A Forrester Consulting
Thought Leadership Paper
Commissioned By Venafi

June 2018

# Securing The Enterprise With Machine Identity Protection

FORRESTER®

# Table Of Contents

**Project Director:**
Chris Taylor,
Senior Market Impact Consultant

**Contributing Research:**
Forrester's Security and Risk
research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

# Executive Summary

Machine identity protection is a critical component of enterprise identity and access management (IAM) security programs. Managing user and machine identities and privileged access to business data and applications is an enormous undertaking that has serious security ramifications if not executed properly. Traditionally, the focus for IAM has been people-centric, but recent technological advancements and new computing capabilities have created a new set of IAM challenges that require increased focus on protecting machine identities.

For example, newer technologies, such as cloud and containerization, have expanded the definition of machine to include a wide range of software that emulates physical machines. Furthermore, these technologies are spawning a tidal wave of new, rapidly changing machines on enterprise networks. To effectively manage and protect machine identities, organizations need: complete visibility of all machine identities across their networks; actionable intelligence about each machine identity; and the capabilities to effectively put that intelligence into action at machine speed and at scale.

In March 2018, Venafi commissioned Forrester Consulting to examine the importance of protecting machine identities in enterprises today, and to explore how prepared companies are to implement those protections. To do this, Forrester conducted a survey of 350 IT and security decision makers across the US, UK, France, Germany, and Australia with responsibility for their firm’s business infrastructure and the security of identity and access management programs. Findings from the study revealed that protecting machine identities is already a central component of IAM efforts. However, enterprises struggle to adequately track and protect all machine identities and they need better automation capabilities to deploy protection more effectively.

Enterprises today struggle to adequately track and protect all existing machine identities and they need automation capabilities to deploy those protections more effectively.

**KEY FINDINGS**

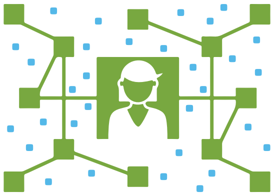
- Ninety-six percent of companies agree that effective protection of machine and human identities is critical to the long-term security and viability of their companies, but 80% struggle with the delivery of important machine identity protection capabilities.
- Seventy percent of companies are tracking less than half of potential machine identities, leaving them vulnerable to a wide range of security risks.
- Automation is critical to addressing the most pressing challenges business face today with machine identity protections (e.g., comprehensive discovery of machine identities, responding quickly to cryptographic security events, and quickly replacing vulnerable or compromised certificates and identities).
- Improvements to machine identity protection programs will drive immediate and long-term security benefits by enabling faster breach detection and remediation and by reducing the overall number of breaches.

# Automated And Effective Protection Of Machine Identities Is Critical To Business Viability

Digital technology has enabled businesses to transform the way they operate and engage with customers. While these new capabilities are a boon to the bottom line, it is paramount that access to and use of the machines that power this transformation are carefully managed and adequately protected. This can be a tall order for enterprises that already have thousands, or even tens of thousands, of human identities (e.g., employees, contractors, partners, and customers) to monitor, and, in addition, are forced by cloud and containerization adoption to protect a rapidly increasing number of machine identities.

Reliably and cost effectively protecting and managing machine identities requires businesses to identify programs and devices that connect to each other to access critical and sensitive information. These machine identities comprise cryptographic keys and digital certificates that govern authentication and encrypted communication. Today nearly three quarters of companies recognize the need to manage and protect both human and machine identities and see them as equally important to their company's future.

The need to protect machine and human identities is universally recognized as critically important today and for the future — 96% of companies agree that effective identity and access protection of machine and human identities is indispensable to the long-term security and viability of their companies. Getting the right technology in place to accomplish automated machine identity protection is a top priority as well — 70% of companies place high importance on implementing dedicated machine identity protection platforms.



96% of companies agree that effective identity and access protection of machine and human identities is critical to the long-term security and viability of their companies.

