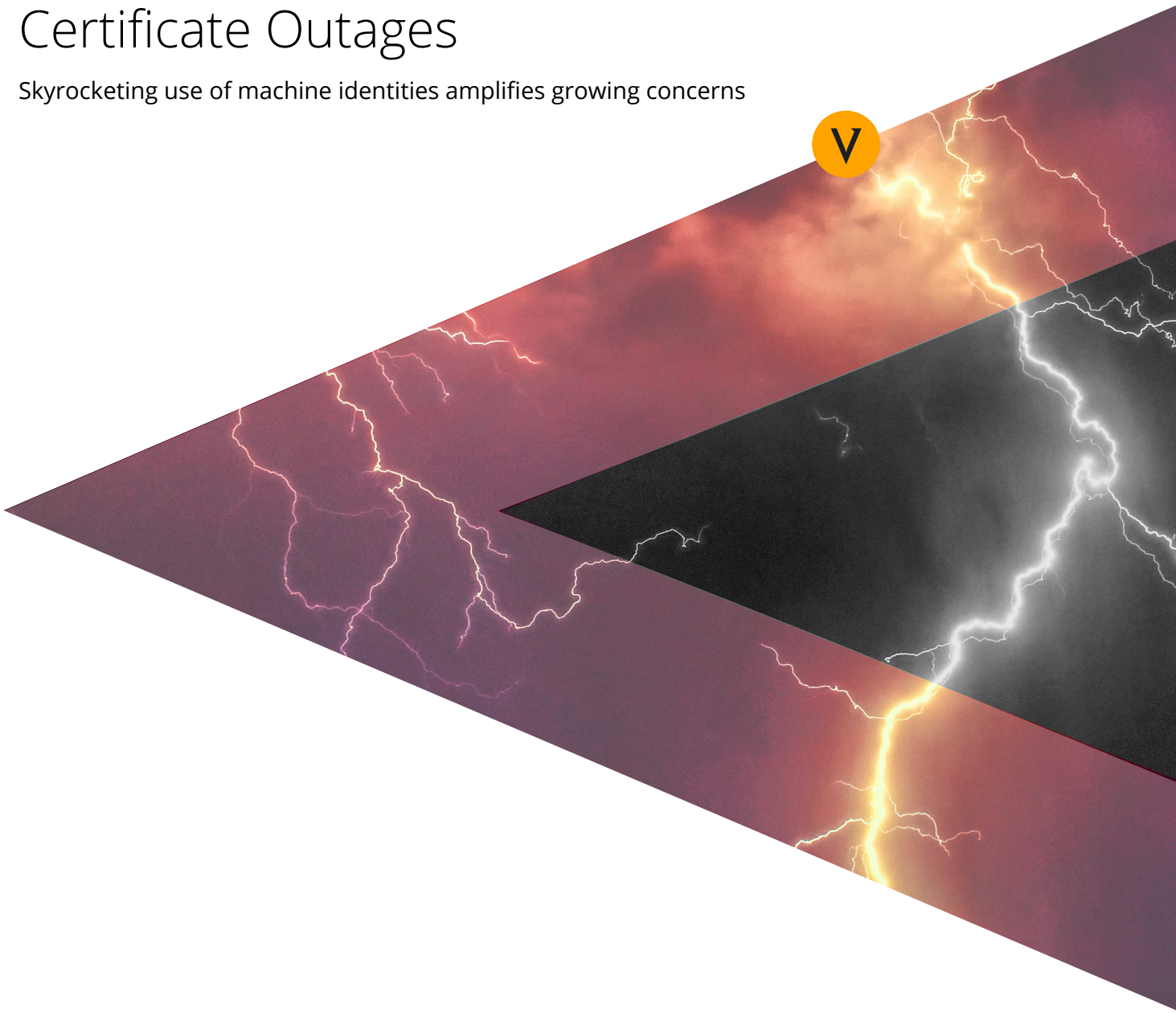
VENAFI®

// CIO Study: Financial Services Organizations at High Risk for Certificate Outages

Skyrocketing use of machine identities amplifies growing concerns



// Executive Overview

Outages caused by expired digital certificates are a common problem plaguing financial services organizations, regardless of their size or region. Despite the direct and indirect costs of certificate-related outages on critical infrastructure, CIOs of financial services organizations still struggle to overcome this growing concern. New research by Vanson Bourne shows that certificate outages are a growing and costly challenge: Of the industry CIOs surveyed in this study, 61% have experienced certificate outages within the previous 12 months.

