Securing Hybrid IT is a JOURNEY

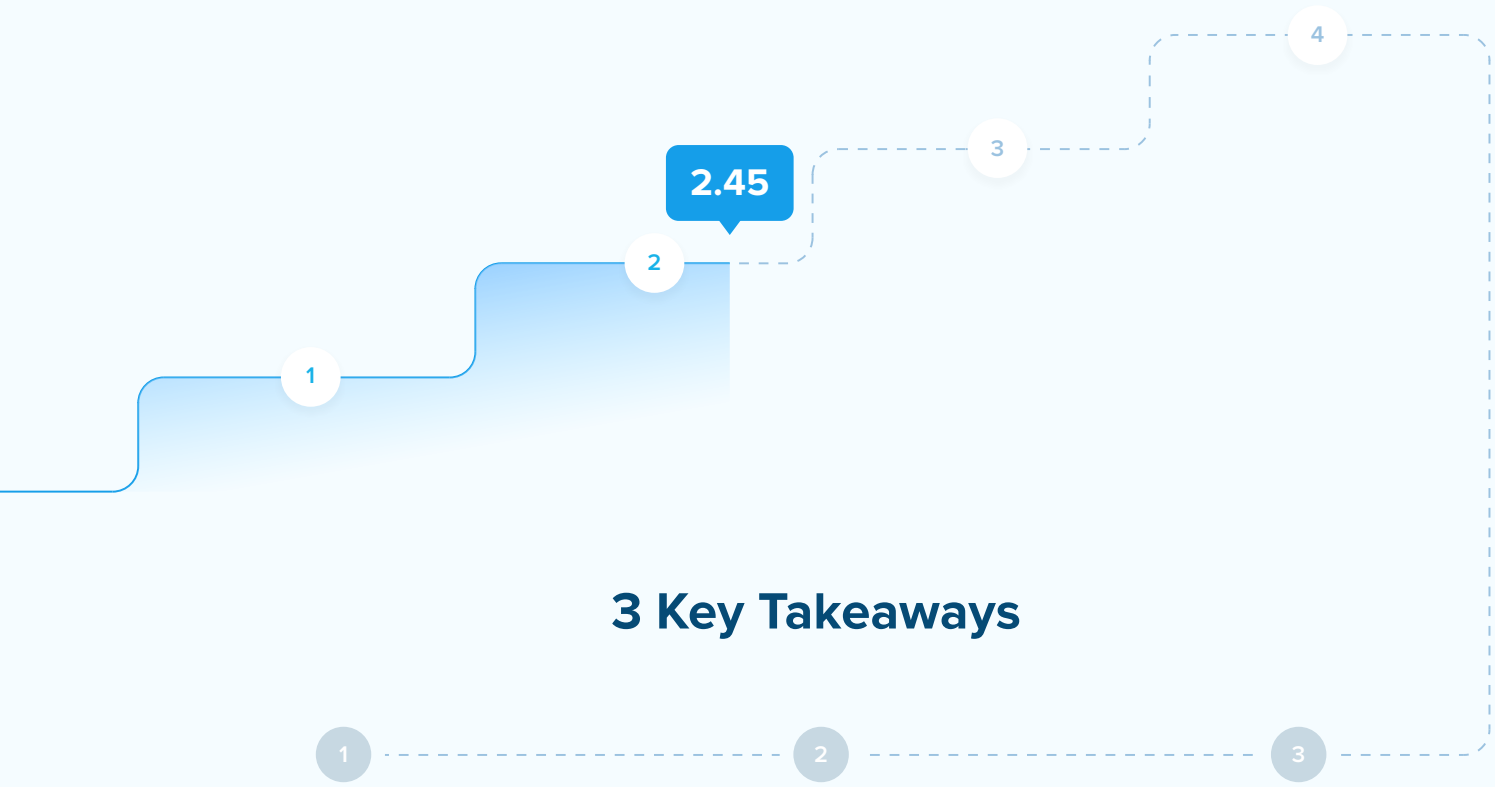
Where Do Organizations Fall on the Maturity Curve Today?

As IT leaders continue to support a distributed workforce, many of them combine solutions hosted on-premises and in the cloud as they adopt a **hybrid IT model**. While using hybrid IT offers greater flexibility and reduced overhead costs, it can also create security challenges.

okta

Hybrid IT Security Maturity across Organizations

The average maturity level of organizations leveraging a hybrid IT model is 2.45 out of 4—leaving significant room for improvement.



