A Forrester Consulting
Thought Leadership Paper
Commissioned By Centrify

April 2016

Managing Privileged Access Security In A Hybrid IT World

The Case For Privileged Identity Management As-A-Service

FORRESTER®

Table Of Contents

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

Succeeding in the age of the customer requires that businesses become digital — embracing digital technology in order to win, serve, and retain customers. Decision-makers, however, must balance the opportunities presented by new technologies and processes with ever-growing security concerns. Particularly given technology's ability to enable more outsourced and remote work, ensuring that employees are empowered enough to deliver value while maintaining control over access is of paramount concern.

In November 2015, Centrify commissioned Forrester Consulting to examine how IT decision-makers are both securing and granting privilege to identities in cloud-based environments. To further explore this trend, Forrester tested the hypothesis that it is the proliferation of multiple identities — not cloud security — that challenges organizations in properly granting privileged access to an increasingly outsourced and remote workforce.

In conducting in-depth surveys with 150 IT decision-makers in the US, Forrester found that the omnipresence of outsourced and remote identities is too large of a concern to overlook. Organizations need a solution that effectively manages access while still allowing employees and business partners to do their work and contribute to the business. Furthermore, decision-makers have found positive results utilizing privileged identity management (PIM)-as-a-service solutions to solve this challenge.

KEY FINDINGS

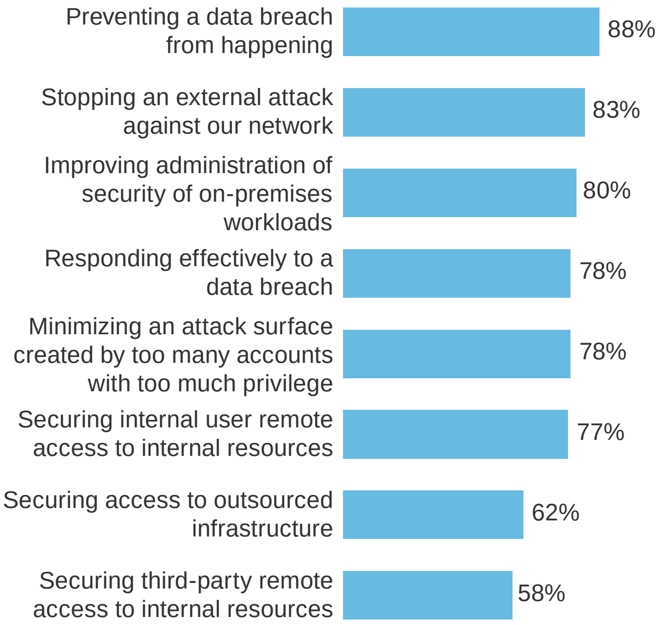
Forrester's study yielded five key findings:

- **Most organizations trust cloud security.** Ninety-three percent of decision-makers stated that their organization stores at least some of their sensitive data types in the cloud, and those with cloud-based workloads reported security levels akin to on-premises workloads.
- **All organizations outsource at least some of their IT, application development, and infrastructure functions.** Decision-makers outsource an average of nearly seven application development functions and nearly six IT functions. Ninety-two percent also stated that they either currently or plan to outsource their security and infrastructure.
- **Nearly all organizations permit privileged remote access.** Ninety-seven percent of decision-makers claimed that they allow employees and outsourced vendors privileged access via either VPN, virtual desktop infrastructure, web application gateways, or hosted file sharing.
- **Decision-makers choose PIM-as-a-service for its ability to reap the benefits of the cloud while still providing quality security.** Improved quality of protection, complexity reduction, speed, and the ability to support a large number of mobile and remote users are just a few reasons that many organizations chose to implement PIM-as-a-service.
- **A majority of decision-makers prefer to manage privileged identity and access management through a single platform.** Fifty-three percent of decision-makers prefer that a single platform handles most or all of the necessary functions of privileged identity and access management. They gravitate toward a single platform specifically to reduce overhead and centralize control, among numerous other reasons.

