BeyondTrust

Privileged Access Threat Report 2019

Greater visibility and improved integration are vital to tackling the modern threat landscape

TABLE OF CONTENTS

Introduction

The world is an uncertain place. Particularly for cyber security professionals, many of whom have learned the hard way that they can't rest on their laurels. New technologies and fresh threats are constantly emerging, and these threats come from both outside and within organizations. In our 2019 privileged access threat research, we discovered that almost two thirds of respondents (**64%**) think it is likely they've suffered a breach due to employee access, while **58%** say the same about vendors.

Meanwhile, the devices intended to make life easier can expose businesses further. Although hostile, external attacks are considered a significant or moderate concern by **61%** of businesses, the threat of misused or abused insider access follows very closely behind at **58%**. At the same time, **57%** of security decision makers perceive at least a moderate risk from Bring Your Own Device (BYOD) policies and the Internet of Things (IoT) at **57%**.

In this fourth edition of BeyondTrust's annual Privileged Access Threat Report, we'll be exploring the 2019 threat landscape in detail, with a focus on how security decision makers are utilizing Privileged Access Management (PAM) solutions to mitigate these risks.

Perceived Threats

From employee breaches to vendor trust, and from preferred solutions to emerging threats, the Privileged Access Threat Report discusses not just the challenges decision makers are facing, but also the most effective ways of addressing them.

Key Findings

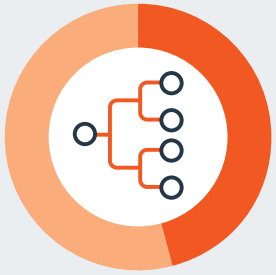
Insider Threats

64%

of respondents believe they have suffered a breach due to misused or abused employee access

90%

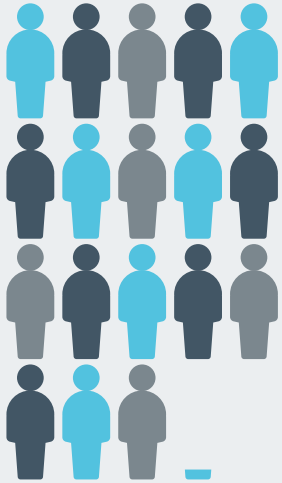
of those with fully integrated PAM tools are confident they can identify specific threats from employees with privileged access



46%

feel their solutions are fully integrated

Vendor Threats



182

average number of vendors logging into IT systems every week

58%

believe to have vendor-related breaches

Trust Level Impacts

37% "I completely **trust my employees**"

25% "I completely **trust my vendors**"

The Risk from Within

When you hear the phrase 'cyber threat', it's natural to imagine an intentional, malevolent external risk. Yet, the reality is that compromised access management for employees is a big problem too.

The level of perceived threat from insiders has remained consistent year over year. Two thirds (**64%**) of our survey respondents believe they've likely had either a direct or indirect breach due to employee access in the last 12 months, in comparison to **66%** to 2018. In France and APAC, the numbers are even higher, rising to **69%** and **70%** respectively.

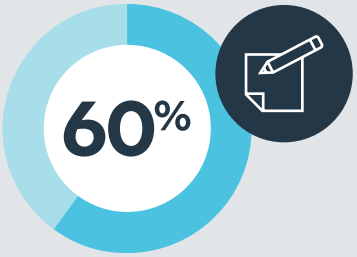
But are these insider breaches the result of intentional, malicious actions or inadvertent errors?

The level of concern around intentional misuse of sensitive data for personal gain has dropped 5% from the year before, and just over half (**52%**) are very or fairly concerned about sabotage from a former employee.

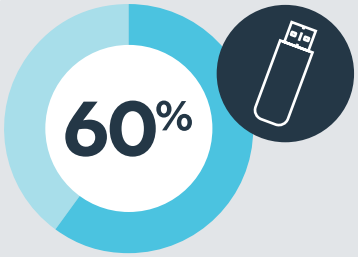
However, unintentional employee breaches are a bigger issue for our respondents, with **62%** worried about the unintentional mishandling of sensitive data by an employee.