3 Key Takeaways

1

The majority of IT leaders are adopting both on- and off-premises infrastructure—but haven't secured both cohesively.

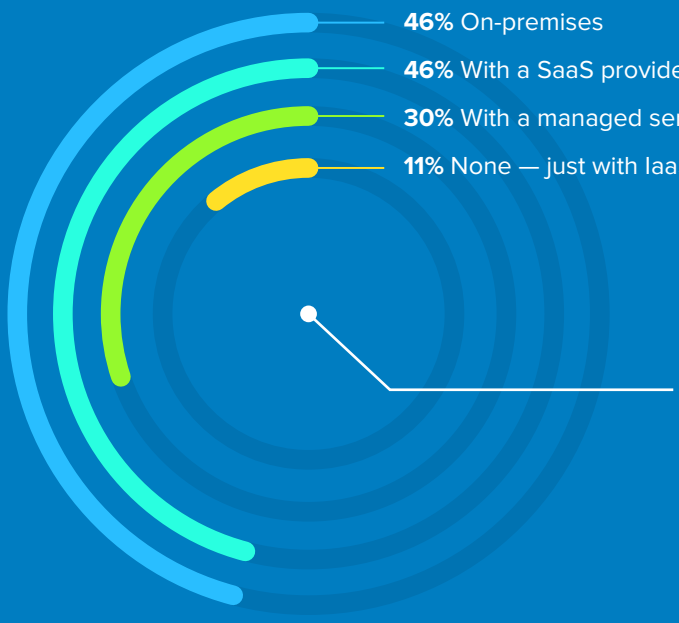
2

IT leaders must future-proof their security strategies for hybrid IT. Especially for remote access.

3

IT teams must improve measurement of technical debt to boost hybrid IT security.

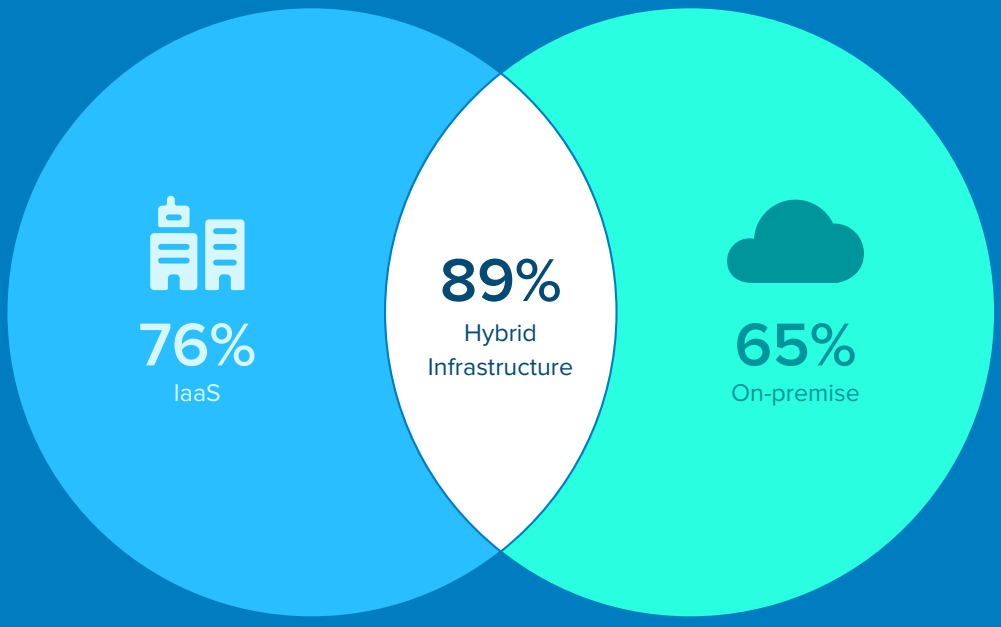
The majority of IT leaders are adopting both on- and off-premises infrastructure—but haven’t secured both cohesively.



Where do you deploy IT systems, in addition to IaaS providers?

