WHITE PAPER

CIO Study: Outages Escalating with Massive Growth in Machine Identities

Uncontrolled growth challenges management and increases the risk of certificate outages and data breaches

Venafi

Exponential growth in machine identities driven by digital transformation

Digital transformation is reshaping our connected world. One of the obvious consequences of this shift is an unprecedented rise in machines on enterprise networks—all of which need to connect, authenticate and communicate securely. Also, the types of machines that need to connect securely have expanded to encompass cloud native entities, including hybrid IT environments that encompass public cloud instances (AWS, Azure, GCP), applications and services made up of microservices, containers and APIs.

The global pandemic that began in early 2020 has accelerated this already exponential growth in these new types of machines because trends, such as the dramatic increase of employees working remotely, have progressed even faster than originally anticipated and often require cloud native applications and services to address them. And all the resulting new machines require machine identities to authorize secure connections.

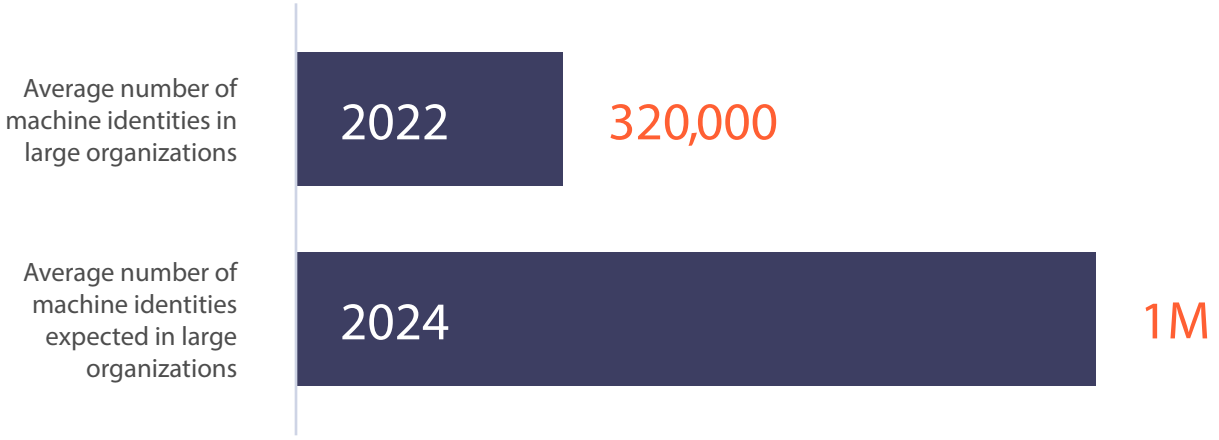
Machines are used in countless ways with lifespans that vary from years (physical servers and mainframes) to days or even minutes (containers). Not surprisingly, managing the corresponding proliferation of machine identities has become a growing problem for organizations. Many organizations are moving so quickly that they don't take time to understand the security or reliability risks connected with machine identities, particularly in multicloud environments that require markedly more machines than traditional data centers.

To better understand the frequency and scale of this problem, Venafi sponsored a study by market research firm Coleman Parkes Research of 1,000 CIOs from six regions: United States, United Kingdom, France, DACH (Germany, Austria, Switzerland), Benelux (Belgium, Netherlands, Luxembourg) and Australasia (Australia, New Zealand). The study explores how the growth of machine identities affect CIOs and their businesses.

Key Finding: 3X average number of machine identities by 2024

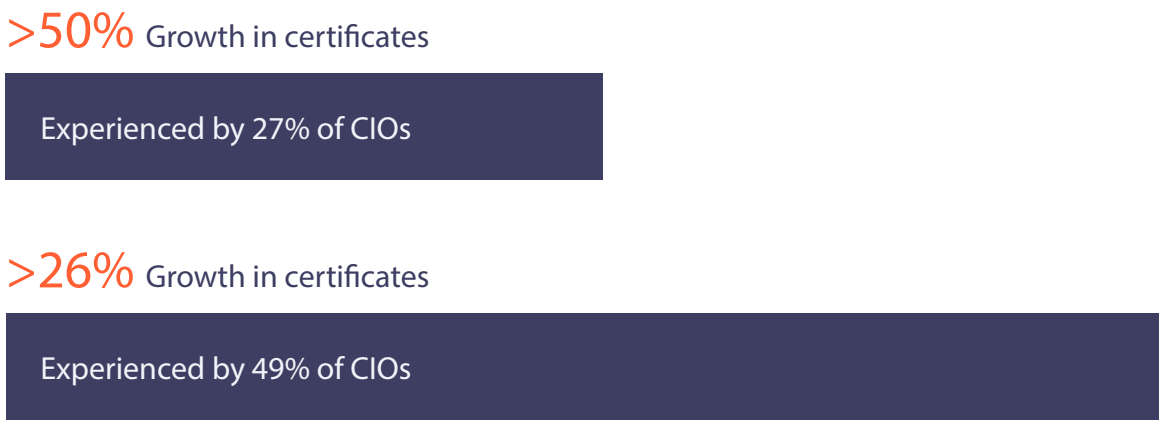
CIOs know that their organizations are using a lot of machine identities, and it's evident in the Coleman Parkes survey. Across companies of all sizes, the average number of machine identities per organization at the end of 2021 was nearly 250,000 and was estimated to increase by 42% per year.