FIGURE 1

Preventing Data Breaches And External Attacks Are Top IT Security Priorities

“Which of the following initiatives are likely to be your organization’s top IT security priorities over the next 12 months?”
(Showing those selecting “critical priority” or “high priority” on a 5-point scale)



Base: 150 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

Digital Businesses Walk A Tightrope In Maximizing Speed And Efficiency While Providing Effective Security

In the age of the customer, any business today that wishes to remain competitive in its quest to win, serve, and retain customers competitively must become a digital business. This means a firm must make ample and judicious use of digital technologies to create new sources of value for its customers as well as increase its operational agility. And in many cases, the preferred technologies for many workloads are cloud-based.

With more digital assets moved to the cloud, however, there is fear over cloud security. Security has become a critical priority not just for security personnel but for IT as a whole.

As such, IT is increasingly mindful of where breaches could possibly occur. In this study, the data shows that:

- **Preventing data breaches is the top IT security concern.** Eighty-eight percent of IT decision-makers stated that their highest priority is to prevent data breaches from occurring, with 77% stating they prioritize initiatives around effectively securing remote access to internal resources (see Figure 1).
- **Most decision-makers recognize the security implications associated with privileged identities.** Seventy-eight percent acknowledge that they must minimize their organization’s attack surface created by allowing too many accounts with too much privilege.

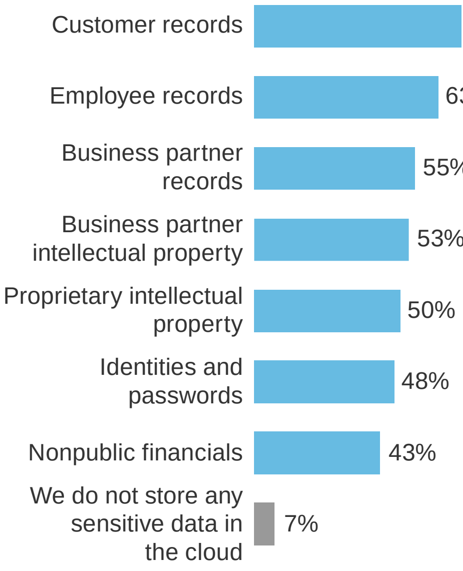
THE CLOUD IS NOT CAUSING THE SECURITY PROBLEM

In attempts to provide effective security, one might conclude that locking down access to the cloud is the only solution — it is understandable to believe that one should do away with

FIGURE 2

A Wide Array Of Sensitive Data Types Are Stored In The Cloud

“Which of the following types of sensitive company data are stored in the cloud?”
(Select all that apply)



93% of companies store at least one type of sensitive data in the cloud.

Base: 150 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees

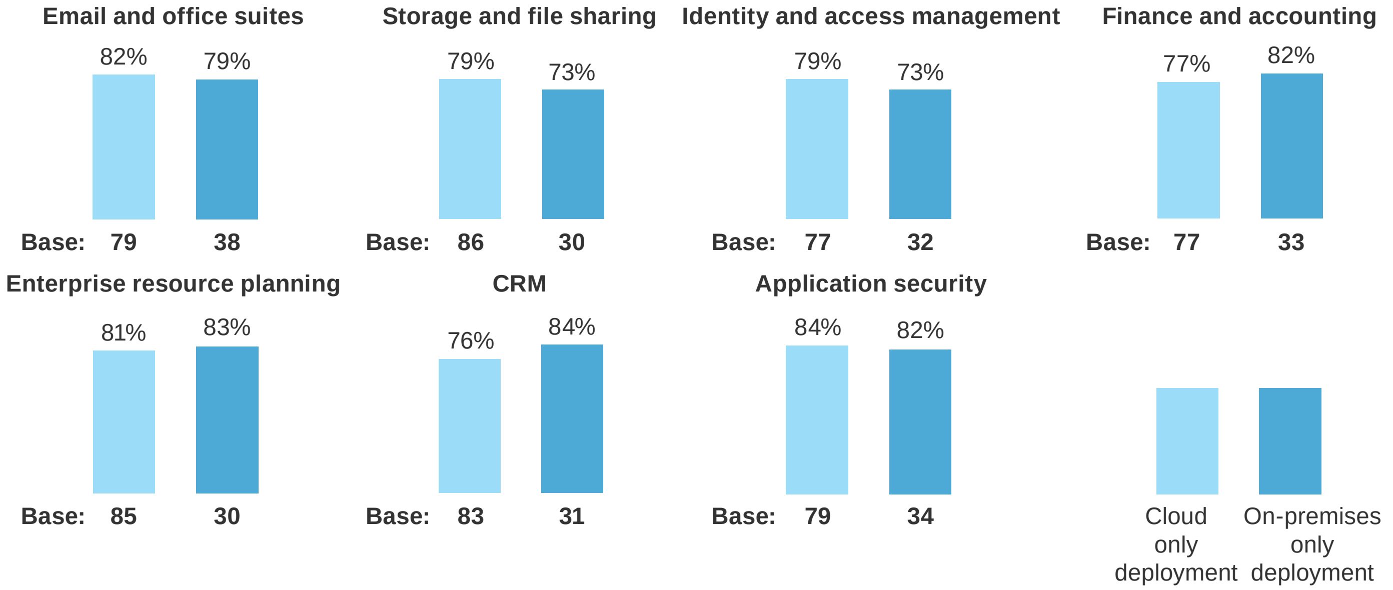
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

