kuppingercole ANALYSTS

Beyond Identity Secure DevOps

Paul Fisher, Lead Analyst

EXECUTIVE VIEW

Organizations that fail to secure access to resources are at risk of suffering from cyberattacks, data loss or compliance failure. As the market grows and business demands become more acute, vendors are innovating to provide secure authentication for dynamic access to resources in the cloud and elsewhere. Traditional IAM platforms rely on password technologies for authentication, but these are now challenged by the demands of rapid delivery, high velocity IT environments.

Beyond Identity was founded in 2019 and offers identity and authentication solutions in three critical operational areas: workforce ID management, customer ID management and DevOps ID management. This paper analyzes its software platform for managing identities within DevOps and other rapid coding environments - some of the most exciting yet difficult parts of modern digital organizations to secure.

Content

Introduction

Business management likes DevOps — they get things done. DevOps produce code, applications and cloud-based services in response to demands from other lines of business. While DevOps took its name from the coming together of traditional Developers and Operations team practices to work towards a common goal, these days DevOps has become a catch all term for various team structures that are responsible for the writing, testing and deployment cycle of code within an organization — delivering a continuous internal software supply chain that the organization feeds on.

While the structure and hierarchy of DevOps teams will differ from one organization to another, the common theme of all DevOps teams is speed, automation, and reliance on cloud infrastructure. Increasingly, those writing code are also responsible for code testing and committing code to popular repository tools such as GitHub, GitLab and Bitbucket for other developers or deployment teams to pick up. It's here that some security risks are introduced into the DevOps process.

Such is the demand for rapid delivery that code can be deployed with errors added after the original clean code was committed by the original, authorized developer. Those shipping code to production have no way of knowing if that code is original or has been modified with possible errors or vulnerabilities added by malicious actors. To counter these risks, organizations are looking to add a security layer within DevOps structures that limits access to code repositories and software lifecycles only to authorized and authenticated identities within the organization. In many complex organizations these identities can be machine or human and the number of identities run into the thousands.

This Executive View considers the Beyond Identity Secure DevOps platform which uses unique commit signing keys and APIs to verify the authenticity of all developer identities.

Product Description

Beyond Identity still is a young company (2019) whose founders have a strong background in Secure Sockets Layer (SSL) and Transport Layer Security (TLS) technologies, provided by Certificate Authorities (CA) and used to establish secure connections, mostly across the web.

The founders took the concepts behind SSL/TLS and developed a passwordless authentication stack to create a trusted connection between identities, devices, and resources within IT infrastructures. This is known as the Beyond Identity Authenticator and the company has developed this core technology to underpin three distinctive identity management products for separate applications. The products are Beyond Identity Secure Workforce, Beyond Identity Secure Customers and the focus of this Executive View; Beyond Identity Secure DevOps (SDO).

Beyond Identity Secure Workforce prevents password-based breaches by ensuring continuous user and device trust and eliminating passwords. Instead of relying on passwords and phishable factors, Beyond Identity creates a public-private key pair where the private key is generated, stored, and never leaves the secure enclave of a user's trusted device. Every

authentication request is processed using certificate-based authentication, with no central certificate authority (CA) needed, and fine-grained user and device security signals for risk-based access policy evaluation. For the end-user, there is no password, one-time code, push notifications, or second devices required.

This architecture allows organizations to achieve frictionless zero trust authentication with phishing-resistant MFA, strong assurance of user identity and device security at login and continuously, and dynamic access policy enforcement based on real-time risk.

The private key securely stored in the TPM cannot be viewed or removed by anyone. The process allows logins entirely through an encrypted process with user and device identities stored in hardware and should in theory allow for faster logins as there are no additional default steps such as One Time Password (OTP) or separate texts needed.

Another advantage of this approach is that it is device agnostic, making it suitable for many Work from Home (WFH) and remote working scenarios. The platform can verify the user and device at the same time, so it does not matter if the device is not officially issued as the user is authenticated through their original registration with the Beyond Identity Authenticator, allowing the users to also use and add unmanaged devices. Configurable policies control whether users are allowed to add devices, and if so, which types of devices can be added by users.

Beyond Identity, by default, captures 25+ user and device “risk” signals from any device making a login request, these signals can be used to create security policies for end users and their devices. This allows for flagging risky or misconfigured devices as well as unusual behavior. Escalation requests can be applied, which, for instance, can be a further security step the end user has to take such as biometric identity check from the device. These checks also serve to see if the device is running out of date software or missing patches.

