CYBERARK®
THE IDENTITY SECURITY COMPANY®

2025 State of Machine Identity Security Report

From Blind Spots to Breaches: The Cyber Debt of Neglecting Machine Identity Security

Table of Contents

3 Organizations Are Leaning Hard into Machine Identity Security

4 Machine Identities Increasingly Vulnerable to Compromise

7 Spotlight: AI Looms Large on the Machine Identity Threat Horizon

8 Machine Identities Growing Faster than Human Identities

9 Value of Machine Identity Security Lauded, But Largely Untapped

12 Machine Identity Security Becoming More Complex to Manage

13 Machine Identity Security Challenges Will Only Intensify Over Time

14 Spotlight: Cloud Native Machine Identities Getting More Attention in Security Strategies

15 Focus on Machine Identities Is Increasing, But Not Fast Enough

16 Why Machine Identity Security Programs Lack Maturity and Need to Be Programmatically Strengthened

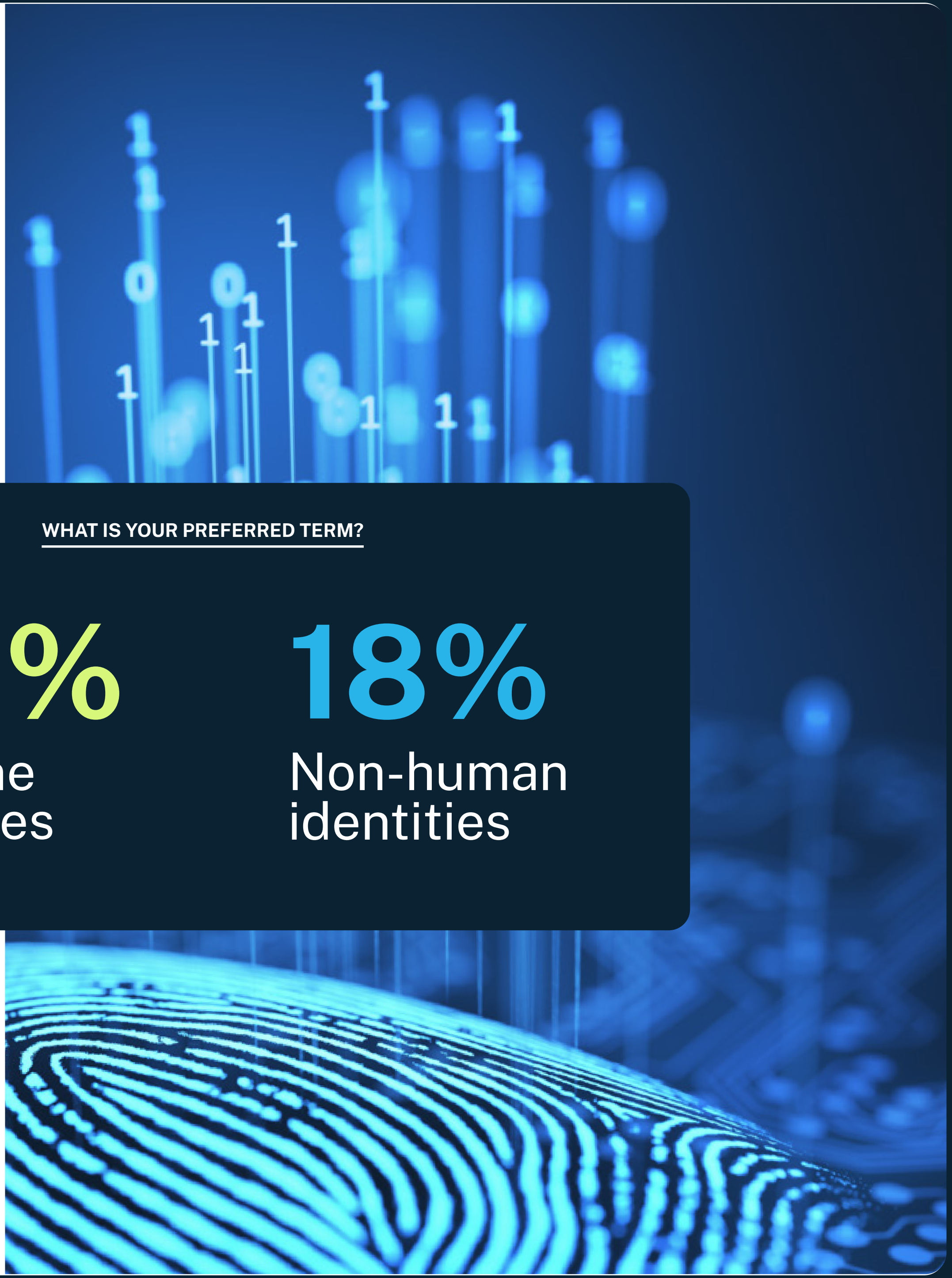
Organizations Are Leaning Hard into Machine Identity Security

