KuppingerCole Report

WHITEPAPER

By Martin Kuppinger, Alejandro Leal

April 05, 2022

The Future is Passwordless. If you do it right.

Passwordless authentication has become a popular topic. Given the security risks and inconvenience of using passwords, many organizations are looking to completely eliminate and replace passwords with more secure authentication methods. As credential theft and ransomware attacks continue to rise, the logical step is to move away from passwords. Done right, it increases both security and convenience. However, with the device becoming a central factor in secure passwordless authentication, device trust is essential and must be incorporated into the security posture of any organization. Only then will passwordless authentication deliver to the expectation and become a cornerstone of zero trust approaches.

By **Martin Kuppinger**
mk@kuppingercole.com

By **Alejandro Leal**

Content

1 Introduction 3

2 Highlights 5

3 Passwordless authentication: under the hood 6

4 Device trust: the foundation for passwordless authentication 8

5 Passwordless authentication: cornerstone of zero trust 10

6 The Beyond Identity's passwordless authentication for the workforce 12

7 Recommendations 15

8 Related Research 16

Content of Figures 17

Copyright 18

Commissioned by BEYOND IDENTITY

1 Introduction

In 1961, MIT was one of the cradles of computing activity and innovation in the world. It was around this time that computer scientists developed the Compatible Time-Sharing System (CTSS), an operating system for multiple users that employed separate consoles to access a shared mainframe and required users to use passwords to secure and access private files.

By developing a system that requested users to verify their identities, the birth of passwords introduced the concept of login and authentication in the digital world. However, only a few months passed between the first password use and the first password compromise.

Following the creation of the CTSS, a software bug infected the system's master password file and made everyone's passwords available to anyone who logged into the system. This breach demonstrated that the first passwords were not designed to provide security for the system but were instead created to keep track of how much time was spent on shared mainframe computers.

While digital identity and authentication have undergone a number of changes since the early days, passwords have remained largely the same. Passwords are a remnant of a time before hacking became a serious and widespread problem. No one could have predicted back then that one day organizations and personal lives would be highly conducted and dependent on cyberspace. As computers became more easily accessible, hackers targeting operating systems increased in frequency, intensity, and sophistication.

Consequently, the IT security community has been looking to replace passwords with alternative methods and more secure solutions. However, many enterprises and individuals still rely on passwords despite the risks and vulnerabilities they present. In 2021, for instance, the Verizon Data Breach Investigations Report revealed that 89% of web application breaches were caused by passwords, either through stolen credentials or brute force attacks.

Although credential theft and password-based attacks continue to increase, many implementations of alternative solutions, including biometrics, magic links and smartcards still frequently use passwords as a backup for these methods. As long as passwords continue to be used, users will remain vulnerable to attacks. Traditional multi-factor authentication (MFA) does not solve the problem either because it usually relies on a password as the first factor while also adding friction to the authentication process. One-time passwords, push notifications, and other 2nd factors of authentication can be bypassed by attackers more easily than most think, thus putting current MFA solutions at risk.

In order to successfully implement a passwordless solution, it is necessary to remove the password for all

aspects of the authentication flow and from the recover process as well. As a consequence, eliminating passwords will add a significant layer to the overall security posture of an organization and increase security and convenience at the same time.

Beyond Identity offers a passwordless MFA solution, which entirely eliminates passwords by using asymmetric cryptography and biometrics while providing a frictionless experience to the user. By protecting the device from password-based attacks, Beyond Identity's MFA is invisible and unphisable. Phishing-resistant authentication refers to processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system. Thus, the solution does not only get rid of passwords and one-time codes, but also enforces device trust and lays the foundation for a zero trust security architecture.

To conclude, migrating from legacy MFA solutions to passwordless MFA products might make all the difference between surviving in a rapidly changing world of working from home, avoiding the harsh penalties of compliance regulations, and defending your organizations from phishing and ransomware attacks.

