FASTPASSCORP

SDI Service Desk Institute

GDPR, Information Security, and the IT Service Desk

A survey-based snapshot of the IT industry in May 2018

Executive Summary

Information security is a growing concern – and budget item – for most, if not all, organisations. It's a technology-related area that has done what most fail to do – that's raising itself to be a topic for board-level attention and concern.
In Q2 2018, and just before the introduction of the new EU General Data Protection Regulation (GDPR) law, the Service Desk Institute (SDI) undertook a survey of UK-based IT Service Desk Managers to understand more about how their organisations are tackling both information security and the implications of the impending GDPR go live.

The key findings were that:

- Close to 20% of IT service desks don't authenticate end-users when conducting password resets
- 31% of service desks have no formal process or technology to support this end-user authentication for password resets
- Nearly two-thirds of IT service desks offer end users an automated password reset capability
- 21% of organisations (that offer an automated password reset capability) successfully see more than 80% of password resets handled by the automated method
- 68% of organisations (that offer an automated password reset capability) see less than 60% of password resets handled this way
- 83% of respondents think that, despite controls being in place, it's still possible for a criminal to gain a password to a legitimate end-user's account (via the IT service desk)
- 22% of survey respondents stated that their IT service desk doesn't have formal mechanisms in place to ensure the identity of service requesters
- 47% of respondents state that all service desk staff have privileged access for Active Directory password resetting, versus 38% where this is limited to a select group, and 12% where no one on the service desk has the ability
- 83% of respondents stated that their organisations use encryption for PCs, with only 11% stating that their organisations didn't
- Only 32% of respondents stated their IT service desk's authentication process(es) are tied in with the organisation's overall GDPR changes. And just as worryingly, 15% of respondents stated that there was no corporate GDPR initiative in place, 26% that said that their's wasn't in line, and a further 28% didn't know
- There's no clear winner for the department/team responsible for GDPR within organisations. 26% of respondents stated that it's the IT organisation, HR 20%, and a different team 44% – which could be a variety of other departments/teams.
The full results of this survey, and their implications, are detailed in this report. Read on to understand where your organisation sits relative to the IT industry as a whole.

Survey Respondent Information

The SDI survey was undertaken by people in management-level IT service desk roles. Their service desks support a range of end users/customers, with the mix as follows:

- Internal business customers – 64%
- External business customers – 29%
- External consumers – 7%

In terms of where their organisations' customer data is located – which could be in IT service management (ITSM), customer help desk, customer relationship management (CRM), or other tools – the breakdown between on-premises and public cloud was:

- On-premises – 31%
- Public cloud – 11%
- On-premises and public cloud – 58%

Meaning that 89% of surveyed organisations currently hold employee/customer data in on-premises systems and 69% in public cloud services. With information security and GDPR applicable to both IT delivery models.

While the survey questions weren't necessarily asked, and responded to, in this order, it seemed logical for this report to feedback on them.

End-User Authentication for Password Resets

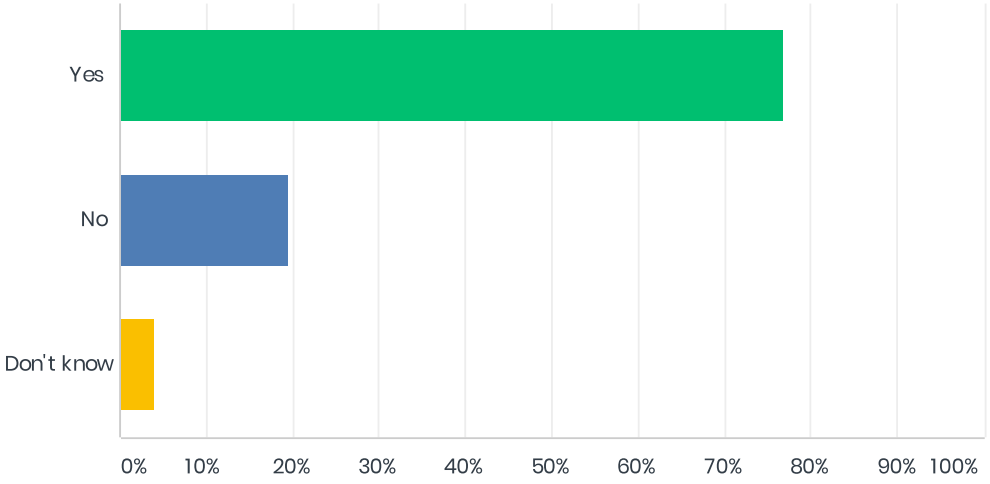
End users' passwords are the virtual keys to accessing a variety of devices, applications, and data. Plus, with the growing use of single sign-on capabilities within organisations, an end-user's Active Directory password provides access to a multitude of services, applications, and data.

End-users are often given strict rules on not sharing passwords, not writing passwords down, logging out when leaving devices (and thus applications and data) unattended, and regularly changing their passwords.

It's therefore surprising that, as shown in Figure 1, nearly one in five respondents stated that their IT service desk doesn't have a management-defined process for end-user authentication for password resets with the possibility of unauthorised access, and the potential adverse consequences, the information-security equivalent of leaving your home's front door unlocked while away.