Additional data points, which are discussed in the body of this study, support the conclusion that financial services CIOs are troubled by the repercussions of certificate outages, including:

- The impact a certificate outage may have on their organizations' reputations
- The skyrocketing use of digital certificates in the financial services sector due to digital transformation
- The concern that future certificate outages will be more painful because of increasing interdependencies among technologies and services that require machine identities

In addition to evaluating the results of the Vanson Bourne study, this white paper provides a list of best practices financial services organizations can begin implementing immediately 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 financial services 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 outages occur on critical infrastructure, the costs can increase dramatically.

And these costs can 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 ones 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 the following 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 outages can easily top seven figures, with severe outages costing much more. According to some reports, the December 2018 Ericsson/O2 outage, which was caused by an expired certificate that left 32 million customers without mobile phone and data services, has been estimated to have cost over £100 million.

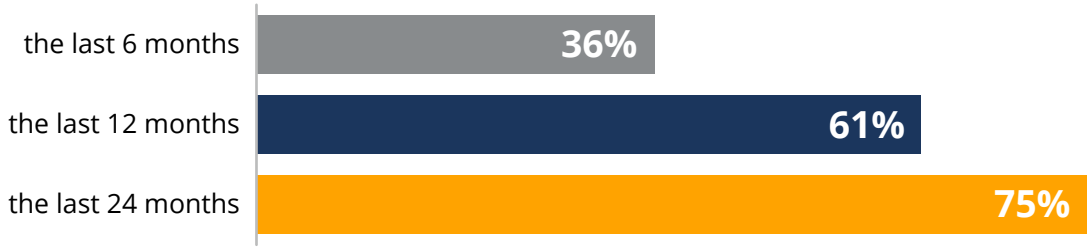
In addition to the direct financial costs, severe certificate outages can disrupt internal and external customer experiences, causing grave damage to financial services brands and reputations. But despite these extreme business pressures, most financial services organizations still routinely experience 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 more than 100 financial services 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 financial services CIOs and their organizations.

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

According to survey respondents, 61% of financial services CIOs surveyed have experienced certificate outages that have affected business applications or services within the last 12 months. Moreover, three out of every four respondents experienced this type of critical outage over the two years prior to taking this survey.

My business has suffered a from a digital certificate outage that has impacted critical business applications or services in...



// 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 financial services CIOs in this study were asked to estimate the growth of digital certificates used in their organizations over the next five years. Almost 83% of respondents predict certificate use in their organizations will grow by 25% or more, and more than 56% anticipate minimum growth rates of more than 50%. These numbers average out to a 56.5% 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 56,500 more certificates over the next five years.

In the next five years, what proportion do you expect your business' use of digital certificates to increase by?

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

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

For one thing, research shows most organizations in all major industries tend to misjudge the number of certificates they currently have. For example, Venafi conducted a July 2018 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 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 infrastructures designed to meet elastic demands.