Machine identity security is rapidly becoming one of the most critical aspects of modern cybersecurity strategies. While CISOs and IT leaders recognize its importance, many are still struggling to build a cohesive approach to protect these digital credentials. Machine identities play a unique and foundational role in both modern and traditional systems, connecting devices, applications, APIs and cloud native technologies securely. However, as their use continues to expand, so does the complexity of managing them effectively.

Machine identities now outnumber human identities by an overwhelming margin. This sheer scale is driven by several factors, including the rise of cloud native technologies, artificial intelligence (AI) and the shrinking lifespans of machine credentials in today's fast-paced development cycles. Each instance requires a unique identity to authenticate and communicate securely, adding to the already staggering growth in machine identities — particularly as organizations begin to embrace agentic AI.

At the same time, malicious actors have taken notice, and cybercriminals are targeting machine identities as entry points for attacks. And machine identity attacks are growing. By exploiting weaknesses in authentication systems or leveraging expired or mismanaged credentials, attackers can move laterally within networks, access sensitive data and disrupt critical operations. The increasing reliance on machine identities magnifies their risks, making them a prime focus for threat actors seeking to undermine enterprise security.

To better understand how these challenges are impacting today's enterprise security, we surveyed 1,200 security leaders across the USA, UK, Australia, France, Germany and Singapore. Read on to learn the findings.



WHAT IS YOUR PREFERRED TERM?

56%	18%
Machine identities	Non-human identities

Machine Identities Increasingly Vulnerable to Compromise

Due in large to their widespread usage, under-managed machine identities have become more and more vulnerable, with 77% of security leaders acknowledging that every undiscovered machine identity is a potential point of compromise. Among the most concerning assets vulnerable to compromise are API keys and SSL/TLS certificates, with SSH keys, code signing certificates and mobile certificates following close behind. It's no surprise that this list is for the most part consistent with the list of machine identities that are perceived as difficult to secure.

77% feel that every undiscovered machine identity is a potential point of compromise

TOP MACHINE IDENTITIES INVOLVED IN A SECURITY INCIDENT

34%	API keys
34%	SSL/TLS certificates
29%	IoT certificates
28%	SSH certificates
27%	Service account tokens
20%	Secrets