2 Highlights

- Phishing and ransomware attacks have been intensifying over the past few years as cybercriminals continue to devise new strategies to launch sophisticated attacks and gain unauthorized access through stolen credentials. Legacy MFA products were supposed to solve the problem of password complexity and reduce phishing and ransomware attacks, but these solutions still rely on a password as the first factor of authentication and easily bypassed second factors.
- To achieve a zero trust model, strong authentication and device trust are essential. Therefore, the implementation of device trust and risk-based controls will ensure that only trusted devices and users have access to company data and resources. A zero trust paradigm should be able to eliminate implicit trust from IT systems and enforce strict identity verification for all users and devices. By getting rid of passwords and adopting a passwordless MFA solution, organizations can prevent password-based attacks and increase their overall security posture.
- Beyond Identity offers a passwordless solution that provides strong MFA and enables zero trust by continuously assessing the security posture of the device and only allowing access to registered devices. Furthermore, the invisible and unphishable MFA solution also allows users to enjoy a frictionless experience while being protected against password-based threats.

3 Passwordless authentication: under the hood

Without secure, enterprise-managed identity systems, attackers can take over user accounts and gain a foothold in an organization to steal data or launch further attacks. Passwordless MFA solutions should be able to eliminate the reliance on passwords, or other easily phishable factors, as an authentication method.

Over the past few years, the world has been affected by phishing and ransomware attacks, which have disrupted organizations already stressed by the COVID-19 pandemic. The most recent Verizon Data Breach Investigations Report shows that phishing was up to 36% in 2020, compared to 25% of attacks in 2019. In addition, the frequency of ransomware attacks doubled compared to the 2019 report, appearing in 10% of breaches in 2021. By removing the risk associated with passwords and adopting a passwordless solution, organizations could prevent password-based attacks while increasing the overall security posture of their organizations.

Password-based attacks are often employed by hackers to obtain stolen credentials and wreak havoc on an organization's infrastructure. Attackers can use compromised data to breach an organization's resources and steal sensitive information. Although authentication has improved over the past few years, cybercriminals continue to use a wide range of techniques and procedures to gain unauthorized access. To stay competitive and reduce security risks, cutting-edge organizations are dumping passwords and adopting new technologies.

Traditional MFA solutions were supposed to overcome the issue of passwords. However, the problem is that MFA still relies on a password as the first factor of authentication. To make matters worse, the second factor is also often vulnerable to password-based attacks. While MFA was designed to protect from attacks exploiting weak or stolen credentials, attackers still can bypass the additional factors that are used today. One-time passwords (OTP) and push notifications that pretend to be security prompts can be used to trick users into giving their account details to attackers. In addition, attackers can send MFA requests over and over to the end user's device until the user accepts authentication, allowing the attacker to eventually gain unauthorized access to the system. Phishing actors are also using man-in-the-middle pages and reverse-proxy tools to deceive users into giving up their credentials further undermining legacy MFA solutions.

Organization's systems must cease supporting legacy authentication methods that are prone to phishing attacks, such as those that require registering phone numbers for SMS text messages, voice calls, or supplying one-time codes. It is much easier for attackers to obtain unauthorized account access, even in systems that use MFA.

As remote work becomes more prevalent and password-based attacks continue to increase, preventing a password compromise is one of the main challenges business organizations and government agencies face today. Recently, the U.S. government published a memorandum emphasizing the need for stronger enterprise identity and access controls, including using phishing-resistant MFA and a zero trust model. The

memorandum goes further and claims that understanding how devices, users, and systems interact within the organization is key to any enterprise-wide zero trust architecture. Thus, organizations and agencies must pursue greater use of passwordless MFA solutions as they modernize their authentication systems.

Although there are different perspectives on passwordless authentication solutions, a passwordless and phishing-resistant MFA authentication solution should be able to provide the following:

- Include an integrated authentication approach
- Support industry standards
- Have a consistent and frictionless login experience across all supported devices
- Enable organizations to control which users and devices can access sensitive information
- Ensure that devices meet the organization's security requirements before granting access
- Completely eliminate the reliance on passwords or other easily phishable factors as an authentication or account recovery method

To strengthen access controls, organizations have to analyze information from multiple sources to make security decisions, such as performing device health checks and evaluating activities conducted on multiple devices. By enforcing device trust and getting rid of passwords, organizations adapting a passwordless solution will lay down the groundwork for a zero trust security architecture.

4 Device trust: the foundation for passwordless authentication

Since devices store sensitive and confidential information, the role devices play in passwordless MFA is critical. To establish device trust, the first step is to verify the identity of the user. The second step consists in determining if the device can be accessed securely prior to granting access. Device trust is therefore an essential building block to strong authentication and achieving a zero trust model.

