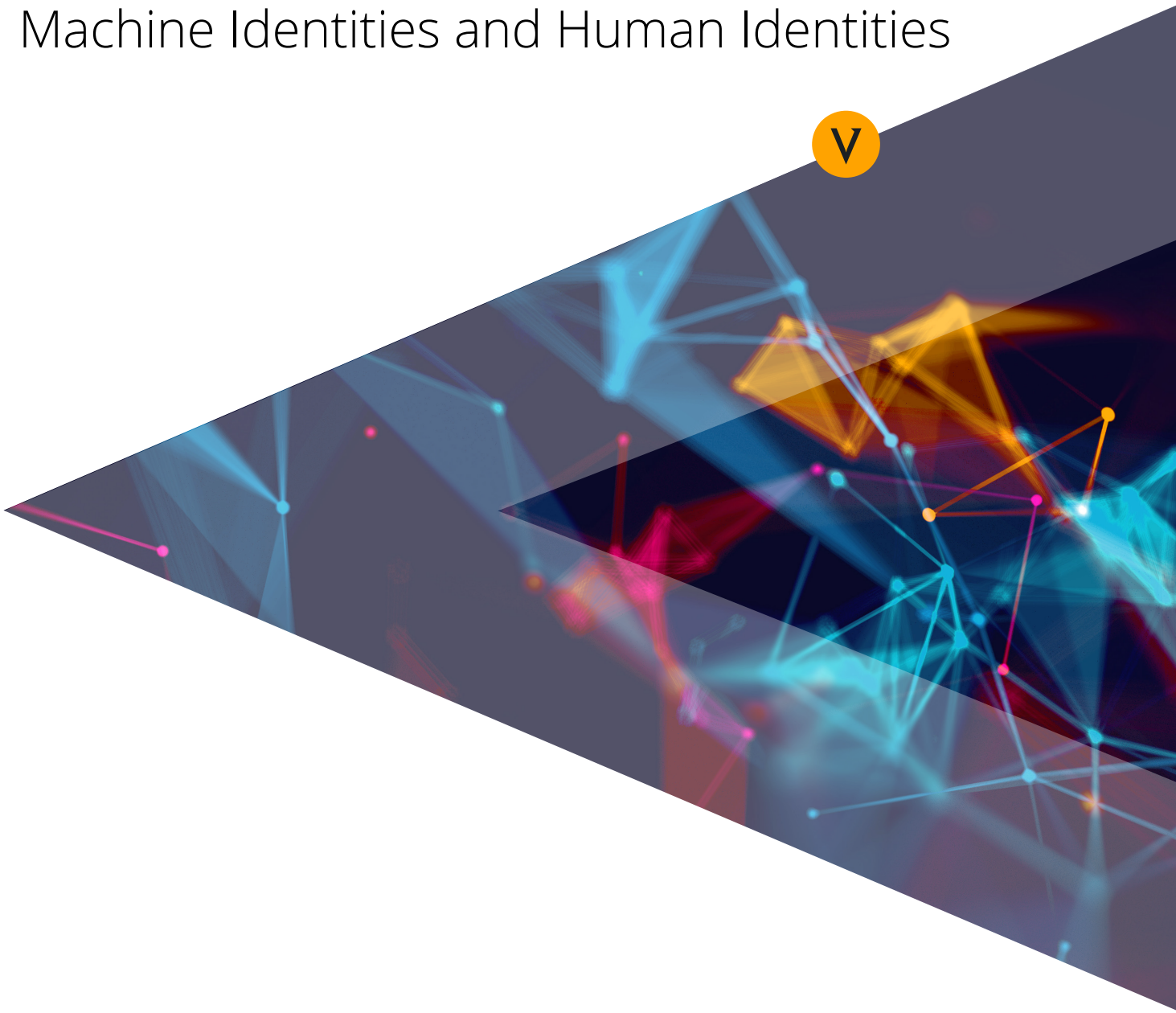
VENAFI®

// Venafi Research Brief: Comparing Security Controls for Machine Identities and Human Identities



// Introduction

On any network, there are two actors: people and machines. People rely on usernames and passwords to identify themselves to machines so they can access networks and data. Machines also need to identify themselves to one another. Unlike people, however, machines don't employ usernames and passwords. Instead, they use keys and certificates that serve as machine identities so they can connect and communicate securely.