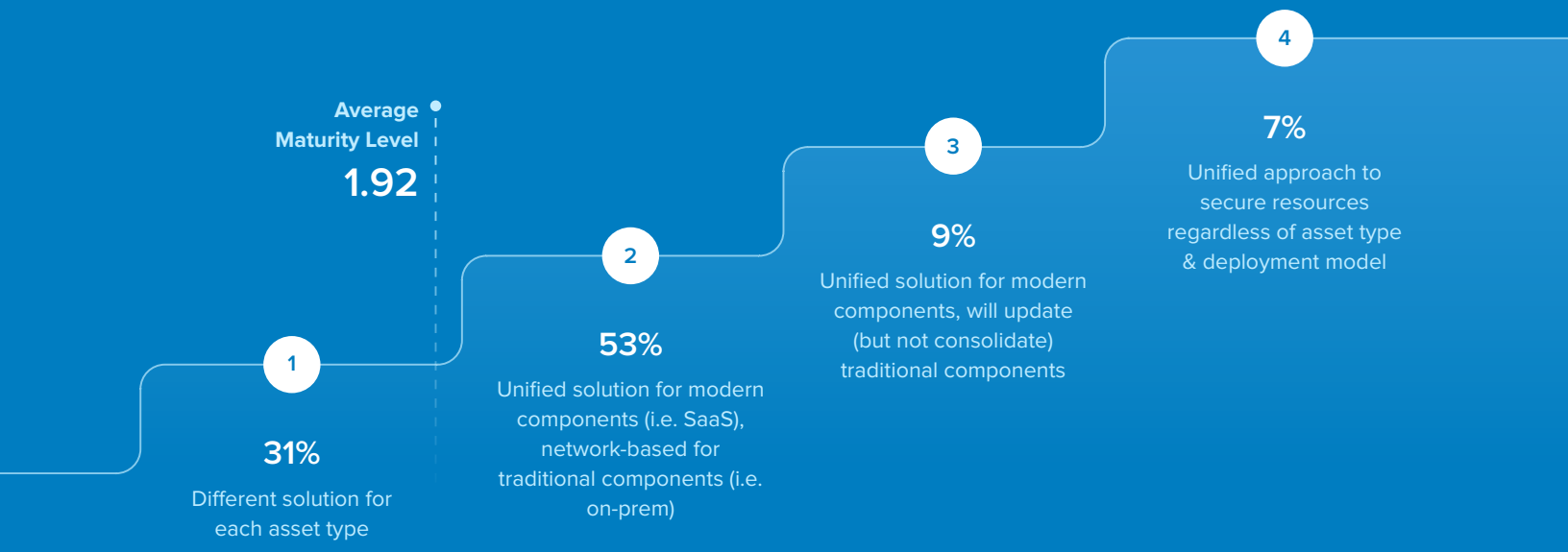
The vast majority of companies (89%) are using a hybrid infrastructure model.

Today, infrastructure-as-a-service (IaaS) providers like AWS and Microsoft Azure (76%) have overtaken on-premises infrastructure (65%) as the most common method used to deploy IT systems. However, **the vast majority of companies (89%) are using a hybrid infrastructure model.**



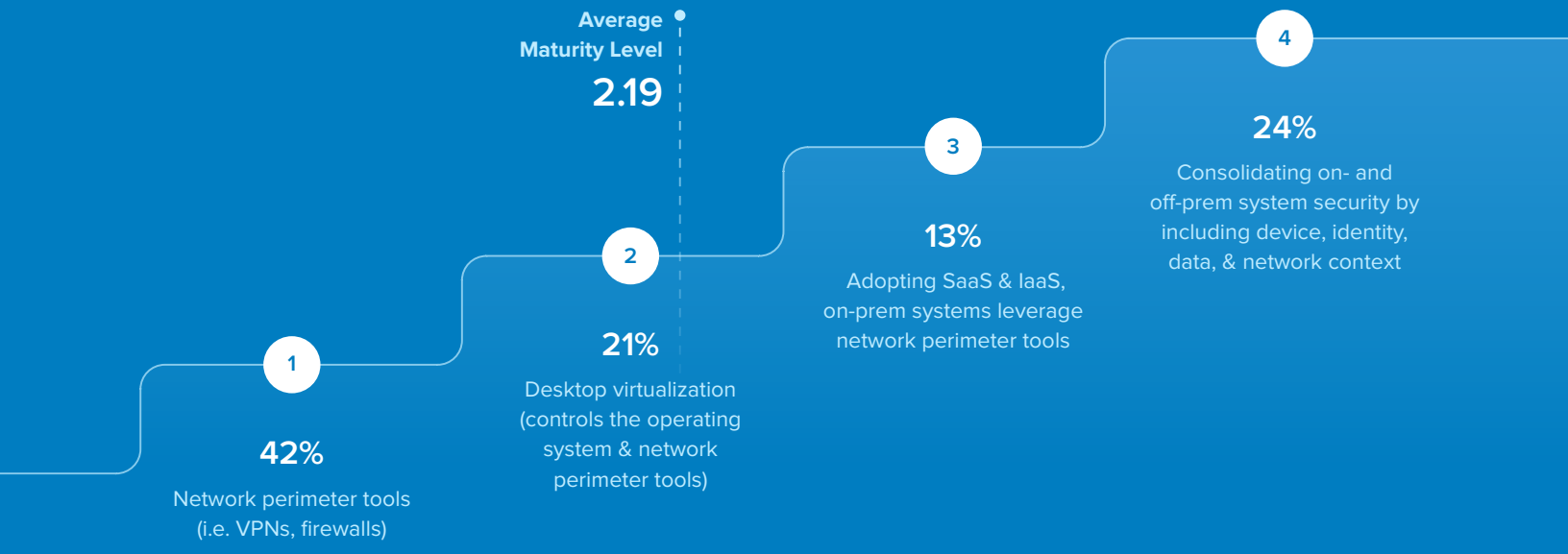
While hybrid IT prevails today, security leaders scored only 1.92 out of 4 on their methods to secure access to their hybrid resources.