Figure 1:

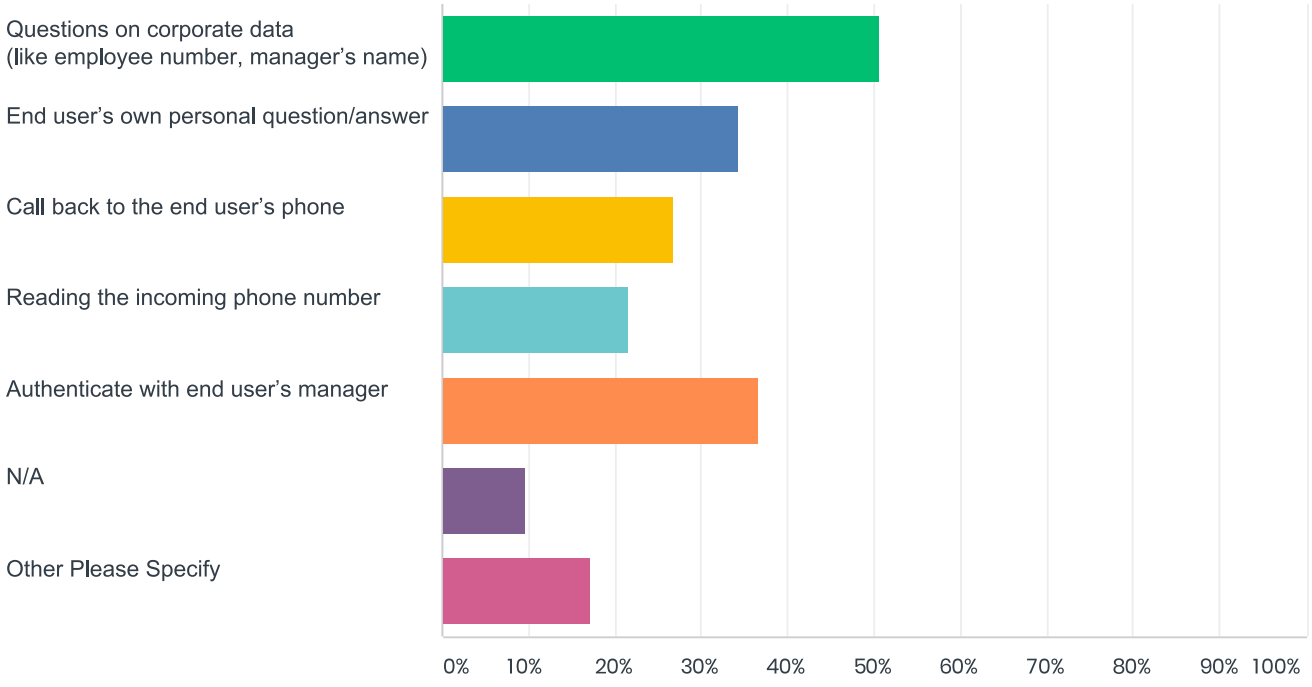
Do you have a management-defined process for end-user authentication when end users call for a password reset?



For the 77% of service desks that do have a management-defined end-user authentication process for password resets, a variety of checks are in place. These, and their usage, are detailed in Figure 2 (please note that multiple selections were allowed).

Figure 2:

End-user authentication checks employed during password reset



However, while many respondents reported that multiple checks are in place, it should be appreciated that the survey question didn't differentiate between scenarios where there's only one check used per passwords reset, i.e. a single check is undertaken, versus scenarios where multiple checks are applied together for a single password reset.

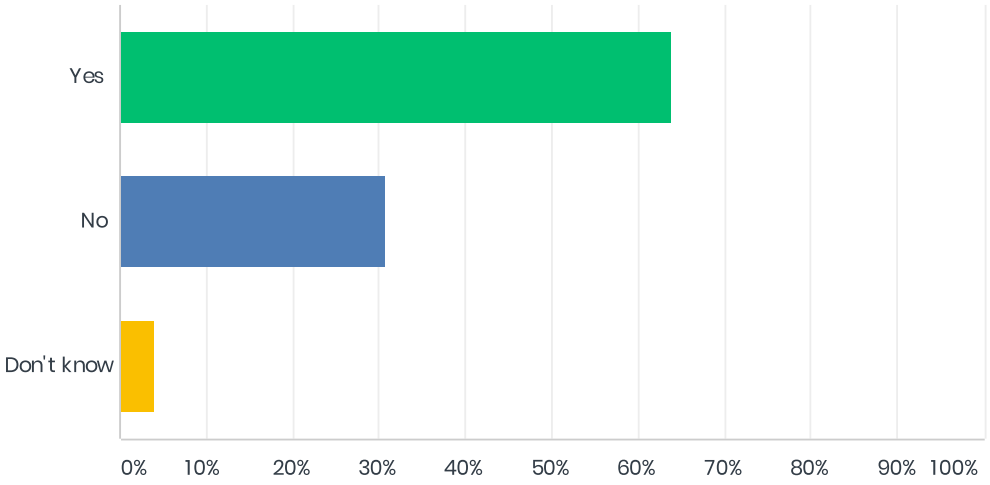
As to whether this identity checking is facilitated by a formal process or technology, further questioning identified that 31% of service desks have no formal process or technology to support this end-user authentication. Plus, not all service desks with a management-defined end-user authentication process use a formal process or technology to support the checks (as per Figure 3).

A deeper analysis of the source data showed that there are two scenarios where a mismatch occurs:

1. Respondents who don't have a management-defined process but do have a supporting process/technology – thus they are a No in Figure 1 and a Yes in Figure 3.

2. Respondents who have a management-defined process but don't have a supporting process/technology – thus they're a Yes in Figure 1 and a No in Figure 3.

Figure 3:
Do you have a formal process or technology to support this?



The above relates to manual password resets, but what about the use of automated password rest capabilities?

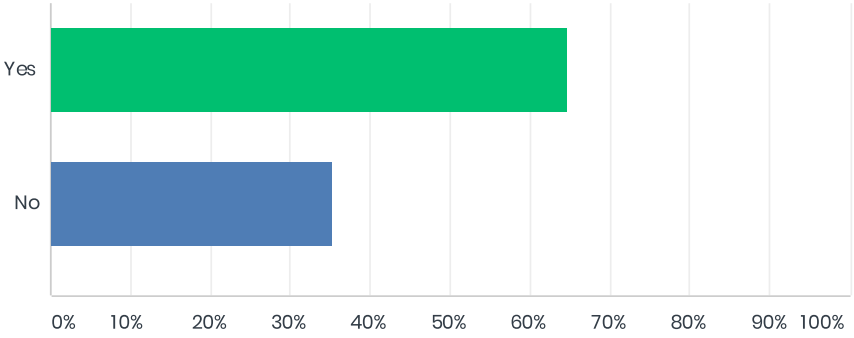
Automated Password Reset Capabilities

Forgotten password related password resets, especially after holiday periods or where frequent password changes are mandated, are the bane of IT service desks. They're commonly high-volume, low-value-adding, manual tasks that prevent over-worked service desk agents spending their time where it makes the biggest difference – in dealing with business-affecting IT issues.