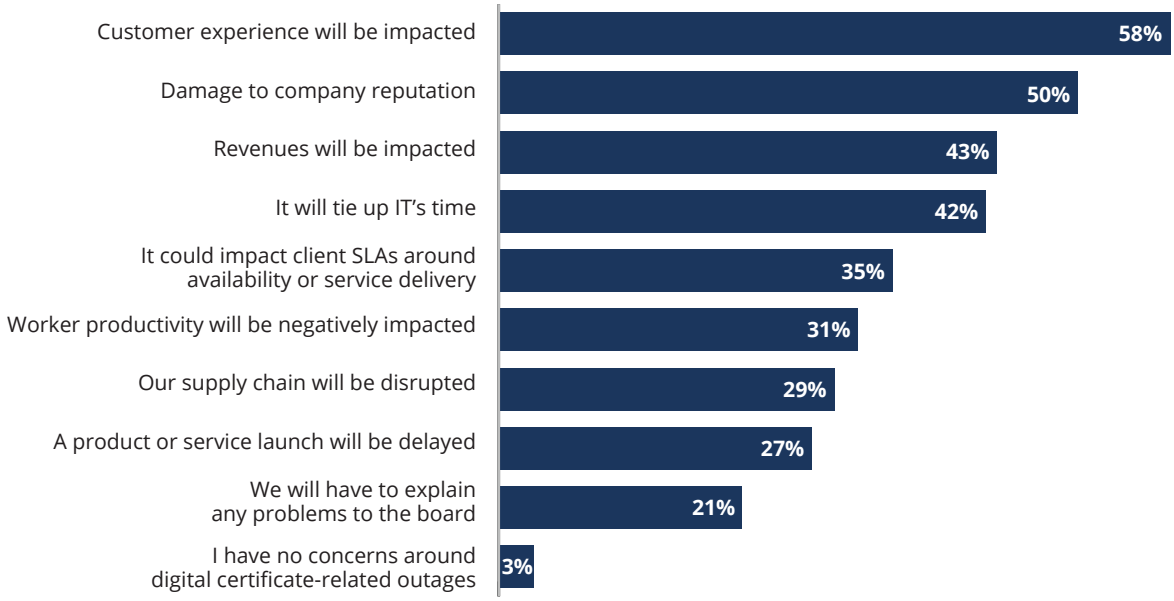
Each of these two factors—organizations misjudging the number of certificates they have and requirements for shorter certificate lifespans—when taken separately, suggests that financial services organizations will face increased complexities as they work toward minimizing the number of certificate-related outages going forward. When taken together, however, CIOs in this industry are all but guaranteed to face significantly greater difficulties in managing certificate-related outages over the next five years. They can avoid this if 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 Outages for Financial Services Organizations

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

More than 97% of respondents had multiple worries in all nine areas, ranging from poor customer experience (58.2%) to facing an angry board of directors (21%). However, the three most common worries for financial services CIOs revolved, not surprisingly, around implicit or overt financial concerns.

What are your biggest concerns around your business experiencing digital certificate outages?



Concerns over degrading customer experience scored highest among financial services CIOs, at almost 60% overall. Respondents from the U.S., U.K. and Australia scored above the overall rate, with percentages of 62.5%, 60% and 70% respectively, although 50% of French and German CIOs shared the same concern.

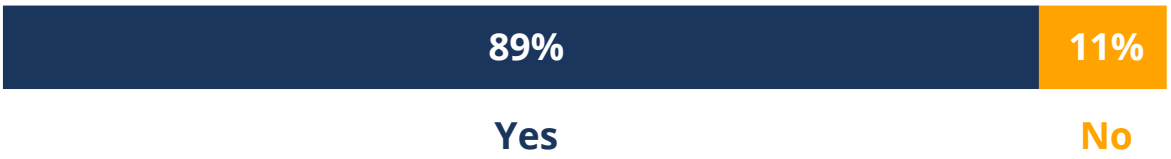
Impact on business revenue frequently goes hand-in-hand with customer experience. For example, if an outage brings down a bank's mobile app, customers may be unable to check their balances or make money transfers. Other examples of disruptions in customer experience in the financial services industry include customer data loss that could lead to fines, penalties and litigation, as well as preventing partners from offering related services to customers. Revenue impact was a concern for almost 43% of respondents.

Finally, 50% of financial services CIOs cited company reputation as one of their top three concerns. Organizations understand the importance of reputation, which directly impacts customer and prospect confidence in the brand—potentially diminishing sales and revenue. Plus, prospective 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.

