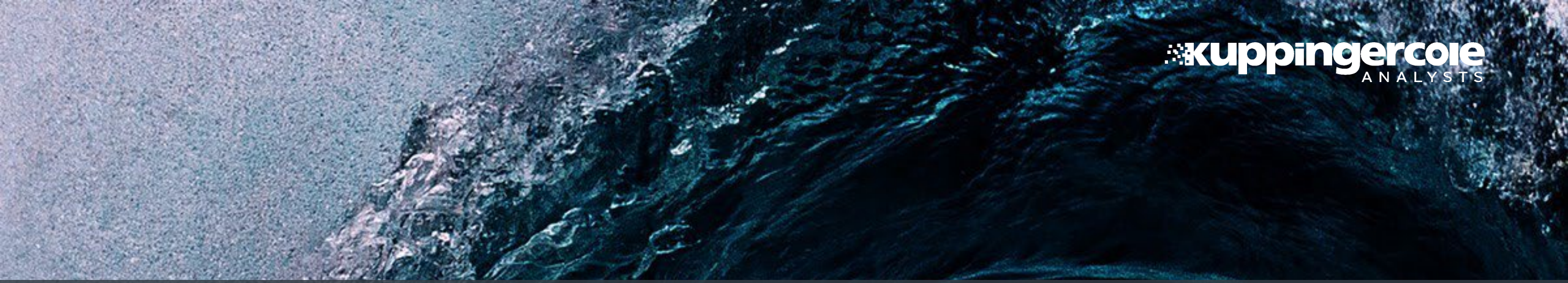


KuppingerCole Survey

Cybersecurity & IAM: 2023 in Numbers

Marina Iantorno

Research Analyst | KuppingerCole Analysts

About this report

Methodology & Sample size

- This report has been created based on accumulated results from a variety of polls that KuppingerCole ran in webinars, at events, via LinkedIn, and on other occasions during 2023.
- The results are based on > 2,000 responses and have been validated by KuppingerCole‘s analysts.
- All predictions can change at any time due to a variety of reasons, including geopolitical and economic changes, innovations in the market, etc. We reserve the right to modify, update, or remove any part of this report.
- The information presented on this report is intended to be for informational purposes only and is based on professional opinions derived from the analysis of survey results and interviews with software vendors, their customers, and our advisory customers.
- This information is not intended to be and should not be construed as legal, financial, or professional advice. In no event will we be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of or interpretation of this report.

© KuppingerCole Analysts AG

Cybersecurity and IAM: 2023 in Numbers

Introduction

Significant advancements happened in identity and access management (IAM) and cybersecurity in 2023. For most organisations, it has become more and more important to strengthen cybersecurity and optimise IAM procedures as they continue to traverse the challenges of digital transformation. This report explores the major figures and trends of 2023 compiled from our polling data and provides insights into the present and potential futures of IAM and cybersecurity.

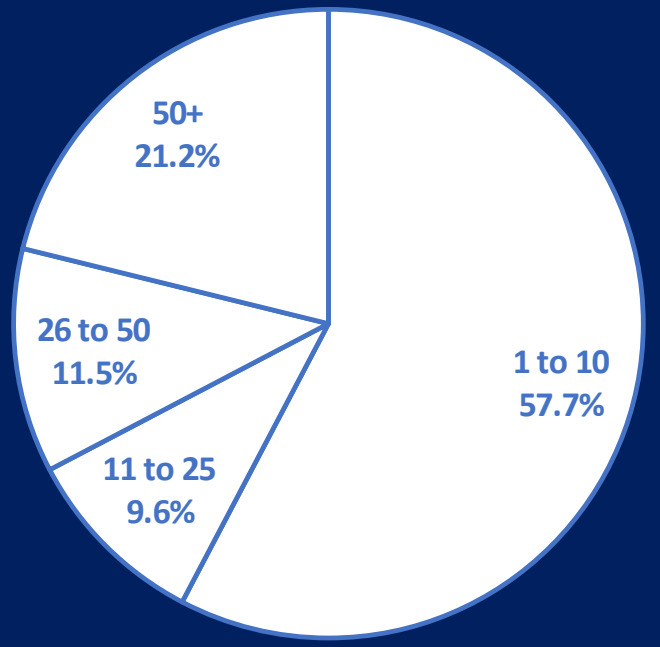
The slides below will show the significant findings.