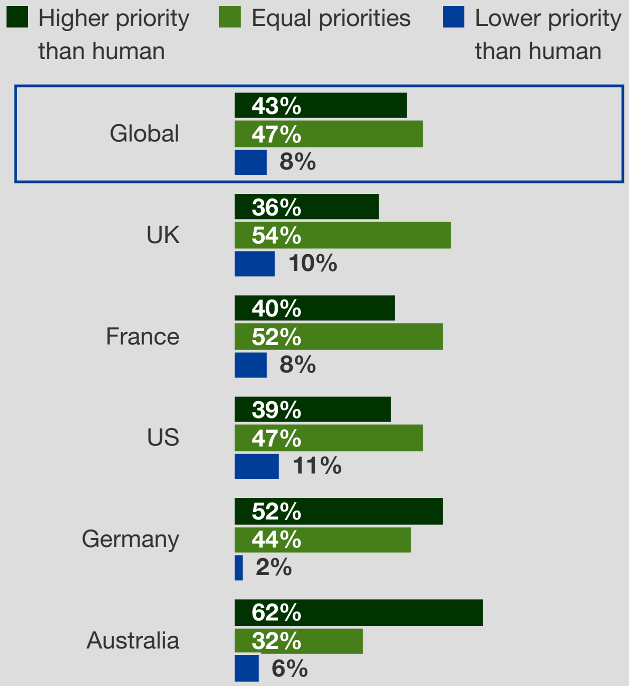
### PROTECTING MACHINE IDENTITIES IS AS IMPORTANT AS PROTECTING HUMAN IDENTITIES

The need to protect machine identities is not part of a tech-hype cycle that will die down in a few months: businesses today face a rising tide of machine identities driven by the adoption of new technologies including IoT, cloud, mobile, as well as new, automated business processes. In addition to these changes, organizations are coping with an influx of security automation, DevOps, and containerization initiatives that further complicate effective machine identity protection.

To successfully secure the enterprise's assets in a de-perimeterised world, IAM programs can no longer focus solely on human identities. Our research found that 47% of companies anticipate that protecting machine and human identities will be of equal priority over the next 12 to 24 months, and 43% believe that machine identities will be a higher priority than human identities. In two of the countries surveyed, Germany and Australia, a larger percentage felt machine identities would be a higher priority going forward (see Figure 1).

Figure 1

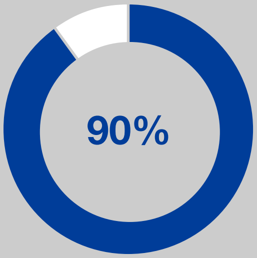
**"Will machine identity protection be of higher, equal, or lower priority than human identity protection in the next one to two years?"**



Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure

Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018

Note: Percentages may not total 100 because of rounding.



of companies believe machine identity protection will be equal or higher in priority than human identity protections.

## Delivering Machine Identity Protection Is Challenging

Businesses today realize that machine identity protection is central to their security efforts. They gauge the success of their human and machine identity protection efforts across three key measures:

- Faster detection of breaches.
- Improving automated compliance with security regulations and policies.
- Reducing the total number of breaches.

While businesses realize that effective protection of machine identities is crucial to their long-term viability, it's easier said than done. The scale and complexity of the problem has increased dramatically due to: a greater number of machines on networks; broader adoption of cloud-based workflows; and new DevOps initiatives. For cloud and DevOps particularly, these new initiatives and workflows create rapidly changing machine identities that need to be managed efficiently. Without the right technology solutions in place, — such as enforcing policies, routine machine identity life cycle management, and responding to machine identity security incidents at enterprise scale — this rapidly fluctuating environment can be perilous. Automation ensures that proper machine identity protection processes are scalable; because orchestrating the creation, provisioning, rotation, renewal, and replacement of machine identities tasks manually is nearly impossible, given the rapid increase in volume of machine identities and the velocity of changes affecting them.