The prevalence of each threat varies from region to region. Only **20%** are worried about downloading data onto a memory stick in the UK, while **42%** see this as an issue in APAC. Employees in Germany are the most likely (**30%**) to tell colleagues their passwords.

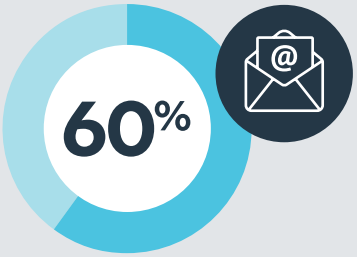
Unintentional Threats



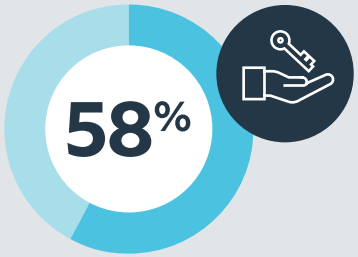
Writing down passwords



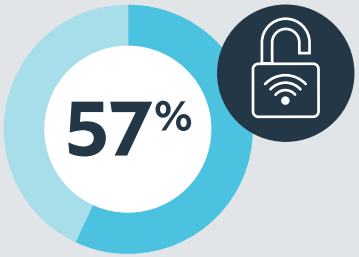
Downloading data onto an external memory stick