© KuppingerCole Analysts AG

1. The Password Paradox:

The research shows that 57.7% of respondents have 10 to 20 passwords in place in their organization, indicating the persistent difficulties with password management. Moreover, 21.2% of users have more than 50 passwords. We expect passwordless solutions to become more popular. These statistics show that, although the passwordless market has been growing in the last few years, it has more room for growth in 2024. Looking ahead, the polls reveal that 47.1% of organizations believe that Passwordless Authentication will have the biggest impact on IAM, followed by 33.8% for Decentralized Identity.

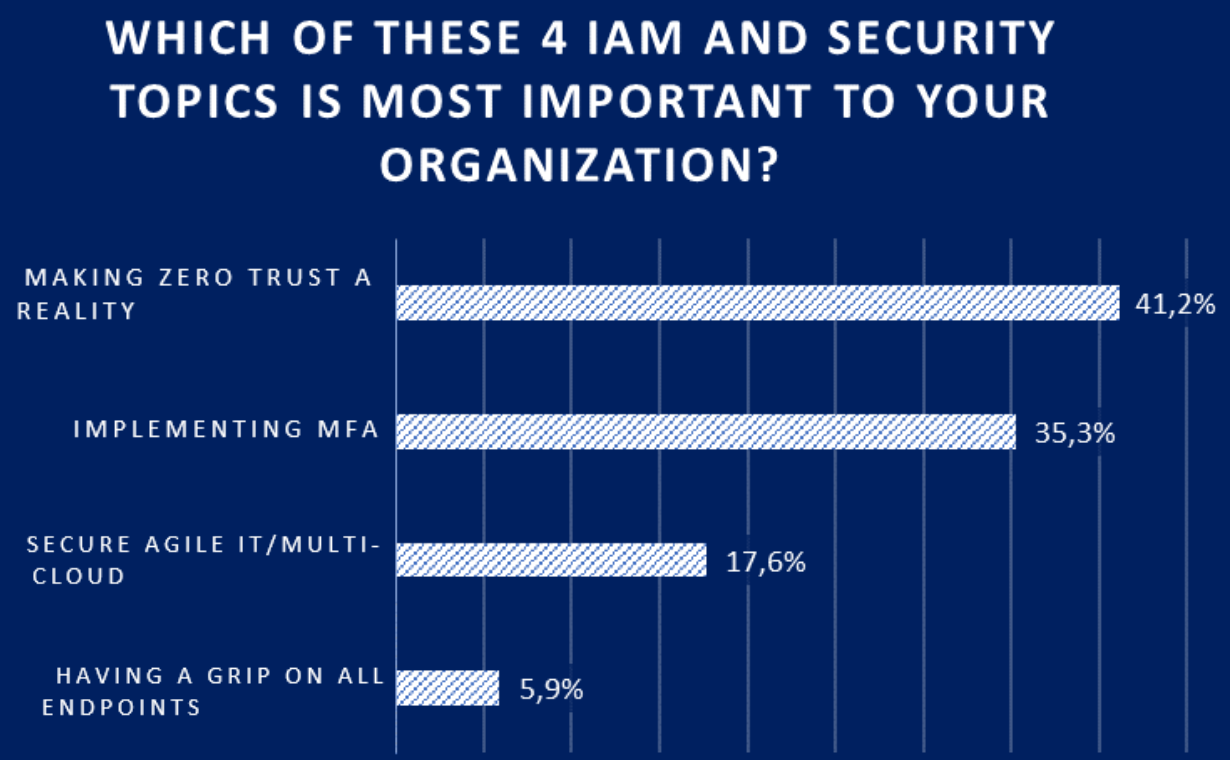
HOW MANY PASSWORDS DO YOU STILL HAVE IN USE (IN BUSINESS)?



