// CIO Study: Certificate-Related Outages Continue to Plague Organizations

Outages caused by expired digital certificates have become increasingly common for organizations, regardless of their size.

// Executive Overview

Outages caused by expired digital certificates have become increasingly common for organizations, regardless of their size, industry or region. Despite the direct and indirect costs of certificate-related outages on critical infrastructure, CIOs still struggle to get a handle on the problem. New research by Vanson Bourne reveals that certificate-related outages is a growing and costly issue:

- Of surveyed CIOs, more than 60 percent have experienced certificate-related outages within the last 12 months.
- CIOs expect the growth of digital certificates to increase by more than 50 percent by 2024.
- The impact of digital certificate-related outages on critical infrastructure can vary, but they all have the potential to threaten business outcomes.

In addition to evaluating the results of the Vanson Bourne study, this white paper provides a list of best practices you can begin using today to address the continuing increase in outages.

// Introduction

SSL/TLS digital certificates are used as machine identities to enable authentication and encryption. But when these certificates expire, they can bring down the services they support. Outages caused by expired digital certificates are a routine occurrence for most CIOs. Because the symptoms of expired certificates mimic many other types of network failures, they are notoriously difficult to diagnose and can be extremely time-consuming to resolve. And when these certificate-related outages occur on critical infrastructure, the impact and costs can increase dramatically.

These costs spiral out of control, particularly when the expired certificate is an intermediate or root certificate. When these types of certificates expire, all leaf certificates chaining up to them must also be found, and new certificates must be issued and installed.

According to leading analysts, the average cost of a critical infrastructure outage in Global 5000 organizations averages $5,600 a minute, or more than $300,000 an hour, while severe outages on large networks—the sort that can take days to resolve—can cost $500,000 per hour or more.

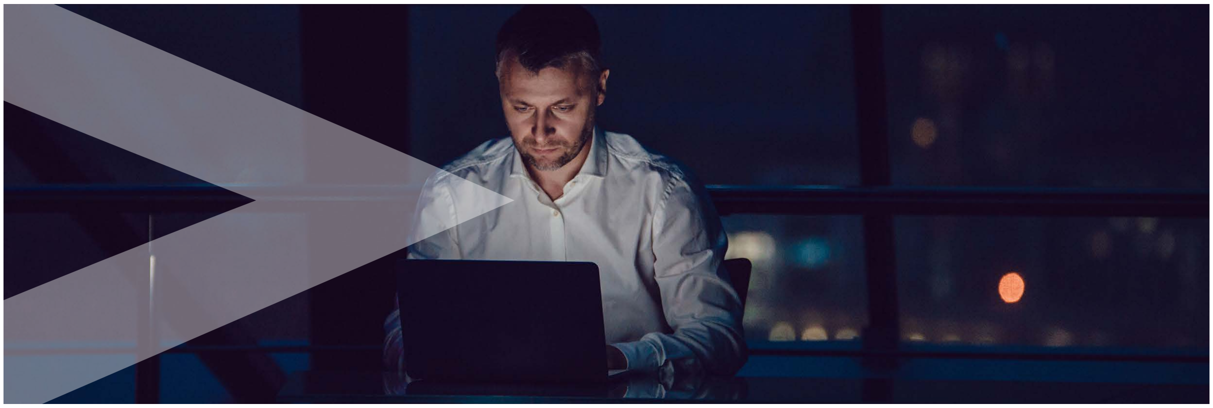
Why is it so difficult for IT teams to quickly solve these types of network outages? Unfortunately, most organizations do not have detailed information on all of the devices where a given certificate is being used. As a result, it can easily take several hours to determine these factors:

- If an expired certificate is the cause of the outage
- Where the expired certificate has been installed
- Who owns access to the machines that may be using the expired certificate

This lack of information is surprising given that the cost of certificate-related outages can easily top seven figures, with severe outages costing much more. According to some reports, the recent Ericsson/O2 outage, which was caused by an expired certificate and caused 32 million customers to lose mobile phone and data services, may end up costing over £100 million.[1]

In addition to the direct financial costs, severe certificate-related outages can disrupt internal and external customer experiences, causing grave damage to corporate brands and reputations. But despite these extreme business pressures, the study found that most organizations still routinely experience unplanned certificate expirations leading to outages on critical infrastructure.