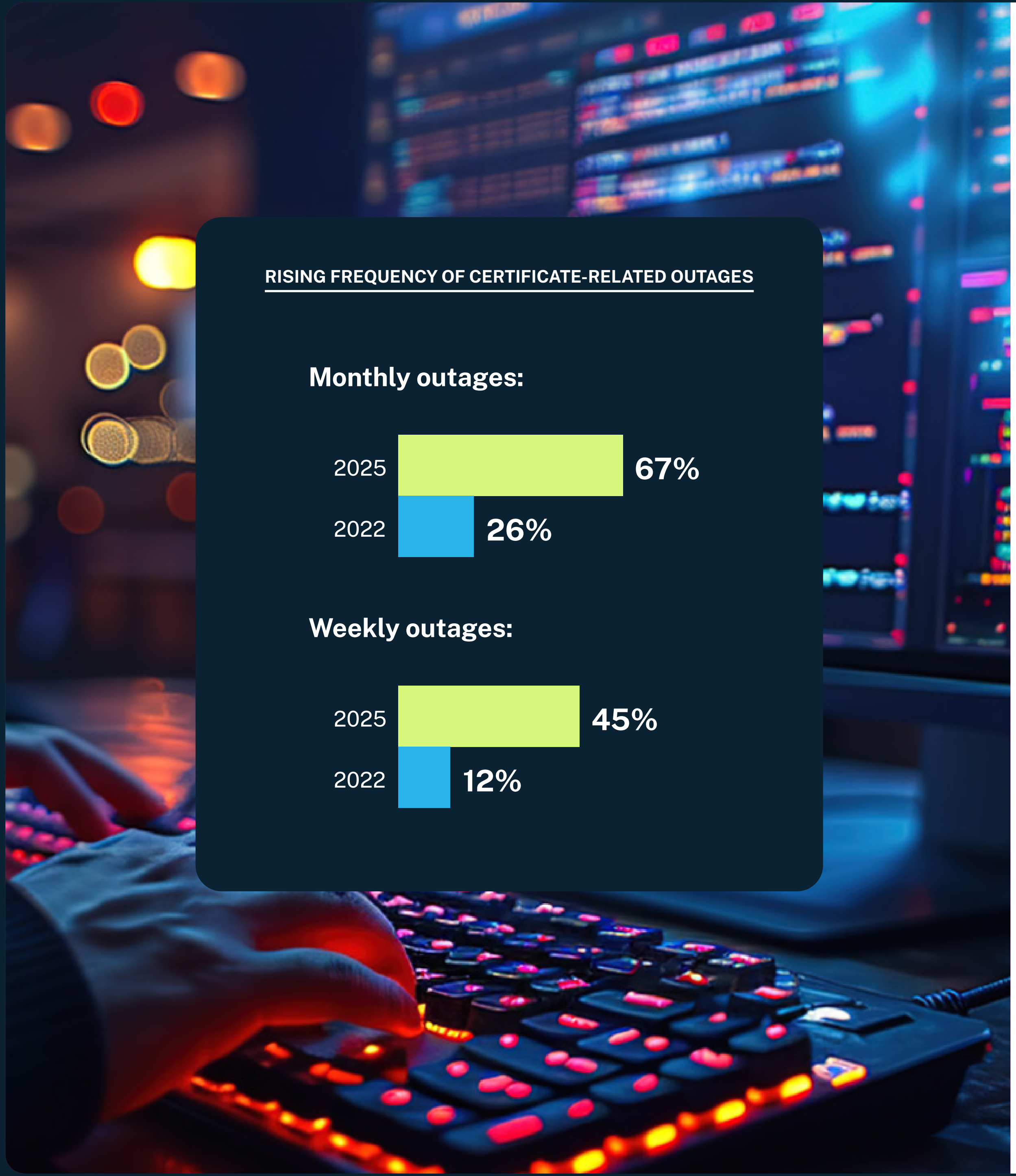
Machine Identities Increasingly Vulnerable to Compromise

BUSINESS IMPACT OF MACHINE IDENTITY-RELATED SECURITY INCIDENTS

51%	Cost time and resources due to delaying an application launch/slowing down production
44%	Caused an outage or disruption that negatively impacted customer experience
43%	Attackers were able to gain unauthorized access to data, networks and systems
33%	Led to a compliance violation and/or audit failure
29%	Negatively impacted developer experience

Alarmingly, 50% of organizations reported security breaches linked to compromised machine identities in the past year. As anticipated, API keys and SSL/TLS certificates topped the list as primary contributors to incidents. And the business impact of these breaches is significant, with 51% reporting delays in application launches, 44% suffering outages that hurt customer experience and 43% experiencing unauthorized access to sensitive data or networks. Compliance violations and diminished developer productivity further compound the damage.