© KuppingerCole Analysts AG

2. Security Priorities

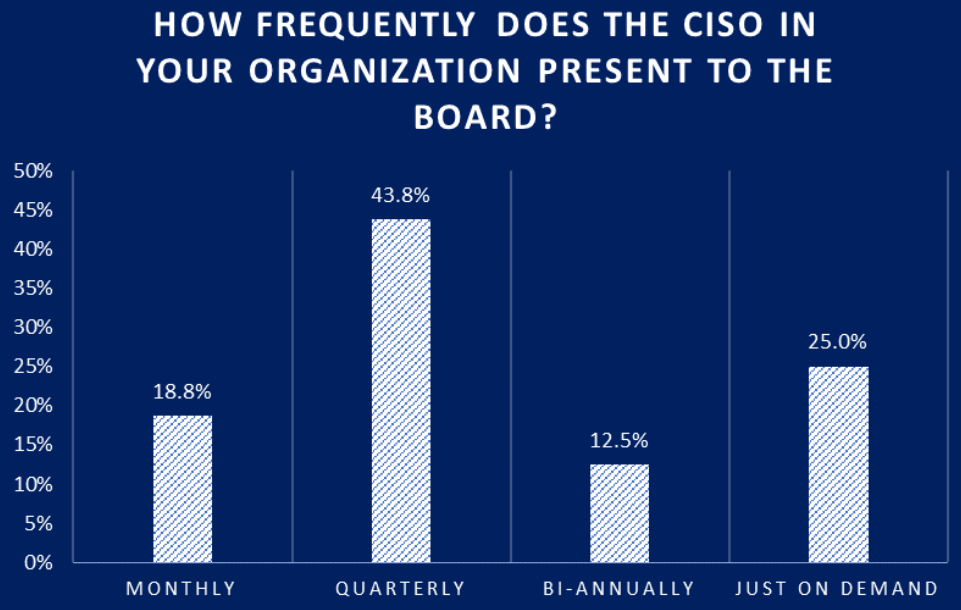
“Making Zero Trust a Reality” was ranked as the top IAM and security goal by 41.2% of participants, while “Implementing MFA/Passwordless” was ranked by 35.3%. These trends demonstrate that both Zero Trust and Passwordless Authentication technologies are mature, effectively productized in the marketplace, and are perceived as excellent investments for improving security architectures. The prominence of these two priorities also shows that most organizations have not fully rolled out Zero Trust and Passwordless.



© KuppingerCole Analysts AG

3. The CISO and its role in organizations

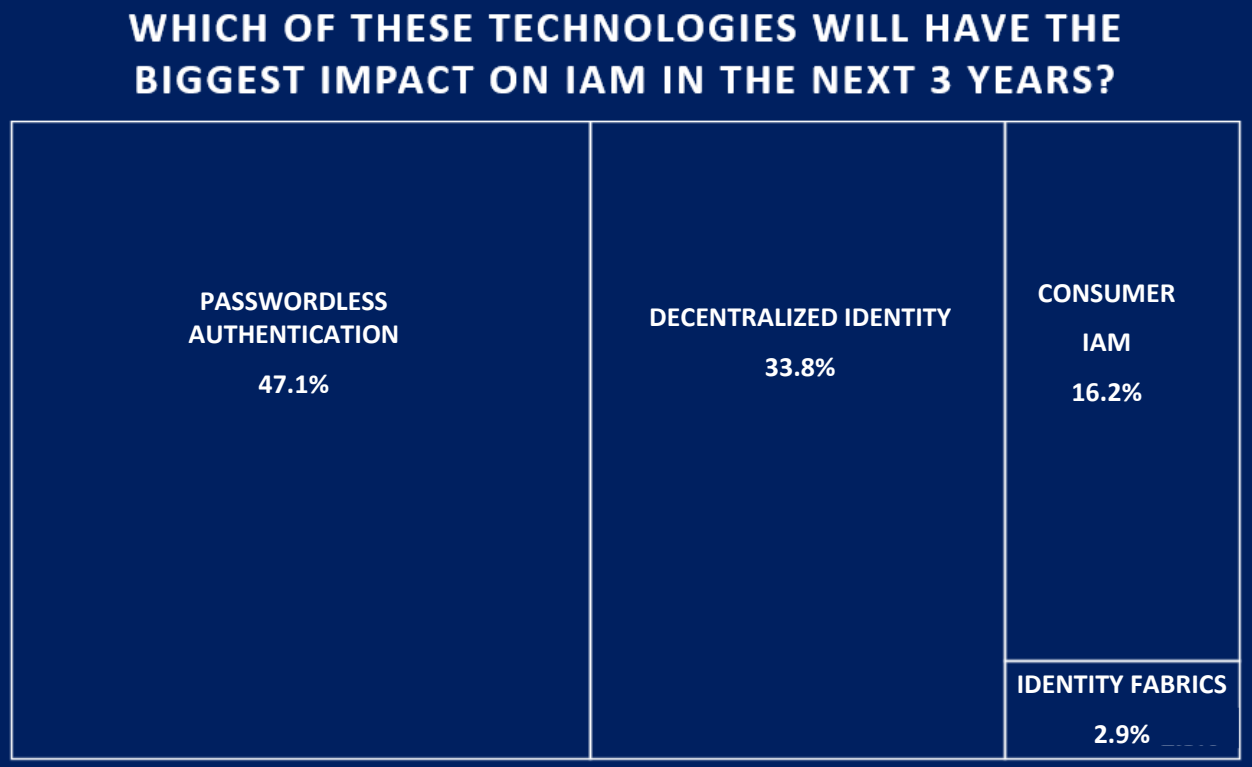
The Chief Information Security Officer (CISO) reports to the Chief Information Officer (CIO) in 40% of organizations. In 34.1% of responding organizations the CISO reports directly to the CEO. This structure reflects the elevated importance of cybersecurity in corporate hierarchies. Furthermore, 43.8% of CISOs present to the board quarterly, emphasizing the growing recognition of cybersecurity at the highest levels of management.