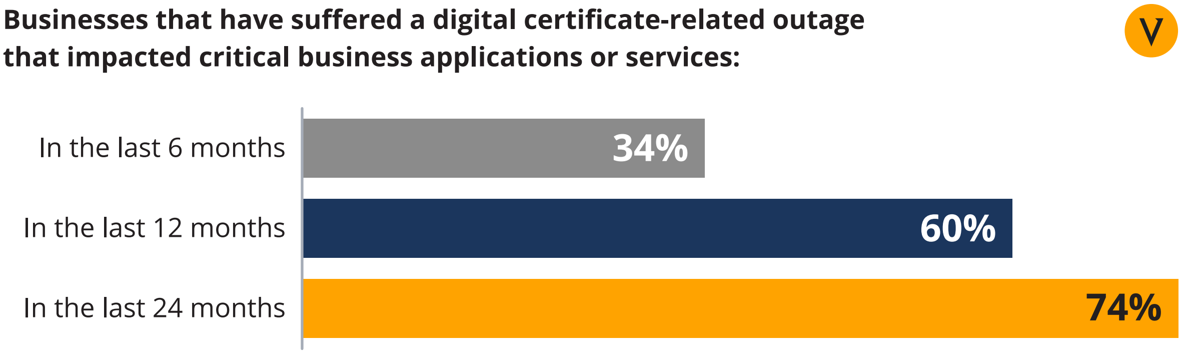
To better understand the frequency and scale of this problem, Venafi sponsored a study by market research firm Vanson Bourne of 500 CIOs from five countries: United States, United Kingdom, France, Germany and Australia. The study explores how often certificate-related outages impact business critical infrastructure and how these outages affect CIOs and their businesses.



// Key Finding: Almost Two-Thirds of CIOs Experienced Critical Certificate-Related Outages Over the Past Year

Globally, over 60 percent of the CIOs surveyed experienced certificate-related outages that affected critical business applications or services within the last 12 months. Moreover, almost three out of every four respondents experienced this type of outage within the past two years.

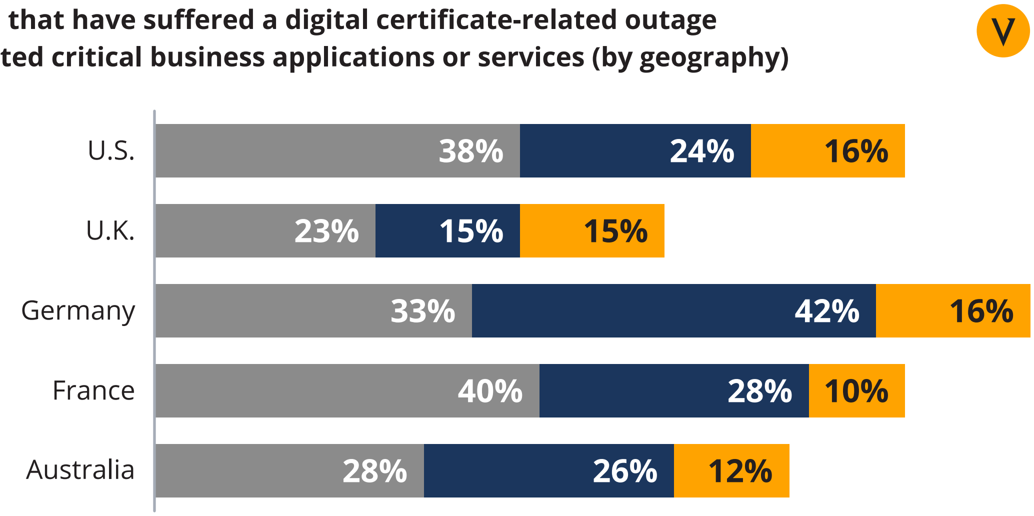
Businesses that have suffered a digital certificate-related outage that impacted critical business applications or services:



Some variance exists among respondents in each of the five countries surveyed. The U.S. respondents came closest to the overall average, with 61.5 percent reporting certificate-related outages over the past year. In contrast, 75 percent of German respondents suffered at least one outage over the past year, and 91 percent said they have experienced a certificate-related outage within the last two years.

At the other end of the spectrum, only 38 percent of U.K. respondents experienced a certificate-related outage over the past year. However, this survey was completed before the Ericsson outage, and the fallout from that event may change the level of attention U.K. CIOs devote to this problem moving forward.