Human identities have helped cybercriminals break into otherwise secure networks for years, which is one reason why organizations currently spend more than $10 billion a year to protect them. Increasingly, however, cybercriminals are finding machine identities to be even more effective attack vectors for infiltrating networks. For example, threat actors frequently hide attacks in encrypted traffic. They also are able to compromise or forge a machine identity that can fool other machines into handing over sensitive data.

Because most organizations have yet to earmark a meaningful portion of their security budgets to focus on machine identity protection, cybercriminals are taking advantage of the fact that in many organizations, machine identities are poorly protected.

To make matters worse, the attack surface connected with machine identities is expanding much faster than human identities. The number of machines being deployed on enterprise networks is growing exponentially because the types of machines that need identities is expanding beyond traditional physical devices and servers to include:

- Virtual servers and devices
- Mobile devices
- IoT devices
- Cloud instances
- Software applications and services, including APIs and algorithms
- Containers that run apps and services

Each of these machines requires an identity that must be managed throughout its lifecycle. As the number of machines continues to proliferate and the volume of identities in use continues to climb, protecting their identities from issuance to revocation is becoming more challenging. Moreover, the potential consequences brought about by ineffectively secured machine identities is proving to be extremely damaging to businesses, their customers and partners.

Stolen and Forged Machine Identities Are Becoming More Valuable—and More Accessible

New research by a prominent group of cybersecurity researchers shows that SSL/TLS machine identities, such as those that provide the highest levels of trust, have become hot commodities on the dark web. And many of these machine identities are being sold as packages with a range of complementary services, including:

- Website design services for fraudulent storefronts[1]
- Turnkey e-commerce webstores—complete with hosting and domain services and the ability to take fraudulent payments from PayPal, Stripe and other merchant payments[2]
- SSL stripping tools that prevent browsers from using an SSL connection and enable man-in-the-middle attacks[3]

As a result of these burgeoning, increasingly creative options, machine identities have become a key part of cybercrime toolkits, particularly for threat actors who lack the technical chops of a traditional hacker. In fact, the variety of stolen or forged keys and certificates—from basic TLS certificates that act as legitimate machine identities to "aged" certificates—is reflective of the growing market for such items. Moreover, the increasing demand for these types of identities suggests that the buying and selling of machine identities has become a successful industry in its own right.

The cost of machine identities, including TLS certificates, is significantly higher than the usernames and passwords that make up most human identities. In early 2019, for example, a cybercriminal offered 620 million hacked human identities from well-known websites like Whitepages and MyFitnessPal for $20,000 in Bitcoin—or about 0.00003¢ per username and password.

In comparison, machine identities, such as TLS certificates, may range in cost from $260 to $1,600 on the dark web, but they provide threat actors multiple ways of infiltrating networks. For example, cybercriminals can leverage machine identities to evade detection by hiding in encrypted traffic or impersonating a trusted machine to gain access to sensitive data or to pivot across a network. Therefore, the money spent up front for a single TLS certificate offers a higher likelihood of success and, therefore, better value overall than millions of username/password identities.

Why the Gap in Protection?

Given the impact that a stolen or fraudulent machine identity can have on an organization, why is there such a yawning gap in allocated budgets for machine identities as opposed to human identities? Among the many factors for this disconnect are:

- Rapid changes in IT infrastructure due to digital transformation have dramatically increased the volume of machines on enterprise networks that need machine identities—a changing reality organizations are only beginning to confront.
- The security and operational risks connected with the keys and certificates serving as machine identities are poorly understood.
- There has been a dearth of concrete standards and guidelines that provide organizations with prescriptive advice on how to effectively protect machine identities in a consistent, measurable fashion.

To better understand the persistent gap in applying effective security controls for human identities versus ones for machine identities, Venafi commissioned a global study of more than 1,500 IT security professionals from a range of company sizes and verticals in July 2019. The study, conducted by Dimensional Research, evaluated the differences between basic security controls for usernames and passwords and TLS machine identities, as they are widely used to encrypt many types of internet communication and transactions. Additionally, the study evaluated a few critical security controls across crucial points in both sets of identity lifecycles, including:

- Creation
- Rotation
- Audit

Although the respondents in this study appear to understand the importance of protecting machine identities and human identities, it's clear that the implementation of security controls for human identities is much more mature than those applied to machine identities.