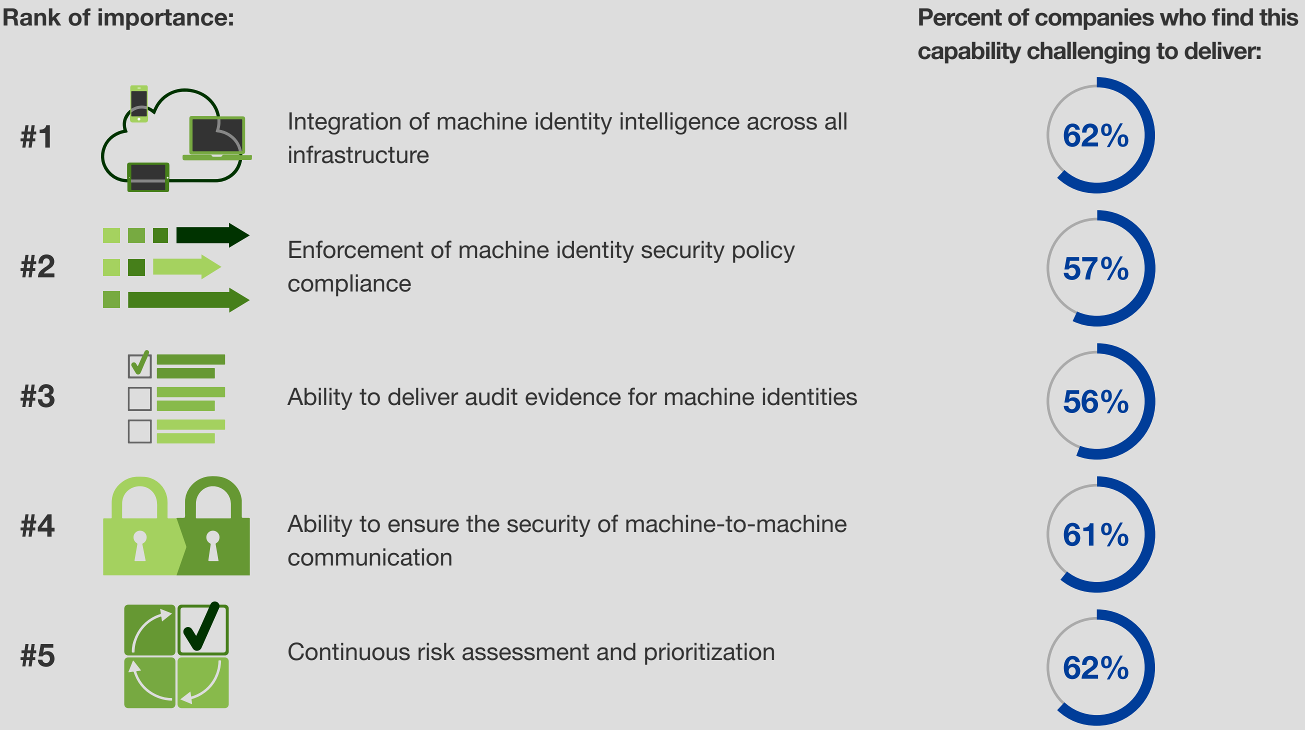
To better understand how respondents think about machine identity protection initiatives, we asked them two questions: 1) how important are specific capabilities to better supporting machine identity protection and 2) how challenging is it for their company to deliver on those capabilities. When comparing the results of these two questions side by side, we found that companies see machine identity protection capabilities as important, but the majority struggles to execute on those capabilities (see Figure 2). The three capabilities most difficult to execute on were:

- Integration of machine identity intelligence across the ecosystem.
- Continuous risk assessment.
- Comprehensive intelligence across all machine identities.

Integrating, enforcing policies for, and auditing of machine identity policies is hard because often these capabilities are not built into most tools. Because these key capabilities are not in place, over 50% of companies experience problems protecting machine identities. This was a consistent trend across all geographies surveyed.

**Figure 2**

**The most important machine identity protection capabilities are difficult to deliver on.**



| Rank of importance: | | Percent of companies who find this capability challenging to deliver: |
|---|---|---|
| #1 | Integration of machine identity intelligence across all infrastructure | 62% |
| #2 | Enforcement of machine identity security policy compliance | 57% |
| #3 | Ability to deliver audit evidence for machine identities | 56% |
| #4 | Ability to ensure the security of machine-to-machine communication | 61% |
| #5 | Continuous risk assessment and prioritization | 62% |

Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018

Because companies recognize their current systems are insufficient to address machine identity priorities, they are justifiably fearful of what is at stake should their efforts to protect machine identities fail. Sixty-one percent of companies say their biggest concern about machine identity and access management failure is internal data theft or loss, followed closely by theft or loss of customer data. At a time when safeguarding data helps generate and protect competitive advantages, it's imperative that firms invest in the tools that deliver comprehensive machine identity protection.