Thankfully, along with a wider spectrum of IT self-service capabilities, automated self-service password reset capabilities are increasingly popular. With this survey showing that they're now used by approximately two-thirds of organisations (see Figure 4 over page).

Figure 4:

Do you offer a self-service password reset capability?

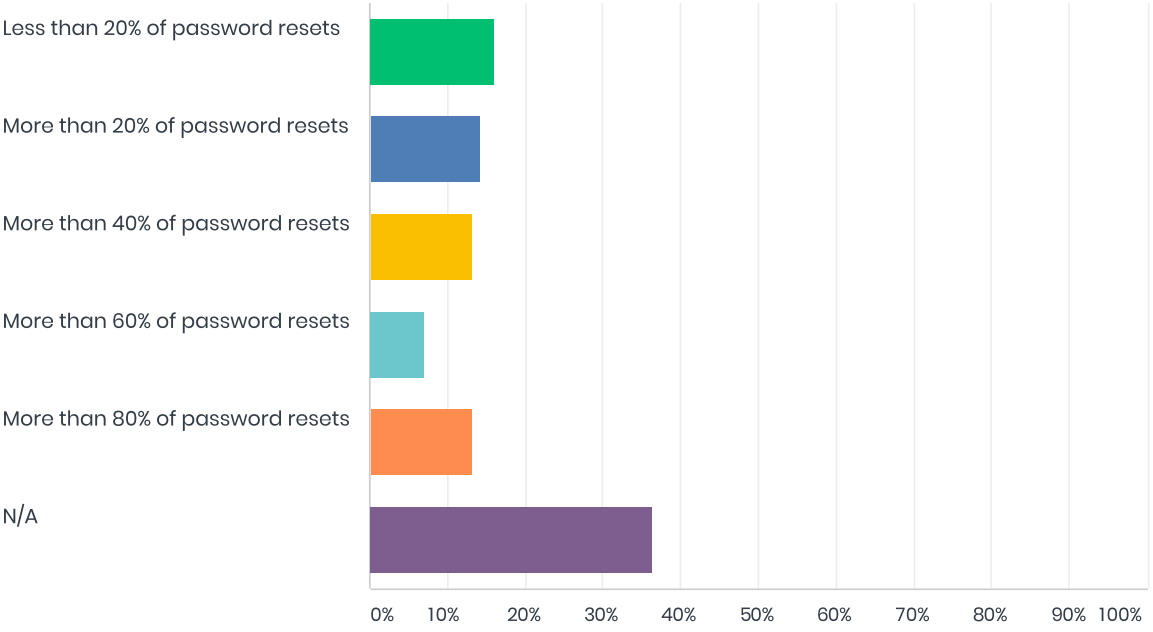


However, again as is common with corporate IT self-service capabilities, there's a gap between technology-availability levels and usage levels. Thus, even though 64% of organisations offer an automated password reset capability, there's a spectrum of success levels.

On the one hand, as shown in Figure 5, 21% of organisations (that use an automated password reset capability) successfully see more than 80% of password resets handled by the automated method. But sadly, on the other, 68% of organisations see less than 60% of password resets handled this way – with the rest defaulting back to manual service desk operations.

Figure 5:

If YES, what is your approximate adoption rate for self-service password reset?



There's thus the need to understand and address the reasons for these low adoption levels. This might be caused by one or more of:

- A lack of awareness, with end users still calling the IT service desk as they always have
- Ease of access, i.e. the automated reset capability isn't easy to find and access when needed
- Ease of use
- Limitations on the types of passwords that can be reset – which not only lowers the percentage of resets handled but also prevents end users returning when their previous attempt, for a non-supported password type, failed.

But, ultimately, you'll need to understand the low adoption levels in the context of your organisation.

Password Management Policies

So far, this report has looked at the security controls related to the unplanned and potentially unauthorised changing of passwords. However, the survey respondents were also asked about their organisations' security-related policies related to password creation and periodic changing.

Starting with the traditional view on password management – the most concerning of responses, shown in Figure 6, is that 7% of respondents stated that their organisations don't mandate, or enforce, periodic password changes. And 4% stated that, whilst this occurs, the frequency is less than every nine months.

Again, taking the traditional view, the "good news" is that 84% of respondents stated that their service desks mandate that end-users must change their Active Directory passwords at least every six months.

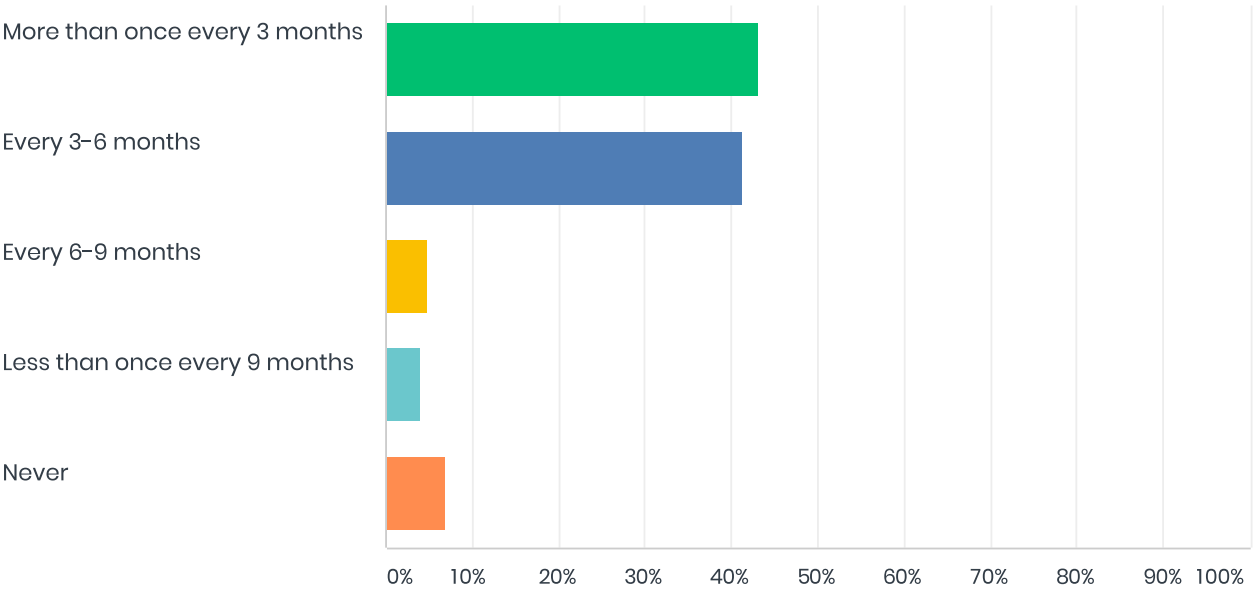
However, the thinking around password-lifecycle policy is changing. For example, the National Institute of Standards and Technology (NIST) – part of the U.S. Department of Commerce – has written extensively on identity and access management (IAM), including that:

"Verifiers SHOULD NOT require memorised secrets to be changed arbitrarily (e.g. periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator."

In other words, passwords should NOT be changed based on a frequency. Thus, your organisation's stance on IAM might need to be reconsidered based on the current thinking of your corporate information security experts who may or may not agree with NIST's advice.

Figure 6:

How often must end users change their Active Directory password?



Another important factor in password management is the set of rules that dictate what needs to be included in, and what can't be included in, passwords. For example, the need for:

- A minimum password length (often eight characters or higher)
- A mix of letters and numbers
- A least one capital letter
- At least one special character such as !, $, %, &, or @
- No consecutively repeated characters
- No "forbidden passwords" such as:
    - "Password" and policy-compliant variants such as: P455w0rd
    - 12345678, 11111111, and other easy-to-remember numerical sequences
    - abcdefgh and other easy-to-remember alphabetical sequences
    - Nouns and proper nouns, i.e. dictionary words.

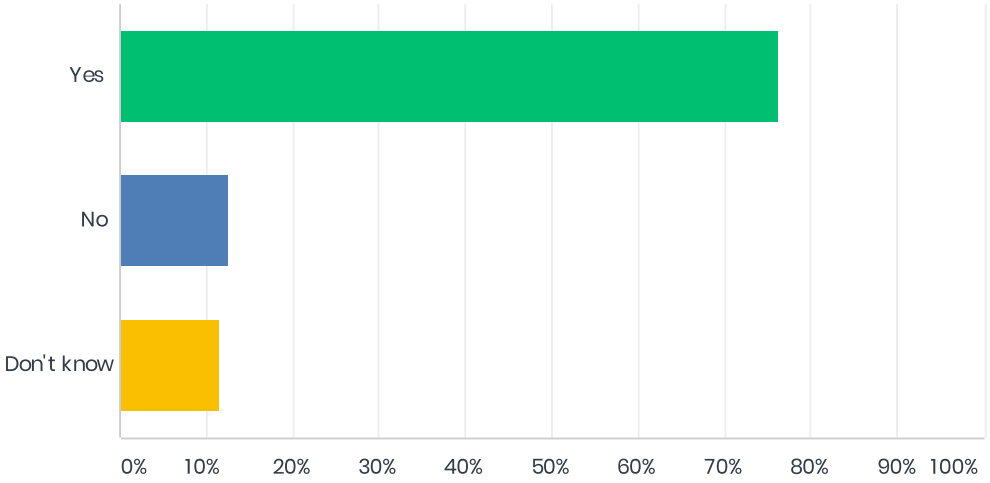
Traditional password management thinking has been to make passwords as complicated as possible – to ensure that they're strong and robust to breaking. However, it also makes them harder for the end user to remember and can bring about unwanted human practices, such as keeping a reminder of the password on a post-it note, that negate the original intention of securing devices, applications, and data.

Modern-day thinking on password composition is also breaking away from tradition, with NIST also stating that: "Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets."

Again, it's a good idea to check with your corporate information security experts as to their current stance on passwords. As to the use of "forbidden" passwords, 76% of respondents stated that their organisations' Active Directory systems will prevent them being used, with only 13% allowing them (as per Figure 7). This latter figure should really be at 0%, so please check the situation within your organisation.

Figure 7:

Does your Active Directory system prevent the use of "forbidden" passwords?



