

CERTIFICATE LIFECYCLE MANAGEMENT

Optimizing certificate management in healthcare with CertSecure Manager

How a leading U.S. healthcare provider replaced manual, error-prone certificate processes with automated, centralized lifecycle management, eliminating outages and reclaiming hours for its IT teams.

NO. OF EMPLOYEES

10K+

REGION

United States

SOLUTION

CertSecure Manager

70–80%

Faster certificate provisioning

Complete

Certificate Visibility

Zero

Surprise certificate outages

A leading healthcare provider, built on a foundation of digital trust

One of the largest healthcare organizations in the United States, recognized for its focus on preventive care, electronic health records, comprehensive health information systems, reducing healthcare costs, and early adoption of telemedicine, operates on a foundation of extraordinarily sensitive patient data. Strong security controls and HIPAA compliance were already firmly in place.

Yet certificate management remained stubbornly manual. Certificates were tracked in spreadsheets and renewed by hand, with limited visibility into who issued what, and where. As the certificate footprint expanded across domains, servers, devices, and cloud services, operational risk expanded with it, quietly undermining the very trust the organization was built to protect.

In healthcare, a single expired certificate can disrupt patient-facing systems. Certificate reliability isn't operational hygiene, it is essential to trust, compliance, and business continuity.



Five problems eroding security and reliability

A manual, spreadsheet based process couldn't keep pace with the scale of certificates the organization relied on to run securely.

1

Manual certificate management

Tracking thousands of certificates in spreadsheets was slow and error-prone, with no way to enforce enterprise-wide policy, audit issuance, or maintain clear visibility.

2

Inefficient certificate discovery

SSL/TLS certificates were scattered across domains, servers, devices, and clouds that hard to track, weakening security posture and letting expirations go unnoticed.

3

Lack of proper enrollment

Without a standard process to request and obtain certificates from a CA, trust eroded, secure communications were at risk, and compliance with standards including HIPAA was threatened.

4

Certificate outages

Expired, invalid, or revoked certificates rendered services unusable causing disruptions and denting user trust, reputation, and financial standing.

5

Limited integration

Existing tools couldn't deploy certificates within the CI/CD pipeline, making integration with existing or new applications in the development process nearly impossible.

“

When We Assessed The Environment, Certificates Were Everywhere And Visibility Was Nowhere. Renewals Were Tracked In Spreadsheets That Could Not Keep Up With The Scale Or The Compliance Burden, And Every Cycle Carried The Risk Of Another Silent Outage.

ENCRYPTION CONSULTING
CERTSECURE MANAGER TEAM

Centralized, automated lifecycle management

CertSecure Manager brought the entire certificate lifecycle under control across inventory, discovery, enrollment, reporting, and alerting.



Centralized inventory control

Automated, centralized certificate management, maintaining security and compliance across the lifecycle through automated revocation, monitoring, and renewal.



Automated lifecycle

An automated approach to lifecycle management reduced the risk of outages from expired or invalid certificates while improving overall security.



Efficient discovery

Seamless NESSUS and discovery-tool integration removed unused and expired certificates, kept critical ones from lapsing, and strengthened the institution's PKI infrastructure.



Streamlined enrollment

Reduced management costs, enforced controls and policies for authorized users, and enabled quick, governed certificate acquisition.



Reporting & alerts

Simplified report generation with automated alerts by expiration date, template, key length, and more.



Outage prevention

A distinct alert system for expiration and revocation, with centralized tracking and renewal reminders so certificates were never missed.

From manual and reactive to automated and resilient

CertSecure Manager replaced manual, reactive processes with automated, resilient certificate lifecycle management, delivering measurable improvements across provisioning speed, visibility, ownership, and operational control.

70–80%



Reduction in certificate provisioning time

BEFORE Hours to day per certificate
AFTER Minutes per certificate



Blind spots eliminated

SeamlessNESSUS and discovery-tool integration, plus intelligent monitoring and vulnerability identification, closed visibility gaps.



Ownership & accountability

Detailed inventory records improved certificate ownership visibility and simplified ownership transfer.



Unified dashboard

A single inventory dashboard increased control and insight, with flexible report customization.



Automated monitoring

Continuous, automated monitoring and maintenance kept critical certificates valid and current.



Zero surprise certificate outages

Automated alerts, centralized expiry tracking, and renewal reminders ensured no certificate expired unnoticed, eliminating the surprise outages that had previously disrupted patient facing systems and operations.

— IN SUMMARY

Managing certificates — and digital trust — without compromise

CertSecure Manager replaced spreadsheet tracking and manual renewals with centralized, automated lifecycle management. Certificate provisioning time dropped by 70-80%, surprise outages were eliminated entirely, and NESSUS integration closed the visibility gaps that had left certificates expiring unnoticed across domains, servers, and cloud services. Detailed inventory records also brought clear certificate ownership and accountability across the organization.

For a healthcare organization handling sensitive patient data under strict HIPAA requirements, every expired certificate is a risk to patient-facing systems, compliance, and trust. With full certificate visibility, automated monitoring, and governed enrollment now in place, IT teams are freed to focus on innovation instead of infrastructure.

SEE IT IN ACTION

Prevent outages. Automate the certificate lifecycle.

[Book a demo →](#)