A Forrester Consulting
Thought Leadership Paper
Commissioned By Centrify

February 2017

Stop The Breach: Reduce The Likelihood Of An Attack Through An IAM Maturity Model

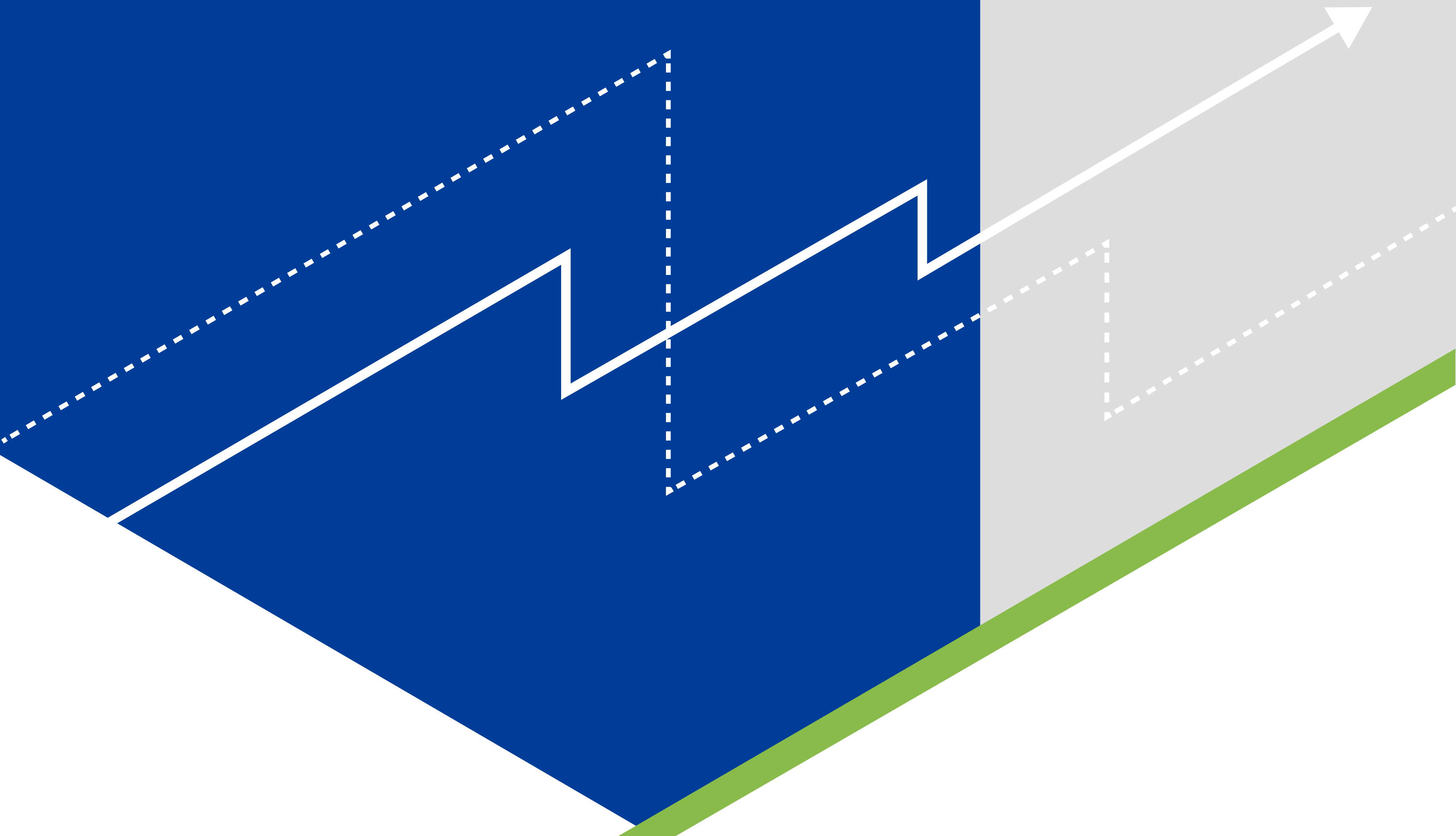


Table Of Contents

Project Director:
Rudy Hernandez, Market Impact Consultant

Project Contributor:
Liz Witherspoon, Total Economic Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

Executive Summary

Security breaches are now commonplace — two-thirds of organizations have experienced one in the past two years, and hackers compromised more than 1 billion identities in 2016 alone.[1] IT security must now become mission critical in order for organizations to both maintain customer trust and prevent financial ruin. It is therefore imperative that they identify the most prescient threats in order to quickly adopt the right practices and technology necessary for survival.