Sending files to personal email



Telling colleagues their passwords



Logging in over unsecured WiFi

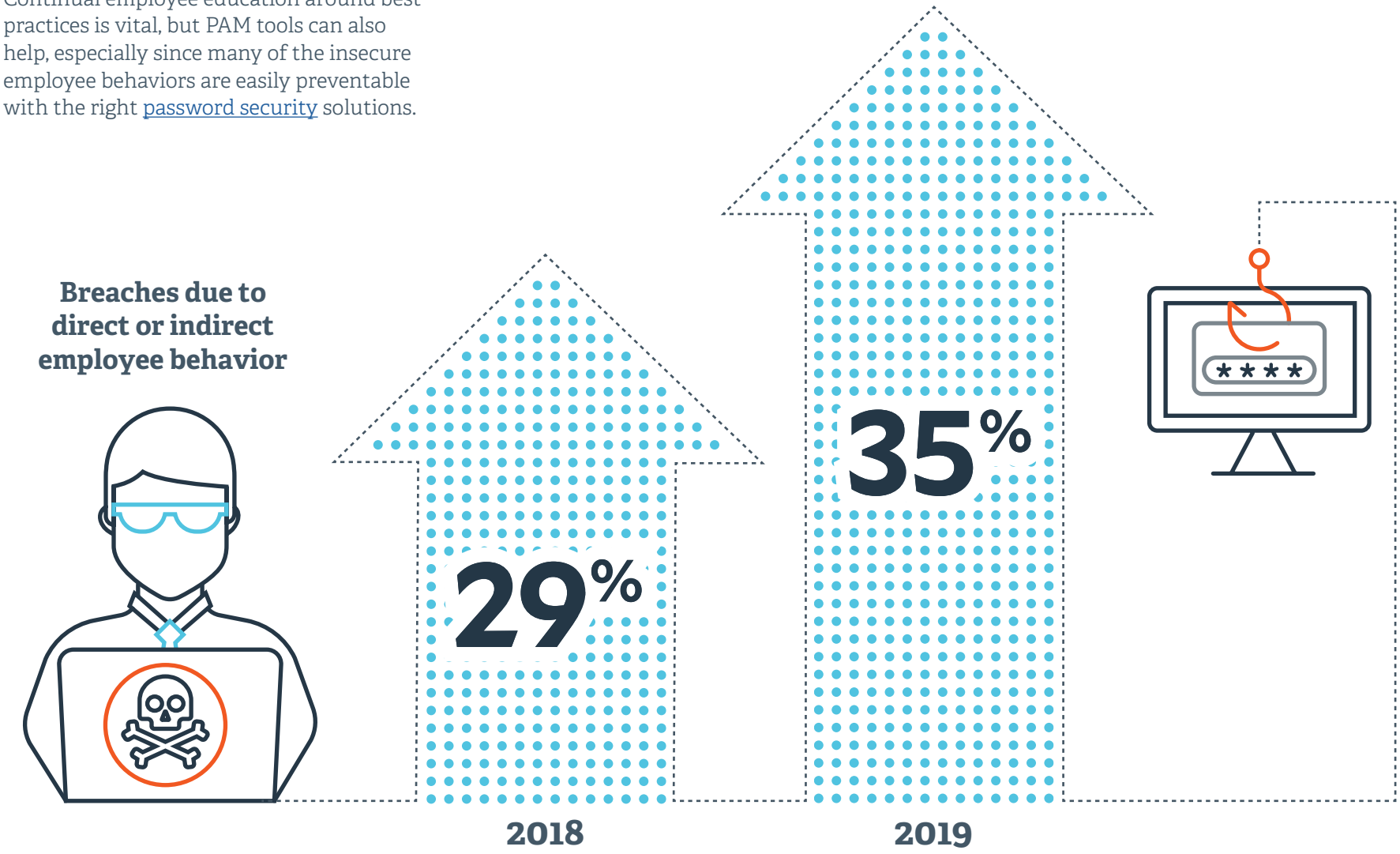
Staying logged on

The Risk from Within

Ultimately, **71%** of organizations agree that they would be more secure if they restricted employee device access. However, this isn't usually realistic, let alone conducive to productivity. So, what can security decision makers do to reduce the risks related to employee access?

Continual employee education around best practices is vital, but PAM tools can also help, especially since many of the insecure employee behaviors are easily preventable with the right password security solutions.

In 2019, **35%** of respondents were certain that they had experienced a breach due to direct or indirect employee behavior, up from **29%** the previous year.



