KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger, Alejandro Leal

February 17, 2022

Beyond Identity Secure Work

Secure Work is a passwordless authentication solution that aims to enable zero trust and enforce device trust (i.e., ensuring the trustworthiness of a device for being authorized to access applications and data), while providing a strong multi-factor authentication and allowing access to only registered devices. Instead of using passwords, users rely on a device-bound certification for zero-friction passwordless authentication. The solution uses asymmetric cryptography in order to validate that each device is registered to a known and authorized user and an advanced authenticator to assess whether the security posture of the device meets security policy and compliance requirements.

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

By **Alejandro Leal**

Content

1 Introduction

Passwords can easily be stolen, guessed, or compromised. Relying on passwords for security has become increasingly risky and problematic for organizations. End-user behavior can put at stake the security of computer and information systems. Numerous studies have shown that most data breaches involve the use of stolen credentials and compromised passwords, making them one of the weakest links in cybersecurity.

To understand why a passwordless solution has the potential to secure and enhance the IT systems of an organization, it is important to recognize why passwords are failing as an authentication system. In most cases, users use or reuse similar passwords across different platforms, increasing not only risk and vulnerability but also the possibility of password-based threats such as brute force attacks, social engineering attacks, and SIM swaps.

As a result, organizations are continuously seeking to address this fundamental security risk. The IT security community has long been aware of the fact that passwords provide little or no security at all as a means of authentication. Therefore, as remote work becomes more prevalent and cyberattacks continue to increase, preventing a password compromise is one of the main challenges organizations face today. In response, investment into cybersecurity has soared but, in most cases, these efforts have not fully addressed the reliance on passwords and the vulnerabilities they present.

The main problem of passwords in the workforce is the security risk they pose to the entire digital ecosystem of an organization. Furthermore, managing existing passwords within an organization can be burdensome, time-consuming, and costly. Since password elimination is recognized as a fundamental goal for the IT security industry, passwordless options are increasingly gaining popularity and widespread adoption. To minimize the reliance on passwords and the associated risk, the industry has been working for a long time on different technical solutions and standards.

However, many solutions claiming to be passwordless do not entirely eliminate passwords, but simply reduce the amount of passwords or add another insecure factor for authentication. Various solutions are still password-bound such as password managers, and legacy multi-factor authentication (MFA) solutions, which utilize passwords as a factor in their authentication process. Solutions that are passwordless employ secure factors such as biometrics and are standard-based, such as FIDO.

Passwordless authentication solutions should provide a consistent login experience across all devices, introduce a frictionless user experience, include an integrated authentication approach, support industry standards, support access management products that use SAML or OIDC, and eliminate the dependence on passwords or other easily phishable factors, as an authentication method.

To stay competitive, secure, and compliant, organizations must actively seek newer ways of assessing and managing security risks without disrupting the users and the business. By removing passwords as an authentication method, organizations will end up with a modern authentication system that does not rely on

users remembering passwords. If successfully implemented, the passwordless solution will add a significant layer to the overall security posture of the organization while providing a frictionless experience to the users. It increases both the level of security and the user convenience.

2 Product Description

Beyond Identity was founded in early 2019. They are headquartered in New York and have offices and customers around the world. As an innovator in passwordless multi-factor authentication solutions, Beyond Identity breaks down the barriers between identity, security, and device management. They offer a broad range of capabilities supporting:

- passwordless MFA
- device trust
- risk based authentication

To secure devices and the access of remote workers, Beyond Identity designed Secure Work as their main product for the workforce, alongside their other offerings for customers and consumers, and for the DevOps space. Secure Work is a passwordless multi-factor authenticaton solution aimed at organizations looking to eliminate passwords as an authentication method. The platform replaces passwords with secure credentials based on their patent-pending solution that uses self-signed certificates and public-private key pairs.

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 Bring Your Own Device (BYOD), in real time is a key advantage.