Larger organizations faced even greater challenges. On average, CIOs at organizations with more than 10,000 employees estimated that they had more than 320,000 machine identities in their enterprises at the start of 2022. If their growth rate stays constant for the next two years, that number will more than triple to around 1 million machine identities by 2024.



Judging from their responses, CIOs are cognizant of this growth. When asked whether digital transformation initiatives have been increasing the number of machine identities used within their enterprises over the last year:

- 49% said the amount has grown between 26–50%
- 27% said the amount has grown by more than 50%



Outage risk increases with growing number of machine identities

The rapid growth in machine identities has created problems that stem from weak machine identity management. The resulting security risks not only threaten organizations themselves but also their customers, as evidenced in several publicized attacks. For example, the Equifax breach was exacerbated by an expired certificate on security infrastructure.

Certificate-related outages, typically the first and most obvious symptom of weak machine identity management, have become commonplace among enterprises. According to the Coleman Parkes survey:

83% of organizations suffered a certificate-related outage during the last 12 months

26% of the CIOs whose organizations experienced outages said these outages impacted business-critical systems.

This 83% outages number represents a sizable jump from 2019, when a Venafi-sponsored survey showed that 60% of CIOs reported at least one machine identity-related outage over the previous year. Given the unrelenting increase in the number of machine identities, organizations face a higher number of outages with more risk to their critical systems unless they dramatically change their approach to managing machine identities.

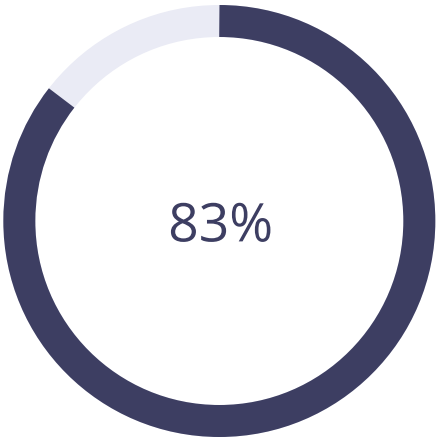
Of the companies that reported outages:

80% had a minimum of three outages per year

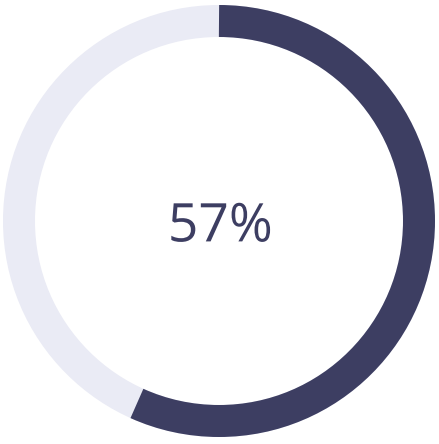
55% had 12 or more outages per year

25% had weekly outages (52+) per year

Moreover, organizations are already facing security ramifications caused by improper machine identity management, over and above outages. An incredible 57% of CIOs said they have experienced at least one data breach or other security incident related to compromised machine identities within the previous 12 months. Organizations should expect these negative consequences to accelerate as the number of machines continue to multiply—and their potential impact to be incalculable.



Experienced certificate-related outages in the past 12 months

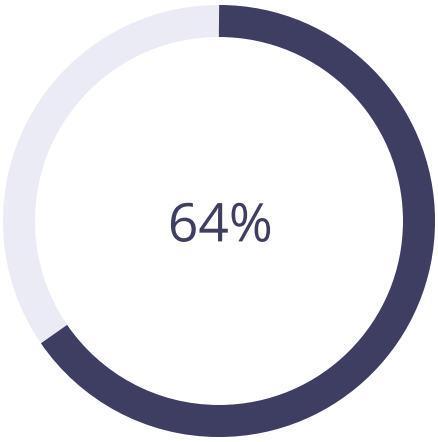


Experienced security incidents involving compromised machine identities

Scattershot management of machine identities impacts success

Why are organizations experiencing so many negative business consequences related to machine identities? A significant contributing factor is that the majority of organizations lack an enterprisewide, holistic machine identity management solution to secure machine identities across their IT environment. To be successful, organizations need to manage machine identities across physical and virtual data centers or colocation facilities, multicloud environments and networks that include mobile, IoT devices and more.