© KuppingerCole Analysts AG

4. Decentralized IAM Solutions

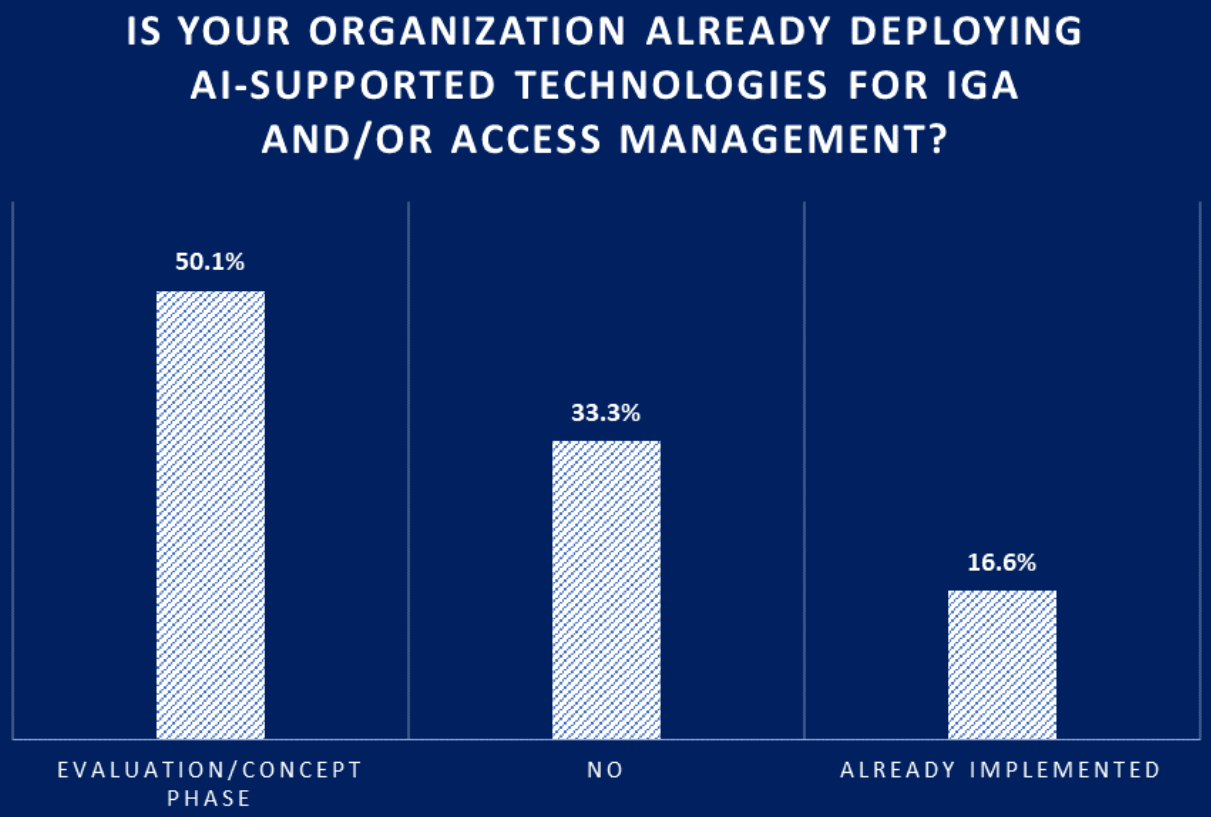
Managing identities and access permissions across multiple platforms and applications is easier with the help of unified systems. Unified IAM systems, or those that are managed identity fabrics, are essential for decreasing complexity and the administrative loads that come with running multiple distinct systems. Organizations can improve operational efficiency, lower error rates, and promote a stronger security posture by combining IAM functions. IAM solutions that are adaptable and scalable are essential as more businesses use mobile and cloud-based services.