50% of organizations reported security incidents or breaches that are related to compromised machine identities in the last year



RISING FREQUENCY OF CERTIFICATE-RELATED OUTAGES

72% had at least one certificate-related outage in the past year

In addition to compromises, certificate-related outages are especially prevalent, with 72% of organizations experiencing at least one in the last year — and 34% suffering multiple. Certificate-related outages prevent access to business-critical systems, causing severe operational disruption. Alarmingly, the frequency of such incidents is on the rise, with 67% reporting monthly outages (up from 26% in 2022) and 45% grappling with weekly disruptions (up from 12%).

Spotlight: AI Looms Large on the Machine Identity Threat Horizon

The rise of AI has elevated the urgency of securing machine identities, with 81% of security leaders emphasizing its critical role in protecting AI's future. Machine identities act as the gatekeepers, helping shield AI models and systems from threats like unauthorized access, model and data theft, and manipulation.

A notable 79% of respondents agree that protecting AI models from compromise demands robust machine identity and stringent authentication and authorization protocols. This focus reflects a growing awareness of how susceptible AI systems can be to exploitation. Manipulated models can generate harmful outputs, while stolen algorithms could endanger proprietary innovation and competitive advantage.

Looking ahead, 72% of leaders predict a shift in priorities, moving from safely utilizing generative AI to directly safeguarding the models themselves. This transition acknowledges the inherent risks of leaving such valuable assets vulnerable in a constantly evolving threat landscape.

81% Believe machine identity will be a vital element of securing the future of AI

79% Believe the need to secure AI models from manipulation and theft is putting greater emphasis on the need for machine identity, authentication and authorization

72% Believe the focus for next year will shift from using generative AI (GenAI) safely to protecting the models themselves from manipulation and theft

Machine Identities Growing Faster than Human Identities

One of the reasons that machine identity vulnerabilities are becoming more commonplace is that there are simply more machine identities than ever — and that means more points of potential failure. The number of machine identities is growing exponentially, outpacing human identities and reshaping enterprise security priorities. It's not surprising that 79% of organizations expect the number of machine identities to grow over the next year, with 63% projecting increases of up to 50% and 16% anticipating more aggressive growth between 50-150% per year.

With machines already radically outnumbering humans in organizations, the growing disparity is clear. Cloud native technologies, AI and microservices drive this rapid growth, as workloads and containers spin up dynamically, often lasting minutes rather than years. Each instance demands unique identities to operate securely, adding to the growing complexity of machine identity security.

79% expect an increase in machine identities of up to 150% over the next 12 months

63% Expect an increase by up to **50%**

16% Project radical growth of **50-150%**

Despite their overwhelming numbers and critical roles, only 23% of organizations prioritize securing machine identities exclusively — while 30% focus on human identities. Even though 47% treat machine and human identities as equal priorities, "equal" attention doesn't necessarily reflect the growing scale or importance of machine identities.

The surge in machine identities is undeniable, and elevating their security as a core priority is essential for safeguarding enterprise operations.