According to the survey, close to two thirds (64%) of CIOs said that rather than using a comprehensive machine identity management solution, they use various combinations of multiple solutions and processes, including point solutions from their approved certificate authorities (CAs) and public cloud providers, as well as homegrown solutions and manual processes like spreadsheets.



Use disparate solutions to manage machine identities

In addition, different business units may use different tools to procure or manage machine identities that prevent senior security leadership from gaining an overarching view of their complete machine identity inventory. This lack of unified visibility—and the seeming inability to achieve such a goal—means that despite having security policies and controls in place, CIOs don't have a means of enforcing them. This lack of consistency and control of machine identities often leads to unexpected and often costly outages, along with a plethora of security vulnerabilities.

And these mishaps can be costly. The average cost of a data breach in 2021 was $4.24 million, a 10% jump from 2020.[1]

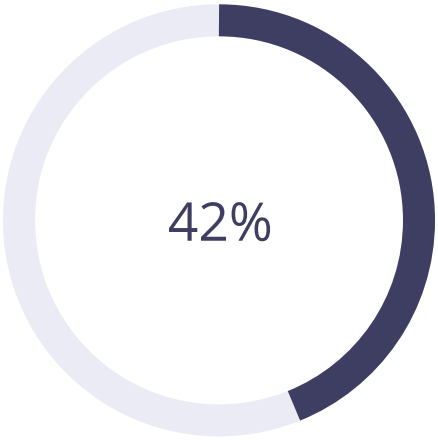
Automation is the only way to tame the scale of today's machine identities

Perhaps the biggest problem with using a hodgepodge of solutions and processes is the inability to automate machine identity management. Given the sheer number of machine identities that organizations currently have, further complicated by the 42% projected yearly growth in these numbers, automation is essential to effective management and protection of them.

In 2020, NIST published Special Publication 1800-16: Securing Web Transactions, TLS Server Certificate Management (SP 1800-16), the first framework that directly addresses specific security controls for TLS keys and certificates used as machine identities. Volume SP 1800-16B, which provides best practices and recommendations on how to develop policies for certificate management, stresses that automation should be used as much as possible for the enrollment, installation, monitoring and replacement of certificates—and any insistence on using manual methods where automation could be used to limit operational security risk must be explicitly justified.

Solutions that are cobbled together lack the integration capabilities that would enable enterprises to automate the bulk of actions required for enterprisewide machine identity management. Without a comprehensive machine identity management strategy in place, problems will only increase and place organizations at even greater risk than they are today.

Why automation is essential



Average projected growth of machine identities per year in organizations of all sizes

Conclusion: automate machine identity management to safely accelerate digital transformation

In our digitally transformed, ever more cloud native world, identity has become the new perimeter. Traditional means of securing enterprise networks are no match for the diversity of cloud instances and the applications and containers that run in them. Therefore, organizations must turn to identity as central to enterprise security of the enterprise because it's the only control that works across modern cloud native environments as well as in traditional data centers.

Companies that fail to grasp this new reality and choose not to adopt enterprisewide machine identity management solutions put themselves at grave—and unnecessary—security risk. Threat actors have moved from targeting human identities to machine identities where it is relatively easier to exploit gaps in manual processes or point tools that lack complete visibility into an organization's machine identity inventory. Such well-known exploits as last year's SUNBURST software supply chain attack and the certificate-related outages that brought down Microsoft Teams in early 2020 and Azure Active Directory in March 2021 have impacted millions of users.

Given the exponential growth of machines and their increasingly transient nature, IT and security teams are discovering that the tools and strategies they are currently using are no match for managing millions of machine identities, particularly in hybrid and multicloud environments. All it takes is the compromise of one machine identity for dangerous threat actors to access an entire network—and alarmingly, the networks of their customers and partners. The fact that 57% of CIOs have already acknowledged they have experienced a recent data breach or other security incident should raise alarms that this will only get worse unless a sea change in the way machine identities are managed and secured takes place.

A comprehensive machine identity management program leverages automation to orchestrate the many actions necessary for securing machine identities throughout their lifecycles. Particularly in cloud native architectures, machine identity management that provides visibility and intelligence into all machine identities—no matter how ephemeral—and the automation to ensure that machine identities adhere to corporate security policies and processes may mean the difference between a successful digital transformation initiative and one that upends an organization and threatens their customers.

Learn how Venafi can help your organization automate your machine identities, no matter how many you have: **venafi.com/automate**

References

1. IBM. Cost of a Data Breach Report 2021.

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
3 OF THE 5 Top Accounting/Consulting Firms
4 OF THE 5 Top Payment Card Issuers
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

Venafi is the cybersecurity market leader in machine identity management, 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