In December 2016, Centrify commissioned Forrester Consulting to evaluate identity and access management (IAM) practices and technology among large enterprises. Forrester specifically tested the hypothesis that increased adoption of IAM best practices — namely those focusing on privileged identity management — correlate to a reduced likelihood of an organization experiencing a breach, which translates to reduced financial loss that an organization must endure. Said one solutions architect from a global bank: "Our biggest fear is that customer data will be stolen with personally identifiable information, leading to data breaches and financial fraud. We're afraid of breaches and unauthorized access that results from that. We're concerned about reputation and data loss — both for the thousands of employees we have and, of course, our customers."

In conducting surveys with 203 IT security decision-makers in North America as well as two in-depth interviews, Forrester found that a maturity hierarchy exists in the marketplace — the most mature groups employ more IAM approaches as well as use integrated IAM technology platforms to reduce security risk and may avoid millions in data breach costs over their less mature counterparts.

KEY FINDINGS

› **Two-thirds of organizations averaged five or more breaches in the past two years.** The number of breaches averaged 4.7 to 7.6 across various areas in the organization, with identities and passwords being primarily targeted.

› **Organizations with the highest IAM maturity experience half the number of breaches as the least mature.** The least mature firms experience twice as many breaches (12.5) as the most mature firms (5.7). Organizations that develop approaches that closely scrutinize and secure both regular and privileged access are more likely to say they have never been breached than those that adopt fewer approaches.

› **IAM maturity saves 40% in technology costs and an average of $5 million in breach costs.** The most mature firms gravitate toward using an integrated platform solution for their IAM technology — reducing technology spend as a proportion of their overall security budget while experiencing fewer costly breaches.

› **IAM maturity generates 90% more productivity and efficiency benefits.** In addition to reducing risk, more mature organizations note that their IAM technology contributes toward improving end user productivity and increasing privileged activity transparency.

An IAM maturity hierarchy exists in the marketplace.

"Our biggest fear is that customer data will be stolen with personally identifiable information. . . . We're concerned about reputation and data loss — both for the thousands of employees we have and, of course, our customers."

Solutions architect, Global bank

Organizations Are Breached At An Alarming Rate

Managing identity in an increasingly mobile, outsourced, and cloud-based landscape presents significant challenges for today's security personnel. Many organizations allow too many employees to have privileged access to systems, neglect to update employees' access when they change roles or leave the company, or do not enforce multifactor authentication. All of these increase the risk of inappropriate access, leading to data breaches.

Indeed, the urgency to come up with solutions in this new landscape has never been greater. Security compromises and data breaches regularly make both business and political headlines. More than 1 billion customer records were accessed by hackers in 2016.[2] Forrester predicts the ramifications of cybersecurity breaches in 2017 will cause more havoc and affect more industries than ever before.[3]

> "The threats we don't know about are even more dangerous — that keeps me up at night. The things I know about I can do something about — the things that I don't know about make me anxious."
>
> *Solutions architect, Global bank*

This study validates these conclusions. Responses indicate that:

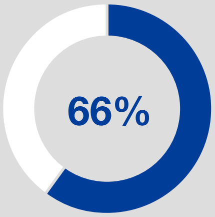
- **Two-thirds of organizations averaged five or more breaches in the past two years.** Sixty-six percent of decision-makers said that they are aware of a security breach that occurred within the past two years, with the number of breaches averaging 4.7 to 7.6 across various areas in the organization (see Figure 1). Every record breached — with an average of 3,450 records per breach — has a cost associated with it. These costs are both direct and indirect, and organizations seek to understand the cause of a breach and provide support to customers affected. Costs can include response and notification costs, lost employee productivity and turnover, lawsuits and settlements, regulatory fines, additional security and audit requirements, and brand recovery costs.[4]

> "Privileged access is how you get breached — with no control over privileged accounts, the bad guys can get a hold of that, and it's typically how they occur. Someone with elevated privileged gets access to your system or network to get the data out. It's a good thing to have tight control over."
>
> *Director of information security, major US consumer product manufacturer*