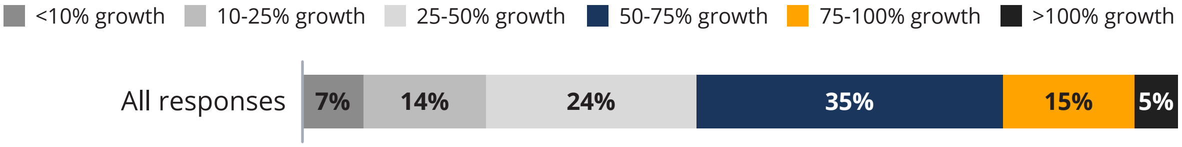
Businesses that have suffered a digital certificate-related outage that impacted critical business applications or services (by geography)



// Outage Problems Will Get Worse Before They Get Better

Because the number of certificates in use is a critical factor in these kinds of outages, the CIOs in this study were asked to estimate the growth of digital certificates used in their organizations over the next five years. Almost 80 percent of respondents estimated certificate use in their organizations will grow by 25 percent or more, and over half anticipate minimum growth rates of more than 50 percent. These numbers average out to a 53 percent anticipated growth rate in certificates across all five countries. In other words, if the average large organization has 100,000 certificates across its environment in 2018, that organization can expect to add 53,500 more certificates over this time period.

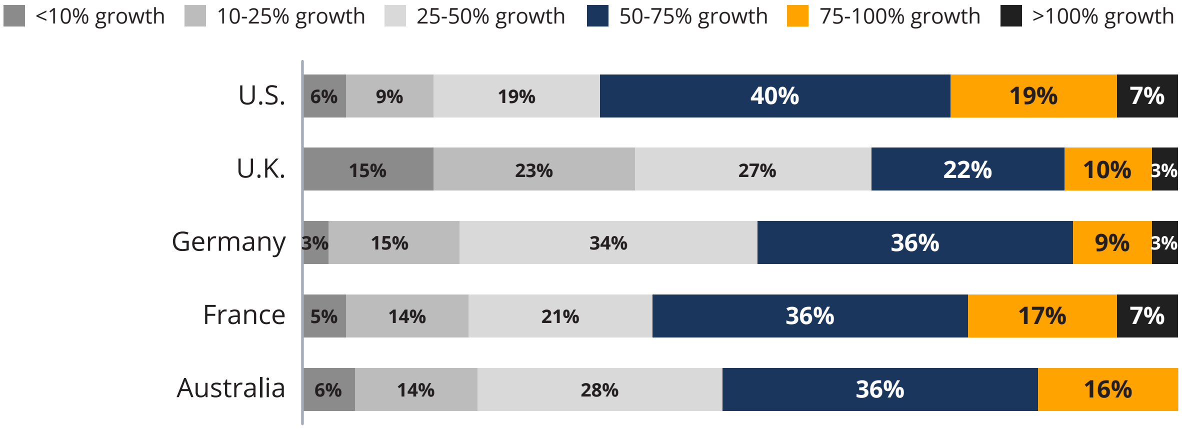
Estimated percentage of growth in digital certificate use over the next five years



While all five countries hewed close to the overall average, a significantly higher percentage of U.S. CIOs (65.5 percent) estimated digital certificate growth at 50 percent or higher. In contrast, CIOs from the three European countries and Australia estimated a higher percentage of growth in certificates to fall between the 25–50 percent range than the U.S.

Interestingly, the division between CIOs at large companies (defined as 3,000 or more employees) and those at smaller companies (1,000–2,999 employees) who predicted at least a 25 percent certificate growth rate differed by only 1.5 percent, suggesting that the digital certificates growth rate is consistent, regardless of company size.

Estimated percentage of growth in digital certificate use over the next five years (by geography)



// Are CIOs Underestimating the Number of Certificates on Their Networks?

Although these numbers indicate CIOs know that certificate-related outages are likely to increase in size and scope, there are several reasons to believe that CIOs are still underestimating how rapidly this problem is growing.

For one thing, research shows most organizations tend to misjudge the number of certificates they currently have. In July 2018, Venafi conducted a TechValidate survey that revealed, on average, IT professionals found an additional 57,420 SSL/TLS keys and certificates they didn't know they had in their networks once they deployed a comprehensive certificate discovery solution.[2] In itself, this number is troubling. Arguably more distressing, however, is the fact that the number of unaccounted for certificates has almost quadrupled since this exact same survey question was asked in 2015.[3] The mainstreaming of cloud computing and DevOps methodologies means that new machine types, including containers, smart applications, APIs and a range of IoT devices—all of which need digital certificates to serve as machine identities—will only cause the number of certificates in use to increase more rapidly in the years ahead.

