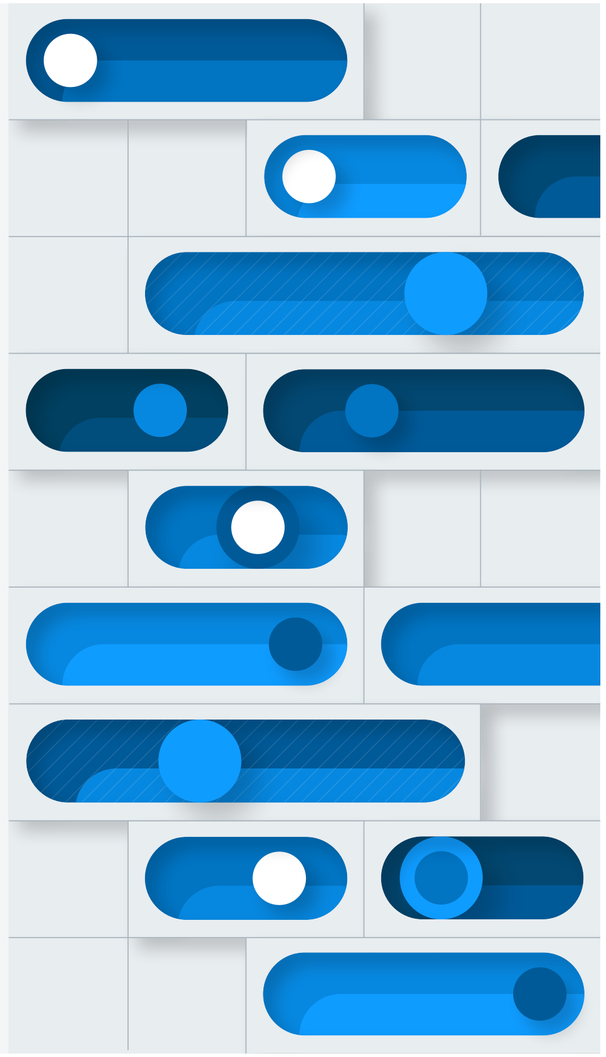
digicert®

IS OUTDATED CERTIFICATE LIFECYCLE MANAGEMENT LEAVING YOU EXPOSED?

Four truths about risk and resourcing from Network, IAM and SecOps managers



digicert®

01

IS OUTDATED CERTIFICATE LIFECYCLE MANAGEMENT LEAVING YOU EXPOSED?

Author
Sean Crouch

Date
3-16-2023

Reviews
★★★★★ 124

02

TABLE OF CONTENTS

67% OF COMPANIES REPORTS AN OUTAGE IN 2021

50,000+ MANAGED SERVER CERTIFICATES PER AVERAGE ENTERPRISE

RELATED RESOURCE

DIGICERT® TRUST LIFECYCLE MANAGER DATASHEET

PART I

IS OUTDATED CERTIFICATE LIFECYCLE MANAGEMENT LEAVING YOU EXPOSED?

Four truths about risk and resourcing from Network, IAM and SecOps managers

If you're concerned about digital trust at your org, you know the past few years have been challenging. From the shift toward remote workforces to rapid increases in the number and kinds of attacks, Network, IAM, and SecOps teams have been pushed to deal with more problems and large, quick transformations.

In some cases, like PKI certificates, these changes and increases in complexity have put a spotlight on how difficult it is to keep up with security when tools and processes aren't built for today's landscape.

We've spent the past few years talking to managers whose teams run PKI certificate operations about what it's like to work with digital trust in the real world. Here's what we heard.

67%
of companies reports an outage in 2021

50,000+
managed server certificates per average enterprise

3X
increase in remote workforce

*2021 DigiCert survey

1. Security is a tug-of-war one day, firefighting the next

"Nobody likes getting a call in the middle of the night, hearing your services are down."

Competing interests create a constant tug-of-war. How robust can I make this solution or service? What's my budget? What's my timetable? How do I verify that everything works, and it will keep working? When the timetable gets reduced, you need to find more resources. But that strains the budget and forces your team to look at the issue on the left, which means the issue on the right gets less attention.

Meanwhile, unexpected events are cropping up all the time, so each day almost never goes exactly to plan. The tug-of-war turns into firefighting. Unexpected outages for the network team. Manually removing a former employee for the identity team. The more fires you and your team need to fight, the less time goes to other projects. Security becomes a reactive task, when you're trying to run a proactive solution that helps you improve functionality in all areas you oversee.

