
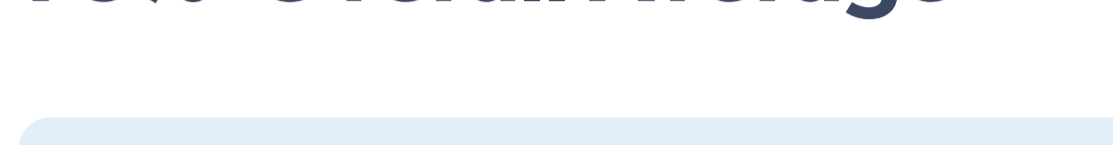


IT is focused on the security benefits of IAM, and prioritizes MFA



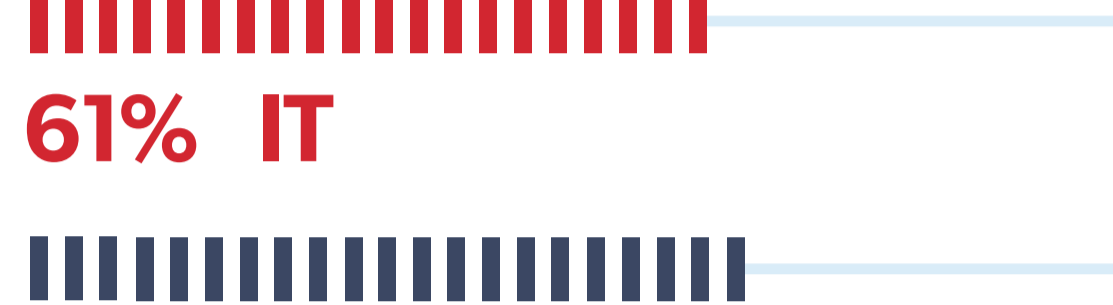
 Information technology (IT) are businesses who operate in the hardware or software markets. As businesses who are close to technology and managing customer's data, it's clear their relationship with technology impacts their IAM strategy.

Securing data is a top priority.



Our Take: If anyone knows the potential risks of data loss, it's IT. **IT is likely managing large volumes of data** - their own, and their customer's especially if they are SaaS.

Upgrading IAM is a priority.



Our Take: It is surprising to see that **improving IAM is less of a focus**. IT may have already upgraded their IAM solutions, or perhaps is not an area they are currently evaluating.

Integrating security infrastructure is my biggest area for improving.



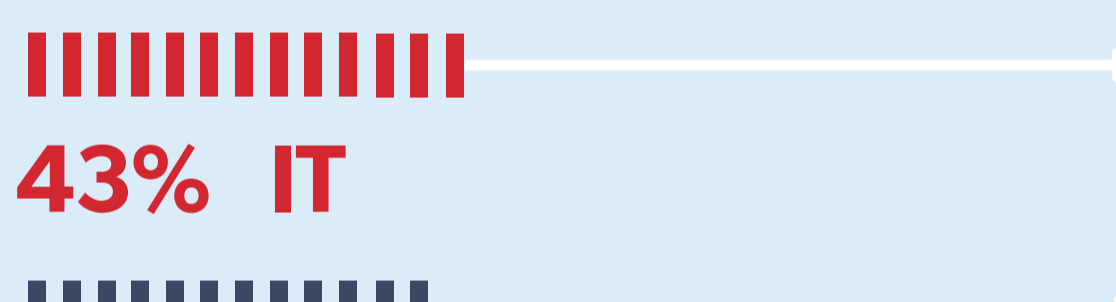
Our Take: IT is also less focused on integrations, which further suggests that IT's IAM upgrade has already occurred. This is also seen in our 2019 Global Password Security Report, which found that IT is leading the pack with both MFA adoption and security posture.¹

IAM could improve employee efficiency.



Our Take: Over the next year, **we can expect IT to place their efforts on improving security** with IAM as they are focused less strongly on the productivity benefits. This focus will also help IT address their priority of securing data.

The security of our IAM solutions is a challenge.



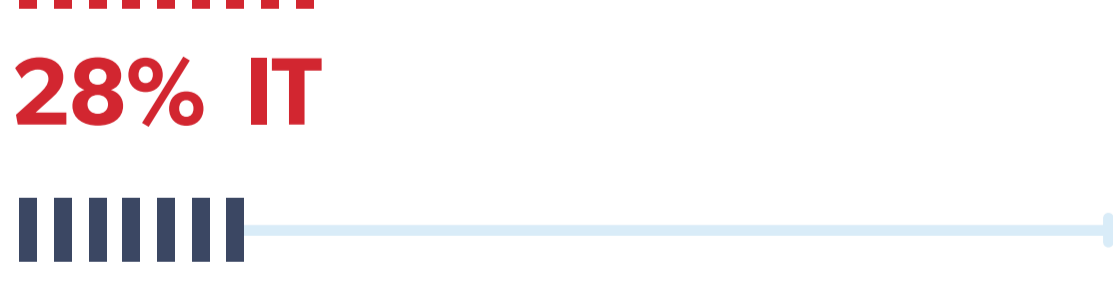
Our Take: Employee productivity as less of a focus for IT makes sense, given the main challenge they face is security. Data breaches exposed 4.1 billion records in the first half of 2019², and as IT manages more amounts of customer data, maintaining control over every access point becomes increasingly complex.

IAM should be a higher priority for my organization.



Our Take: However, **IT is aware that IAM needs to be a higher priority**. Every employee has access to 17 million files³ on average, and when IT is managing customer data as well, this number not only grows but so does the need for tighter controls.

I'm planning to invest in MFA.



Our Take: We can expect to see IT **focus on MFA over the coming year**, which will help achieve their security challenges because MFA helps ensure only the right employees are able to access sensitive data.

OUR RECOMMENDATIONS FOR IT:



Prioritize ease of use for employees.

With a baseline IAM strategy already in place, now is the time for IT to focus on employee behavior to increase adoption, and ultimately company security.



Evaluate whether their IAM approach is holistic.

IT should evaluate whether their current IAM program covers all aspects of the employee lifecycle and every access point in the business.



Upgrade to adaptive MFA.

Adaptive MFA adds increased friction for abnormal login attempts, all while enabling employees to seamlessly authenticate. This will give IT more trust in user's behavior, without getting in the way of their work.

Learn more: <https://www.lastpass.com/products/identity>

Sources:
1. <https://www.lastpass.com/state-of-the-password/global-password-security-report-2019>
2. <https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report>
3. <https://www.varonis.com/2019-data-risk-report/>
4. LastPass survey data