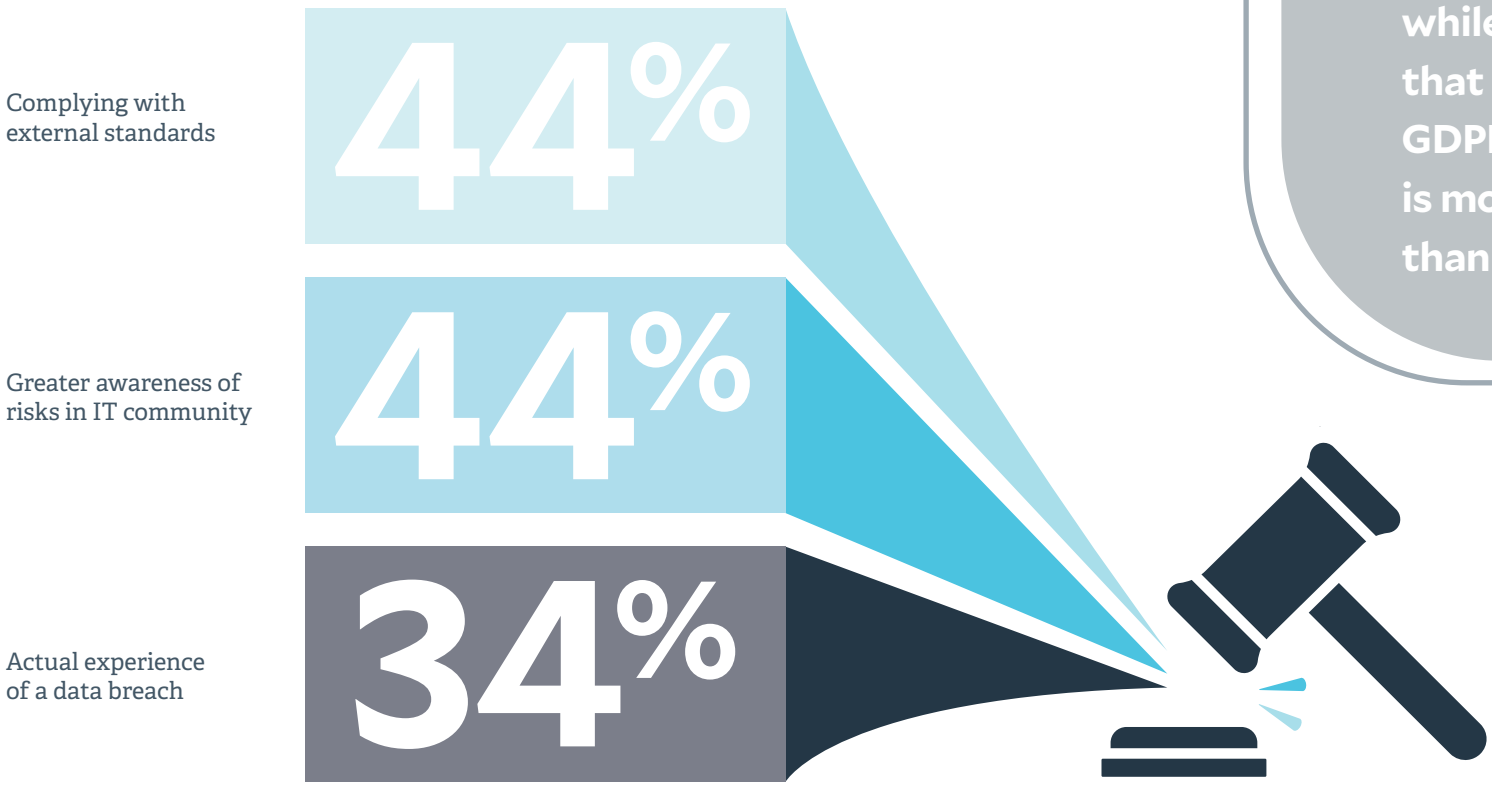
What's Driving Policy: Internal Problems or External Factors?

External factors such as compliance mandates are imposing a big impact on employee access practices. Almost half (**44%**) say that complying with external standards is having a significant effect on the way they're governing employee access. This is even more notable in Germany (**54%**) and France (**53%**), which may be a consequence of heightened concerns around GDPR or other regulatory compliance.

On top of this, **44%** feel that greater awareness among the IT community is driving policy – while four in ten are battling unintended data loss from employees using unsecured devices. The actual experience of data breaches from employees or ex-employees is less of a factor, with just **34%** saying it's impacting their procedures and policies. However, this rises significantly to **53%** in APAC – a region in which decisions makers are also much more driven by focus from the Board (**41%**).

Since implementation one year ago, GDPR is making its impact felt: 65% agree GDPR compliance continues to affect their business, while 58% say that remaining GDPR compliant is more difficult than expected.

Policy Drivers



More Vendors, More Exposure, Less Confidence

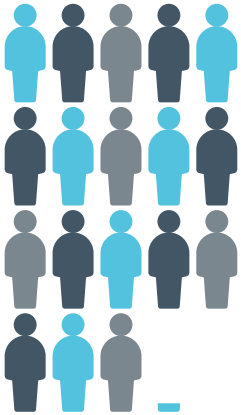
In addition to managing employee access, security professionals must also control vendor access, where the perceived threat remains high. In 2018, **62%** believed they'd had a breach due to vendor access. This year, **58%** say the same, with a quarter believing they have definitely had a breach as a result of vendor behavior. The figures vary by region. UK and Germany perceive the least number of breaches while APAC sees significantly more.

Unfortunately, the certainty decision makers feel around managing vendor access has fallen year over year. Just **25%** are very confident that they know how many third-party vendors are accessing their systems, down from **38%** last year. Only **31%** are very confident they know how many individual logins can be attributed to third-party vendors.