Shorter and changing validity periods increase the frequency of monitoring and renewal.

Expanding enterprise infrastructures have led to more certificates issued without Network IT's knowledge.

2. Too many critical processes are slow and often manual

"Ideally, everything is commodity. You want to know that if something goes wrong, the fix is automatically rolled out, and the only thing you get is a notification."

Your people are your greatest asset. But your people need sleep. They make mistakes. They differ in education, experience, style, and even technical intuition. Managing functions that require manual work takes time away from other functions, and they tax your people.

In many cases, teams who oversee large, sophisticated enterprise infrastructures are still using spreadsheets and email to manage parts of their certificate landscape. Even a quick response to an issue during business hours can still lead to downtime, operations disruption, or bad user experience for customers
or employees.

The solution is automation, but a lot of automated tools are standalone certificate managers that lay over your certificate landscape. These 3rd party and CA-agnostic solutions have to be set up, they cost money, and their workflow capabilities are often limited. If you're building custom APIs to integrate them, or you need multiple software solutions to manage different use cases, the resource burden doesn't go away, it just shifts to another area of your team—another example of tug-of-war.

Free CAs are extremely limited while DIY PKI can't easily be updated to fit evolving needs.

Currently, the industry standard Time To Recovery for a certificate outage is hours, not minutes.

3. A lot of solutions don't solve the problem, and then you have to build it.

"The fun thing with smart technologies is they're smart until they're not."

When it comes to practical use, your oversight is different from the next teams, and theirs is different from the next team over, too. To make your certificates work, you need solutions that fit your use case and your resources. But when it comes time to find a software solution for management, automation, notification, or integration, it turns out a lot of solutions don't do what they promise, or they do one part but not the other.

As a result, if you're not buying multiple certificate managers and CAs, you're turning to scrappy solutions and building your own tools and processes, because you don't have the budget or you can't find a pre-built system that fits your needs. But DIY solutions take time to construct, and they have to be managed. In the case of certificates, in-house CAs require enough PKI expertise for correct configuration, and they don't come with automation. This means more effort from your team when it comes to management, and the potential for problems down the road.

CA-agnostic management software doesn't offer integrated reliability and resilience.

Vendor solutions rarely come with workflows that fit specific team needs.

4. Doing more with the same—or fewer—resources makes security even more difficult

"Businesses are trying to find ways to cut budgets while growing, which means getting creative about doing more with less."

Even though the threats have grown over the past few years, a lot of teams aren't seeing budget and people increases in proportion to the number of fires they have to put out. It's nearly impossible to be proactive, mitigate risk, and streamline operations as much as you'd like when dealing with the same number of team members and less money.

At the same time, the digital landscape is expanding and growing more complicated, even for individual organizations. More things connect, every day. The boundary between one team and another team, and between the inside and the outside of a company have become blurry over recent years. It's sometime difficult to tell where one thing ends and another begins. More certificates mean more managing, but with slow or manual processes, that simply means more opportunity something gets missed. And with more threats out there, and more complex connections, that increase in risk isn't just a problem for your team, it can threaten the entire org.

2023 IT budget growth is projected to fall short of inflation rates.

In recent years, IT leaders consistently report talent shortages as one of the most significant barriers to tech initiatives.

67% OF COMPANIES REPORTS AN OUTAGE IN 2021

50,000+ MANAGED SERVER CERTIFICATES PER AVERAGE ENTERPRISE

RELATED RESOURCE

DIGICERT® TRUST LIFECYCLE MANAGER DATASHEET

digicert®

01

IS OUTDATED CERTIFICATE LIFECYCLE MANAGEMENT LEAVING YOU EXPOSED?

Author
Sean Crouch

Date
3-16-2023

Reviews
★★★★★ 124

02

PART II

WHAT DOES THIS MEAN FOR CERTIFICATE LIFECYCLE MANAGEMENT?

What we're seeing now is the need for a shift in the way we think about and work with certificates in large organizations. More complexity, more PKI use cases, and more threats mean teams need solutions that deliver excellent 24x7x365 trust for any group, whether you're in Network IT, SecOps, or IAM. And those solutions need to work in practice, not just on paper.