- **IT security doesn't know what it doesn't know.** For every data breach that occurs, there may be others that have yet to be discovered or may remain undiscovered for months or years. Said one customer interviewed for this study, "The threats we don't know about are even more dangerous — that keeps me up at night. The things I know about I can do something about — the things that I don't know about make me anxious."
- **Breaches affect identities and passwords over other records.** When asked to recall the effects of the last breach they experienced, decision-makers noted that identities and passwords (57%) are more likely to be affected than customer records (49%), intellectual property (27%), or nonpublic financials (21%) (see Figure 2). Said one acting chief information security officer (CISO): "Privileged access is how you get breached — with no control over privileged accounts, the bad guys can get a hold of that, and it's typically how they occur. Someone with elevated privileged gets access to your system or network to get the data out. It's a good thing to have tight control over." Indeed, Forrester estimates that 80% of security breaches involve privileged credentials.[5]

Figure 1

"To the best of your knowledge, has your organization ever experienced a security breach?" (Those indicating they have experienced a breach within the past two years)



"Think of the last breach — how many data records were affected?" (Average among those not selecting "Don't know")*

3,450

"How many breaches have occurred during the past two years?" (Average among those not selecting "Don't know")

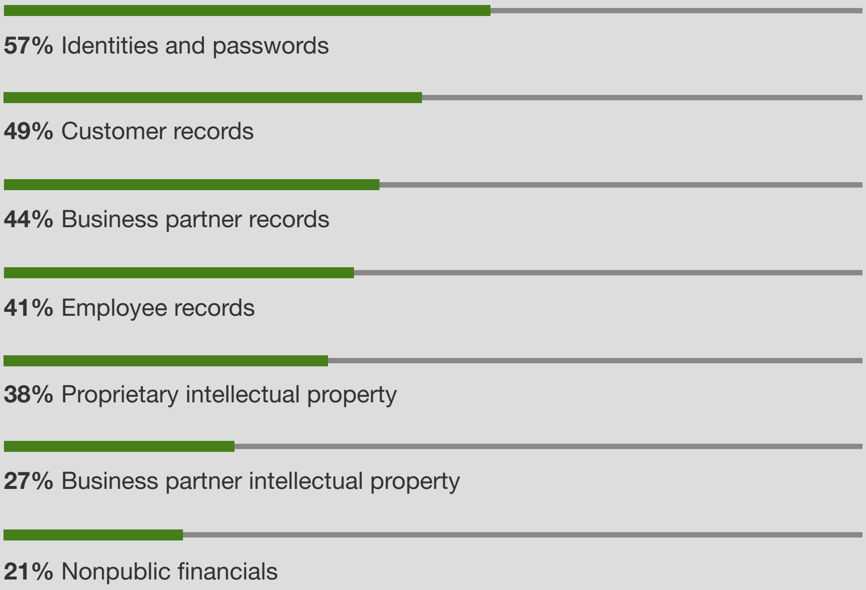
Servers	**4.7** (N = 75)
Endpoint devices	**6.6** (N = 72)
Databases	**5.2** (N = 65)
Network	**5.8** (N = 79)
On-premises apps	**5.4** (N = 66)
SaaS apps	**7.6** (N = 64)
IaaS/PaaS	**6.2** (N = 49)

Two-thirds of decision-makers say that they are aware of a security breach that occurred in their organization within the past two years.

Base: 100 identity and access management decision makers in North America
*Base: 133 identity and access management decision makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Figure 2

"Which of the following types of data were affected in the last breach that occurred?" (Select all that apply)



Identities are affected more than any other type of data when breaches occur.

Base: 203 identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

An IAM Maturity Hierarchy Exists Across Organizations

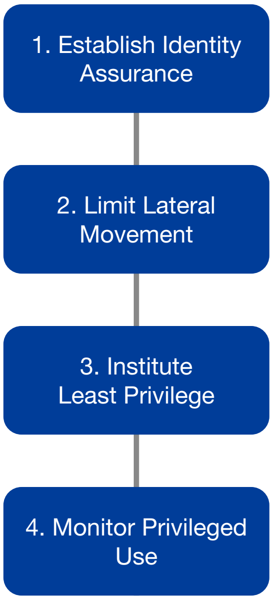
In order to reduce the incidence of security breaches, this study assessed whether organizations that apply more identity and access management approaches are less likely to encounter risk. We specifically evaluated 15 different identity and access management approaches organizations can take — observing both how widespread they are and what benefits they bring to the organizations that employ them. Additional weight was given to approaches that are more advanced and seek to prevent the problem of improper use of privileged access — the rationale being that accounts that have a greater sweep of power would be able to wreak more havoc if misused.