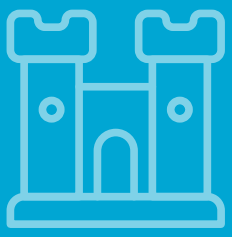
How do you secure access to different asset types (i.e. apps, servers, APIs, and data) and hosting models (i.e. on-prem, MSP, IaaS, SaaS)?



As well, though **65% of respondents say they currently use on-premises infrastructure**, the most common security strategies they use to protect these systems **meet a maturity level of only 2.19 out of 4**.

Which of the following best describes your security strategy for systems currently hosted on-premises?

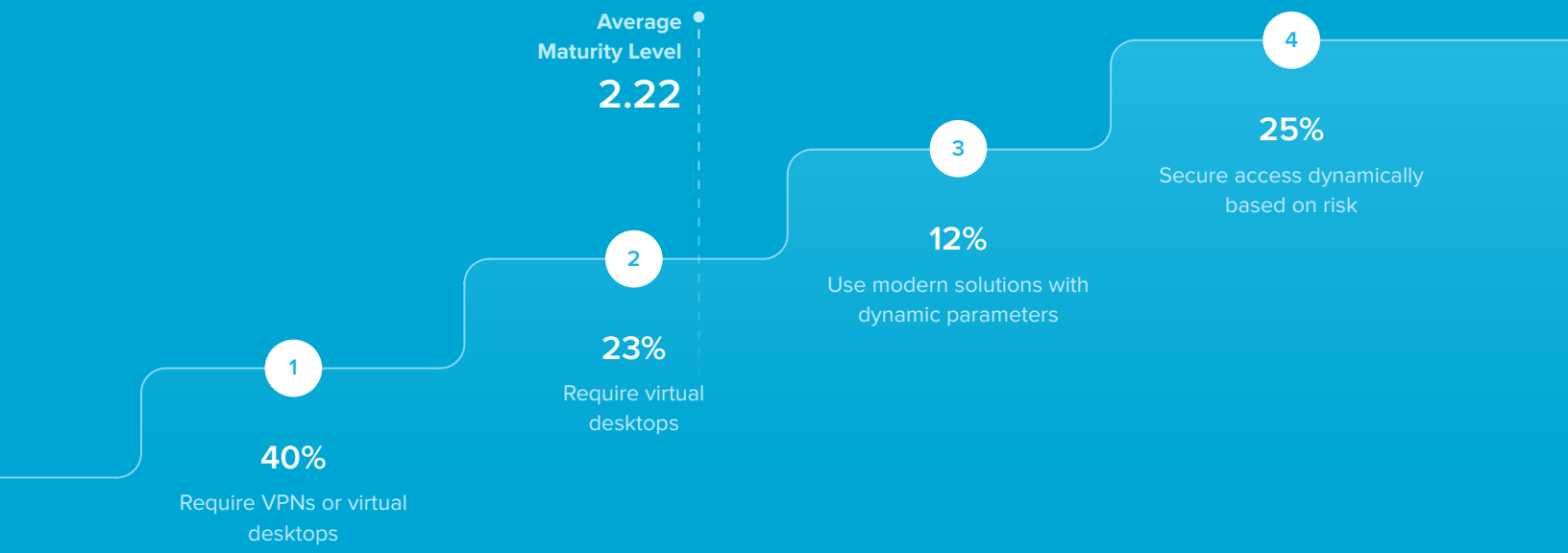




IT leaders must future-proof their security strategies for hybrid IT, especially for remote access.