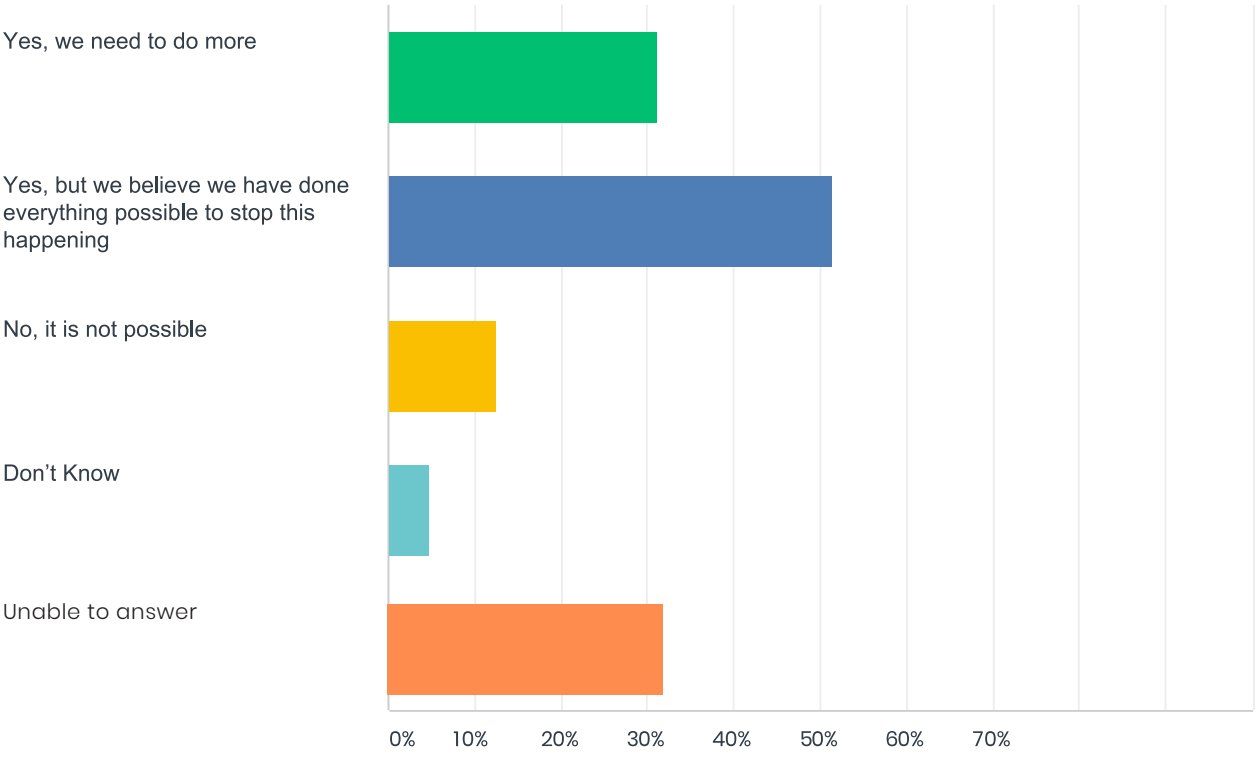
Unauthorised Password Use

Whilst the previous survey questions looked at the controls in place, additional survey questions were asked about the robustness of the controls – starting with respondent opinions as to whether their organisation's controls are sufficient to protect end-user passwords (and thus prevent unauthorised access to the corporate network, applications, and data).

As shown in Figure 8, 83% of respondents think that, despite the controls being in place, it's still possible for a criminal to gain a password to a legitimate end-user's account. 31% think that their service desk needs to do more to prevent this but 51% believe that it could still happen despite "doing everything possible" to prevent it. These statistics equally apply to both the respondents who don't have a management-defined authentication process and those who do.

Figure 8:

In spite of your authentication process, do you think it's possible for a criminal (internal or external) to get a password for a legitimate end user's account?



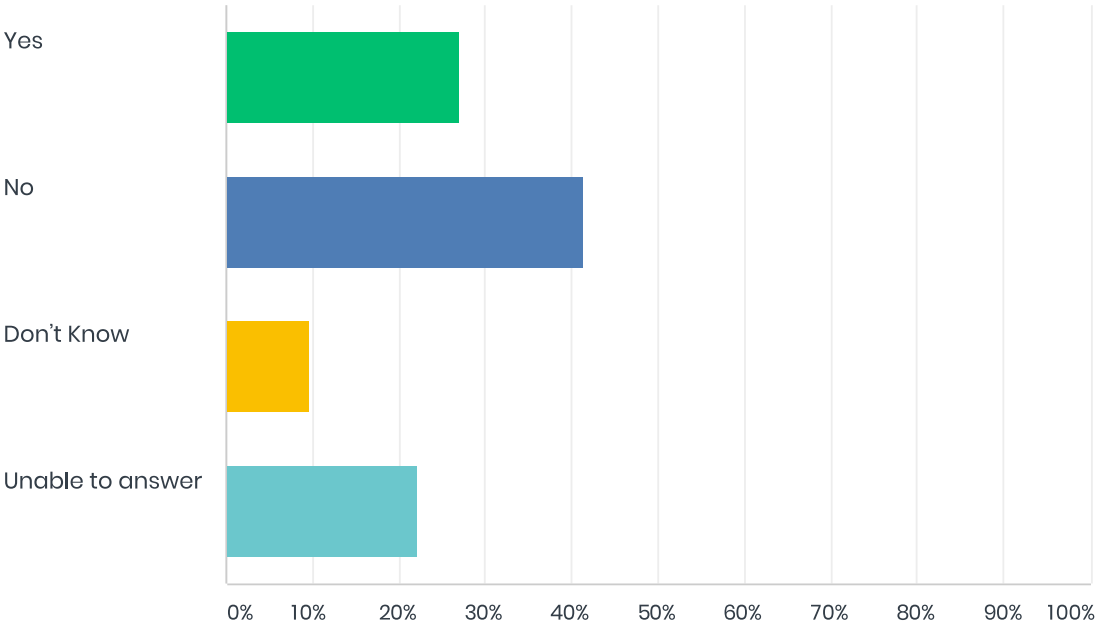
As to the reality of the risks of unauthorised access to end-user data, Figure 9 shows that 27% of respondents stated that their organisation had identified unauthorised access attempts. Although, this might be just the tip of the iceberg because, ignoring the 32% that responded with either "Don't know" or "Unable to answer", how many of the 42% who stated that their organisation hadn't identified any unauthorised access attempts (in the last 12 months) were either not:

1. Monitoring for unauthorised access attempts, or:
2. Suitably equipped to identify unauthorised access attempts?

The point being that, just because no attempts were identified, it doesn't mean that none were attempted or even successful.

Figure 9:

Has your organisation identified any attempts to gain unauthorised access to end-user data in the last 12 months?