Each approach was first assigned a point value from 1 to 4 (see Figure 3), with:

- **Approaches assigned a value of 1 indicating attempts to establish *identity assurance*.** At this level, organizations are moving beyond passwords and attempting to require more identifiers for authenticating users accessing applications. This encompasses requiring multifactor authentication from end users, consolidating identities across systems of use into a single directory, and implementing single sign-on for multiple applications and log-ins.
- **Approaches assigned a value of 2 indicating attempts to *limit the lateral movement of users* toward acquiring privileged access.** These approaches move further — from confirming a user's identity to confirming that granting privileged access to the system is controlled and automated. This ranges from conducting periodic reviews of privileged accounts, limiting the access given to remote accounts, establishing time-bound parameters for privileged use, and automating role-based provisioning/deprovisioning.
- **Approaches assigned a value of 3 indicating the institution of *"least privilege."*** Approaches at this level focus on limiting the access level of privileged accounts — reducing the number of accounts, distributing privileged permissions, etc. Specific approaches here include eliminating shared administrative accounts, centrally controlling access to privileged accounts, and managing privileged access at either the command or application level.
- **Approaches assigned a value of 4 indicating efforts to *monitor privileged use*.** At the highest level, privileged access is even more tightly controlled. All privileged access and actions are monitored and logged in an effort to give security decision-makers a clear view of all activity occurring in their organization. Organizations are able to "record" actions taken by these users and play them back to review their actions if needed.

We then applied this scoring to the IAM approaches each organization employed, tallying up a score based on the rank assigned to each approach (see Figure 3). As a result, each organization received an overall score from 0 through 34. When observed across the entire sample, four levels of maturity emerged — from those at Level 1 with the lowest score to those at Level 4 with the highest. The distribution was relatively even across the sample, but tilted toward lower levels of maturity (see Figure 4).

Four Elements Of IAM Maturity



1. Establish Identity Assurance
2. Limit Lateral Movement
3. Institute Least Privilege
4. Monitor Privileged Use

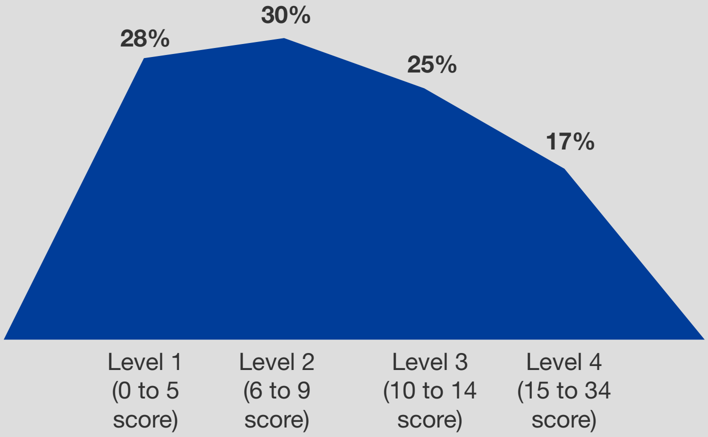
Figure 3

Identity and access management approach	Value given
Enforcing context-aware multifactor authentication	1
Consolidating identity stores into a single directory	1
Implementing single sign-on	1
Conducting periodic access review for administrative and privileged users	2
Limiting access for remote identities to just the applications or systems they immediately require	2
Governing access through time-bound and temporary privileged access	2
Automating role-based provisioning and deprovisioning to apps and infrastructure	2
Automating mobile app provisioning and deprovisioning	2
Automatically deprovisioning privileged users' access rights in high-risk environments when they terminate	3
Implementing least-privilege access for administrators	3
Centrally controlling access to shared and service accounts	3
Eliminating shared administrative accounts	3
Managing privileged access at the granular command or app level	3
Actively monitoring all privileged sessions and commands	4
Recording all privileged sessions and commands	4

Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Figure 4

Levels Of Identity And Access Management Maturity



An IAM maturity hierarchy exists in the marketplace.