This problem is compounded by shorter certificate lifespans. Starting in March 2018, the CA/Browser Forum dropped the maximum validity period of SSL/TLS certificates from three years to two, and free certificate authorities (CAs), most notably Let's Encrypt, issue certificates that expire in 90 days. The drive to shorten certificate validity periods is part of a broader recognition by the security community of the foundational role digital certificates and cryptographic keys play in data security and privacy. Experts predict this trend will continue,[4] and so we should expect certificate lifespans to continue to shrink. In addition, certificates are also required for virtual, cloud and DevOps infrastructure designed to meet elastic demands.

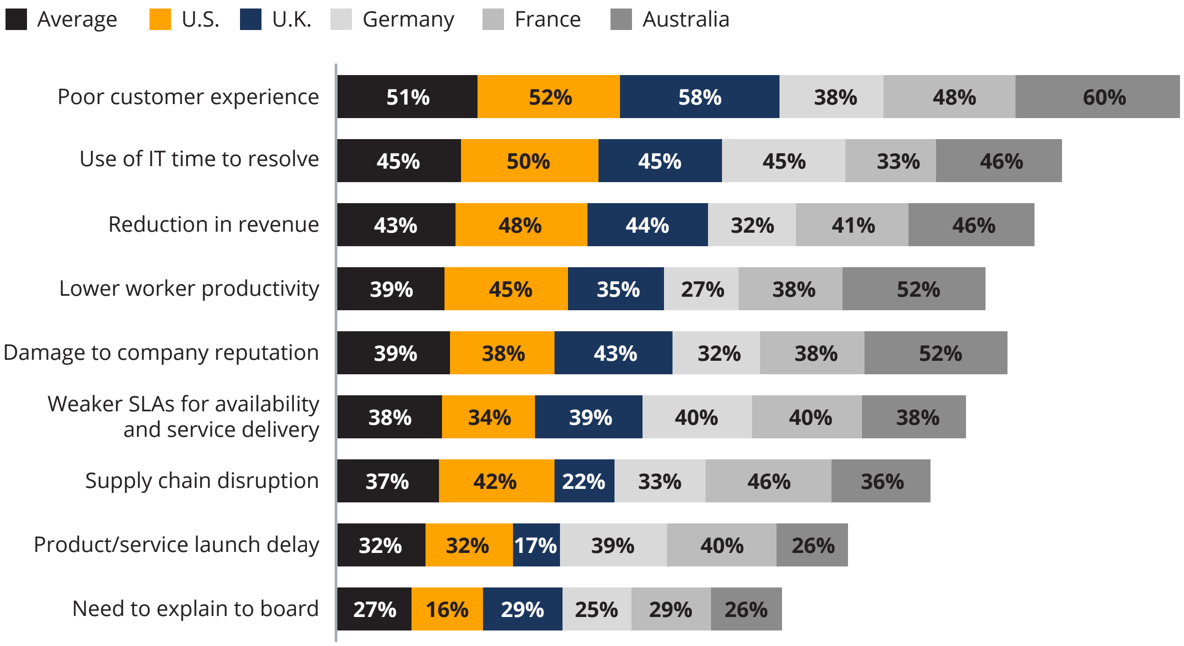
Each of these two factors—organizations misjudging the number of certificates they have and requirements for shorter certificate lifespans, when taken separately, suggests that CIOs will face increased complexities as they work toward minimizing the number of certificate-related outages going forward. When taken together, however, CIOs are all but guaranteed to face significantly greater difficulties in managing certificate-related outages over the next five years, unless they treat the management of machine identities as a fundamental component of their IT security and operations plans and invest in technology that provides visibility, intelligence and automation of the entire certificate lifecycle.

// The Business Impact of Certificate-Related Outages

As part of this study, the CIOs surveyed were given a list of nine potential business concerns they could face in the event of a certificate-related outage and instructed to select those most relevant to them.

The overwhelming majority had multiple worries in all nine areas, ranging from supply chain disruptions (42 percent of U.S. CIOs) to facing an angry board of directors (29 percent of U.K. and French CIOs). The top five concerns were similar from country to country.