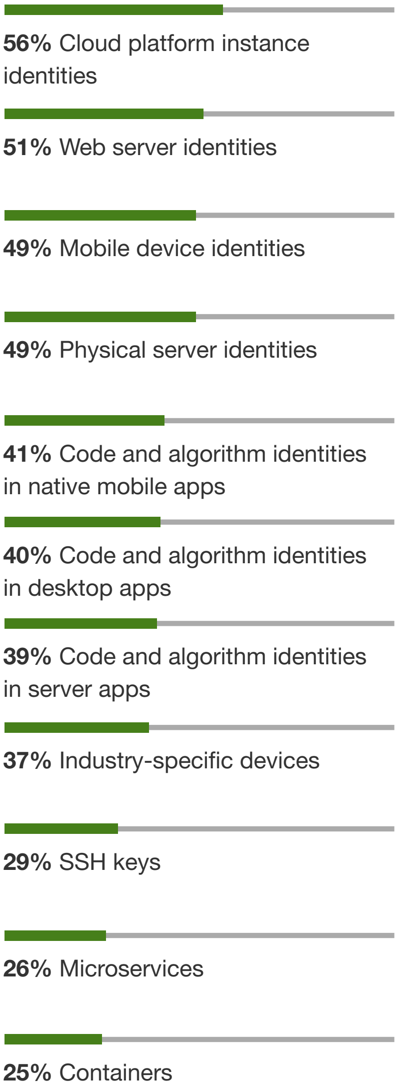
## FIRMS LEAVE MANY CLASSES OF MACHINE IDENTITY UNPROTECTED, COMPOUNDING RISKS AND CHALLENGES

Firms find machine identity protection difficult for two main reasons:

- **Many forms of machine identity are going untracked and unprotected.** Our survey evaluated 11 types of machine identities commonly found on enterprise networks and, on average, we found that firms track less than half of them. Identity types include web-server identities, code/algorithms in applications, containers, and others (see Figure 3). Because firms are not tracking all possible types of machine identity, they may be blind to existing vulnerabilities, evolving threats, and attack patterns. This makes these machines a vulnerable target for malicious attacks. For example, mobile has been around for over a decade, but the expansion of bring-your-own-device (BYOD) initiatives has created new code and algorithm machine identities in native mobile apps that automatically connect to each other and to enterprise networks that must be protected. Also, rapid adoption of containers and cloud platforms requires careful adjustment of machine identity protection programs because the setup of these platforms is almost always fully automated; in many cases machines are spinning up and down other machines in minutes or seconds. These identities can slip through the cracks if not carefully tracked and protected.
- **Firms are using disparate tools to protect machine identities.** Each type of machine identity has its unique challenges and complexities. Organizations are already adopting new technologies to address these challenges; this includes hardware security modules, internally developed and managed spreadsheets/databases, and dashboards from certificate authorities. The problem is that many of these tools are limited in scope and are used in silos. This makes them complex to maintain and difficult to scale up. Moving forward, firms need fewer tools that do more — tools that improve visibility across all types of machine identities (wherever they are being used) and tools that deliver the comprehensive intelligence required to drive automated protection and response.

**Figure 3**

**"What machine identities are companies tracking?"**



Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018

On average, companies track less than 50% of all possible machine identities.