Base: 203 identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

IAM Maturity Reduces Risk Of Breaches

In observing the IAM maturity across the sample in this study, more mature groups — those adopting a greater number of more advanced approaches (in addition to more approaches overall)—were found more likely to experience fewer security breaches. There are likely a number of different factors determining why certain organizations are less likely to experience security breaches, but this study finds a correlation between implementing more IAM capabilities — especially adopting best practices around privileged identity management — and a reduction in security incidents. Results show that:

- **High IAM maturity means employing more IAM approaches.** Organizations in the least mature group in this study, Level 1, employ an average of two identity and access management approaches. This number increases as maturity increases. It jumps to 3.5 for those at Level 2, about five for those at Level 3, and then culminates in an average of eight approaches for Level 4, the most mature group (see Figure 5).
- **Privileged identity management (PIM) approaches align with high IAM maturity.** PIM approaches precipitously increase as firms move along the maturity spectrum — particularly recording privileged sessions (53%) and implementing least-privilege access (41%) among the Level 3 firms versus Level 2 firms (7% and 23%, respectively). Naturally, Level 4 firms are the most likely to employ privileged identity management approaches. They are no less than 40% likely to implement least-privilege access and up to 77% likely to record privileged sessions. Meanwhile, only 37% of those at Level 1 will periodically conduct reviews of privileged accounts and are less than 20% likely to employ any other single PIM approach (see Figure 5).

Figure 5

"Are any of the following approaches to identity and access management performed at your organization?"

	Level 1 (N = 57)	Level 2 (N = 60)	Level 3 (N = 51)	Level 4 (N = 35)
Record all privileged sessions and/or commands	5%	7%	53%	77%
Actively monitor privileged sessions and/or commands	12%	23%	37%	71%
Conduct periodic access review for administrative and privileged users	37%	32%	31%	69%
Limit access for remote administrators, contractors, outsourced parties	14%	33%	43%	69%
Centrally control access to shared and service accounts	7%	27%	27%	69%
Automatically deprovision privileged users' access as they terminate	9%	25%	27%	69%
Manage privilege elevation at the granular command or app level	9%	30%	45%	57%
Enforce context-aware multifactor authentication	26%	22%	20%	57%
Do not have shared administrative accounts	7%	15%	27%	57%
Govern access through time-bound and temporary privileged access	9%	23%	18%	49%
Automate mobile application provisioning	14%	23%	35%	46%
Implement single sign-on	16%	20%	31%	43%
Implement least-privilege access for administrators	4%	23%	41%	40%
Automate role-based provisioning to apps and infrastructure	9%	18%	22%	37%
Consolidate identity stores into a single directory	21%	27%	24%	34%
Average number of approaches performed	**2.0**	**3.5**	**4.8**	**8.4**

Level 4 firms are far more likely to perform **privileged identity management approaches.**

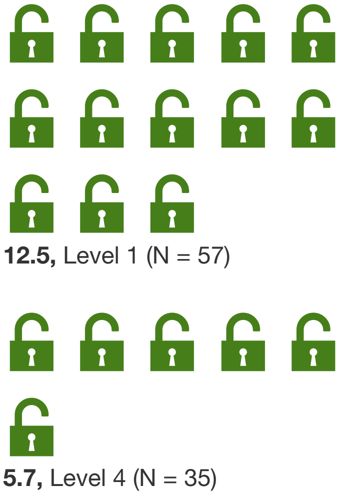
Base: Identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

- **Forty-nine percent of Level 4 firms, on average, are likely to never experience a security breach across six key areas, compared with 32% of Level 1 firms.** In a number of areas within an organization — the network (43%), across servers (46%), among on-premises apps (46%), in databases (51%), and in cloud applications (46% for SaaS, 63% for IaaS/PaaS) — an average of 49% of Level 4 firms reported that they have never experienced a security breach. This is higher than those in Level 3 (27%), Level 2 (29%), and Level 1 (32%) (see Figure 6).
- **The most mature firms experience half as many breaches as the least mature firms.** Across all areas, Level 1 firms experience an average of 12.5 breaches. By comparison, Level 4 firms only experience 5.7 (see Figure 7).

Level 4 firms experience about **50% fewer breaches** than Level 1 firms.

Figure 7

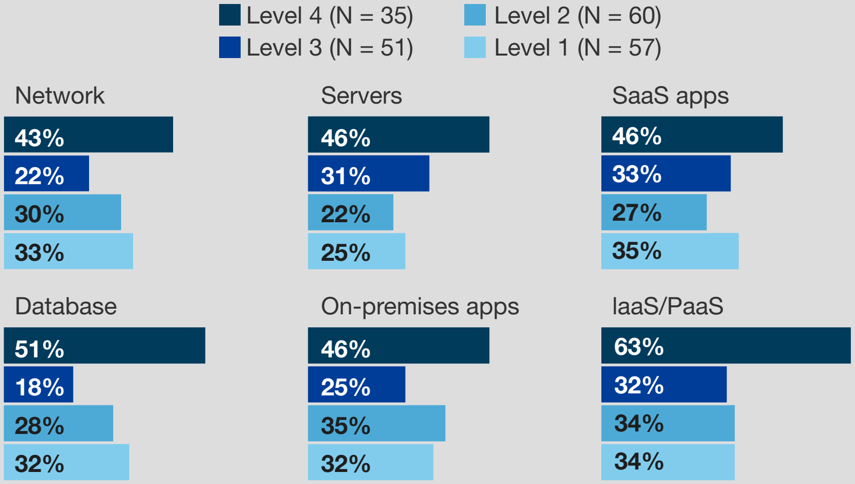
"How many breaches have occurred during the past two years?"
(Average among those not selecting "Don't know")