FIGURE 3

Cloud-Based Applications And Workloads Are Generally As Secure As Those That Are Solely On-Premises

"How secure are each of the applications/workloads?"

(Showing percentage selecting "completely secure" or "mostly secure" for workloads that are either entirely on-premises or entirely cloud-based)



Base: Variable US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees (workloads/applications with bases lower than 30 are not shown)

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

technology that is not completely under your organization's umbrella. This belief, however, is unfounded. The cloud-based applications are more than capable of securing data, and cloud-based workloads are as secure as those that are solely on-premises. Decision-makers in this study stated as much, with results indicating that:

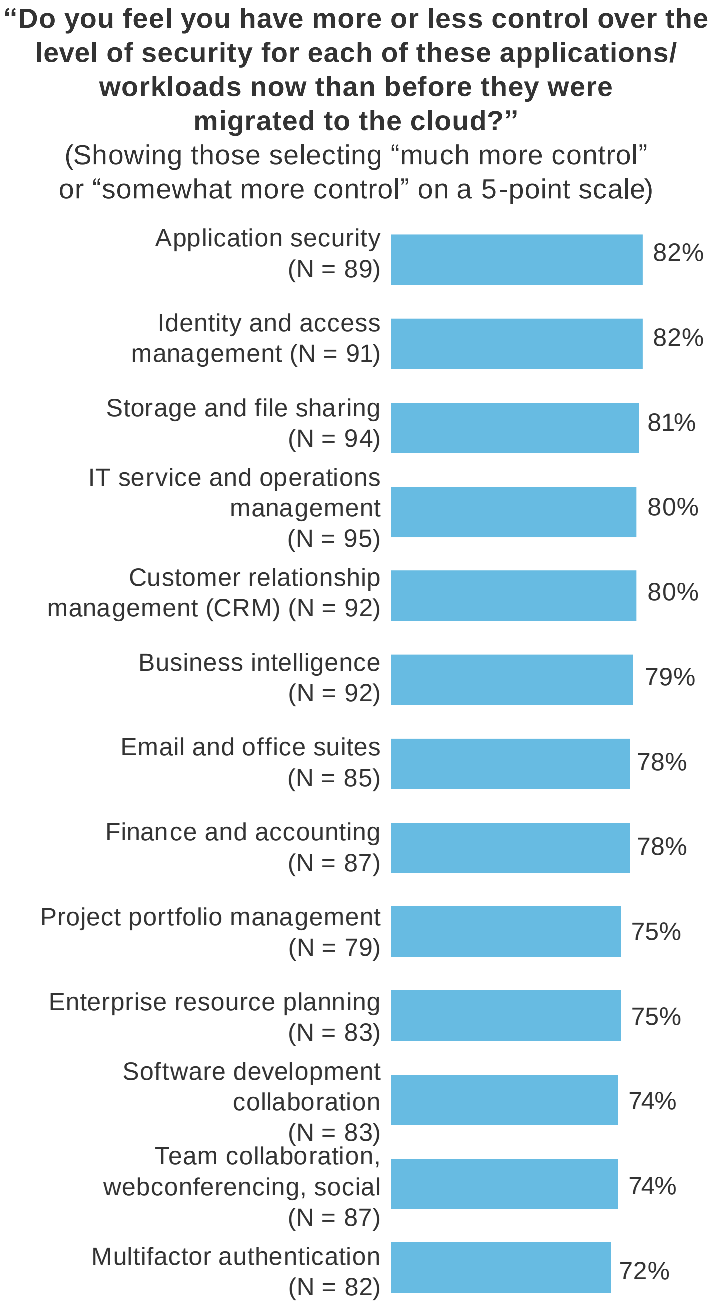
- **An overwhelming number of organizations store sensitive data in the cloud**. Ninety-three percent of decision-makers stated their organizations store sensitive data in the cloud, with data types ranging from customer records to proprietary IP and passwords (see Figure 2).