Strong authentication cannot be achieved without eliminating passwords and enforcing device trust at the same time. Device trust is the process of analyzing whether a device should be trusted, and therefore, is authorized to do something. It requires solutions to possess the ability to verify the user behind the device and continuously validate the security posture of the device to make sure only authorized users will get access to the company\'s data and resources.

It is essential that the devices accessing company data are secured and determining which devices should be trusted is a unique decision made by each organization. By enforcing device trust, not only the employees of an organization get access to the right information and resources, but also contractors and vendors that need certain data. However, since sensitive information and intellectual property can now easily be accessed from any web browser and device, this presents a serious challenge for organizations in the era of bring-your-own-device (BYOD). Thus, providing security across multiple devices is fundamental, for zero trust, especially in the context of BYOD.

As BYOD became more common after the COVID-19 pandemic hit, the convenience of new BYOD policies came at the cost of security. Organizations that implement official BYOD policies need to better understand the inherent risks associated with BYOD, such as unpatched software on devices, authenticating personal devices, and using insecure networks. Increasing remote work and BYOD support can have significant benefits for an organization, but the security implications cannot be ignored. If you cannot trust the integrity of the device that is attempting to authenticate, even with MFA in place, you're still at risk of giving access to bad actors leveraging compromised devices.

By ensuring trust in all devices (managed and unmanaged) before authenticating, security teams can be more confident that sensitive company data is secure and protected. However, since unmanaged devices are not registered to users, it makes it very difficult to know who actually owns the device. Furthermore, unmanaged devices can already be compromised and become an attack vector. Although managed devices are registered with a user, these might not have the security settings configured properly or the security software installed and running, and therefore do not guarantee security. Whether the device is managed or unmanaged, conducting real-time device health checks and risk signals adds an additional layer to the overall protection of the device. As a consequence, continuously checking a device\'s security posture at the time of login seems to be the only way to ensure that the device is in compliance with security requirements.

The ability to constantly evaluate the security posture of multiple devices in a seamless manner at the exact

time of login addresses many of the challenges that the emergence of BYOD has introduced, including the authentication of multiple devices and the volume of requests. Since the concept of zero trust starts with the assumption that every access request is unauthorized, device trust tackles many of the challenges associated with BYOD.

As organizations continue to embark on their zero trust journey, it is vital to establish trust in endpoint devices and make sure that only the right people are allowed to access a company\'s resources. Managing BYOD and unmanaged endpoints can be challenging, however, the only way to ensure all your endpoints are trusted is to evaluate them all in real-time. Having strong device trust policies in place gives organizations the confidence to control access to critical cloud applications and secure company's sensitive data and information.

5 Passwordless authentication: cornerstone of zero trust

Passwordless authentication is essential to zero trust because it secures both the identity and the device, if done right, it becomes a foundational block of a zero trust model. This analysis will be based on the concept of "seven pillars of zero trust" by KuppingerCole, with identity and the device being two of these pillars.

Due to its catchy name and appeal to many vendors, zero trust has unfortunately created some unrealistic expectations. In response to a massive marketing push from network and cybersecurity vendors, some organizations got caught up in the hype surrounding zero trust security. Zero trust, however, is not a product or even a technology - it is a concept, and it requires a major shift in many aspects of IT and even core business processes of an organization.

The zero trust paradigm focuses on eliminating implicit trust from IT architectures and enforcing strict identity verification and access controls for every user or device. It helps to redesign your cybersecurity architecture to function consistently and holistically across multiple IT environments and systems - and thus implementing zero trust properly will affect multiple existing and new security controls within your organization.