Base: Identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Figure 6

"To the best of your knowledge, has your organization ever experienced a security breach that affected any of the following areas?"
(Showing those selecting "Have never experienced a breach in this area")



Base: Identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

High maturity correlates with reduced likelihood of experiencing a security breach.

IAM Maturity Reduces Technology And Breach Costs

Interestingly, this study found that Level 4 firms — those with the most mature identity and access management stance — gravitate toward integrated platforms, which are solutions that allow them to consolidate multiple IAM technologies in order to employ the approaches above. Said one solutions architect: “As companies mature, the tendency is to go toward a single platform as much as possible. Overall, with a platform, our environment is more secure, and we can deploy things more easily and quicker and manage access more efficiently as result.”

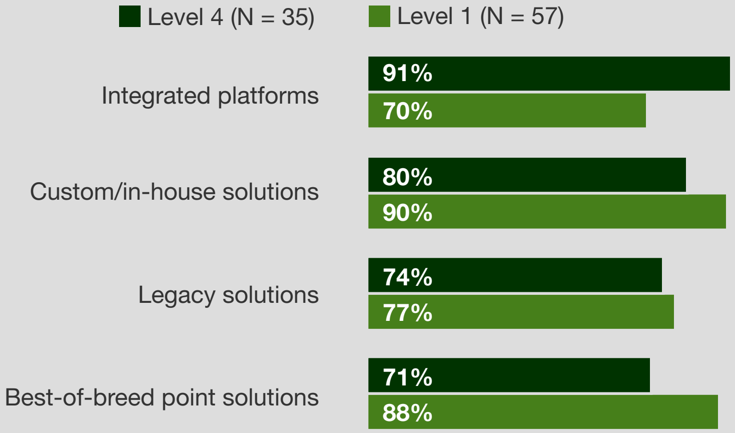
> “As companies mature, the tendency is to go toward a single platform as much as possible. Overall, with a platform, our environment is more secure, and we can deploy things more easily and quicker and manage access more efficiently as result.”
>
> *Solutions architect, Global bank*

This technology preference correlates to even more benefits, given that the Level 4 firms can utilize more technology through an integrated platform at a lower cost than by buying point solutions. When considering that they are also less likely to experience a security breach, Level 4 firms experience less of a financial cost due to their combined process and technology stance over their less mature counterparts because:

- **Level 4 firms are most likely to use integrated platforms and least likely to use point solutions.** Ninety-one percent of these organizations have an integrated platform for IAM, which is more than those using custom solutions (80%), existing legacy solutions (74%), or individual point solutions (71%). Meanwhile, integrated platforms are the least used technology solutions (70%) among Level 1 firms (see Figure 8).
- **Level 4 firms save 40% on IAM technology costs.** Integrated platform use among Level 4 firms contributes to overall technology cost savings. While Level 4 firms spend more in overall IAM as well as in IT security generally versus Level 1 firms, they spend 40% less on the actual IAM technology as a percentage of their entire IAM budget (19% versus Level 1 firms’ spend of 27%) (see Figure 9). That equals $2,582,000 that a company could reinvest elsewhere if it matched its mature counterparts’ approaches. It is important to note that those interviewed for the study cautioned about the cost of switching technologies along with associated labor costs.
- **Level 4 firms average $5 million in cost savings.** Fewer breaches translate to less money lost. Assuming that an average of 3,450 of records are affected per breach (see Figure 1), there is a stark difference between the costs absorbed for Level 4 and Level 1 firms. The cost avoidance for Level 4 firms can total in the millions of direct and indirect costs avoided. On average, Level 1 firms endure $5,184,600 more in costs than Level 4 firms (see Figure 10).

Figure 8

“Which of the following types of identity and access management (IAM) technologies/platforms does your organization currently have in place?”
(Rolled up for all technologies selected)



Base: 203 identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Organizations with the highest level of IAM maturity are more likely to use integrated platforms.