- **Cloud-based workloads are generally as secure as on-premises workloads.** When we asked respondents how secure their applications/workloads were, we compared the responses of those from organizations with workloads only in the cloud with those that were only on-premises. Results indicated that those with workloads deployed solely in the cloud rated their security at a similar level to those with workloads deployed solely on-premises — ratings were not different to a statistically significant degree (see Figure 3).

- **Moving to cloud-based workloads results in gaining control, not losing it.** Indeed, an overwhelming percentage of decision-makers feel they have more control of their workloads since migrating to the cloud — with workloads ranging from multi-factor authentication (72%) to application security (82%) (see Figure 4).

FIGURE 4

Most Feel They Have More Control Of Workloads That Have Migrated To The Cloud



Base: US director or higher IT decision makers in regulated industries at organizations with 500 or more employees who are using each application/workload in the cloud

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

The Challenge Lies With The Proliferation Of Identities That Require Privilege

Our data clearly indicates that the cloud itself is not causing a security problem. The cloud does, however, contribute to what is presenting a formidable hurdle: the large number of outsourced identities and increase in remote access. IT prioritizes minimizing its attack surface created by too many accounts with privilege (see Figure 1). However, an outsourced infrastructure and increased third-party remote access create a *larger* attack surface and raise the risk of a breach. Nevertheless, digital businesses increasingly rely on moving parts of their infrastructure and IT operations to the cloud, while granting employees remote access in order to increase efficiency and satisfaction. The result is a multitude of identities that require privileged access, challenging IT decision-makers. And with so many identities demanding privilege, organizations are inconsistent in how they designate privilege across accounts. Results from this study support this assertion, indicating that:

- **All organizations outsource at least part of their IT and application development.** All decision-makers in this study stated that their organizations outsource at least one IT function and at least one application development function (see Figure 5). Sixty-seven percent also stated they currently outsource at least some part of how they secure their infrastructure, as well as the infrastructure itself.
- **Nearly all organizations permit privileged remote access.** Ninety-seven percent stated that they permit remote access to employees and outsourced vendors (see Figure 5). Access ranges from VPN to virtual desktop infrastructure and hosted file sharing.

FIGURE 5

Every Organization Outsources At Least Some Of Its IT, Infrastructure, And App Dev Functions

"How often does your organization outsource any of the following parts of your application development process?"	**"How often does your organization outsource any of the following IT functions?"**	**"Which of the following best describes your organization's plans to outsource the following security and infrastructure functions?"**	**"Which of the following best describes your organization's implementation of the following to provide privileged remote access to employees and outsourced vendors?"**
Requirements UX design General design Development Testing and QA Integration Project management Release management or other delivery activity	Operations Networks (voice and data) Maintaining client devices Help desk support Database administration Server support Storage support	Premises-based infrastructure with outsourced security Outsourced infrastructure with insourced (our own staff) security Outsourced infrastructure with outsourced security (same provider for both) Outsourced infrastructure with outsourced security (different provider for both)	Desktop VPN Site-to-site VPN Virtual desktop infrastructure (VDI) Web application gateway Hosted file sharing
All outsource at least one of the above functions and outsource an average of **6.9**	All outsource at least one of the above functions and outsource an average of **5.8**	**67%** currently outsourcing at least one of the above functions. **92%** outsource or plan to outsource within 12 months.	**97%** allow remote privileged access through at least one of the above.