// Comparison No. 1: Written Policies for Human Identities vs. Machine Identities

Written policies delineating how to best safeguard human and machine identities are essential because they are the first step organizations need to create measurable security controls. These policies enable security practitioners to take specific actions that will secure and protect both forms of identities. Specifically, written policies describing the complexity and rotation frequency of both types of identities provide first-level instruction organizations need to clearly understand what is required to protect them.

Written Policies for Complexity of Passwords vs. Keys and Certificates

Currently, however, organizations do not have access to the same level of guidance for defining the qualities of a certificate or private key that they do for passwords used in human identities. For example, the latest version of the Payment Card Industry Data Security Standard, PCI-DSS 3.2.1, provides specific criteria for a secure human identity. The standard not only states in multiple places, including its "High Level Overview," not to use vendor-supplied passwords or other default passwords under any condition,[5] it also states in section 8.2.3 that all passwords for human identities must meet the following benchmarks:

- Require a minimum length of at least seven characters
- Contain both numeric and alphabetic characters[6]

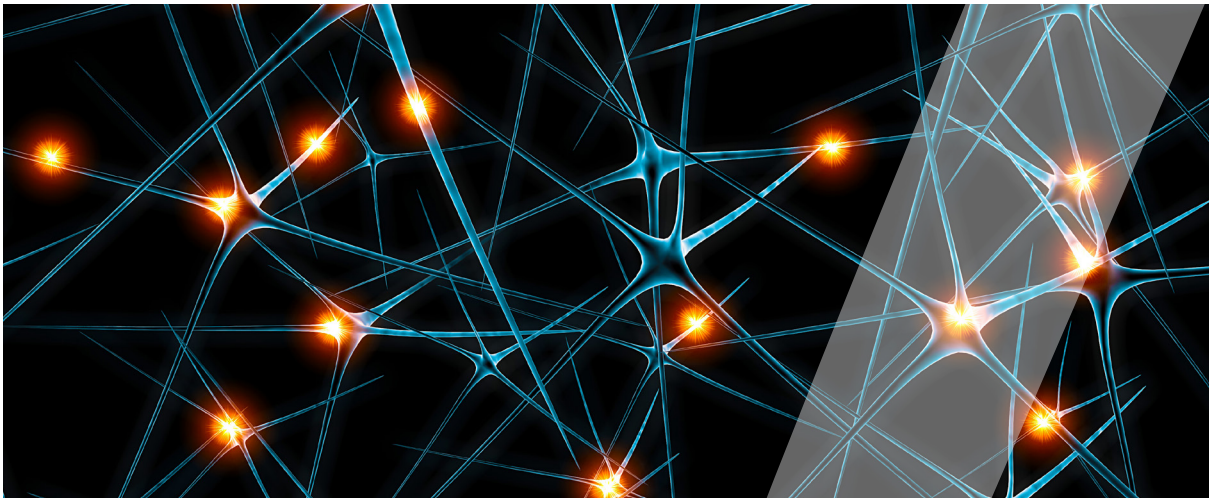
In contrast, PCI-DSS 3.2.1 only provides advice on what fails to constitute a secure machine identity:

> SSL/early TLS is not considered strong cryptography and may not be used as a security control…[7]

As a result, the PCI-DSS leaves organizations to their own devices when deciding what makes up a secure machine identity, relying on their own understanding of the situation to best determine what they can do to protect them. And that understanding may not reflect the most up-to-date information concerning machine identity protection, let alone the rigorous testing and expert reasoning that goes into defining a standard or regulation.

Therefore, it isn't surprising that questions examining the strength and complexity of human identity passwords in comparison to those of TLS machine identities show a significant disparity, as seen in the chart below.

My company has a written policy on…



This difference in prescriptive guidelines underscores why a 30-percent discrepancy might exist between the two types of written policies. If an organization isn't sure what would be an acceptable threshold for a secure certificate, defining the standards for this written policy can be problematic.

Despite this lack of clarity, however, the fact that a modest majority of respondents say they do have written policies in place for TLS key length and randomness suggests that many organizations consider the issue pressing enough to attempt to define these critical security policies.