The trust level for vendors also trails that of employees, with only **20%** saying they completely trust vendors, in comparison to **37%** who feel similarly about employees.

With two thirds of businesses believing it's likely they have experienced a breach from compromised vendor access, the need to address how they control vendor access is clear. While businesses can't avoid giving vendors and other legitimate users the access they need, they do need to find ways of providing Secure Remote Access that maintains the integrity of an organization's security.

Vendor Access by the Numbers



182

Average number of vendors logging into IT systems every week

58%

Believe to have vendor-related breaches

only 29%

are very confident they know how many third-party vendors are accessing their systems

At organizations with 5,000+ employees, 23% say they have more than 500 vendors logging in regularly, highlighting the sheer scope of risk exposure.

3 = Magic Number

As our research indicates, organizations are clearly confronted with a number of challenges around privileged access for both employees and vendors. So, what are decision makers currently doing to combat these threats, and what strategies should they employ to make the most of Privileged Access Management (PAM) solutions in the future?

On average, organizations are currently using four different methods of password management for privileged credentials. When it comes to mitigating breaches, almost all (**96%**) organizations try to control access through privileged credential management tools. Three quarters restrict the use of shared admin passwords, while **72%** regularly rotate admin passwords.

Only a small fraction (**7%**) of businesses don't have any distinct PAM tools in place. Over half have one or two PAM-related tools, while **40%** have three or more installed. For this last group, remote access and password management seem to be the most widely adopted technologies. The majority (**91%**) have Secure Remote Access / Support, while **87%** have a Privileged Password Manager / Credential Store solution in place.

The value of these solutions is self-evident. Organizations with three or more PAM tools have more confidence in their visibility of threats and where these have originated from, enabling them to more successfully address these risks. Of this group, **43%** believed they had the ability to definitively attribute a cyber breach to employee access, in comparison to just **15%** of those with no PAM tools. Likewise, **61%** with three or more tools could possibly or definitely attribute cyber breaches to vendor access, while only a quarter (**26%**) of those with no tools could say the same.

Meanwhile, those with more PAM tools feel significantly more confident monitoring enterprise-wide visibility into privileged user access, reporting on individual user activity, and identifying specific threats from employees with elevated user privileges.

Tactics to Combat Threats

96%

try to control access through privileged credential management tools

66%

restrict the use of shared admin passwords

72%

regularly rotate admin passwords

40% of respondents are using three or more PAM tools in their organization; of those 43% can definitively attribute breaches to employee access (vs. only 15% of those with none).