Base: 150 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees

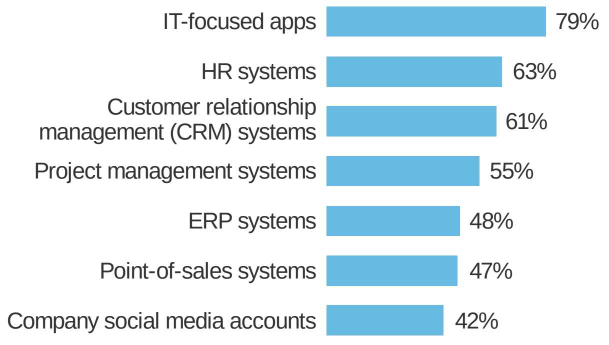
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

› **Not all accounts are treated equally.** Given the above results, it stands to reason that most organizations (79%) generally consider IT-focused apps to be privileged. They do not, however, extend this consideration to other vital accounts and systems: Results precipitously dropped when we asked organizations about HR systems (63%), project management systems (55%), and company social media accounts (42%) (see Figure 6).

FIGURE 6

Most Recognize Privilege In IT-Focused Apps But Do Not Consistently Acknowledge Privilege Elsewhere

"Which of the following types of business application accounts does your organization classify as administrative or privileged?"
(Select all that apply)



Base: 150 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

Both Privileged Identity Management As-A-Service And A Single Platform Approach Show Promise

In an effort to solve security problems and effectively control privileged identities, decision-makers at organizations that have chosen as-a-service solutions in this study reported promising results. Indeed, their answers suggest that PIM-as-a-service is especially effective in solving the pressing challenges associated with proliferating identities by taking advantage of its inherent benefits as a cloud-based solution while still providing quality security.

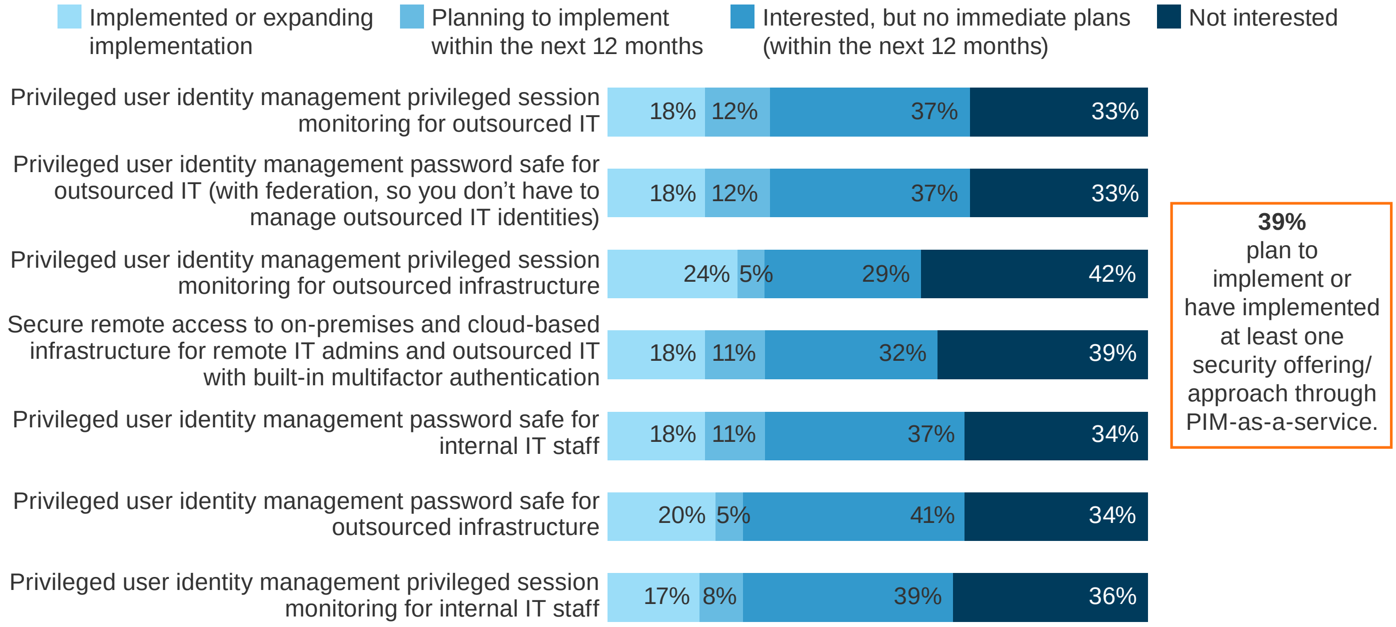
The responses from decision-makers in this study indicate that PIM-as-a-service:

- › **Sees increased adoption**. Nearly two out of five decision-makers (39%) stated that their organization has implemented at least one offering now or plans to implement an offering within 12 months (see Figure 7).