Written Policies for Rotation Frequency of Passwords vs. Keys and Certificates

Numerous standards provide guidance on how frequently passwords should be changed and the results in the chart below show the vast majority of organizations have written policies on password rotation—but less so for certificates and private keys. For certificates, starting from March 2018, the CA/B Forum dictated that all SSL/TLS certificates issued must have a maximum lifespan of approximately two years (825 days), down from the three-year validity period that was previously enacted. However, there is also a drive by the security community to shorten certificate validity periods. But this need for frequent certificate and private key rotation is not well understood and this is reflected in fewer written policies around this important security control.

A 24-percent gap exists between respondents whose organizations have written policies in place for the frequency in which passwords are rotated as compared with rotation of certificates and private keys that make up machine identities.

My company has a written policy that states...

Written Policies for Disabling or Rotating Passwords vs. Keys and Certificates

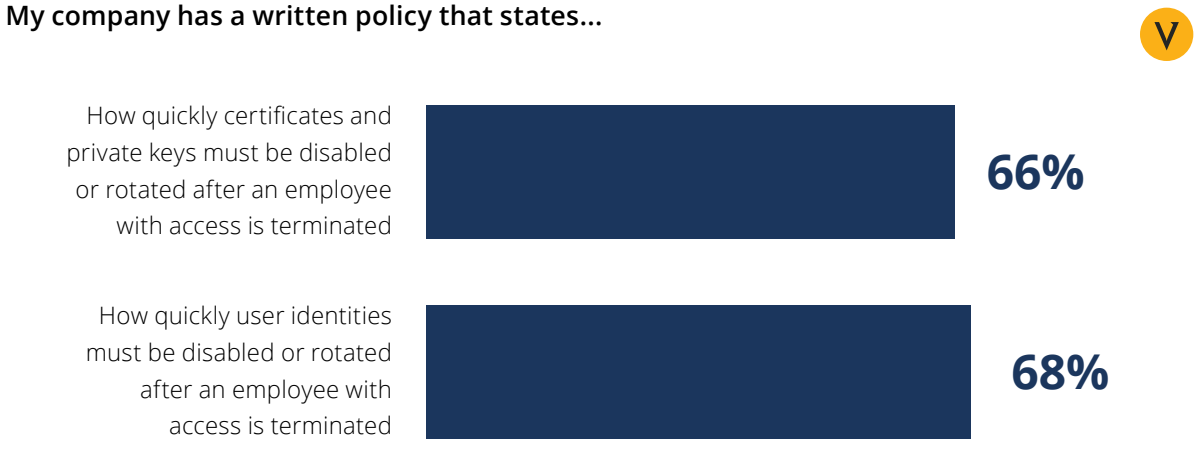
Perhaps the most important security control required for all identities—machine or human—is the one that disables it when an owner is terminated or reassigned. Allowing insider access to systems or data puts an organization at risk for a breach because of the unnecessary insider threats it poses.

Not surprisingly, the percentage difference among organizations with these types of written policies in place for usernames and passwords and those with similar written policies for certificates and private keys is fairly small (10%) relative to the percentage gaps in the first two charts. This suggests that a healthy majority of organizations understand the risks connected with unauthorized use of both types of identities and have invested in creating a set of policies that govern rotation for both. At the same time, however, it also supports the hypothesis that human identity protection guidelines are more mature than those for machine identities.

Still, it's encouraging that over two-thirds of respondents say their organization requires quick rotation or revocation of both types of identities once an employee with access is terminated. Even though most organizations may not have robust machine identity protection programs in place, they at least have some key elements of policy that indicate the importance of protecting these critical security assets.

My company has a written policy that states...

My company has a written policy that states...



// Comparison No. 2: Audit Policies for Human Identities vs. Machine Identities

The fact that a majority of respondents have written policies for the rotation of human and machine identities is reassuring. However, the 31-percent discrepancy between written policies concerning the strength of human identities versus the strength of machine identities discussed above is concerning.

At the same time, written policies are not sufficient if they are not paired with structured programs that measure the degree of their success—they are aspirational at best. Therefore, the only way to ensure the goals of these (or any) policies are being reached is through regular audits.

The results in the following two charts reflect the difference in implementation maturity between security controls for human identities and those for machine identities. A primary factor in this difference is the number of industry regulations governing human identities, including PCI-DSS, HIPAA and FISMA.