## MACHINE IDENTITY PROTECTION REQUIRES AUTOMATION

Building an inventory of machine identities to improve visibility is a good first step that can immediately improve companies' machine identity risk posture. However, this information isn't enough if the proper people, processes, and technology are not in place to protect them. Automation can help companies alleviate their current challenges with protecting machine identities by enabling firms to:

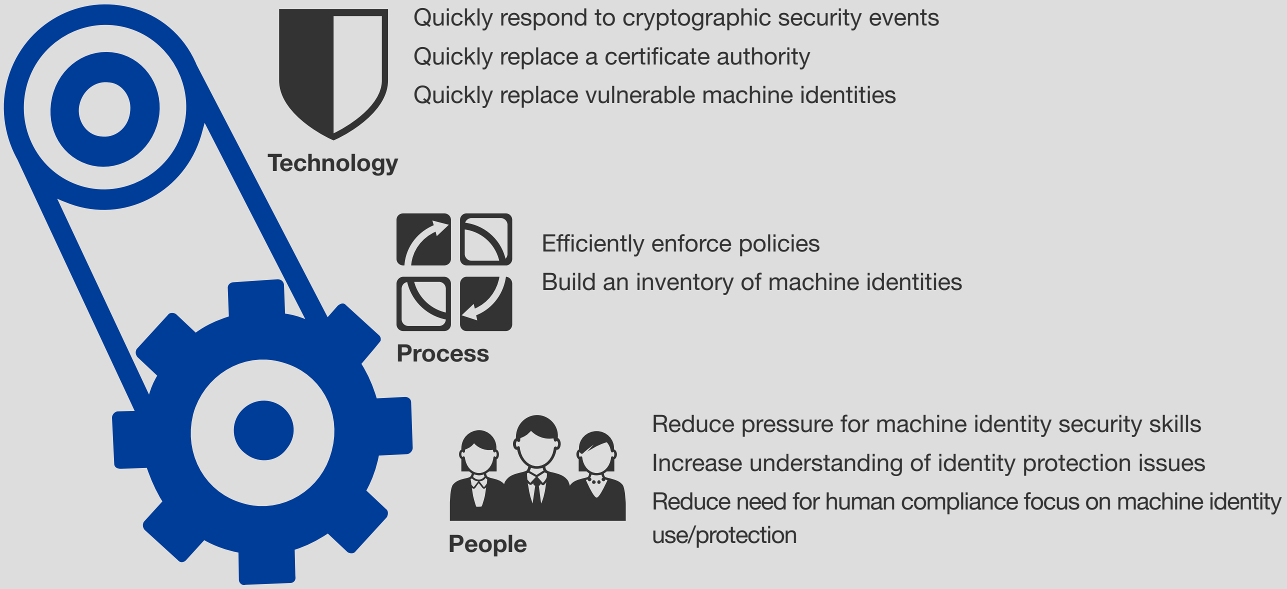
- **More quickly respond to security threats.** Security incidents are inevitable, but the most significant challenge that companies report is their inability to quickly respond to machine identity cryptographic security events and replace/fix vulnerabilities (see Figure 4). Companies want to be better prepared to mitigate the risks posed from these threats as quickly as possible; automation is critical to identify and respond to threats at machine speed.

- **More efficiently track identities and enforce policies.** When asked to rank the top process-related challenges with machine identity protection, the lack of automation to enforce policies and the need to inventory machine identities rose to the top of the list. Many companies could greatly benefit from more automated processes that can improve monitoring and protection of machine identities, especially as the volume of identities continues to grow rapidly.
- **Reduce reliance on specialized skills for machine identity protection.** Many companies find they lack the skills to implement the protection they need. One key contributing factor to this challenge is that 37% of companies say they lack a full understanding of the business risks that result from weak machine identity protection. Automation can reduce the number of human touchpoints needed to protect machine identities and can help firms focus their resources and skills in specific areas where human interactions are required.