FIGURE 7

Nearly 40% Have Implemented Or Plan To Implement PIM-As-A-Service

"With some vendors starting to offer cloud-based solutions for privileged user identity management, what are your firm's plans to adopt the following privileged user identity management solutions as cloud-based solutions, meaning that the password safe is in the cloud (and *not* on-premises), and the privileged session monitoring components are in the cloud (and *not* on-premises)?"



39% plan to implement or have implemented at least one security offering/ approach through PIM-as-a-service.

Base: 76 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees

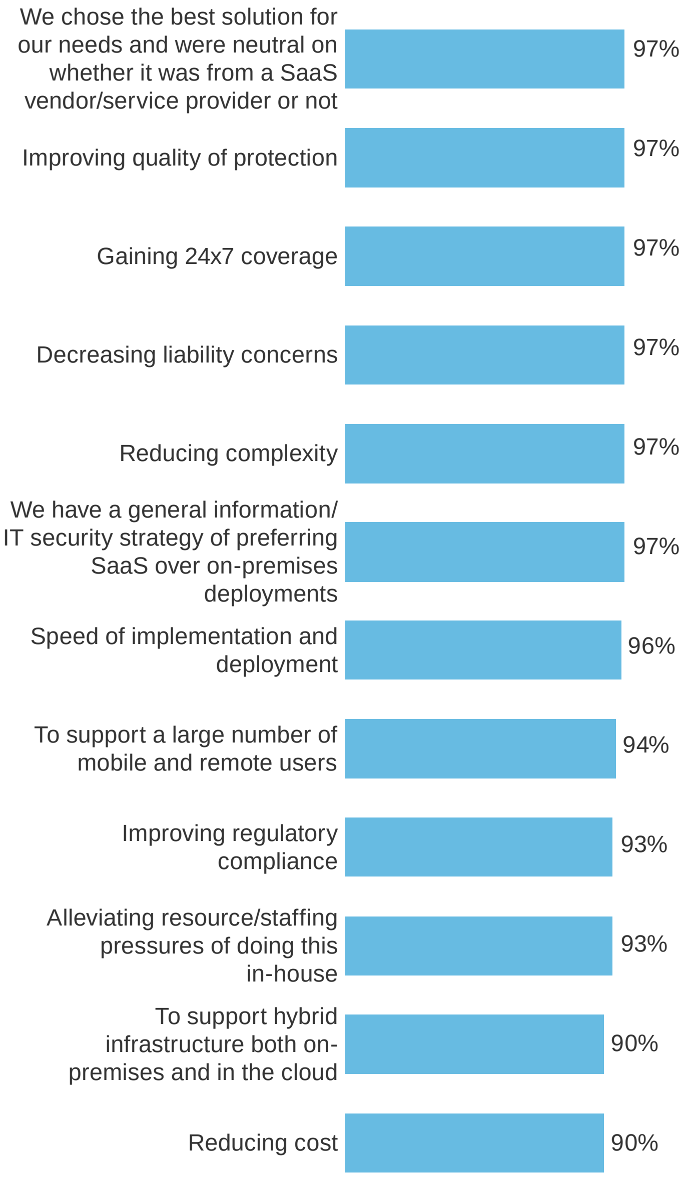
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

- **Secures as effectively as on-premises solutions.** An overwhelming number of decision-makers who have implemented PIM-as-a-service stated it was the best solution, regardless of whether it was cloud-based (97%). Ninety-seven percent also stated that PIM-as-a-service's ability to improve the quality of protection was an important consideration (see Figure 8).
- **Provides unique cloud-based benefits.** Decision-makers who have implemented PIM-as-a-service claimed that the cloud-based advantages were important in their decision to choose the solution. Having 24x7 support (97%), increasing the speed of implementation and deployment (96%), alleviating resources and staff pressures (93%), supporting hybrid infrastructure both on-premises and in the cloud (90%), and reducing costs (90%) were all important or very important considerations (see Figure 8).
- **Promises to solve the problem of numerous identities.** Importantly, 94% of decision-makers chose PIM-as-as-service to solve the pressing challenge of supporting a larger number of remote and mobile users (see Figure 8).