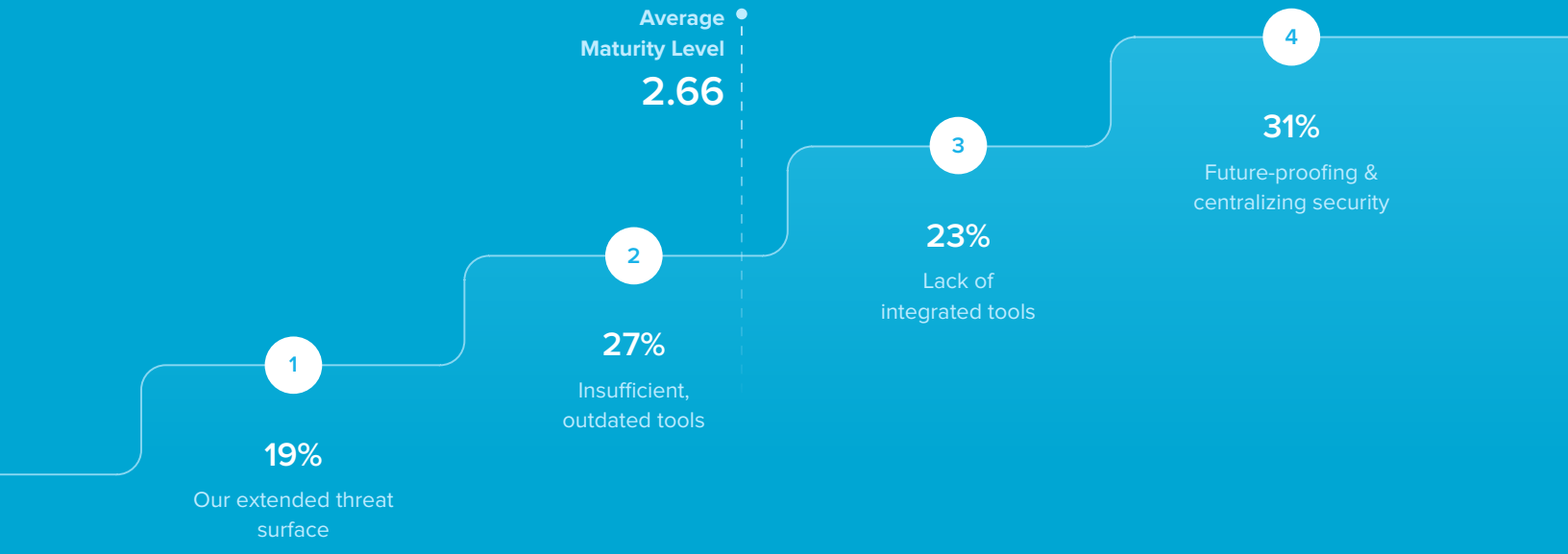
As IT and security leaders continue to enable remote work, users will access resources from a variety of locations. **However, the strategies these companies have in place to secure remote access rate a maturity score of only 2.22 out of 4.**

What's your strategy for securing remote user access to your IT resources?