Comparable regulations governing the strength, frequency or rotation of machine identities are still vague for the most part, as evidenced by PCI-DSS 3.2.1. This is changing, however. In 2019, the National Institute of Standards and Technology (NIST) released a new framework, *NIST 1800-16B for TLS Server Certificate Management*, that offers specific guidance on protecting TLS machine identities. Despite its draft status (it is expected to go officially into effect in 2020), it already is one of the most downloaded NIST publications ever—no doubt because the need for it is so great.

It shouldn't be surprising that a significantly higher percentage (70%) of organizations currently audit for password strength than for key and certificate strength (49%) or that a similarly high percentage (72%) of organizations audit how frequently passwords are changed while just over half (53%) audit how frequently certificates and private keys should be changed. It would be surprising, however, if these percentages do not progressively grow closer in the next several years as other standards bodies use NIST 1800-16B as a blueprint for more precise guidelines going forward.

The following areas in my company are audited...

My company audits...

// Comparison No. 3: Use of Automation to Enforce Human Identities vs. Machine Identities

Automation plays a key role in making many security controls effective. Most organizations have so many human identities to protect access to data, services and applications that trying to manually perform such tasks would be an inefficient process requiring an unreasonable amount of money and human resources. Automation is necessary to maintain compliance with these security controls.

The use of automation to manage machine identities is as important as it is for human identities. And it may be more important going forward because the number of machine identities is quickly dwarfing the number of human identities.

For example, enforcing the rotation of TLS certificates is significantly more complex than doing so with passwords. Besides the volume of certificates that must be rotated, organizations must deal with a number of additional challenges that are difficult to address without the help of automation, including:

- The rotation of private keys associated with certificates
- Multiple types of certificates to rotate, all with varying lifespans
- Different time frames for renewals or revocations—something that becomes even more complex as organizations move toward the cloud and DevOps processes

Even though many organizations seem to understand the importance of automating the rotation of machine identities, it still isn't surprising that only half do so relative to human identities, as shown in the chart below. After all, if organizations have difficulty writing clear policies for securing machine identities or lack the means to effectively audit policies, they are unlikely to have the necessary building blocks to deploy automated programs that ensure these things are enforced.

My company has...

Commercial technologies to automate the management of usernames and passwords have been widely available to organizations for at least a decade. In contrast, organizations only recently have become aware of similar commercial technology solutions designed to automate TLS certificates and other machine identities. Many larger organizations have tried building in-house solutions to manage machine identity automation, but these homegrown solutions tend to be expensive to maintain and rarely scale to keep up with the volume, variety and velocity of change in the population of machine identities on enterprise networks.

The good news for organizations, however, is that technologies for automating machine identity lifecycles *are* available—and more and more, organizations are becoming aware of the need for these solutions.

// Conclusion

Based on the percentage of respondents who say they have basic machine identity policies in place, a majority of organizations grasp the importance of safeguarding their machine identities. In fact, it's gratifying that, according to the data in this study, a majority of organizations have written policies in place to secure machine identities just as they do for human identities. This is in spite of the fact that the security challenges created by the proliferation of machine identities only recently has gained traction.

Nevertheless, there is still a large number that do not have written policies in place—for some security aspects discussed above, close to half—and organizations struggle with the implementation and auditing of their written machine identity policies because they don't yet have the level of guidance they have had for human identities over the last decade or so. But new standards from regulatory bodies of all stripes can be expected to follow with more prescriptive guidance, especially now that the release of the *NIST 1800-16B* framework provides a template for protecting TLS machine identities.

NIST 1800-16B explains the use of TLS server certificates:

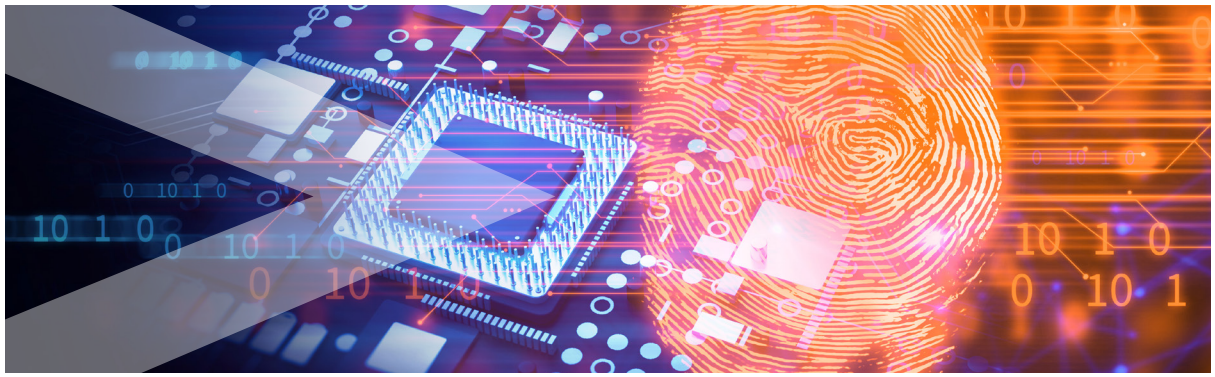
> TLS server certificates serve as machine identities that enable clients to authenticate servers via cryptographic means…[8]

The framework then provides specific definitions, as well as best practices, for TLS server certificate management. This new standard provides organizations—and perhaps more importantly, other standards bodies like PCI and HIPAA—with specific parameters concerning strong machine identity security controls, including what sort of automation is needed to enforce these standards throughout the machine identity lifecycle.

This news couldn't come at a better time. Gartner analyst Ant Allen states that:

> Password policies cannot ameliorate the inherent weaknesses of passwords themselves. Security and risk management leaders responsible for IAM should not focus on crafting the perfect policy and should invest in new authentication methods and other compensating controls in line with business needs…Through the end of 2020, enterprises that invest in new authentication methods and compensating controls will experience 50% fewer identity-related security breaches than peers that do not.[9]

Although Allen's research is focused on passwords and other human identity protection methods, we believe his comments apply equally to machine identity protection. After all, if enterprises investing in new authentication methods and compensating controls for human identities can expect a significant drop in identity-related security breaches, then it makes sense that this is likely to be the case for machine identities as well. Even though most organizations are just getting started protecting machine identities, this is a positive sign that indicates a growing awareness of the critical role these security assets play in protecting sensitive data and reducing risk.



What Are Machine Identities, and How Are They Used?

Machine identities are required for a wide range of transactions including:

- **Securing web transactions with HTTPS:** Digital certificates, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS) certificates, enable encrypted connections between a web browser and web server.
- **Securing privileged access:** Secure Shell (SSH) is often used to secure system-administrator-to-machine access for routine tasks. SSH is also used to secure the machine-to-machine automation of critical business functions, such as automatically triggering operations and routine file transfers.
- **Securing Fast IT and DevOps:** Development teams are focused on speeding up the delivery of software. To do this, developers use cloud computing and software-defined containers to run individual microservices. These function as separate machines and use SSL/TLS certificates that serve as machine identities for secure authentication and machine-to-machine communication.
- **Securing communication on consumer devices:** Digital certificates are a vital element of mobile security because they provide the foundation for authenticating mobile devices that access enterprise networks. Also, mobile device certificates are increasingly being used to enable access to enterprise Wi-Fi networks and for remote enterprise access using SSL and IPSEC VPNs. In addition, mobile access to Internet of Things (IoT) devices on enterprise networks relies on certificates for authentication.
- **Authenticating software code:** Software is usually signed with a certificate to verify its integrity. Users implicitly trust products when they are signed by a reliable publisher's code signing certificates.

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

References

1. Maimon, David; Wu, Yubao; McGuire, Michael; Stubler, Nicholas and Qiu, Zijie. Evidence-Based Cybersecurity Research Group at the Andrew Young School of Policy Studies at Georgia State University and the University of Surrey. SSL/TLS Certificates and Their Prevalence on the Dark Web (First Report). 2019. 6.
2. *Ibid*. 6.
3. *Ibid*. 9.
4. *Ibid*. 2.
5. *Ibid*. 5.
6. *Ibid*. 73.
7. *Ibid*. 32.
8. Haag, William and Souppaya, Murugiah; Turner, Paul; Barker, William; Pleasant, Brett and Symington, Susan. National Institute of Standards and Technology. NIST SPECIAL PUBLICATION 1800-16B: Securing Web Transactions—TLS Server Certificate Management, Volume B: Security Risks and Recommended Best Practices. July 2019. 2.
9. Allan, Ant. Gartner. Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls. Refreshed 4 April 2019, Published 27 July 2017. 1–2.