**Figure 4**

**Remove obstacles to better machine identity protection through automation.**

**Automation alleviates skills shortcomings by solving technology, process, and people challenges.**



**Technology**

Quickly respond to cryptographic security events
Quickly replace a certificate authority
Quickly replace vulnerable machine identities

**Process**

Efficiently enforce policies
Build an inventory of machine identities

**People**

Reduce pressure for machine identity security skills
Increase understanding of identity protection issues
Reduce need for human compliance focus on machine identity use/protection

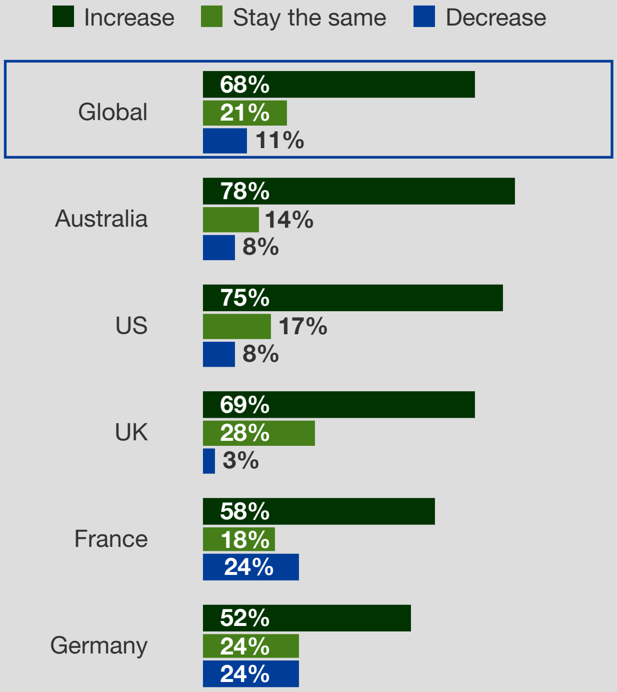
Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018

# Better Security Requires Increased Focus On Machine Identities

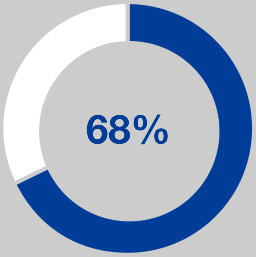
With a keen awareness of their current challenges with machine identities, 68% of companies say that the priority of machine identity protection will increase in the next one to two years. Globally, our survey showed that decision makers in Australia and the US were much more likely to report an anticipated increase in priority than other countries (see Figure 5). Respondents in France and Germany were less inclined to predict a rise in prioritization of machine identity protection as both already recognize the rising significance of protecting machine identities and have realigned priorities to reflect that.

Figure 5

"How do you predict machine identity protection priorities will change over the next one to two years?"



Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018



of companies say that the priority of machine identity protection will increase in the next one to two years.

As machine identity protection increases in priority, companies will need a clearer focus on specific capabilities needed to address current challenges, including:

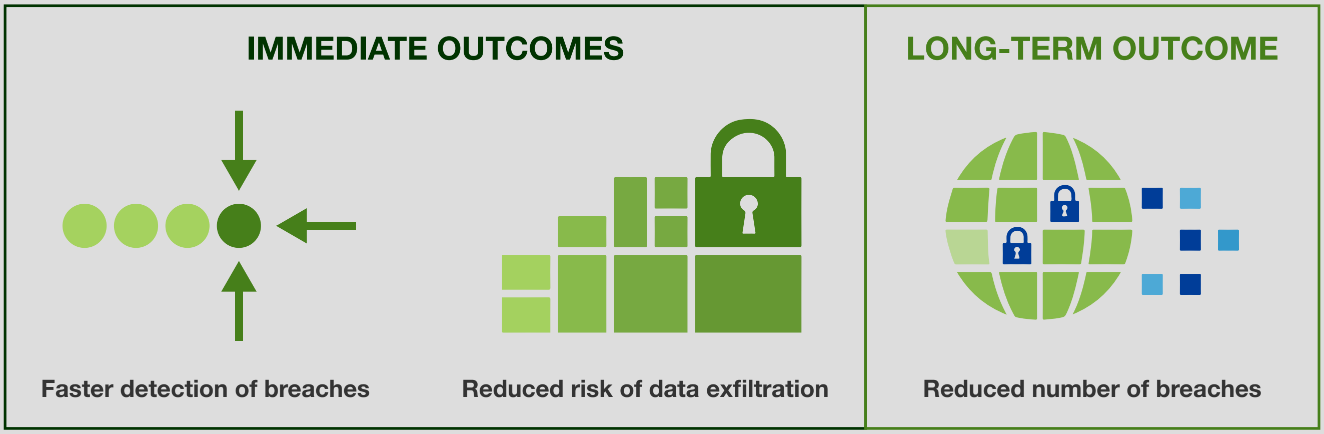
- Continuous visibility and intelligence of all machine identities across the enterprise: 1) to rapidly identify unauthorized access and privilege escalation and 2) to prevent lateral movement using cryptographic keys.
- Comprehensive intelligence across the entire machine identity life cycle including certificate generation, installation, deployment, rotation, and removal to protect and secure authorized, encrypted communications between machines.
- Self-service capabilities to help remove complexity and reduce reliance on high-skill personnel to address day-to-day security operations.