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

According to this study, almost 90% of financial services CIOs in this study 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 to 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 of the machines they use. This finding is consistent across each of the countries surveyed.

Are you concerned that the increasing interdependencies between technologies and services will make digital certificate outages even more painful in the future of your business?



// Digital Certificate Management Needed for Outage Prevention

Given the frequency, scale and potential impact of certificate-related outages, it may seem surprising that financial services CIOs have not solved the problem. Corporate networks continue to grow in complexity with the addition of more machines, increased HTTPS traffic and stronger controls on the flow of data. Because of this, 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.

A recent study conducted by Forrester Consulting covering multiple industries, including financial services, found that 70% of companies admit they track fewer than half of the most common types of machine identities.[5] 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. Financial services CIOs are confronting an unsustainable 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, which increases the potential for human error. And many databases don't contain critical pieces of data that are necessary to resolve a certificate 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 these approaches do not eliminate certificate 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 of 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 machine types.

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 financial services CIOs suffering from regular certificate 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, supply the capability to consistently apply corporate security policies across a hybrid IT environment. And even if these solutions have helped financial services 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 continues to 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

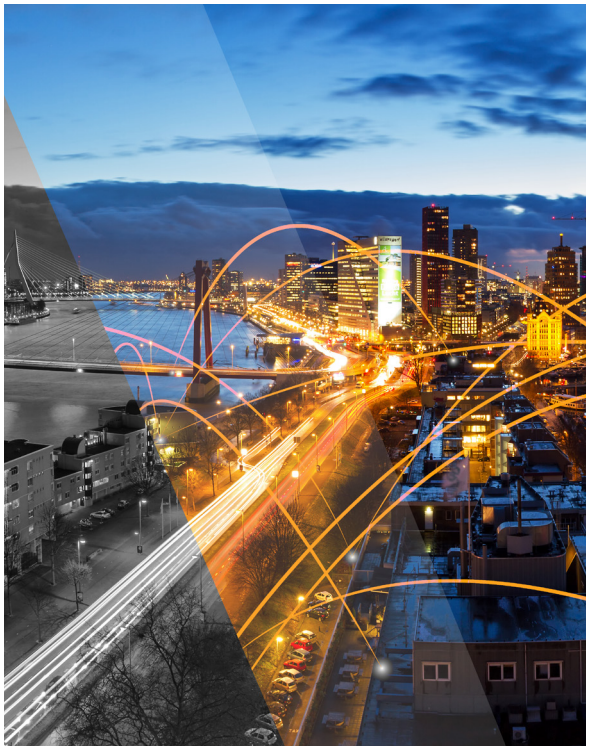
To eliminate your risk of outages, you need to be able to discover, track and continuously monitor all of your certificates in real time across your entire enterprise network—including those used in the cloud and in virtual and DevOps environments. In complex, rapidly changing networks, this is a tall 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.
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 increases, financial services CIOs who do not adopt a machine identity protection strategy will suffer from more outages. In addition, 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 financial services 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: **venafi.com**



Study Demographics

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

References

1. Williams, Christopher. The Telegraph. O2 to Slap Ericsson With Multi-Million Pound Bill Over Network Failure. December. 8, 2018.
2. TechValidate. TVID: 997-36B-8D1
3. TechValidate. TVID: 363-53E-598
4. Helme, Scott. Why We Need to Do More to Reduce Certificate Lifetimes. February. 23, 2018.
5. Forrester Consulting. Securing The Enterprise With Machine Identity Protection. June 2018. Study commissioned by and conducted on behalf of Venafi.

Trusted by

5 OF 5 TOP U.S. Health Insurers
5 OF 5 TOP U.S. Airlines
3 OF 5 TOP U.S. Retailers
3 OF 5 TOP Accounting/Consulting Firms
4 OF 5 TOP Payment Card Issuers
4 OF 5 TOP U.S. Banks
4 OF 5 TOP U.K. Banks
4 OF 5 TOP S. African Banks
4 OF 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 venafi.com