Figure 9

	Level 1 (N = 57)	Level 4 (N = 35)
Average total IT security budget (in USD)	$161,000,000	$263,000,000
Average total IAM security spend (in USD)	$32,200,000	$52,600,000
Average IAM technology spend (in USD)	$8,700,000	$9,900,000
Average percent of IAM technology spend of entire IT security budget	**27%**	**19%**

Base: Identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Level 4 firms spend 19% of their overall IAM budget on technology — **40% less** than Level 1 firms.

Figure 10

	Level 1 (N = 57)	Level 4 (N = 35)
Average number of breaches experienced	12.5	5.7
Average number of records affected during a breach	3,450	3,450
Cost suffered (at an average of $221 per record)	**($9,530,625)**	**($4,345,965)**

Base: Identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Level 1 firms endure **$5,184,600** more in costs than Level 4 firms.

IAM Maturity Generates 90% More Productivity And Efficiency Benefits

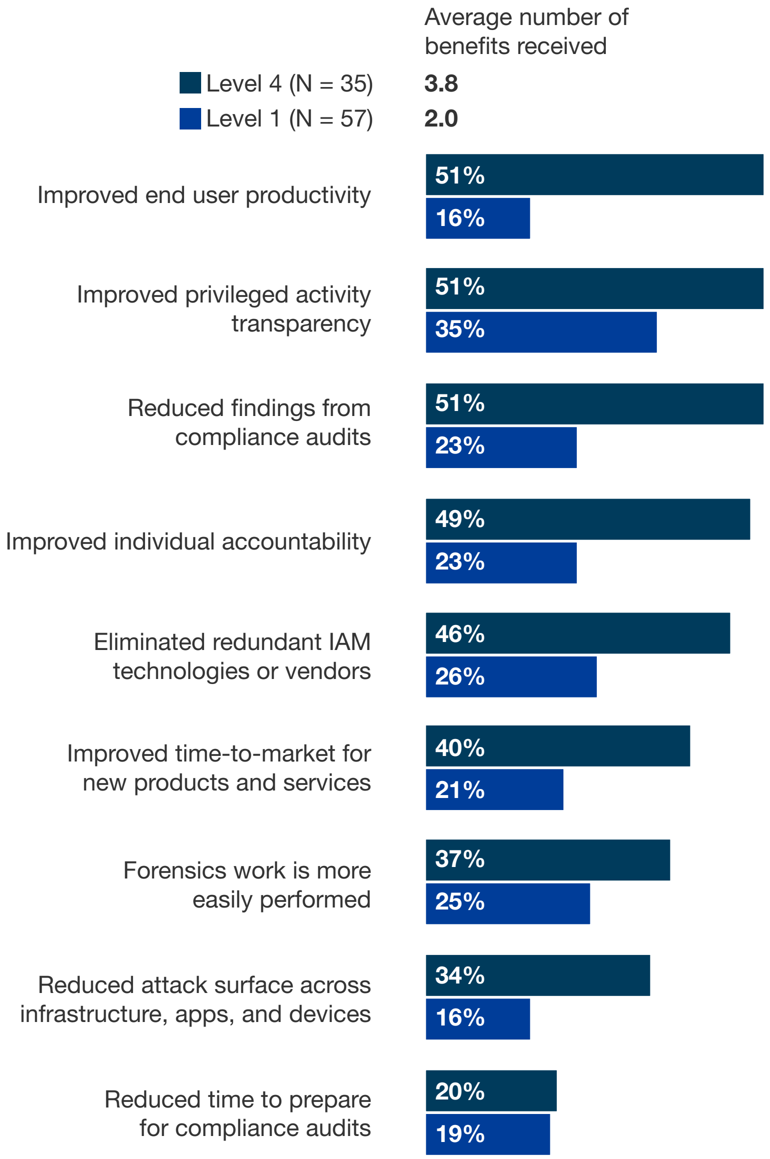
Benefits extend beyond technology cost savings and reduced breach costs. The tendency of Level 4 firms to lean toward integrated IAM platforms means that they can gain efficiency, productivity, and transparency benefits as well. These translate down the line to overall business efficiency, helping the bottom line. Results indicate that:

- **Level 4 firms receive 90% more benefits from their choice in IAM technology.** They receive an average of 3.8 benefits while Level 1 firms receive two. Notably, they are more likely to observe end user productivity gains (51%), improved privilege activity transparency (51%), reduced findings from compliance audits (51%), and reduced IAM technology redundancy (46%) benefits than other groups (see Figure 11).
- **Tactical benefits translate to overall savings.** Although not quantified in this study, these additional benefits could result in thousands of dollars more in calculated financial gains for an organization. For example, compliance audits require a significant investment of IT resources to prepare for and — if firms are not compliant — remediate the issues through process and technology redesign. Said one solutions architect: "As a security organization, we obviously have to deal very often with audits — compliance and regulation is a big-time suck, and it's a big factor in everything we think about and do. We focus on security for the sake of security in the hopes of having more secure systems, data and, if at the end of the day we've achieved higher levels of security, we know that we comply better."