Here are the seven pillars of zero trust architectures by KuppingerCole:

1. All access decisions are performed on a per-resource basis, where resources are defined as any kind of a device, data source, application, cloud service, and so on.
2. All communications between resources must be secured properly, regardless of their locations. In practice, this implies end-to-end encryption of any network traffic between resources.
3. Access to a resource is granted according to the principle of least privilege and on a per-session basis, after an explicit evaluation of trust in the requester. Authorization for one resource does not enable implicit access to other resources.
4. Access is driven by dynamic policies that continuously evaluate the state of the resource, requester, and other context attributes. Each access decision is made based on real-time risk evaluation that may include behavioral analysis, environmental conditions, history of previous accesses, etc.
5. Integrity and security of all assets must be continuously monitored and deviations in security posture must be mitigated promptly.
6. Authentication and authorization must be dynamic and strictly enforced. This includes the use of strong multi-factor authentication, scanning for cyberthreats, and reevaluating trust before each transaction.
7. The information about the current state of assets and their communications must be collected,

analyzed, and used to improve the organization's security posture.

The transition to a passwordless solution will be smoother and more secure if the basic components of zero trust are implemented first, such as SSO, MFA, and device trust. In the zero trust model, users wishing to access information and data must be authenticated, authorized, and continuously validated for security configuration and posture checks before they can gain access to the organization\'s resources.

Furthermore, zero trust is not primarily about networks, but about identities, devices, systems and applications. It is about ubiquitous and continuous verification of device security and identity authentication. Generally speaking, Zero Trust requires proper authentication and authorization for each session involving users, applications, networks (including clouds), and data.

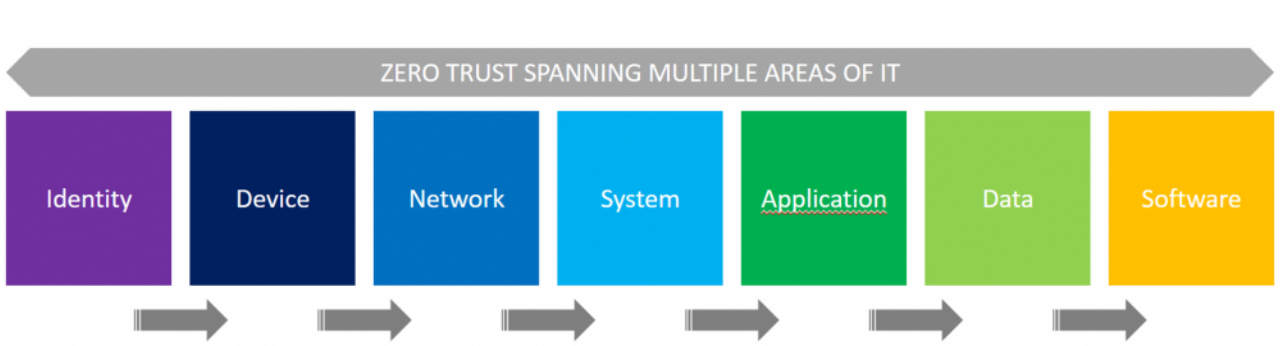

Figure 1: zero trust spanning multiple areas of IT [Provided by KuppingerCole]

Different organizations may face different challenges when implementing certain technologies, however, it is important that organizations take into account the basic Zero Trust principles. A Zero Trust model must have clear targets, a vision, and a strategy. Once these components are in place, policies, processes, and organizational components must be followed.

Zero Trust is a journey that begins with a long-term business strategy and focuses on a step-by-step implementation, using existing or readily available tools and technologies, while maintaining the continuity of business processes and avoiding adding even more complexity to the existing architecture.

6 The Beyond Identity's passwordless authentication for the workforce

Beyond identity introduces a passwordless authentication solution that aims to enable zero trust and enforce device trust, while providing strong multi-factor authentication and allowing access to only registered devices. Instead of using passwords, users rely on a device-bound credential for zero-friction passwordless authentication that uses asymmetric cryptography and adaptive risk-based controls that continuously assess the security posture of the device.

Headquartered in New York City, Beyond Identity aims to rid workforces of passwords everywhere. Through Beyond Identity's cloud-native solution, customers can achieve complete passwordless identity management, increase security and convenience, and implement new business models.

The prevalence of remote work and the use of cloud-based applications has made device trust an essential part of the security architecture of an organization. Beyond Identity\'s capacity to deliver a cryptographic method to validate the identity of a person using multiple devices, including unmanaged devices and BYOD, in real time is a key advantage that sets them apart from many competitors in the market.