Companies that invest more time and effort into improving protection of machine identities do so with the expectation that it will enable immediate and future benefits (see Figure 6). Key outcomes include:

- **Faster detection of breaches.** This is the most immediate, short-term outcome that companies expect, as identified by 42% of companies. The added visibility and intelligence provided by better machine identity protection can enable security teams to more quickly recognize and remediate machine identity threats.
- **Reduced risk of data exfiltration.** Once breaches are detected, automation and escalation capabilities can quickly terminate access, revoke certificates, rotate keys, and seal off breaches to minimize data loss. This was a top outcome for 39% of firms surveyed.
- **Reduced number of breaches.** While the other outcomes are more immediate in nature, 39% of firms have long-term vision of improved machine identity protection delivering a measurable reduction in the total number of breaches. Being able to fix problems quickly is great but preventing problems before they happen is the ideal outcome.

**Figure 6**

**The key outcomes of improving security around machine identities and privileged access.**


IMMEDIATE OUTCOMES
LONG-TERM OUTCOME
Faster detection of breaches
Reduced risk of data exfiltration
Reduced number of breaches

Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018

# Key Recommendations

Evolution of the digital landscape is continuing to accelerate; this means that the number of machine identities on enterprise networks will continue to grow dramatically, while the number of humans on enterprise networks is expected to remain relatively constant. Companies can no longer be complacent about their machine identity protection efforts because the number and variety of machines identities will continue to climb. Security programs that only focus on protecting a subset of their machine identities (e.g., servers or critical infrastructure) will expose organizations to increasing security risks as new mobile, cloud, IoT, and containerized infrastructures expand and as new technologies, such as blockchain and AI, are used to support business functions.

Many companies are ill-equipped to address this dilemma because they rely on manual processes or siloed machine identity protection tools that are not designed to address the complexities of machine identity protection. Without the right intelligence, driven by automation, firms will struggle to respond quickly to the increasing number of machine identity threats. The reality is that many organizations are already bogged down by cumbersome processes and are unable to effectively enforce machine identity policies.

To more quickly identify breaches, reduce the loss incurred by breaches, and ultimately, overall, reduce the number of breaches, firms must institute effective, automated machine identity protections. To do this, Forrester recommends that firms follow these best practices:

**Establish a continuous visibility capability that is actively surveilling machine identities.** The scope and number of machine identities in your environment is greater than you think — as is the speed at which they appear and change. In addition to the technologies already discussed, database connections, chatbots, intelligent agents, and off-the-shelf applications all need unique machine identities to authenticate connections to sensitive data sources. The prerequisite of an effective and automated machine identity protection program is a solid, continuous understanding of what you have and need to protect.

**Apply intelligence.** Once you are aware of the existence of a machine identity, you need to know if it conforms to your security policies: Is it from a known source? Are there dangers in the way it is set up? Could it expire and cause systems to fail? Is it being used in unexpected ways? Does it need to be replaced? These and many other attributes need to be constantly evaluated to properly protect machine identities.

**Automate, automate, automate.** The number of machine identities and their shrinking life cycles require a completely different approach so that they can be protected. Manual tools and processes cannot fully address new machine identity protection challenges: automation is the best way to match responses to the speed and scale of machine identity changes. In addition, machine identity protection should be an ongoing, scalable process that can address rapid shifts in the machine identity population. It also must be centrally auditable. Both capabilities require automation.