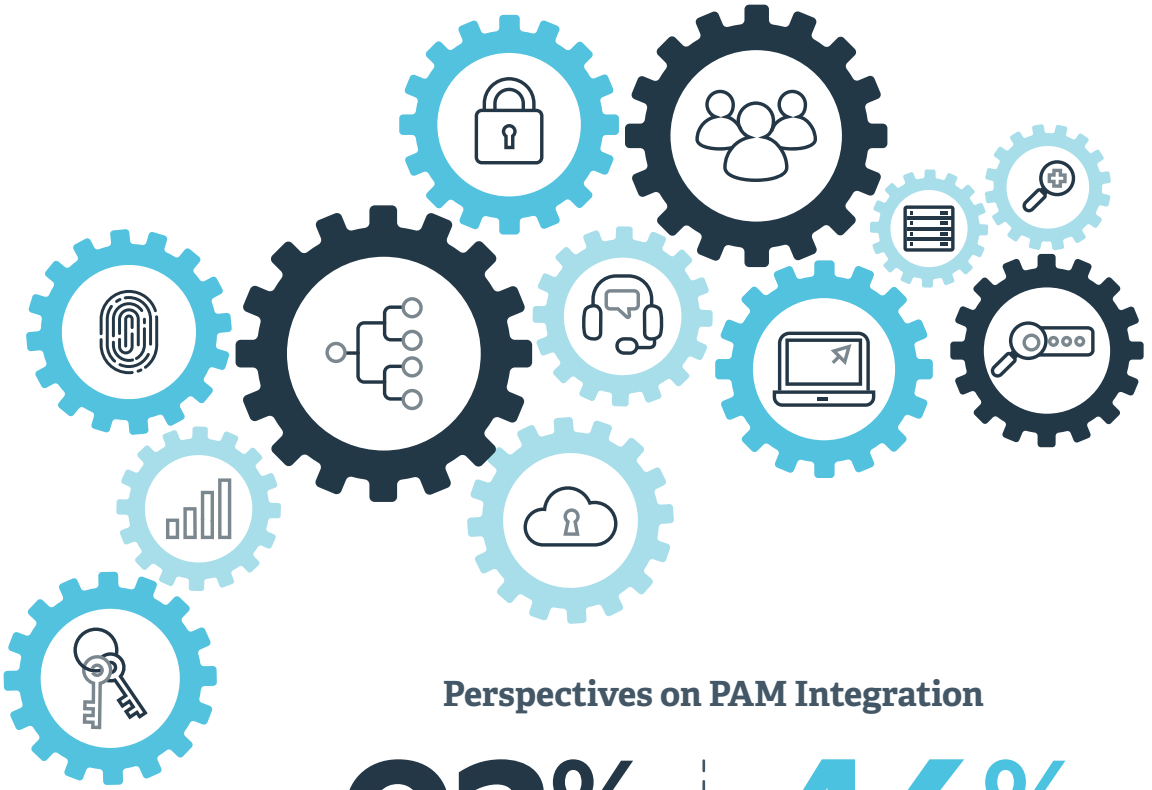
Integration Is Fundamental For Success

Businesses don't just need a wider array of PAM tools. The solutions they have need to be integrated more effectively, to better achieve security goals. Nearly all organizations (**93%**) believe it's important for PAM solutions to be integrated and almost two thirds (**63%**) believe 'integration with the tools we already have' would enhance security more than having 'better tools, but with no integration'. And, in cases where businesses have more than three PAM tools, integration is also correlated with improved visibility.

Those with fully integrated tools are more confident in their ability to monitor threats from employees and vendors. Unfortunately, only **46%** currently think their solutions are fully integrated. The majority of other respondents are either working towards integration or are simply taking an ad-hoc approach.

With greater visibility, organizations have better control over privileged access at both the individual and enterprise level. They also have an enhanced ability to identify threats and thus more rapidly address them.

The message is clear - all businesses should be assessing what types of tools they have in place and how they can better integrate them in the future.



Perspectives on PAM Integration

93%

believe it's important for PAM solutions to be integrated

46%

currently think their current solutions are fully integrated

Businesses don't just need a wider array of PAM tools. The solutions they have need to be integrated more effectively to better acheive security goals.

The Next Big Issues In Cyber Security Threat Management

Although the level of perceived threat has remained fairly consistent for both insiders and vendors, the threat landscape itself continues to evolve with a number of emerging threats that need to be considered.

New technologies and platforms often introduce new risks. The Internet of Things (IoT), for example, promises many benefits and supports many use cases, but also introduces a number of security concerns. As IoT usage grows, so too will the associated threats. The visibility of logins from IoT devices isn't the most pressing issue. Three quarters (**76%**) of our survey respondents are confident they know how many IoT devices are accessing their systems, while four in five are confident they know how many individual logins can be attributed to these devices. Manufacturing is the sector with the most confidence (**85%**), while government and the public sector have the least (**68%**).

But for both the number of IoT devices accessing their systems and attributable IoT logins, less than a third feel they can be completely sure. And even with this perceived visibility, IoT devices do pose a serious threat, particularly if access isn't effectively managed.