Value of Machine Identity Security Lauded, But Largely Untapped

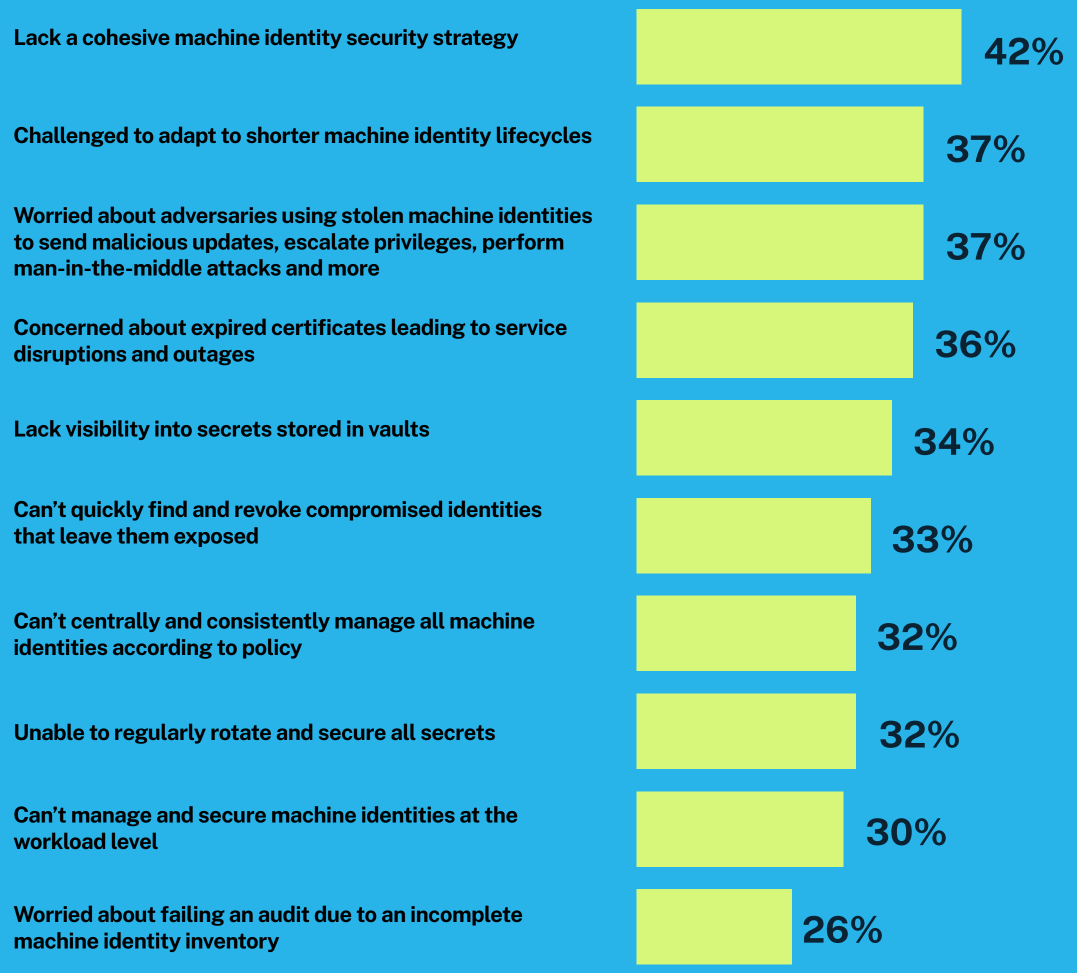
Overall, machine identity security is widely recognized as critical, with 92% of security leaders reporting some form of a machine identity security program. Yet, this broad adoption doesn't always equate to maturity. Many organizations face significant obstacles in delivering effective protection for their machine identities. Nearly 42% of security leaders admit their organizations lack a cohesive machine identity security strategy across environments, business units and machine identity types.

23% prioritize securing machine identities exclusively

42% lack a cohesive machine identity security strategy

Value of Machine Identity Security Lauded, But Largely Untapped

TOP MACHINE IDENTITY SECURITY CONCERNS



Other challenges are just as pressing — 37% struggle to adapt to shorter machine identity lifecycles, while the same percentage worry about adversaries misusing stolen identities to execute attacks such as privilege escalation, malicious updates or man-in-the-middle exploits. Another 36% express concerns about expired certificates that lead to service disruptions and outages. Furthermore, 34% lack visibility into secrets stored in vaults, and 33% cannot promptly identify and revoke compromised identities, leaving them vulnerable to attacks.