FIGURE 8

Numerous Considerations Drive Decision-Makers Toward PIM-As-A-Service

"How important were the following in driving your organization's interest in adopting cloud as-a-service security offerings?"
(Showing those selecting "important" or "very important" on a 5-point scale)



Base: 30 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees implementing or planning to implement at least one PIM-as-a-service security offering/approach

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

THE MARKET PREFERS A SINGLE PLATFORM

Decision-makers must also understand that there are multiple aspects of privileged identity management that have to be addressed. They need solutions capable of everything from revoking and preemptively denying privileges to users to enforcing context-aware multifactor authentication (see Table 1). The question becomes how to employ all of these functions effectively and in a cohesive manner.

Our study shows that decision-makers gravitate toward a single platform solution to manage all aspects holistically. Results indicate that:

TABLE 1

The Many Aspects Of Effective Privileged Access Security

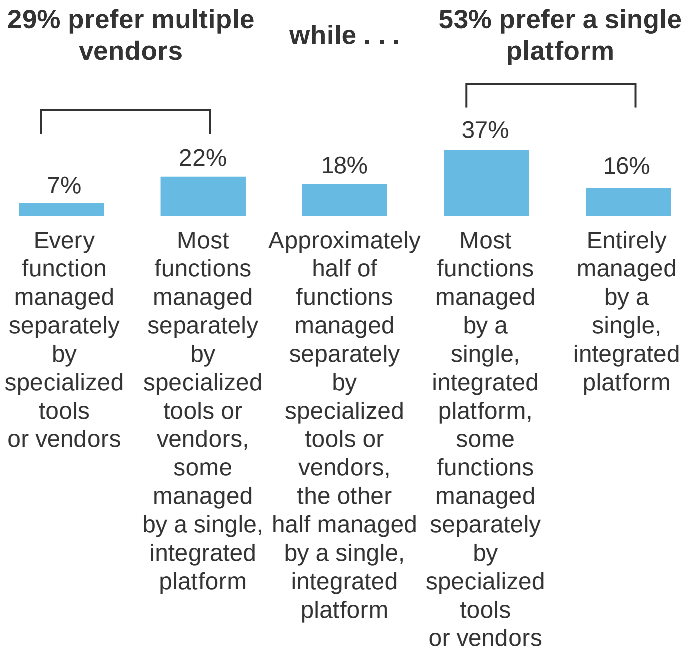
Revoking and preemptively denying extra privileges to users
Conducting periodic access reviews for administrative and privileged users
De-provisioning users' access rights in all applications as soon as they terminate
Enforcing context-aware multifactor authentication
Governing access through time-bound and temporary privileged access (request and approval workflows)
Monitoring privileged sessions
Implementing least-privilege access for administrators
Controlling access to accounts that are shared
Limiting access for remote administrators, contractors, outsourced IT, and outsourced developers to just the systems they manage instead of giving VPN access
Supporting break-glass access to passwords from a mobile device

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015.

FIGURE 9

Decision-Makers Gravitate Toward A Single Platform To Manage Privileged Access Security

"When considering the following aspects of administrative and privileged identity and access management, do you feel these functions would most effectively be executed by either a single, integrated platform or separately as multiple solutions?"



Base: 150 US director or higher IT decision makers in regulated industries at organizations with 500 or more employees