> "As a security organization, we obviously have to deal very often with audits — compliance and regulation is a big-time suck, and it's a big factor in everything we think about and do. We focus on security for the sake of security in the hopes of having more secure systems, data and, if at the end of the day we've achieved higher levels of security, we know that we comply better."
>
> *Solutions architect, global bank*

Figure 11

“Which of the following benefits has your organization experienced with its current set of identity and access management (IAM) technology?” (Select all that apply)



Base: Identity and access management decision-makers in North America
Source: A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016

Level 4 firms experience **90% more** benefits than Level 1 firms.

Key Recommendations

The conclusions from this study highlight a path forward for IT security decision-makers who wish to guard their organization against an exponentially growing number of threats and their associated costs. Those who seek to make identity and access management a priority and wish to mature their organization's IAM posture should:

Utilize integrated suites as a key part of moving up the IAM maturity ladder. Most organizations have hybrid environments and rely on a mix of on-premises and cloud applications. While point products may still be required to meet certain needs, moving toward centralized control and access results in lower management costs and better monitoring and visibility into potential identity and access management threats. As such, IT security decision-makers should make best efforts to streamline operations with a single, integrated platform whenever possible in order to better develop consistent IAM policies and better achieve operational efficiency.

Understand that PIM is a quick and easy win for the least mature organizations to pursue. A key marker of IAM maturity is preventing unauthorized use of privileged accounts. Forrester predicts that 80% of breaches involve privileged credentials. Developing an IAM framework and putting practices into place that put privilege front and center will have an immediate effect on lowering your organization's threat exposure.

Know that IAM is 70% people, process, and politics and only 30% technology. Adopting the best technology solutions can only get you so far. Decision-makers must first clear the ground and ensure that their organization is ready to make necessary changes to procedures, personnel, and culture in order for a mature security framework to effectively operate. This includes getting executive sponsorship, developing clear metrics for success, and establishing clear lines of communication between key stakeholders.

Acknowledge that, most importantly, high IAM maturity brings business agility. IT security decision-makers must be mindful of how the security procedures and technologies they pursue affect the business' ability to win, serve, and retain customers in a quick-moving marketplace. When companies live or die by their ability to deliver digital experiences, business agility is all-important. That is why it is important to stress that high IAM maturity goes hand in hand with agility — employing IAM approaches that work with the flow of business and not against it. Ultimately, this more mature posture results in fewer breaches, meaning less downtime and damage control and increased end user productivity.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 203 IT decision-makers in North America belonging to organizations with 2,000 or more employees to evaluate identity and access management practices. Survey participants were required to have authority over identity and access management decisions in their organization. Forrester also conducted in-depth qualitative interviews with two organizations in the financial services and manufacturing industries that have implemented IAM platforms within the past five years to understand the benefits and costs of that implementation. Questions provided to the participants asked about budget spend, technology usage, approaches employed, challenges faced, and benefits received. The study began in November 2016 and was completed in December 2016.

Appendix B: Supplemental Material

RELATED FORRESTER RESEARCH

"Optimize Your Identity And Access Management Program For Success," Forrester Research, Inc., June 14, 2016

"Calculate The Business Impact And Cost Of A Breach," Forrester Research, Inc., November 17, 2016

"The Forrester Wave™: Privileged Identity Management, Q3 2016," Forrester Research, Inc., July 8, 2016

Appendix C: Endnotes

[1] Source: "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016," Forrester Research, Inc., January 9, 2017.

[2] Source: "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016," Forrester Research, Inc., January 9, 2017.

[3] Source: "Predictions 2017: Cybersecurity Risks Intensify," Forrester Research, Inc., November 1, 2016.

[4] Source: "Calculate The Business Impact And Cost Of A Breach," Forrester Research, Inc., November 17, 2016.

[5] Source: "The Forrester Wave™: Privileged Identity Management, Q3 2016," Forrester Research, Inc., July 8, 2016.