Essentially, Secure Work replaces passwords with a strong asymmetric cryptography for authentication in order to validate that each device is registered to a known and authorized user by assessing whether the security posture of the device meets the compliance requirements. Current solutions with cryptography processes and mechanisms rely on a certificate authority (CA), which can either be costly or very complex to set up, secure, and manage. However, instead of relying on a CA managed by a third party, Beyond Identity turns devices into their own CA. By employing their self-signed X.509 certificates on endpoint devices, this innovative and key differentiator solution extends the server-to-server chain of trust established with Transport Layer Security (TLS) to users and their devices.

Thus, Secure Work enforces device trust by combining an identity device-bound solution together with real-time device checks for secure access. 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 create a cryptographic private key by generating a X.509 certificate. 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.

With Beyond Identity, there is no need for passwords, secondary hardware devices such as one-time password (OTP) generators, one-time codes, or push notifications required to authenticate. Using the self-signed X.509 certificate and the public-private key pairs 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. In addition, the solution validates and makes sure that each device is registered to a known and authorized user by assessing whether the device meets the security requirements.

During authentication, the solution runs data through the cloud and acts on customizable risk signals from the user and their device's security posture to make sure that there's a secure enclave, biometric authentication and firewall are enabled, the hard drive is encrypted, processes are running smoothly, etc. If some of these elements are absent, the device won't be secured and able to be authenticated. Also, the solution strengthens access control and risk-based policies with mobile device management (MDM) and endpoint detection and response (EDR) checks.