Fewer than one in five decision makers feel they have eliminated the dangers from IoT device security. Six in ten say that default passwords retained in IoT are a moderate or significant threat, and the same number of respondents are worried about IoT device passwords being stored as plain text. This risk is exacerbated by the fact that management systems to control access to IoT devices are still manual. Although most organizations have some sort of access management program in place, **40%** are doing it manually, while **13%** don't have anything in place at all. With usage of IoT devices in the workplace only set to grow, security decision makers need to take action and seek out improved solutions.

Fortunately, it's also clear that using solutions to manage IoT devices does give decision makers more confidence in their ability to monitor and control access. The vast majority (**91%**) of businesses using a specialist solution are confident in their ability to do so, compared to just **71%** of those working manually, and **57%** of those who don't have any IoT management solution in place. Those who have embraced an IoT security solution are also more likely to be confident with respect to the number of individual logins and knowing how many IoT devices are connected to their networks.

The specific type of solution required will vary depending on business needs. Privileged Remote Access can be used to control and monitor access, while Endpoint Privilege Management can help to implement a strategy of least privilege, enabling organizations to remove admin rights and manage what actions can be performed on particular endpoints. In addition, a solution like Password Safe can be used to store, manage, and rotate privileged accounts passwords, minimizing the risk of default credentials.

IoT Access Threats

60%

feel that unchanged default IoT passwords pose a moderate or significant threat

40%

are manually managing IoT access

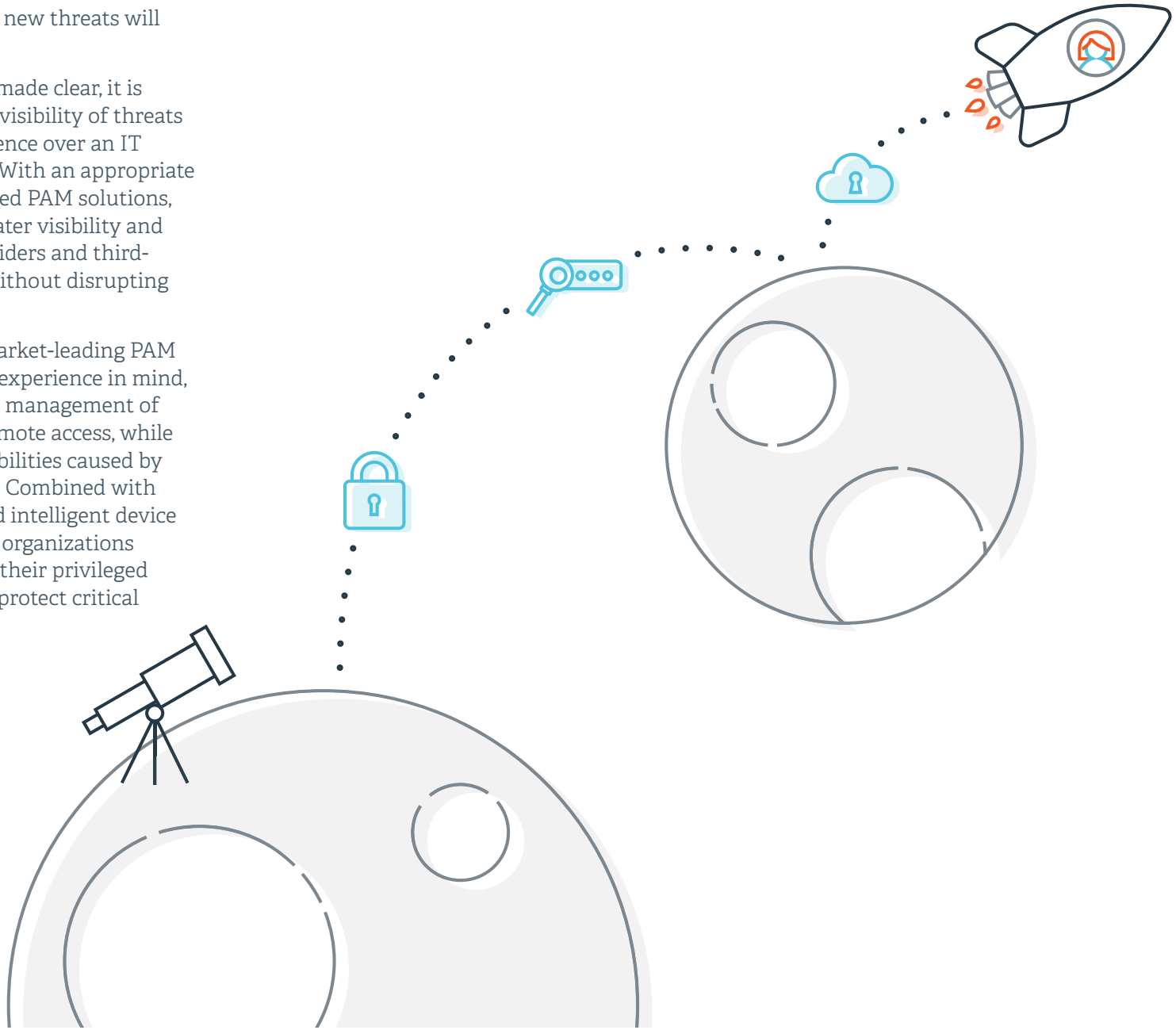
Fewer than one in five decision makers feel they have eliminated the dangers from IoT device security.