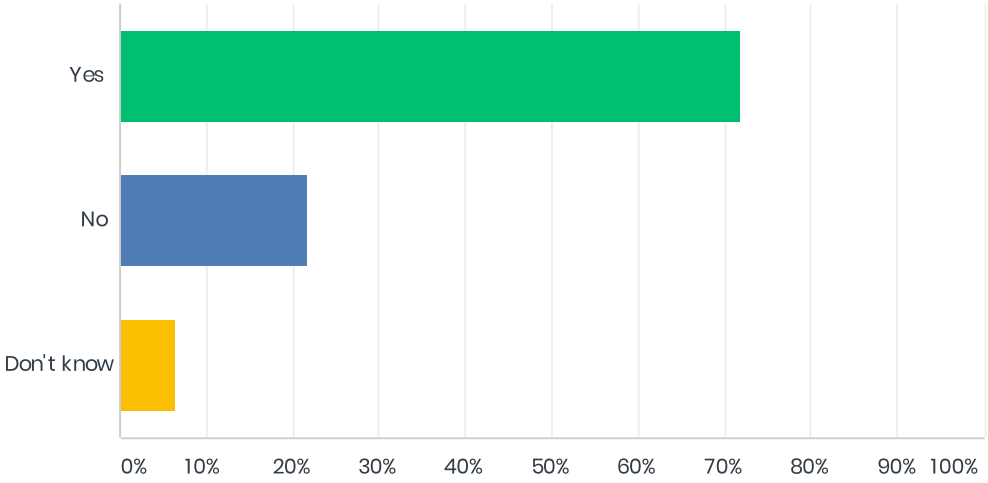
Service Desk Operations and Security

Whilst the topic of password security might seem obvious – because it's something that has significant business value in preventing unauthorised access to the corporate network, applications, and data – what about other aspects of IT service desk operations?

As with the question on using a management-defined process for password reset authentication, approximately 20% of survey respondents stated that their IT service desk doesn't have formal mechanisms in place to assure the identity of service requesters (see Figure 10). However, this wasn't the same set of respondents – with a less than 25% overlap between the two.

Figure 10:

Are there steps taken to authenticate a person asking for services in general from the service desk?



The risks associated with unauthorised access to service desk services will differ between organisations and the services that their service desks provide. The important thing is to understand what's at risk for your service desk, and organisation, if service desk agents engage without checking the identity of the caller, chat-participant, or emailer. For instance, the easy-to-believe scenario of a service desk agent unwittingly providing the home address of a home worker to a third-party purporting to be them: "Do you still live at...?". This also ties in with the personal data related GDPR risks and requirements in the next section.

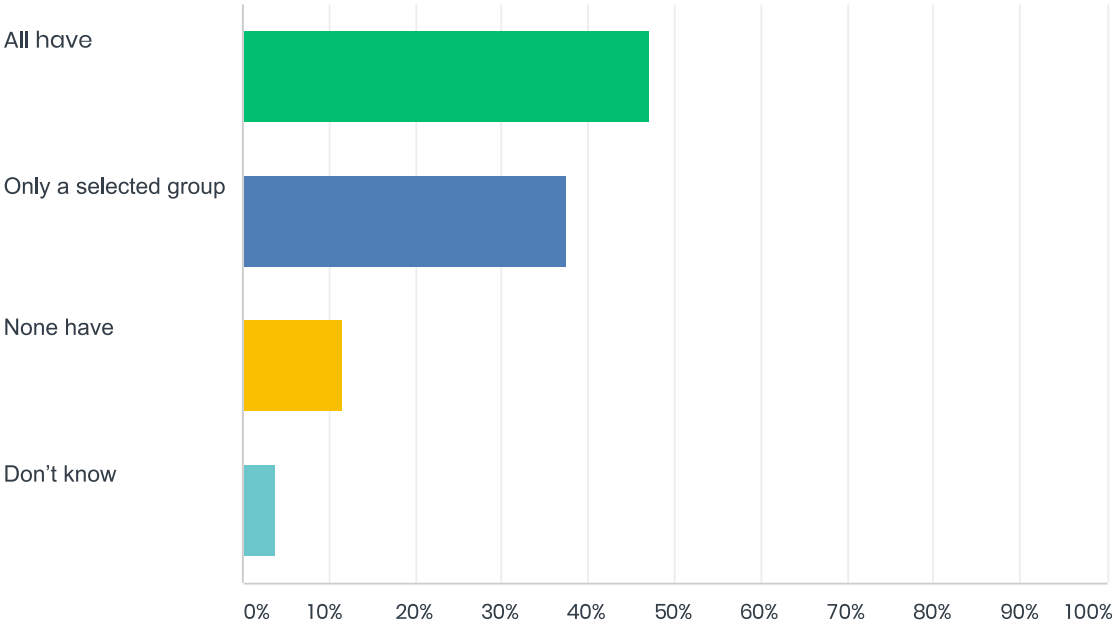
But the risk or threat might not always come from outside, it can also come from within the IT service desk. Thus, the survey respondents were asked who, within the service desk, can reset end-users' passwords.

The results are shown in Figure 11, with 47% of respondents stating that all service desk staff have the capability, versus 38% where this is limited to a select group, and 12% where no one on the service desk has the ability.

While still at an unfortunately low level in 2018, the latter reflects modern-day password management good practice – where password manager tools are used instead of relying on service desk staff with privileged passwords. We could expect this number to grow over the next few years, with the technology replacing both unwanted manual efforts and the inherent security risks.

Figure 11:

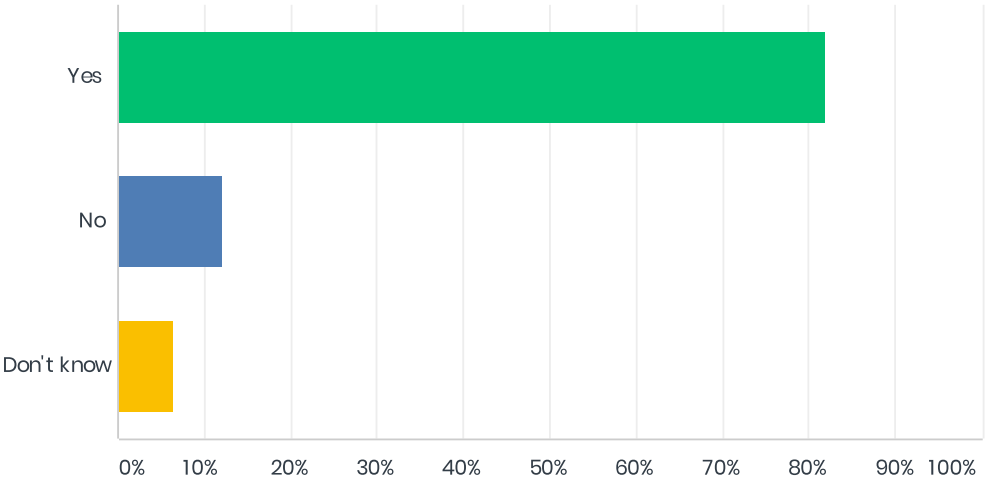
Do service desk analysts have privileged passwords to the Active Directory to reset end users' passwords?