03

Based on our conversations with these team managers, a certificate solution needs to offer these characteristics:

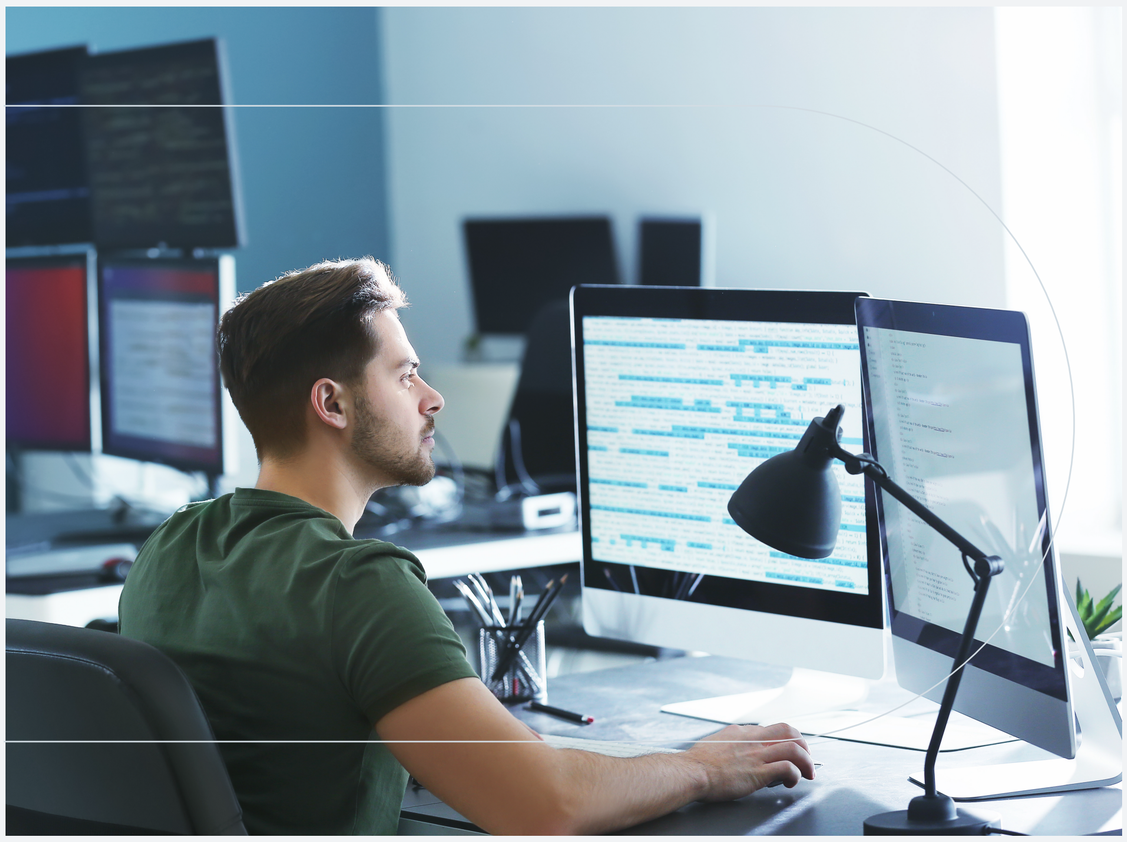
04

1. It needs to be proactive rather reactive, eliminating tug-of-war and firefighting for certificate control.

2. It needs to be automated rather than manual, so risks due to human error, lack of visibility, and after-hours issues are reduced or eliminated. It also needs to be seamless and smart, with few or no touches involved.

3. It needs to operate as a true technical solution, not as selling points, so teams can put certificate trust to work in real settings without running into issues or the need for scrappy fixes.

4. It needs to reduce the burden on resources as much as it reduces threat risks, so teams can turn their attention to other mandates and trust their certificate landscape to effortlessly run.



WHAT WE'RE SEEING NOW IS THE NEED FOR A SHIFT IN THE WAY WE THINK ABOUT AND WORK WITH CERTIFICATES IN LARGE ORGANIZATIONS.

RELATED RESOURCE

DIGICERT® TRUST LIFECYCLE MANAGER DATASHEET

PART III

HOW CAN YOU TELL IF OUTDATED CLM IS LEAVING YOU EXPOSED?

10 questions CISOs and network architects should be asking.