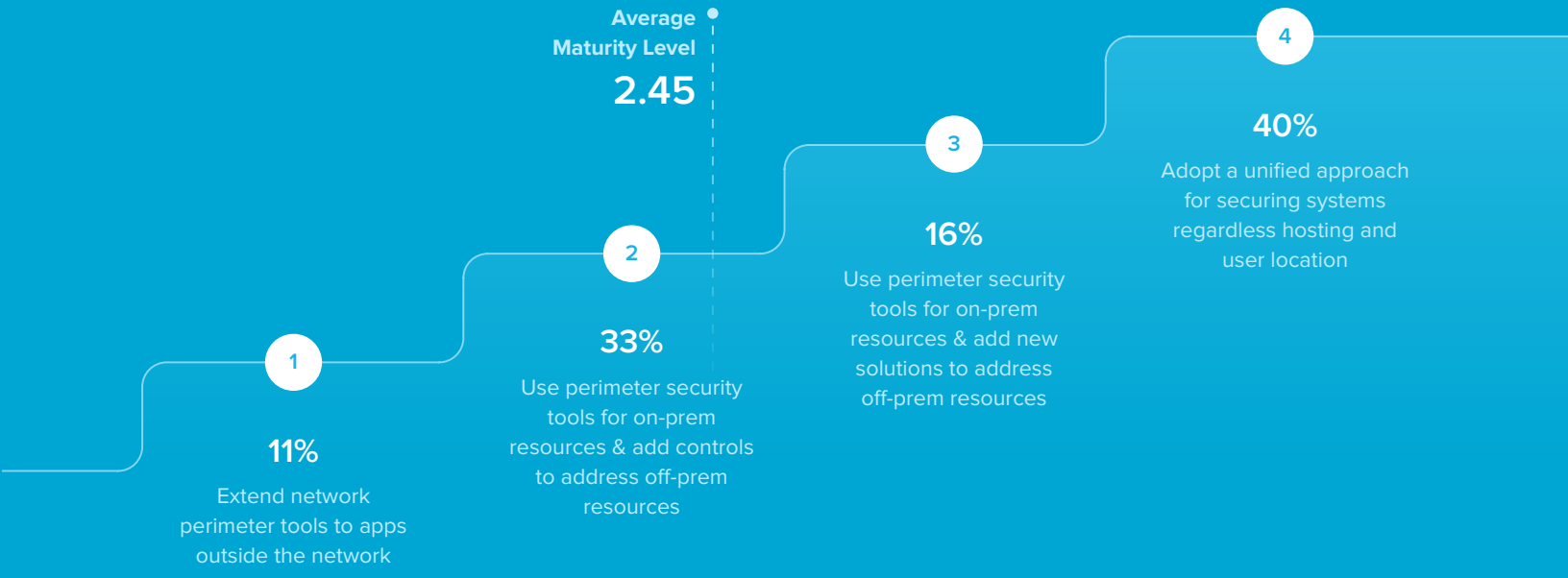
Future-proofing is the most common challenge barring executives from improving their hybrid IT security. **Across the board, respondents scored an average of 2.66 out of 4 for their security challenges.**

When it comes to securing systems access from and hosted in different locations, which of the following challenges does your team struggle with the most?



Most professionals agree: Adopting unified security is the right future-proof security strategy for the Hybrid IT (40%).

What's your strategy for future-proofing your security for new IT assets?

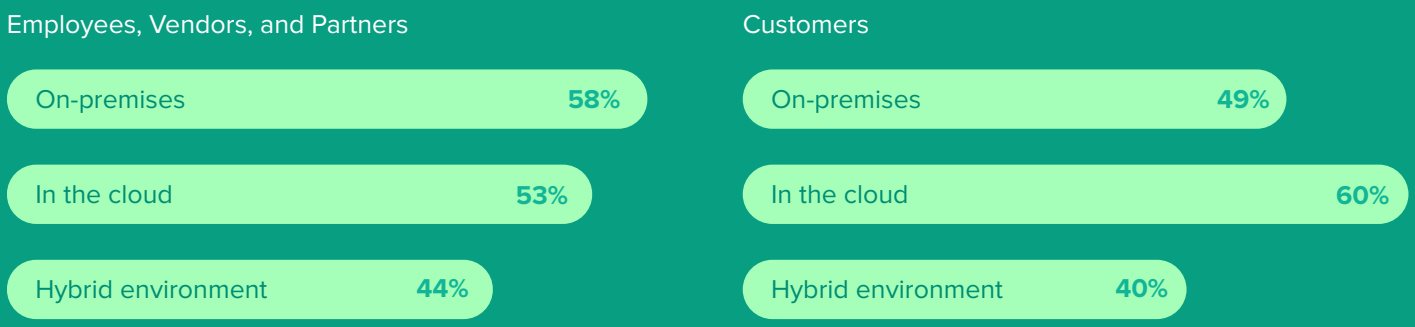


IT teams must improve measurement of technical debt to boost hybrid IT security.

As organizations adopt more technologies, security cohesiveness is key for keeping hybrid IT safe. But this can be challenging when businesses carry technical debt and are far behind on patches, security maintenance, and protection against the latest threats.