Value of Machine Identity Security Lauded, But Largely Untapped

To complicate matters further, ownership of machine identity security remains fragmented. While 53% of security teams assume responsibility for preventing compromises, development (28%) and platform teams (14%) are still heavily involved. Similarly, other tasks such as managing certificates or creating policies are divided among teams, creating inefficiencies and gaps in management.

WHICH TEAMS ARE RESPONSIBLE?

	SECURITY OWNS	DEVELOPMENT OWNS	PLATFORM OWNS
Setting policies that secure machine identities	45%	32%	18%
Ensuring that machine identities are secure from compromise	53%	28%	14%
Enabling machine identity management	40%	31%	24%
Ensuring security policies and best practices are followed	54%	26%	13%
Managing certificates	43%	28%	25%
Managing secrets	51%	26%	16%

Machine Identity Security Becoming More Complex to Manage

The expansion of digital ecosystems has dramatically expanded the complexity of managing machine identity security. Organizations now contend with a wide variety of machine identities, each requiring robust protection. Leading the list of the most challenging assets to secure are API keys (36%) and SSL/TLS certificates (34%), followed by IoT certificates, SSH keys, mobile certificates and secrets.

Security's Most Challenging Machine Identity Types

1. 36% API keys
2. 34% SSL/TLS certificates
3. 33% IoT certificates
4. 27% SSH keys and certificates
5. 26% Mobile certificates

Compounding this complexity is the sheer volume and velocity of machine identities, which are rapidly growing as organizations adopt cloud native technologies and IoT devices at scale. Protecting these machine identities is no small task. Key challenges are split pretty evenly, including the ability to quickly revoke and replace certificates, identifying who controls access to applications or devices using a machine identity, pinpointing the locations or applications where machine identities are in use, maintaining accurate inventories and determining who is authorized to access these identities.

Security's Machine Identity Challenges

1. 38% Quickly revoking and replacing machine identities
2. 38% Identifying the business group or administrator who controls access to the application or device using the machine identity
3. 37% Identifying the location or application where the machine identity is in use
4. 36% Gaining an accurate inventory of machine identities
5. 35% Understanding who is authorized to access and use the machine identity

Despite the rising stakes, automation remains underutilized. Given the nature of today's modern networks, an alarming 34% of organizations still use manual or non-automated methods to manage their machine identity lifecycles. This limits visibility, increases risks and slows response times to potential threats.

34% still use manual or non-automated methods to manage machine identity lifecycles

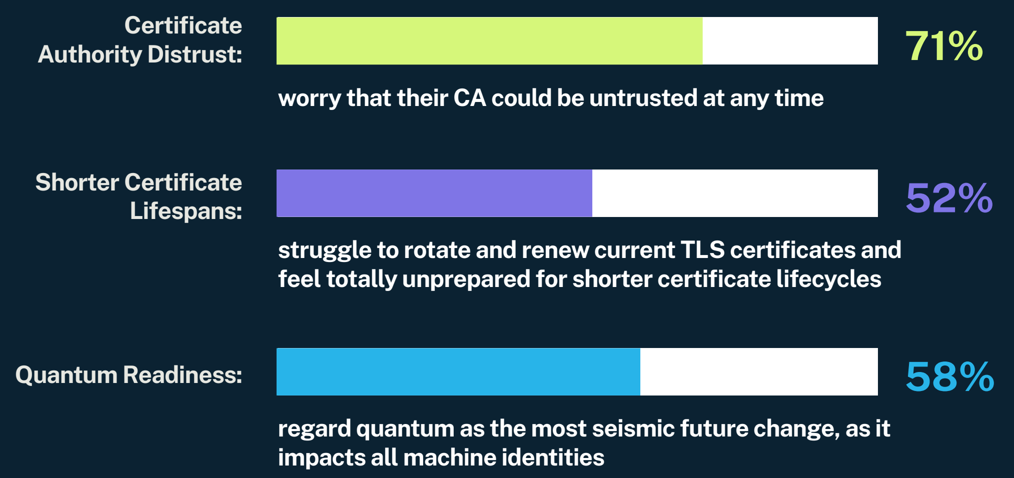
Machine Identity Security Challenges Will Only Intensify Over Time