Beyond Identity's solution provides a strong, invisible, and unphishable method of authenticating users that completely eliminates passwords and replaces them with self-signed X.509 certificates and strong asymmetric cryptography for authentication in order to validate that each device is registered to a known and authorized user. Furthermore, it continuously assesses whether the security posture of the device meets the compliance and security requirements.

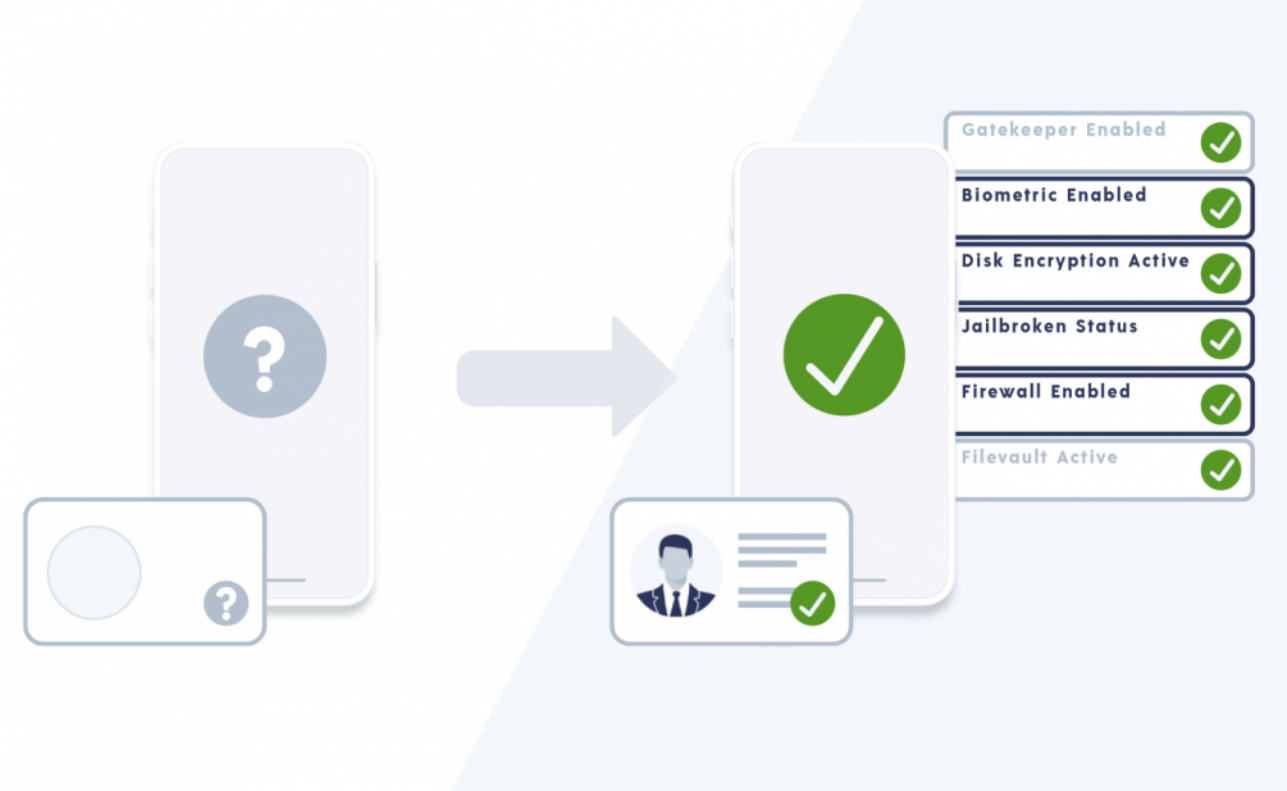

Figure 2: The access flow of Beyond Identity risk-policy engine [Provided by Beyond Identity]

With Beyond Identity, there is no need for passwords, secondary hardware devices, one-time passwords (OTP), one-time codes, or push notifications. Instead of relying on a certificate authority (CA) managed by a third party, Beyond Identity turns devices into their own CA. By using the self-signed X.509 certificate, the solution ensures that users are in possession of only two attributes: "something you are" from the device biometric and "something you own" from the possession of a private key.