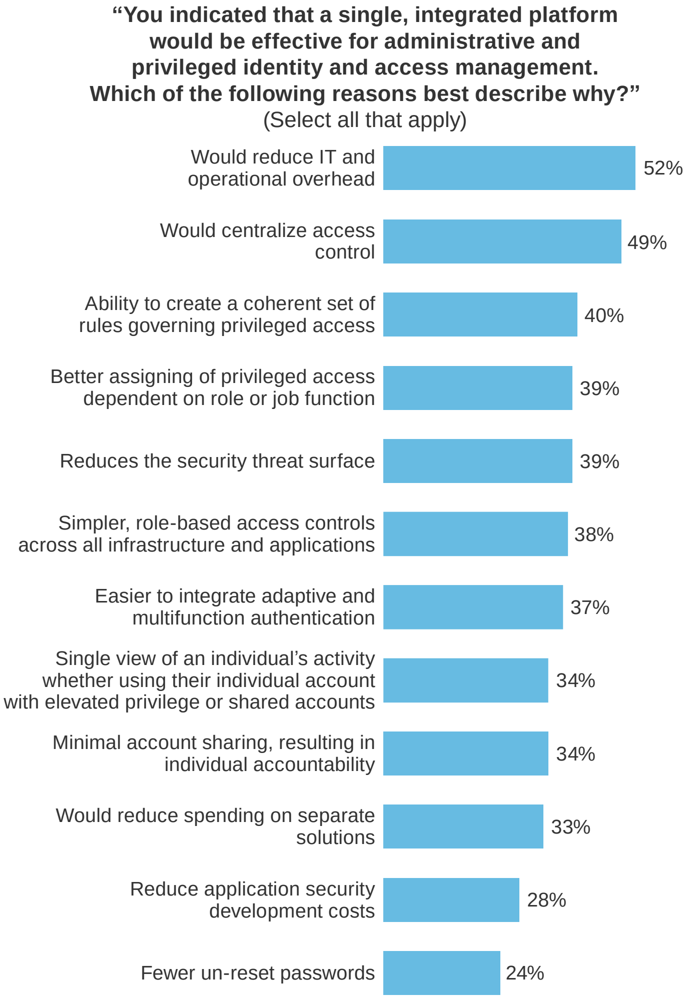
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015.

- **A majority would rather manage most or all functions through a single platform.** Fifty-three percent of decision-makers stated they would prefer to manage the many aspects of administrative and privileged identity management (see Table 1) either mostly or entirely through a single platform, while less than a third prefer working with multiple, specialized vendors to achieve the same end (see Figure 9).

- **Increased efficiency and centralization drive the preference for a single platform**. Reducing IT/operational overhead, centralizing control, and enabling creation of a coherent rule set are the top three reasons decision-makers prefer a single platform (see Figure 10). However, they acknowledge a wide range of potential benefits, including reducing the security threat surface (39%), allowing for minimal account sharing (34%), and easing integration of adaptive authentication (37%) (see Figure 10).

FIGURE 10

Increased Efficiency And Centralization Are The Perceived Benefits Of A Single Platform



Base: 106 US director or higher IT decision-makers in regulated industries at organizations with 500 or more employees who indicate a single, integrated platform would be effective for executing administrative and privileged identity and access management

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2015

Key Recommendations

Data protection and the move to the cloud are business imperatives that security and risk professionals cannot ignore — while they also cannot give up custodianship and protection of data they collect for their customers. Increased use of the private and public clouds has also resulted in more administrative privileges delegated to workforces that are less well understood, such as contractors and outsourcers. This weakens traditional, on-premises controls for identity-centric data protection. To meet these challenges, Forrester recommends the following:

- **If you want to protect your data, pay attention to identities.** Identities are the glue or conduit that actually accesses data and can be used to steal it. Understanding and being able to answer the million dollar question of "Who has access to what, why, and how do we enforce that access?" goes a long way in avoiding a data breach.

- **Do not separate business and privileged access management when it comes to cloud applications.** Threats come not only from business account misuse but also from hackers using privileged accounts — Forrester estimates that 80% of data breaches use some kind of stolen privileged credential. Therefore, it is vital that companies look at business and privileged credentials through the same single pane of glass, and this includes governance as well as enforcement of access control policies.

- **Embrace the cloud for managing business and privileged identities.** As your workloads move to the cloud, secure data in those workloads by having your business and privileged identity management systems follow your data into the cloud. Beyond the trivial cost savings of the implementation and upgrade effort, cloud-based identity and access management systems for business and privileged users offer greater flexibility and better support for cloud-based workloads and remote and outsourced administrators.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 150 IT decision-makers from companies in the US with a title of director or higher to evaluate the current state of privileged identity management, along with associated challenges and benefits gained with solutions in place. Questions provided to the participants asked about their strategic IT security priorities, their use of cloud-based workloads and applications, the extent to which they outsource IT functions and allow remote access to employees, and their stance toward privileged identity and access management. The study began in November 2015 and was completed in December 2015.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

“Navigate The Future Of Identity And Access Management,” Forrester Research, Inc., August 3, 2015