Aside from the emerging challenges of securing agentic AI, the future of machine identity security will be fraught with complex challenges, driven by major shifts such as certificate authority (CA) distrust events, shrinking certificate lifespans and the rise of quantum computing. Alarmingly, 71% of security leaders worry their CA could become untrusted at any time, and 46% fear the need for immediate reaction without adequate preparedness.

Shrinking certificate lifespans add to the strain, with 23% of teams concerned about Apple's plan to reduce public TLS certificate validity to 47 days by 2028 — a drastic change that would require nearly nine times as many rotations and renewals. Over half of organizations already struggle to manage certificates with the current 398-day lifespan, with 51% recently experiencing critical outages due to expired TLS certificates.

Quantum computing also looms large in the minds of security leaders, with 57% acknowledging its threat to all machine identities. Yet, 31% of teams admit they cannot track all identities, leaving gaps in security, while 30% feel it's already too late to begin the transition to quantum-resistant cryptography.

TOP FUTURE MACHINE IDENTITY CONCERNS



worry that their CA could be untrusted at any time

struggle to rotate and renew current TLS certificates and feel totally unprepared for shorter certificate lifecycles

regard quantum as the most seismic future change, as it impacts all machine identities

74% Say attackers are zeroing in on machine identities in cloud native and development environments

74% Say the rapid adoption of cloud native technologies and AI are fueling complexity and increasing risks associated with machine identities

73% Say they are shifting to a more distributed way of managing and securing machine identities at the workload level

Spotlight: Cloud Native Machine Identities Getting More Attention in Security Strategies

As we've highlighted before, attackers are zeroing in on machine identities, with 74% of security leaders worried that cloud native and development environments are becoming prime targets. The rapid adoption of both cloud native and AI technologies is further compounding the complexity of managing machine identities, amplifying the risks associated with protecting these critical assets.

The sheer scale and dynamic nature of cloud native environments present a unique challenge. With workloads spinning up and down in seconds, static and centralized management of machine identities falls short. Recognizing this, 73% of organizations are focusing on shifting towards a more distributed approach to managing and securing machine identities at the workload level. This shift ensures that even the most ephemeral environments have identities safeguarded in real-time.

Focus on Machine Identities Is Increasing, But Not Fast Enough

Most organizations recognize the critical role of machine identities in securing systems and data, with 92% working under a machine identity security program and 44% planning to expand their use as a key component of their cybersecurity strategies. However, the pace of progress may not be sufficient to counteract emerging threats.