Business impact concerns from certificate-related outages



// Certificate-Related Outages Impact Customer Experience, Revenue and Company Reputation

The potential impact outages could have on customer experiences is the top concern shared by half of all respondents. Poor customer experiences due to outages was of greatest concern to CIOs in the U.K. and Australia, at 58 percent and 60 percent, respectively.

Impact on business revenue frequently goes hand-in-hand with customer experience. For example, if an outage brings down an e-commerce website, customers are unable to purchase products or services while it is offline. Other examples of customer experience disruptions include the inability to gain valuable information about a potential product purchase because of a downed website and data loss in regulated industries that may lead to fines, penalties and litigation.

Revenue impact was a concern for about 43 percent of CIO respondents across all regions. CIOs based in the U.S. scored it the highest at 48 percent, with Australia and the U.K. following close behind at 46 percent and 44 percent, respectively. However, German CIOs differed significantly from the overall average, with only 32 percent citing it as a potential issue.

Finally, over 39 percent of the CIOs surveyed cited company reputation as one of their top five concerns. Organizations understand the importance of reputation, which directly impacts customer and prospect confidence in the brand—potentially diminishing sales and revenue. Plus, potential investors and partners might be reluctant to commit to a company that appears to be plagued by reliability and availability issues from severe and repeated outages. That lack of validation could lead to problems securing loans, setting up favorable deals with potential partners and, in extreme cases, shareholder confidence.

// Certificate-Related Outages Impact Scarce IT Resources and Worker Productivity

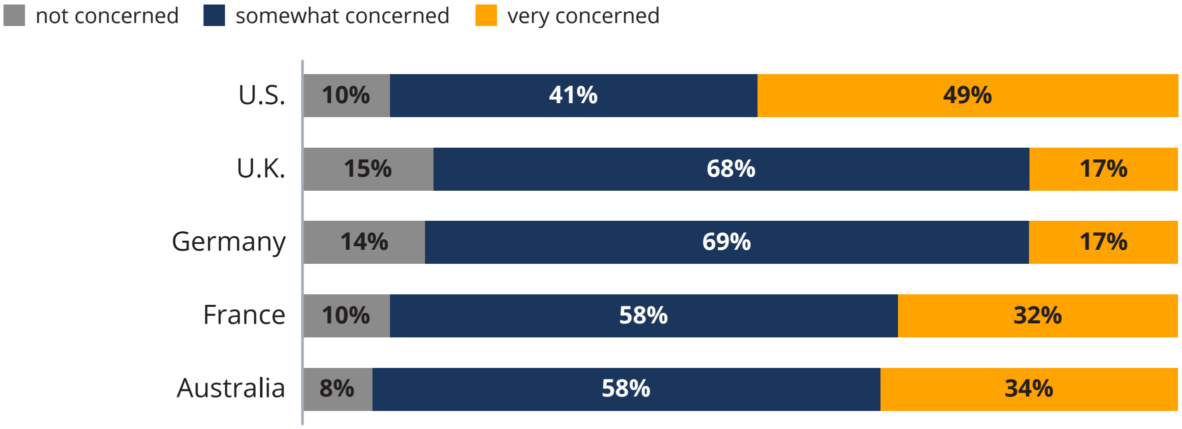
A substantial number of CIOs (almost 45 percent) across all regions expressed concern about the impact certificate-related outages have on IT resources. U.S.-based CIOs were more worried than CIOs from the other countries, with 50 percent citing unease about IT resources. In contrast, French CIOs were the least concerned, at 33 percent.

Similarly, 39 percent of CIOs were worried that certificate-related outages could disrupt worker productivity. The digital transformation of businesses means that more business processes have moved or are in the process of moving online. Workers routinely use SaaS solution apps for everything from complex manufacturing tasks to Microsoft Office. If these services are offline for an extended period of time, worker productivity is compromised.

// Increasing Machine-to-Machine Interdependencies Create More Worries for CIOs

The overwhelming majority of CIOs in this study (more than 88 percent) expressed concern about the increased complexities and interdependencies caused by the surge in machine-to-machine communications, as well as the resulting challenges. This finding reflects the new reality businesses face—IT infrastructure is required to manage nearly every aspect of an organization, and digital certificates are essential in providing machine identities for automated machine connections. As a result, organizations face steady increases in complexity connected with managing the lifecycle of digital certificates required for all the machines they use. This finding is consistent across each of the countries surveyed.