**Sync machine identity and other credential repositories.** If your company already uses a combination of solutions to protect SSH keys, SSL/TLS certificates, and other privileged credentials for machine to machine communication, consolidate or at least synchronize these repositories to a single platform with consistent APIs so you have the ability see what is going on a single pane of glass. This unified security interface can better protect all machine identities, deliver significant improvements in efficiencies, and reduce complexity.

**Integrate machine identity intelligence with all infrastructure that produces and consumes machine identities.** In today's corporations, the number of consumers and producers of machine identities is in the thousands. Servers, VPNs, mobile devices, cloud workloads virtual machines, laptops, WAF, WAP, CAs, blockchain, IoT, active directories — all either produce or consume machine identities. Integration of machine identity intelligence with all types of machine identities is required to achieve optimal visibility, intelligence, and automation.

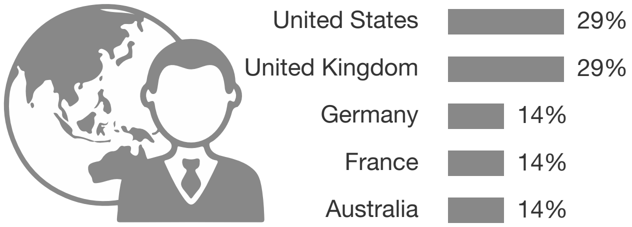
**Don't try to use in-house tools or non-machine identity specific tools.** These solutions are rarely able to deal with the complexity, centralized audit and policy management, and automation requirements of machine identity protection. Instead, investigate how specific machine identity protection solutions can help meet your needs.

# Appendix A: Methodology

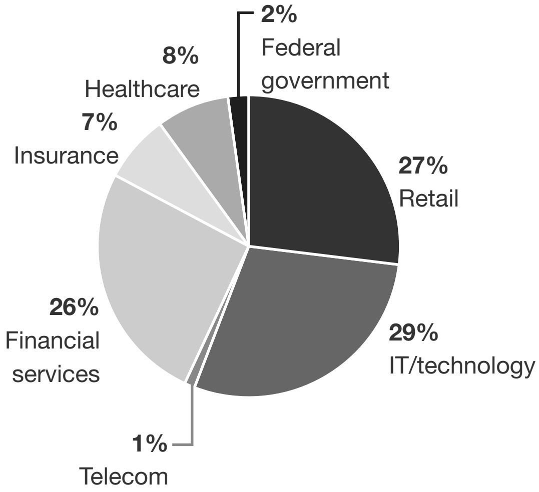
In this study, Forrester interviewed 350 IT decision makers responsible for their firm's business infrastructure and identity and access protection security. Questions provided to the participants asked about their firms' approach to managing privileges for both human and machine identities. Companies surveyed were from the US, UK, DE, FR, and Australia and had employee counts of 500 or more. The study was completed in March 2018.

# Appendix B: Demographics/Data

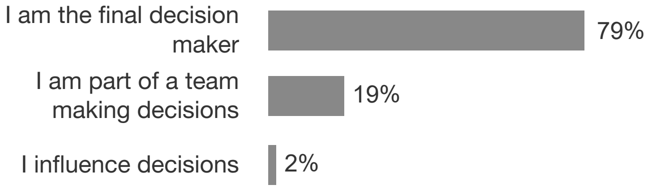
**"In which country are you located?"**

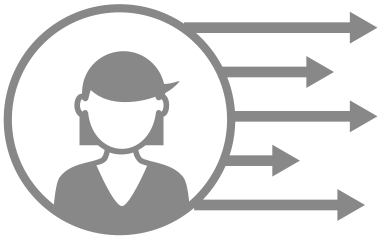


**"Which of the following best describes the industry to which your company belongs?"**



**"What is your level of responsibility for your company's identity and access management security strategy?"**





**100% in IT roles**

Base: 350 US, EMEA, and AU IT decision makers responsible for their firm's business infrastructure
Source: A commissioned study conducted by Forrester Consulting on behalf of Venafi, March 2018