During the initial registration, the public key is stored in the Beyond Identity cloud. The public-private key pairs cryptographically bind the end user with their device (or multiple devices). So, during each login request the Beyond Identity authenticator asks the device's Trusted Platform Module (TPM) or other secure element, depending on the technical platform, to prove it possesses the cryptographic private key by generating a X.509 certificate signed using the private key. The TPM, and other types of secure elements, are designed to store sensitive information and carry out cryptographic operations by securing hardware through integrated cryptographic keys.

The private key cannot be viewed or removed by anyone from Beyond Identity, nor by the user. Following the creation of the private key, the private key is securely stored in the TPM of the personal device and used to sign the certificate. The certificate is then forwarded to the public cloud to be validated by the corresponding public key, which verifies that the certificate was issued from the same device.

As part of its passwordless authentication service, Beyond Identity now collects more than 25 attributes from users, devices, and applications. The identity-bound solution enforces device trust by **verifying** the user

behind the device, evaluating whether the user is authorized to use the device, and detecting with real-time device checks if the device is secure enough for accessing the application or service being requested. This solution acts on customizable risk signals from the user and their device's security posture to make sure that biometric authentication and firewall are enabled, the hard drive is encrypted, other security settings are in order and security processes are running smoothly, etc.

While replacing legacy MFA with passwordless solutions is not possible in one single step, Beyond Identity ameliorates the process by introducing a frictionless MFA that makes it easier to integrate with a single sign-on (SSO). To integrate with SSOs, Beyond Identity uses the OAuth and OIDC protocols with downstream support for SAML. With Beyond Identity\'s invisible MFA and strong authentication, users are able to enjoy a passwordless experience while being protected by high-trust security that validates identity and ensures device access and security at the same time.

In addition, Beyond Identity uses a standards-based approach which integrates easily with other Access Management solutions and endpoint security tools such as Okta, Auth0, Ping Identity, ForgeRock, Microsoft Azure AD, and Microsoft ADFS (for on-prem or hybrid deployments).

Traditional MFA providers that rely on passwords have demonstrated a number of weaknesses. Since passwords are often re-used and stored in insecure places, organizations must adapt to new threats and incorporate new authentication technologies. By adapting Beyond Identity's passwordless MFA, users are protected against phishing and ransomware attempts by using authentication factors that cannot be easily manipulated by attackers, thus, increasing the overall security posture of the organization.

7 Recommendations

As password-based threats continue to rise, organizations must move away from passwords and replace them with strong passwordless multi-factor authentication solutions. Done right, organizations will increase both security and make authenticating more convenient for users. Device trust is also an essential component and should be incorporated into the security posture of any organization. Only then will passwordless authentication meet expectations and become a cornerstone of zero trust approaches.

While there are many things to look at and do, there are some key recommendations:

- **Define your organization's requirements**: It is important to determine the business needs of your organization and define them in a measurable way.
- **Follow a zero trust path**: Create a logical architecture that unifies different services and provides the capabilities your enterprise needs by aligning these defined requirements to a zero trust model.
- **Implement a phased implementation approach**: Take the necessary steps that better suit your business model by replacing legacy MFA providers with passwordless, invisible, and unphishable authentication solutions.
- **Design a comprehensive, multi-layered, defense-in-depth security architecture:** In order to be able to address any kind of password-based attack, including phishing and ransomware attacks, it is crucial to **pursue greater use of passwordless multi-factor authentication** and modernize your organization's authentication systems.
- **Select a deployment model:** Make sure that the solution you decide to incorporate into your organization supports your requirements, specifically the elasticity and scale required for supporting digital services.

Passwordless MFA authentication is a new approach specifically designed for organizations with a hybrid workforce wishing to eliminate and replace passwords. Therefore, it is important for organizations to consider a phased implementation approach that is well-suited from a technical and business standpoint.

Ultimately, embarking on a zero trust journey depends on your business model and requirements. Therefore, look for trusted advisors and competent vendors that will support you along your mission

Be sure to define the business requirements in measurable terms and to understand them.

8 Related Research

LeadershipBriefHowtoGetRidofPasswords-Today
LeadershipCompassAccessManagement
LeadershipCompassEnterpriseAuthenticationSolutions

Content of Figures

Figure 1: zero trust spanning multiple areas of IT [Provided by KuppingerCole]

Figure 2: The access flow of Beyond Identity risk-policy engine [Provided by Beyond Identity]

Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole´s initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.