Concerns that increasing interdependencies between technologies and services will make certificate-related outages more painful



// Digital Certificate Management Needed for Outage Prevention

Given the frequency, scale and potential impact of certificate-related outages, it may seem surprising that CIOs have not solved this problem. As corporate networks continue to grow in complexity with the addition of more machines, HTTPS traffic and stronger controls on the flow of data, the need for visibility, intelligence and automation surrounding machine identities, including the creation, installation and lifespan of all digital certificates, is becoming more pressing than ever before.

Yet according to a recent study conducted by Forrester Consulting,[6] 70 percent of companies from these five countries admit they track fewer than half of the most common types of machine identities. The results of both the Vanson Bourne and Forrester Consulting studies, along with the increasing number of machine identities and complexities of the resultant networks they inhabit, demonstrate an urgent need to solve the problem of certificate-related outages. CIOs are confronting an untenable drain on IT resources and increasing scrutiny by customers, partners, investors and regulators.

In many cases, organizations are actively investing in solutions to help resolve this problem. But they are using internal databases that track certificates, dashboards from authorized CAs, and internally developed custom software tools. Unfortunately, this mishmash of point and homegrown solutions has serious shortfalls. Databases designed to track certificates often need to be manually updated, increasing the potential for human error, and many don't contain critical pieces of data necessary to resolve a certificate-related outage quickly. Meanwhile, even if the sheer volume of certificates didn't make this task unattainable, using any manual process to keep track of certificates is nearly impossible in the wake of shrinking certificate validity periods and increasingly complex networks, most of which include multiple cloud instances and changing virtual infrastructure. Because none of these approaches eliminates certificate-related outages entirely, automation has become essential.

Although CA-provided dashboards can provide some automated certificate discovery capabilities, they cannot provide the crucial intelligence necessary to prevent outages, including all IP addresses where each certificate is being used, the owner of the machines where it has been installed, and automated processes to replace it, as well as all the certificates that chain up to it if it is a root or intermediate certificate. And while these tools have some policy enforcement capabilities, any organization that uses multiple CAs will have difficulty standardizing policy enforcement across different tools.

Because of these shortcomings, many organizations have concluded that the only solution is custom, internally developed software. And while this approach initially provides some relief for CIOs suffering from regular certificate-related outages, the problem is complex enough that these tools require deep, long-term investments. Moreover, even significant investment does not guarantee internal tools can reliably provide accurate visibility and intelligence on the ephemeral certificates used in both cloud and DevOps environments.

Finally, none of these homegrown solutions, regardless of the combination, supplies the capability to consistently apply corporate security policies across a hybrid IT environment. And while these solutions may have helped CIOs limit the number of outages on their networks, they don't succeed in preventing them entirely. And as the number of machines on enterprise networks climb and the duration of certificates gets shorter, there is no way these approaches can effectively scale to solve machine identity outages in the future, let alone eliminate the risk today. You may think you are saving money by building on these various solutions, but these jury-rigged solutions end up being more expensive than anticipated—and still fail to prevent certificate-related outages.

// Conclusion: Use a Structured, Holistic Certificate Management Program

To eliminate your risk of outages, you need to be able to discover, track and continuously monitor all of your certificates in real time across your entire enterprise network, including those used in the cloud and in virtual and DevOps environments. In complex, rapidly changing networks, this is a tall order.

So, how do you start to address the problem? Here are five steps Venafi recommends you take to eliminate outages in your organization:

1. **Discover all certificates.** Choose a discovery tool that allows you to look across your entire extended network—including cloud and virtual instances and various CA implementations. This will help you locate every certificate that can impact the reliability and availability of your organization's critical infrastructure.
2. **Create a complete inventory.** Catalog your entire inventory of certificates and store it in a centralized repository where you can track and manage the status and details of all certificates. This makes it easy to rotate your certificates before they expire.
3. **Verify security compliance.** Invest in a solution that will ensure all certificates have the proper owners, attributes and configurations no matter which CA issues them. This will guarantee all certificates meet key security regulations.
4. **Continuously monitor certificates.** Conduct nonstop surveillance of all certificates so that you'll know well in advance if a certificate is going to expire, giving you ample time to replace it. This approach also helps detect and prevent certificate fraud and misuse, addressing critical security concerns.
5. **Automate renewals.** Eliminate the risk of human error by automating certificate renewals, so you can install, configure and validate certificates in seconds. You'll not only improve availability, but you'll be able to do it in a fraction of the staff hours previously required.