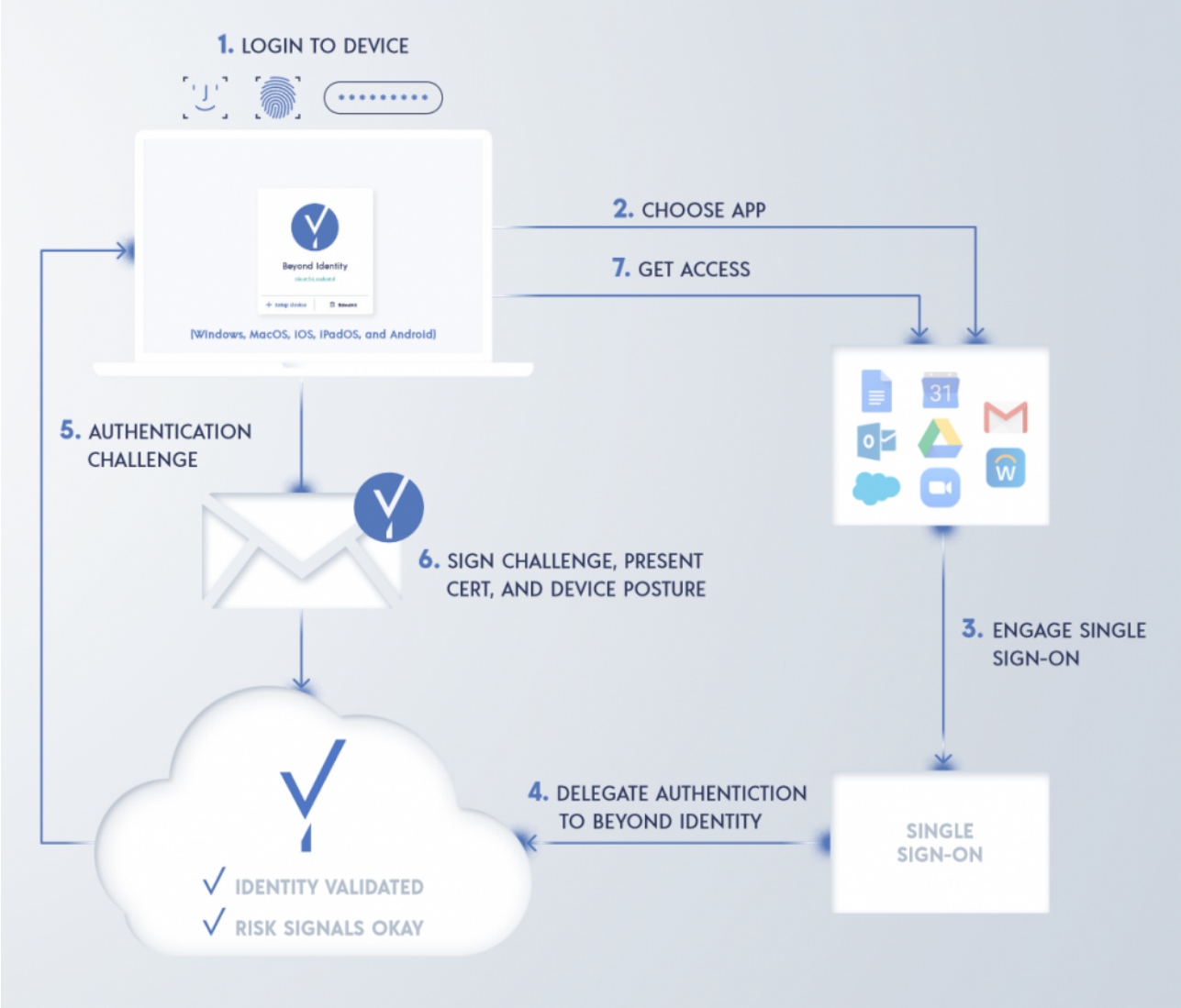

Figure 1: The login flow of Beyond Identity Secure Work [Provided by Beyond Identity]

Beyond Identity uses OAuth and OIDC protocols with downstream support for SAML to integrate with single sign-ons (SSOs) as a delegate identity provider. Going passwordless is not something that can be achieved in a single step, but Beyond Identity provides frictionless MFA and makes it easier for organizations to connect a passwordless solution to a SSO.

The platform integrates easily with a variety of Access Management solutions including Okta, Auth0, Ping Identity, ForgeRock, Microsoft Azure AD, and Microsoft ADFS (for on prem or hybrid deployments).

As cybersecurity threats continue to increase in scope, organizations need to innovate their authentication methods, get rid of passwords, attain an approach that is both secure, convenient, easy to administer and supports modern standards and a wide range of platforms.

3 Strengths and Challenges

Secure Work provides an innovative solution for organizations wishing to eliminate the reliance on passwords and the inconvenience of legacy MFA that just adds another layer of, often easily phished, authentication factors to passwords. The platform aims to enforce device trust and lay the groundwork for the foundation of a zero-trust architecture.

However, the challenge for strong authentication and MFA solutions is to find a win-win solution between security and convenience. Beyond Identity's unique patent-pending solution model that creates self-signed certificates is what sets them apart from most of its competitors. It not only provides a secure authentication method, but it also presents a frictionless and convenient interaction for the user.

To further enforce device trust and security, the solution verifies that the user behind the device (or multiple) is authorized to use the device and detects if the device is secure enough for accessing the application or service being requested. The ability to continuously evaluate the security posture of multiple devices in a seamless manner at the exact time of login reinforces the notion that identity and the endpoint are the main security perimeters. This is another key advantage that Beyond Identity's solution introduces to the market.

However, one of the challenges facing Beyond Identity's Secure Work is the capacity to be able to support legacy systems on premises that continue to rely on passwords. Also, since working from home has become the new norm, it would be advantageous if Beyond Identity offers integration with VPN solutions and Windows Hello for Business in the long run.

Strengths

- Frictionless user experience.
- Control access based on continuously analyzing risk signals.
- Innovative and highly secure approach for binding human and device identities.
- Built to work well for users with multiple devices.
- Utilizes hardware security, i.e., secure elements such as the TPM chip.
- Strong authentication method with public-private key pairs and the use of asymmetric cryptography.
- No need for maintaining an own CA or relying on third-party CAs.
- Broad set of integration to Access Management platforms, based on support for common standards.

Challenges

- Lack of support for legacy systems that continue to rely on passwords.
- Lack of out-of-the-box integration with VPN solutions.
- Lack of out-of-the-box support for integrating with Windows Hello for Business.

4 Related Research

Leadership Brief How to Get Rid of Passwords - Today
Leadership Compass Access Management
Leadership Compass Enterprise Authentication Solutions

Content of Figures

Copyright

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.