In addition to password-related security, the survey also asked respondents a question related to device-based encryption. The results, as shown in Figure 12, are that a resounding 83% of respondents stated that their organisations use encryption for PCs, with only 11% stating that their organisations didn't.

Figure 12:

Does your organisation use encryption for PCs? (such as Bitlocker, McAfee, Checkpoint, etc.)



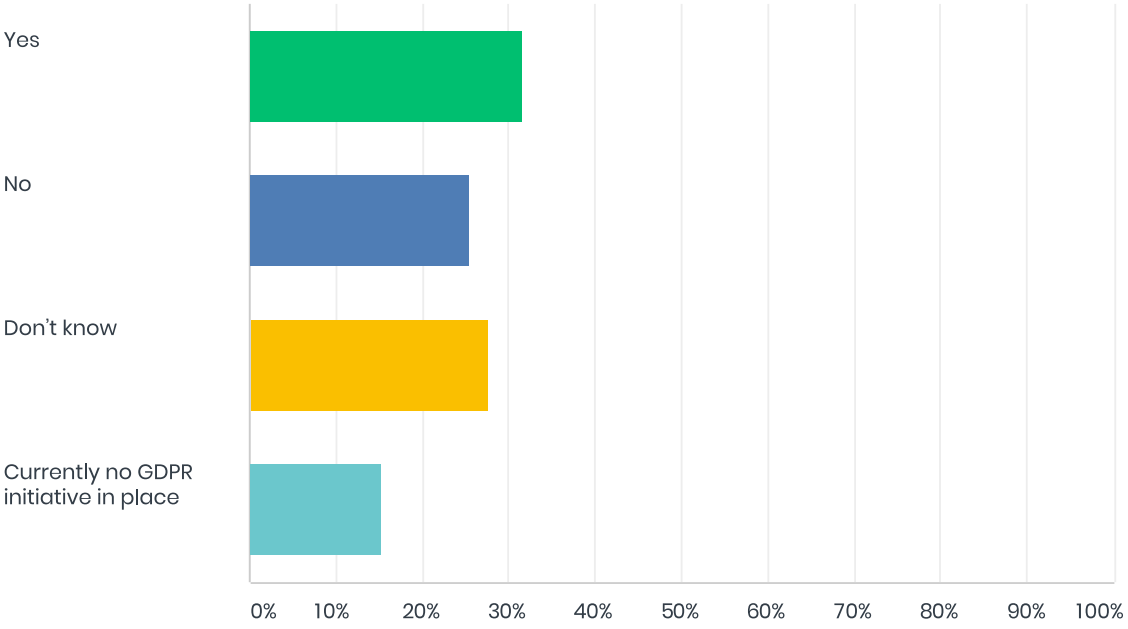
GDPR Preparedness

The new GDPR legislation applies to the personal data processing carried out by organisations operating within the EU plus those outside the EU that offer products/services to individuals within the EU.

Under GDPR, those controlling or processing personal data are subject to a number of legal obligations. For instance, those processing personal data are required to maintain records of their personal data and processing activities and what must happen after a data breach.

The survey looked at GDPR through a number of lenses, starting with whether the IT service desk's authentication process(es) is tied in with the organisation's overall GDPR changes. Rather worryingly, only 32% of respondents stated that it was and just as worryingly, 15% of respondents stated that there was no corporate GDPR initiative in place, 26% that said that it wasn't, and a further 28% didn't know (see Figure 13).

Figure 13:
Is the service desk's authentication process part of your organisation's GDPR initiative?

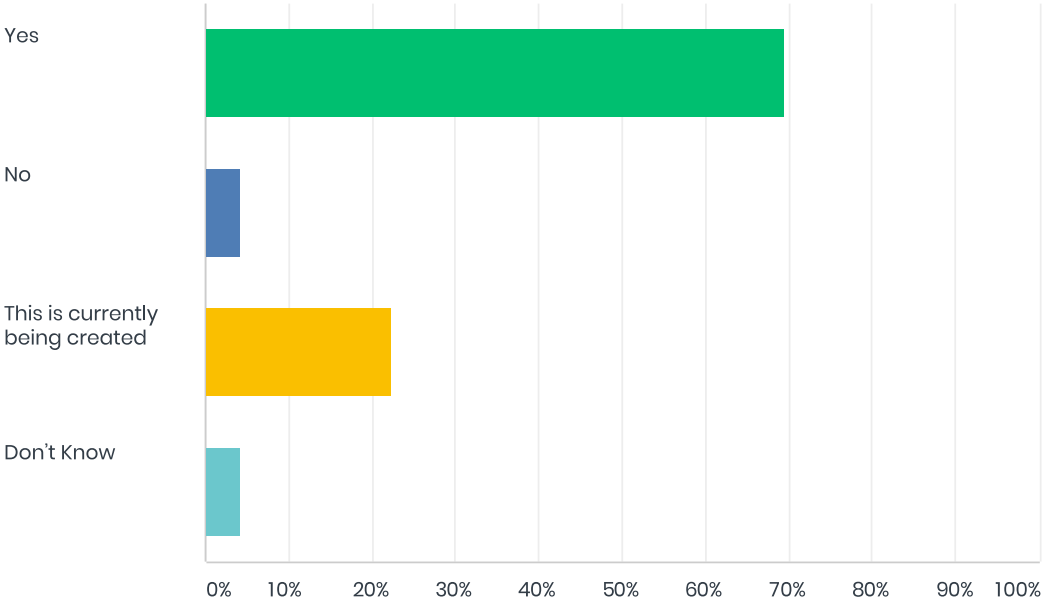


Whether the service desk is supporting employees, business customers, or consumers, GDPR still applies to the protection of their personal data. It stipulates that organisations must have procedures in place to detect, report, and investigate data breaches, and GDPR imposes aggressive timescales in which to respond to the required authorities.