Do you have a single book of record for discovering and inventorying all certificates?

Do you have a reliable, multi-channel system in place for notifying the appropriate team members of problems?

Do you have strong integration that didn't require you to write or license the software yourself?

Do you find that you have less IT turnover now than five years ago?

Do you find it's easy to track the number of CA logins?

Do you have fewer than two vendors for your PKI infrastructure?

Do you have good security coordination between IAM and networking teams?

Have you reduced the number of new digitization solutions and processes over the past few years?

Have you set up solutions that allow you to move away from self-written and managed private CAs or private PKI?

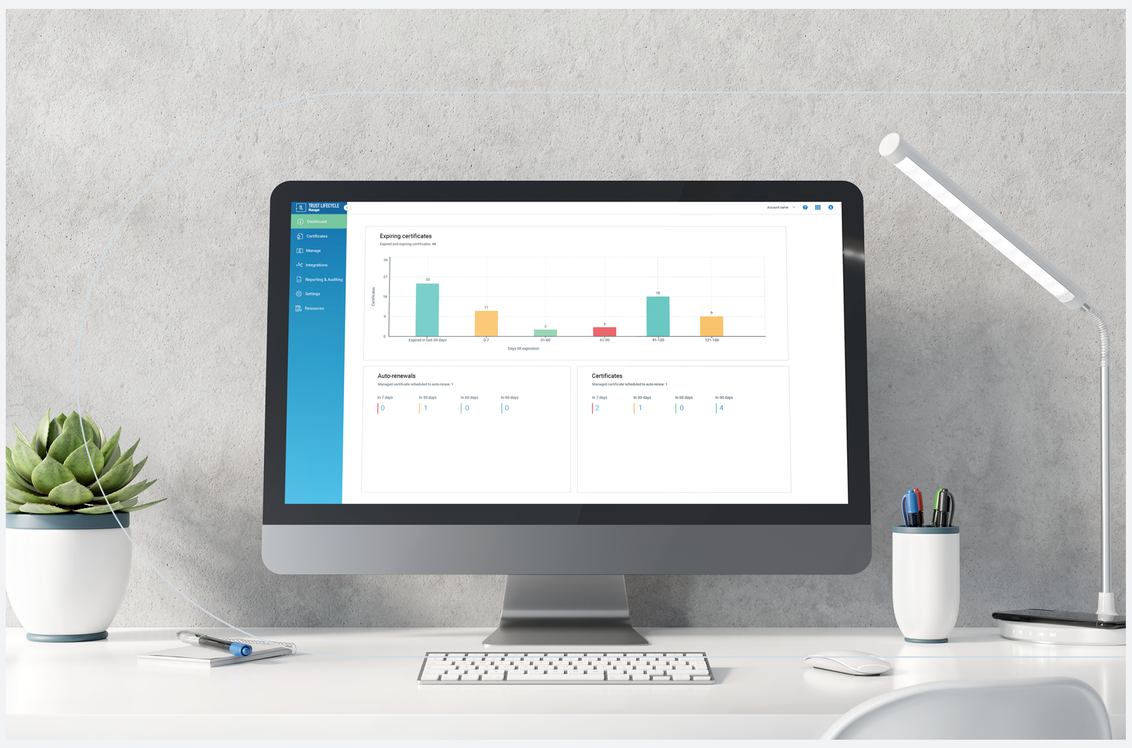
Do you have automation for networks, devices, and users?

Every no answer signals a greater possibility of risk exposure due to outdated certificate management.

Certificate Lifecycle Management, as the Information Technology world has defined it for years, doesn't meet these needs. The ideal tool for managing complexity and risk combines CLM with PKI services in a single full-stack solution that includes the kinds of integrations and configurations your team needs to customize a working, automated certificate landscape.

What we're seeing here isn't the end of Certificate Lifecycle Management, but rather the next step into Trust Lifecycle Management—a comprehensive, automated, technically proven solution for real world certificate application.

You can learn more about eliminating outdated CLM risks by moving to DigiCert® Trust Lifecycle Manager. SEE A DEMO>



EVERY NO ANSWER SIGNALS A GREATER POSSIBILITY OF RISK EXPOSURE DUE TO OUTDATED CERTIFICATE MANAGEMENT.

RELATED RESOURCE

DIGICERT® TRUST LIFECYCLE MANAGER DATASHEET