDC sent pre-qualification surveys to vendors that offered CLM. For this evaluation, vendors had to meet the following criteria:

- Product generally available with demonstrable revenue as of December 31, 2024
- CLM solution with demonstrable revenue, whether from an SKU or as a module in a platform
- Revenue of $10+ million
- Revenue from CLM in a minimum of two regions
- Offers — at minimum — the following capabilities: centralized storage and management, as well as automation
- Support for more than one certificate type
- Support of at least two CAs (one can be their own)

There are many cloud vendors that offer certificate lifecycle management tools. However, as noted in the criteria, the CLM solutions evaluated needed to have demonstrable, standalone revenue and also needed to support multiple CAs. This means that CLM solutions available from cloud vendors (e.g., Google Certificate Manager) were not included in this evaluation.

There are a few standalone CLM solutions available from organizations that are not included in this evaluation, including, but not limited to, vendors that serve specific geographies and newer solutions with limited revenue and time on the market. These companies are featured in the "Vendors to watch" section.

ADVICE FOR TECHNOLOGY BUYERS

Commercial tools can offer several advantages over internally developed solutions

In the past 10–15 years, the world has increased its reliance on the internet for personal business as well as organizational operations and products. When it comes to digital certificates, what used to be relatively easy to manage has become untenable. Most organizations are responsible for managing hundreds of thousands to millions of digital certificates. Internally developed management solutions may have been an optimal choice at one time — and maybe for some users, still is — but the increased number of certificates, the changing regulatory landscape, and future transitions have made these solutions harder to maintain. Commercial CLM solutions have come a long way in the past 10 years. They are more customizable, and most can work with multiple types of certificates. The onus is on the vendor to keep pace with compliance changes as well as the general maintenance and innovation of the product. This can eliminate a lot of process and time burden from cryptography and security teams.

Automation is necessary to stay ahead of cryptography changes

As stated previously, the number of certificates that organizations have to manage is increasing rapidly, into the millions for some users. Users interviewed for this evaluation fall into this group and noted that keeping up with regulations, such as the 47-day TLS certificate lifecycle, was simply not manageable without automation. This is true for transitioning to post-quantum cryptography as well. Finding a vendor that offers a comfortable level of automation is essential for success during these changes.

CLM is just one piece of the cryptographic ecosystem — and companies have a choice in how to integrate these pieces

It was clear from this evaluation that CLM is just a single piece of the cryptographic puzzle. The cryptographic ecosystem is very broad and variably complex. PKI, keys and secrets management, secrets vaults, and hardware security modules also require management and automation for optimal operation. Many CLM vendors offer additional functionality for these other ecosystem tools. Using a multifunctional cryptographic platform has many advantages. They may offer shared technology services within the platform; seamless integration and cost savings are just some of benefits. However, there may also be some

(understandable) reticence to "put all of your eggs in one basket," so to speak. The good news is that most vendors offering pieces of the cryptographic ecosystem can work with other vendors in the space through APIs and integrations, offering similar outcomes. When evaluating cryptographic solutions, this is something to consider and will vary based on each organization's risk tolerance and preference.

CLM is not just for large enterprises

While large enterprises often have a larger volume of certificates to manage, small to midsize business can benefit from CLM as well. Even the largest enterprises often have small teams dedicated to CLM (and cryptography in general). Smaller companies have even fewer — if they even have anyone dedicated to CLM at all. Automating certificate management or empowering self-service can free up resources for organizations of all sizes. For teams without dedicated cryptography or certificate practitioners, this can alleviate the burden that may be foisted onto team members as an "extra task" to their regular day job.

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

DigiCert

DigiCert is positioned in the Leaders category in this 2026 IDC MarketScape for worldwide certificate lifecycle management software.

DigiCert, headquartered in Lehi, Utah, was founded in 2003. The company was created to simplify certificate purchases and has evolved to also offer management of those certificates and other digital trust assets. DigiCert is privately held with a mission to help customers modernize PKI to reduce outages, address compliance risk, and improve operational overhead. DigiCert acquired DNS Made Easy in 2022 and Vercara in 2024, expanding its digital trust portfolio.

DigiCert is both a certificate authority and a vendor of CLM. Its CLM, Trust Lifecycle Manager (TLM), is a CA-agnostic architecture offering the full spectrum of certificate operations including discovery, governance, and automation of certificates and related cryptographic assets, such as code signing, authentication, email document signing, IoT certificates, and SSH keys. Key details and differentiators include:

- **Discovery and inventory:** DigiCert's TLM aims to discover and centralize certificate inventory using sensors, agents, CA integrations, and certificate transparency logs across the organization. It is designed to continually track and augment each certificate with context-based metadata such as type, issuer, key strength, and expiration. Two-way connections with SIEM vendors offer both vulnerability and risk updates to certificate inventory and organizationwide visibility and remediation.
- **Certificate issuance and distribution:** The solution supports CA-agnostic issuance workflows for public and private CAs across DV, OV, EV, client, S/MIME, code signing, IoT, and other certificate types with policy-driven templates and profiles. Distribution is automated via integrations and agents to web servers, load balancers, devices, cloud services, and other endpoints, as well as through DevOps and ITSM connectors that embed issuance into deployment and change workflows.
- **Automated renewal and replacement:** DigiCert TLM is designed to trigger auto-renewals ahead of expiration, generate keys and CSRs per policy, and redeploy updated certificates to endpoints. The solution offers bulk replacement for compliance or incident-driven events. One manufacturing customer used this tool to automate a majority of its environment and reduced workload to only a limited weekly effort.
- **Certificate revocation and compromised handling:** DigiCert TLM aims to provide workflows for efficient revocation of compromised or unneeded certificates and rapid re-issuance. Audit trails, policy-driven escalation paths, and automated notifications support incident response and provide traceability.
- **Security and compliance:** DigiCert TLM offers capabilities for secure key generation and storage (often integrated with customer HSMs or cloud vaults), role-based access control, detailed audit logging, compliance-oriented reporting, and monitoring for shadow or unauthorized certificates.
- **Reporting and analytics:** DigiCert TLM aims to provide dynamic, customized dashboards to offer users visibility into the information they need, including certificate health, compliance scores across geographies, expiration timelines, policy compliance, risk profiling, and PQC readiness, plus APIs to export data to analytics and business intelligence (BI) tools. An AI analytics assistant helps users identify anomalies (e.g., weak keys, shadow certs, or noncompliance) or forecast certificate replacement needs.
- **Scalability and automation:** DigiCert TLM uses a multitenant SaaS architecture and automation framework designed for high certificate volumes across complex hybrid environments, including organizations managing hundreds of thousands of certificates with limited PKI staff.
- **PQC readiness:** DigiCert TLM includes PQC-ready certificates across private CA offerings and supports migration for algorithm substitution and hybrid cryptographic

profiles. As a company, DigiCert provides customers with a PQC Tool Kit, readiness workshops, and professional services, with the aim of making the transition as low risk as possible.

DigiCert TLM can be sold individually as a CLM and is a core component of the DigiCert ONE platform, alongside Software Trust Manager, Device Trust Manager, and Document Trust Manager, integrating DNS, PKI, and content trust into a unified digital trust ecosystem.

DigiCert TLM offers flexible deployment, including SaaS, software on a virtual appliance, hybrid options, and delivery as a managed service via third parties.

Strengths

- DigiCert TLM can be delivered via managed service, extending reach to customers of different sizes and geographies that want CLM automation and support from trusted partners.
- DigiCert TLM offers automation to support smaller teams managing high certificate volumes. One customer reported that large portions of its device and user certificate operations are able to run automatically and require minimal effort to operate.
- Another customer replaced its in-house PKI for DigiCert TLM SaaS to manage S/MIME, private TLS, and public TLS across a complex hybrid environment. This customer noted significant cost benefits of relying on the platform for CLM activities.

Challenges

- Customer feedback highlights challenges with licensing constructs, particularly when mapping user- or seat-based licensing to large numbers of device certificates, creating complexity during rollout and renewals. The company readjusted its pricing constructs in September 2025 as this evaluation was underway.
- While overall satisfaction with support is positive, interviews noted variability in support and account management, including communication gaps between resellers, sales, and technical teams and limited proactive best practice guidance.

Consider DigiCert when

Smaller teams managing high volumes of certificates across complex hybrid infrastructures may see value from the company's CA-agnostic lifecycle automation across multiple CAs and certificate types. Organizations of all sizes and industries can benefit from flexible deployment, including managed services. The DigiCert ONE platform is cloud-first and multitenant SaaS, with hybrid and on-premises options to address data sovereignty and regional regulatory needs.

APPENDIX

Reading an IDC MarketScape graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

The weighting for the graph for this IDC MarketScape for CLM software was split 60:40, with emphasis on the strategies section. Many vendors currently offer the same set of capabilities and functions. Although these capabilities may vary, as the market changes, it is important to see where these companies are differentiating their solutions.

IDC MarketScape methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market definition

Digital certificates are part of an essential foundation for good security practices. These certificates provide authentication of public cryptographic keys by binding them to an identity — e.g., a user or a device. IDC defines certificate lifecycle management (CLM) as software that acts as a library for an organization's certificates and the relevant information about

them, including ownership and expiration dates. The purpose of the CLM is to take care of the life span of the certificates from creation to destruction.

LEARN MORE

Related research

- *When Do You Plan on Implementing Quantum-Resistant Encryption into Your Organization* (IDC #US53831225, September 2025)
- *Worldwide Digital Trust Software Forecast, 2025–2029* (IDC #US52402425, August 2025)
- *Worldwide Digital Trust Software Market Shares, 2024: Thales Leads an Increasingly Consolidated Market* (IDC #US52402625, July 2025)
- *IDC Market Glance: Cryptographic Identity Technologies, 2Q25* (IDC #US50210223, June 2025)
- *Post-Quantum Cryptography: Top Questions and Practical Ways to Get Started* (IDC #US53268125, March 2025)

Synopsis

This IDC study provides an overview of certificate lifecycle management software. Certificate lifecycle management is getting more executive attention with PQC on the horizon. However, practitioners are currently focused on more immediate challenges such as shortened TLS lifecycles. Buyers are looking for ways to get a handle on increasing certificate volume — a move that can help prepare the organization to handle both transitions. Vendors in the space have the tools and approaches to help customers achieve their desired outcomes for automation and compliance preparedness. These vendors need to work closely with their existing customers to identify and invest in capabilities that help attract and retain new customers.

"Certificate expiration–related outages continue to challenge enterprises of all sizes. This becomes an operational and business-level issue that will only get worse with shrinking TLS lifecycles and the transition to PQC," said Jennifer Glenn, research director for IDC's Security and Trust Group. "Vendors in this space need to meet customers wherever they are in their certificate management journey. At the same time, these vendors will need to clearly demonstrate how their capabilities are uniquely designed to help customers demonstrate technology and business value in the long term."

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com