Currently, the majority of user data and credentials are stored in a combination of on- and off-premises systems, leading to a wide sprawl of data:

Where do you store your users data?



Which of the following best describes your security technical debt?

43%
Each department keeps its own inventory

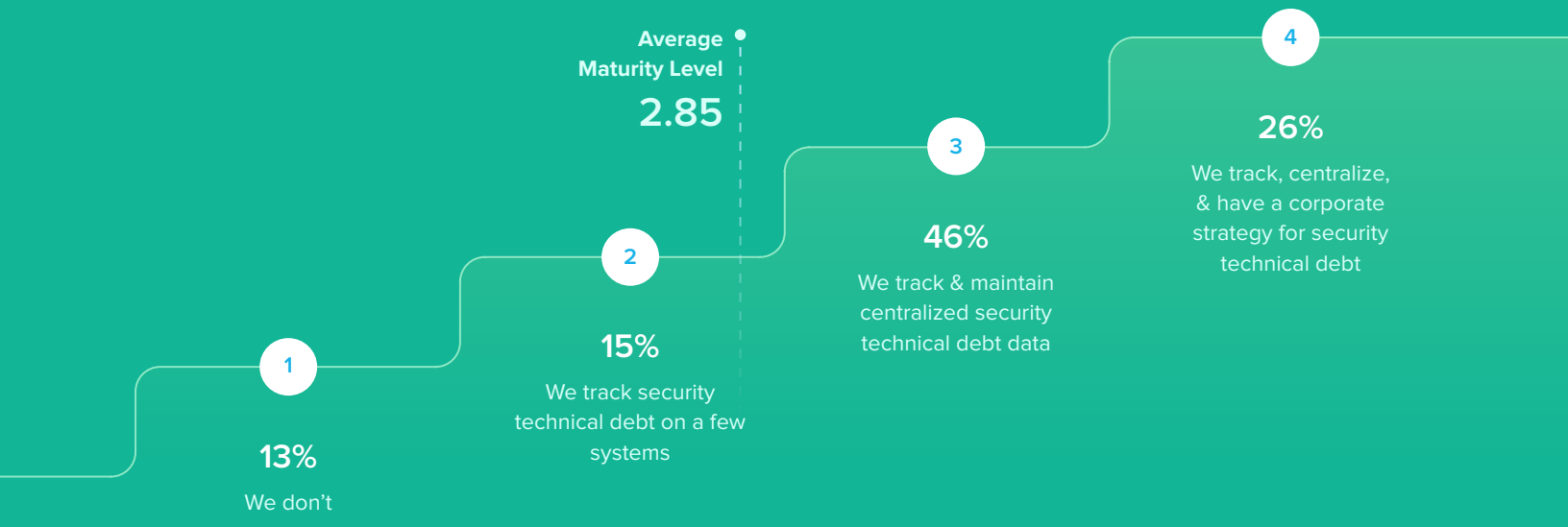
32%
We don't have a unified approach across the organization

20%
We don't know which solutions are falling behind

20%
All our solutions are falling behind

Right now, the strategies these organizations are using to **manage the security technical debt that they're aware of meet a maturity level of 2.85**. Although there's still room for improvement, the management of technical debt was the most mature aspect of the respondents' hybrid IT security practices.

How do you secure access to different asset types (i.e. apps, servers, APIs, and data) and hosting models (i.e. on-prem, MSP, IaaS, SaaS)?



Conclusion

As hybrid IT environments become more prevalent, the complexity of securing various types of infrastructure affects many organizations. While almost a third (31%) of IT and security leaders plan to future-proof these hybrid IT security strategies, they must first take steps to improve the maturity of their current security practices.

To handle such complex problems, IT teams need tools capable of both centralizing security and protecting all assets and resources—regardless of their location.

Unlock the Business Value of Securing the Hybrid IT with a Unified Identity

okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. More than 8,950 organizations, including JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers. To learn more about Okta, visit us at www.okta.com

PULSE

About this survey: To find out organizations maturity securing their Hybrid IT environments, we commissioned a survey from Pulse from Aug. 4, 2020 to Sep. 1, 2020 with 100 IT leaders in North America:

Company Size	
10,001+ employees:	30%
5,001-10,000 employees:	17%
1,001-5,000 employees:	28%
<1,000 employees:	25%

Title	
C-suite	25%
VP	12%
Director	54%
Manager	9%