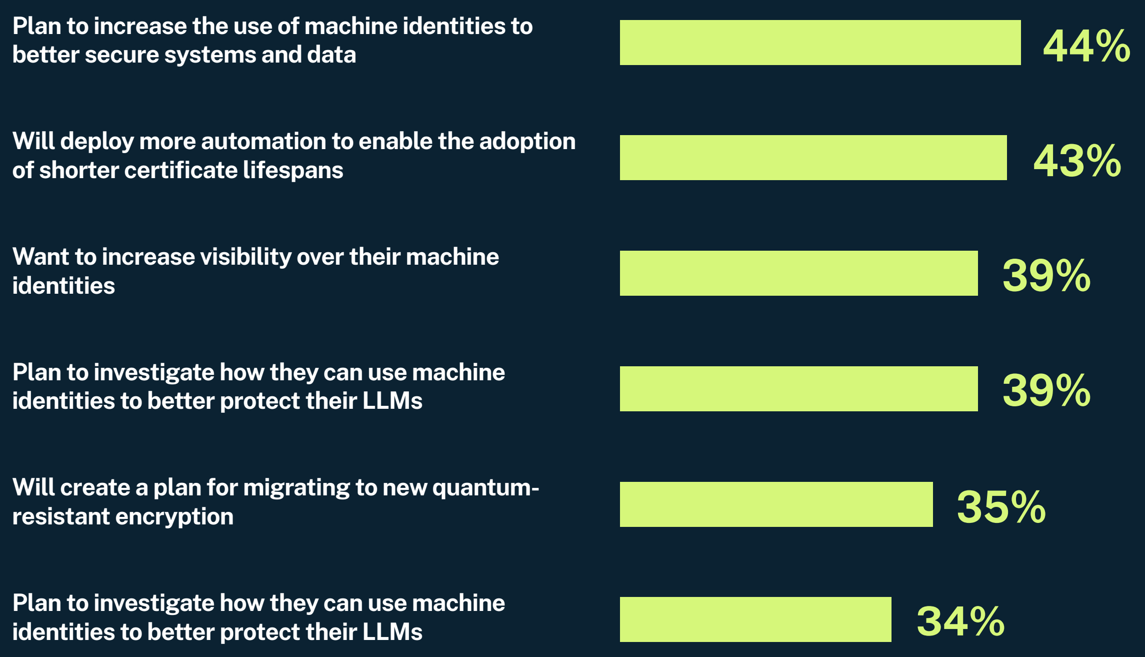
Automation is surfacing as a top priority, with 43% of respondents focusing on its deployment to handle the rising complexity introduced by shorter certificate lifespans. Managing certificates dynamically through automated processes will be essential for maintaining security without compromising business efficiency.

Visibility remains another critical challenge, with 39% reporting plans to improve oversight of all machine identities. Without clear insight into existing identities, gaps and blind spots can quickly turn into vulnerabilities.

To underscore the growing emphasis on safeguarding AI assets from manipulation or theft, 39% plan to explore how machine identities can further protect Large Language Models (LLMs). Meanwhile, 35% of organizations are beginning to address the looming threat of quantum computing by preparing migration plans toward quantum-resistant encryption.

On the cloud native front, 34% see the need to secure machine identities at the workload level as an inevitable step to meet the demands of dynamic cloud native environments. These priorities reflect a growing awareness of the risks tied to machine identities, but they also expose gaps.

FUTURE PLANS FOR MACHINE IDENTITY SECURITY



Why Machine Identity Security Programs Lack Maturity and Need to Be Programmatically Strengthened

Let's not forget that machine identities outnumber human identities by orders of magnitude, making them an undeniable priority for every organization. With the rapid adoption of cloud native technologies, AI advancements and the shift toward shorter certificate lifespans, the reliance on machine identities will only continue to grow. This surge brings not only operational complexity but also greater risk.

Cybercriminals are acutely aware of these trends and are targeting machine identities to exploit vulnerabilities, compromise systems and disrupt critical infrastructure. Many organizations remain vulnerable with weak links in visibility, automation and preparedness. From cloud native workloads to quantum cryptography, gaps in machine identity security can leave even the most advanced organizations dangerously exposed.

The solution lies in establishing a comprehensive machine identity security program. Such a program must prioritize automation to meet the demands of dynamic environments, visibility to avoid blind spots and crypto agility to prepare for emerging threats like quantum computing. These foundational elements not only prevent attacks but also ensure the availability of critical systems, letting organizations scale securely and innovate with confidence.

To learn more about how CyberArk can secure the full spectrum of your identities — including machine identities — contact our experts**.**

About CyberArk

CyberArk is the global leader in identity security, trusted by organizations around the world to secure human and machine identities in the modern enterprise. CyberArk's AI-powered Identity Security Platform applies intelligent privilege controls to every identity with continuous threat prevention, detection and response across the identity lifecycle. With CyberArk, organizations can reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities, including workforce, IT, developers and machines, to securely access any resource, located anywhere, from everywhere.