© KuppingerCole Analysts AG

5. AI Became a Game Changer in IAM Solutions:

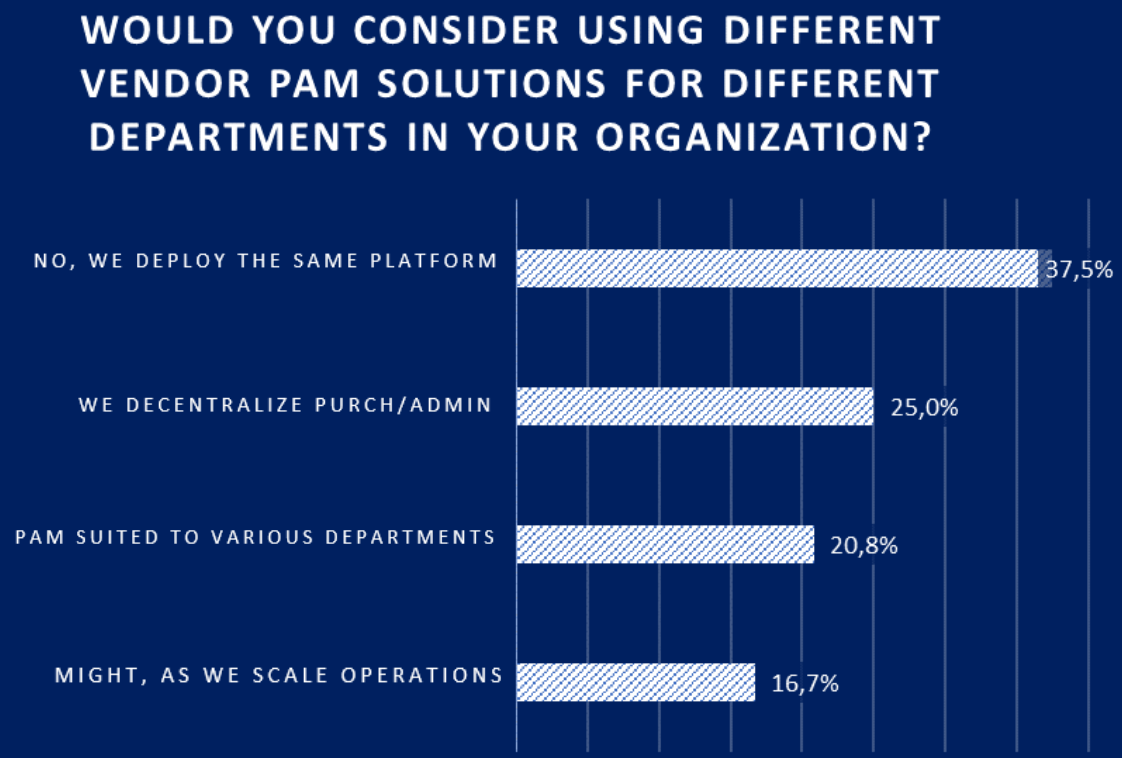
There is a growing recognition of AI's potential to enhance IAM systems. However, the trend towards AI integration is more prevalent across a range of technologies and is not limited to IAM alone. Businesses are realising AI's advantages, such as how it can automate difficult IAM tasks. This is a part of a broader trend where AI is being taken into consideration and applied to a variety of technical solutions although still under close human supervision to guarantee efficacy and handle issues like data privacy and compliance.



© KuppingerCole Analysts AG

6. PAM Solutions

The approach to Privileged Access Management (PAM) has evolved significantly, reflecting the understanding of its critical role in cybersecurity. The data shows that different strategies are used to implement PAM systems. 16.7% of respondents are willing to switch their PAM systems, even though 37.5% of them use the same PAM platform across many departments. The variation found in PAM systems is indicative of an adaptive approach, which recognises that various departments could have distinct security requirements and risk profiles.



© KuppingerCole Analysts AG

Conclusions

The evolution of IAM and cybersecurity in 2023 clearly highlighted an industry at a junction of innovation and adaptability. The results of our studies show that the cybersecurity landscape is changing, with organisations having to deal with issues like managing password complexity, implementing passwordless authentication and Zero Trust, and CISOs playing a more crucial role in directing organisational security strategies.

Integrated IAM solutions are becoming more popular, which indicates a strategy change that is in line with organisations' larger objectives for digital transformation. This change not only aligns with the evolving requirements of digital organisations but also helps operational efficiency and a unified security approach. In addition, the investigation of AI's function in IAM and the variety of approaches in PAM implementation demonstrate comprehension and adaptability to the complex problems associated with cybersecurity. The environment is ready for sustained growth and innovation in 2024.

In conclusion, the insights obtained in 2023 provide strong basis for the advancement of IAM solutions and cybersecurity. Future cybersecurity strategies will continue to be designed with an emphasis on integrated solutions, AI adoption, and strategic PAM deployment, making sure that businesses are better prepared to safeguard their digital assets in a world that is becoming more interconnected by the day.

© KuppingerCole Analysts AG

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

E: info@kuppingercole.com
www.kuppingercole.com