Thankfully the majority of respondents stated that their organisations already have a process in place or are currently creating one (in time for GDPR go-live) – only 4% of respondents stated that their organisation doesn't have such a process. Interestingly though, the majority of respondents didn't know of any specific changes that had been made, in terms of personal-data handling, to reflect the demands of GDPR.

Figure 14:

Do you have a process for when you identify a data breach?

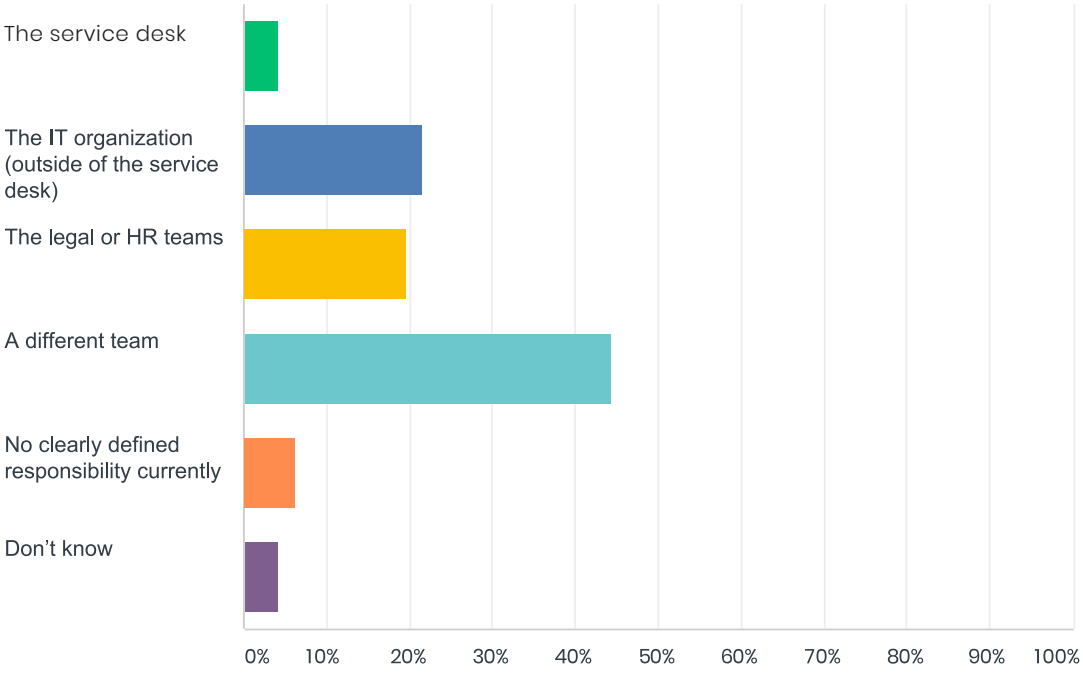


As to the part of the overall organisation that's responsible for GDPR, the respondents' responses showed that it differs considerably between organisations. For example, as shown in Figure 15, 26% of respondents stated that the IT organisation is responsible for GDPR within their company, HR 20%, and a different team 44% – which could be made up of a variety of other departments/teams.

Over time, however, there will no doubt be GDPR good practices arising that cause the responsibility for GDPR to gravitate towards one particular business department/team over others.

Figure 15:

Who is responsible for GDPR policies within your organisation?



Overview

This report offers an interesting insight into the current state of GDPR readiness, information security, and the IT service desk as the introduction of the new GDPR looms.

Starting with password-related controls:

- Close to 20% of IT service desks don't authenticate end users when conducting password resets and 31% of service desks have no formal process or technology to support this end-user authentication for password resets.

- Nearly two-thirds of IT service desks offer end users an automated password reset capability. But only 21% of organisations (that offer an automated password reset capability) successfully see more than 80% of password resets handled by the automated method. 68% of organisations see less than 60% of password resets handled this way.

- Despite controls being in place, 83% of respondents think that it's still possible for a criminal to gain a password to a legitimate end user's account (via the IT service desk).

In terms of some specific IT service desk control points and potential weaknesses, 22% of IT service desks don't have formal mechanisms in place to assure the identity of service requesters. Then, 47% of respondents state that all service desk staff have privileged access for Active Directory password resetting, versus 38% where this is limited to a select group, and 12% where no one on the service desk has the ability. There is good news, however, in that 83% of organisations use encryption for PCs, with only 11% that don't.

And finally, in terms of GDPR preparedness, only 32% of IT service desks' authentication processes are tied in with the organisation's overall GDPR changes. And just as worryingly, 15% of respondents stated that there was no corporate GDPR initiative in place, 26% that said that their service desk wasn't (in line), and a further 28% didn't know.

There's no clear winner for the department/team responsible for GDPR within organisations – 26% of respondents stated that it's the IT organisation, HR 20%, and a different team 44%. This lack of consistency for GDPR responsibility is a concern but perhaps expected for something that's still very new to, and untried by, organisations and their people. Time will tell.

About SDI

The SDI company mission is to inspire service desks to be brilliant. To achieve this mission SDI has developed a set of goals by which it aims to inspire service desks to:

Embrace:
To raise the quality of service delivery by valuing best practice

Engage:
To create an inspiring and engaging customer experience

Invest:
To empower their teams to be inspired, take action and be better

Shine:
To demonstrate and deliver exceptional business value

SDI sets the globally recognised best practice service desk standards that provide clear and measurable benchmarks for service desk operations and professionals. The standards are designed to encourage service desks to embrace and value best practice in order to raise the quality of service delivery.
For more information about SDI please visit
www.servicedeskinstitute.com

About FastPass

FastPass is the leading solution for corporate self-service of passwords. Combined with "FastPass Best practices" customers achieve high adoption rates of 75-90%. The solution is available on-premise and cloud for AD/ Windows password and other corporate passwords.

NEW: FastPass offers a secure and compliant manual authentication process for password reset in the service desk – this should be a GDPR requirement. Strong integration to most ITMS systems. FastPassCorp is listed on Nasdaq/Copenhagen/FirstNorth