What's Next For Access Management

As we approach the next decade, issues around employee and vendor access are not going away. As long as businesses have data and IT assets to protect, new threats will continue to emerge.

Yet, as 2019's report has made clear, it is possible to improve the visibility of threats and increase the confidence over an IT environment's security. With an appropriate number of well-integrated PAM solutions, businesses can gain greater visibility and control of privileged insiders and third-party vendors, and all without disrupting productivity.

BeyondTrust designs market-leading PAM solutions with the user experience in mind, enabling the automated management of privileged access and remote access, while minimizing the vulnerabilities caused by employees and vendors. Combined with continual education and intelligent device management, this gives organizations control and visibility of their privileged access, helping them to protect critical data and systems.



ABOUT THIS REPORT

Four Years of Insight

The first iteration of this report, titled the Vendor Vulnerability Index, was introduced in 2016 to help quantify the risks related to vendor access management. Over time, the scope of the report was expanded to uncover trends in other areas of risk related to privileged access across the entire threat landscape.

Now in its fourth edition, the Privileged Access Threat Report is an annual touchpoint accessible to anyone looking to gain a better understanding of the risks related to unmanaged privileges and how to mitigate them.

Research Methodology

BeyondTrust surveyed 1,006 network access and security decision makers to understand their perceptions, behaviors, intentions, and usage of different solutions for managing privileged access.

Respondents were drawn from a range of industries, including finance, manufacturing, healthcare, government, retail, and professional services.

Working with Loudhouse, an independent research agency, the survey was conducted across the USA, EMEA, and APAC.

4
years of insight

The Privileged Access Threat Report is an annual touchpoint accessible to anyone looking to gain a better understanding of the risks related to unmanaged privilege and how to mitigate them.

1006
respondents surveyed in 2019

About BeyondTrust

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust gives organizations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 100, and a global partner network.

About Endpoint Privilege Management

BeyondTrust's Endpoint Privilege Management solutions give you the power to enforce least privilege and eliminate local admin rights. Remove excessive end user privileges and control applications on Windows, Mac, Unix, Linux, and network devices - all without hindering end-user productivity.

About Password Safe

BeyondTrust Password Safe unifies privileged password and privileged session management, providing secure discovery, management, auditing, and monitoring for any privileged credential. Password Safe enables organizations to achieve complete control and accountability over privileged accounts.

About Privileged Remote Access

BeyondTrust Privileged Remote Access provides visibility and control over third-party vendor access, as well as internal remote access, enabling organizations to extend access to important assets, but without compromising security.

beyondtrust.com