As networks become more complex and the number of devices, applications and algorithms that require machine identities rise, CIOs who do not adopt a machine identity protection strategy will suffer from more outages, and the direct and indirect costs of certificate-related outages will continue to escalate. The only way to eliminate these problems is with a program that delivers comprehensive, up-to-date visibility for every machine identity in use across the organization and detailed intelligence on where and how it is being used. Forward-looking CIOs who put these programs in place will then be able to leverage automation that can replace certificates before they expire, no matter where they are used, eliminating risks to reliability and availability and freeing up IT resources to focus on other tasks.

Learn how Venafi can help your organization stop certificate-related outages that threaten security and disrupt business: www.venafi.com

Trusted by:

5 OF THE 5 Top U.S. Health Insurers
5 OF THE 5 Top U.S. Airlines
3 OF THE 5 Top U.S. Retailers
4 OF THE 5 Top U.S. Banks
4 OF THE 5 Top U.K. Banks
4 OF THE 5 Top S. African Banks
4 OF THE 5 Top AU Banks

About Venafi

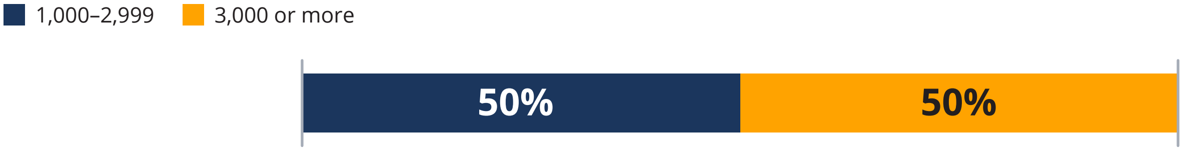
Venafi is the cybersecurity market leader in machine identity protection, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to- machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access.

To learn more, visit www.venafi.com

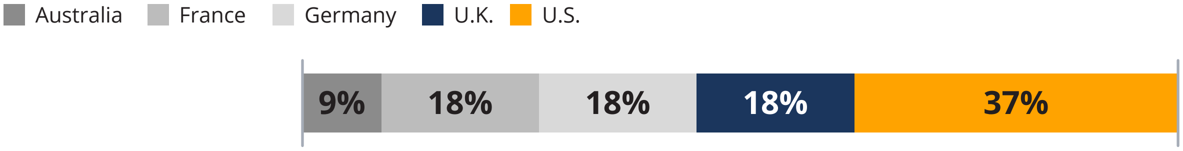
Study Demographics

This study was conducted by market research firm Vanson Bourne in December 2018.

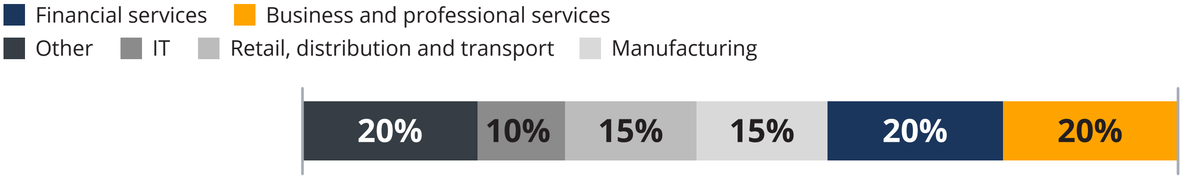
How many employees does your organization have in your country?



What country do you reside in?



Within which sector is your organization?



References

1. Source: Williams, Christopher. The Telegraph. O2 to slap Ericsson with multi-million pound bill over network failure. Dec. 8, 2018.
2. Source: TechValidate. TVID: 997-36B-8D1
3. Source: TechValidate. TVID: 363-53E-598
4. Source: Helme, Scott. Why we need to do more to reduce certificate lifetimes. Feb. 23, 2018.
5. Source: Ydstie, John. NPR. How Germany Wins At Manufacturing — For Now. Jan. 3, 2018.
6. Source: Forrester Consulting. Securing The Enterprise With Machine Identity Protection. June 2018. Study commissioned by and conducted on behalf of Venafi.