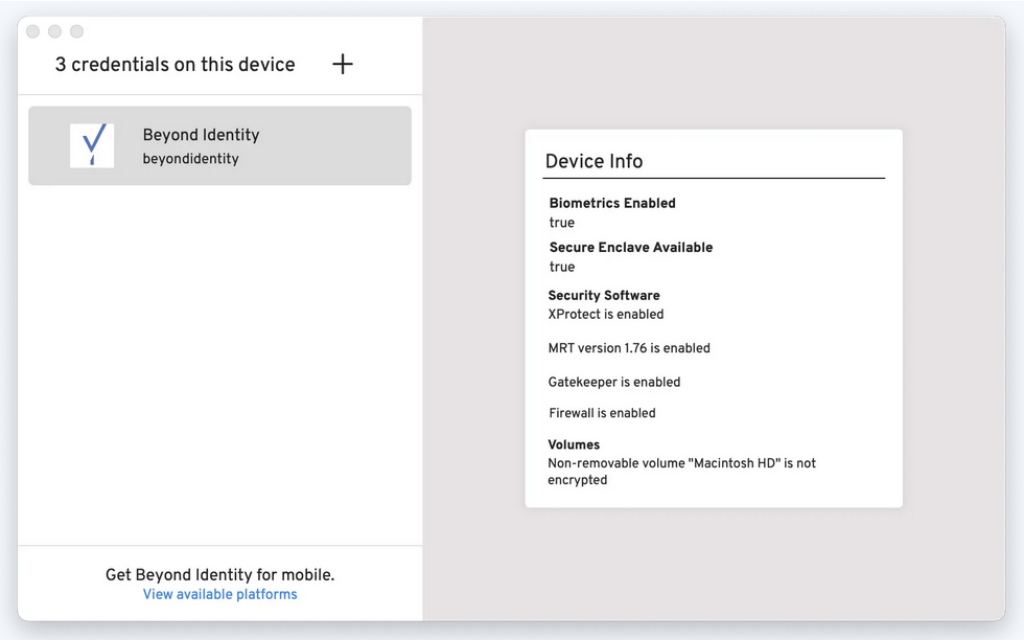

Figure 1 Beyond Identity Authenticator admin console can monitor device state (Beyond Identity).

Engineers can use one or multiple devices, but each user must register each device separately with the Beyond Identity Authenticator to set up unique credentials and each log in then provide admins with a degree of Mobile Device Management (MDM) to assess the security posture of every device and authentication event.

Beyond Identity Secure DevOps

Malicious code or even just buggy code is an increasing risk to enterprise software supply chains as expected code commit and deployment targets have been shortened considerably. Beyond Identity Secure DevOps uses the Beyond Identity Authenticator technology to ensure that only code created by a valid and authorized engineer is pushed into CI/CD pipelines and that signatures are regularly checked for authenticity.

In order to stop malware from getting introduced in the first place, you need a much tighter control on your version control system. The most popular distributed version control system in use today is git, which has its own set of loopholes that hackers actively exploit.

These loopholes are related to git's use of SSH keys to authenticate to the git remote and its use of the gitconfig file to identify the author of code changes. Hackers can potentially steal the private SSH keys to gain command line access to the git remote and use the modified gitconfig file to spoof the identity of the author. Apart from external hackers, malicious insiders can also use this same loophole to pretend to be someone else who is more trusted within their organization and check in malicious code.

Beyond Identity's Secure DevOps Solution takes a Zero Trust approach toward solving this problem and provides integrity, authenticity, and non-repudiation qualities to code. Instead of using an SSH key to access git or a GPG key to sign code, Beyond Identity generates a public/private key pair that binds identity to each device used, providing cryptographic traceability between developers and the code they access and check in to the repository. If you configuration issues or malware in code are found, it can be traced to its origin with certainty.

Beyond Identity further evaluates device security posture to ensure that developer devices comply with the corporate security policies. The policies can include, checking for the presence of antivirus, firewall, hard disk encryption, MDM, etc., and checking for the Crowdstrike Zero Trust assessment score for that device. Beyond Identity also verifies that the code commit was signed by a corporate identity that is still present in the corporate directory and its public key matches to the one stored in the cloud. Administrators can configure their CI/CD pipeline to abort if any of these checks fail.

Strengths and Challenges

Developers do not sit in cubicles or crowded in rows anymore. Modern life and technology allow these important employees to develop from anywhere, and on multiple devices. This is good for them and good for the business, so we like that. Developers also have access to multiple open-source tools used with the blessing of their own management, but all this good stuff can involve risk. Beyond Identity has identified this risk and applied its Authenticator

platform to go some way to plugging the security gaps in modern, distributed DevOps and CI/CD environments.

The simplicity of Beyond Identity Authenticator makes it perfectly suited to the speed and pressure of coding environments. A one-time install and registration process is all that is needed for developers to authenticate their code on any device they are using. The organization can control, via policy, which devices they allow engineers to register and use to submit code. This could be a work-issued and managed device, or a BYOD or contractor owned device. This is enhanced by a similarly simple process when the code is sent to GitHub or similar coding repository. The process removes the risk of bogus or bad code being entered into the software supply chain by an unauthorized user and ensures that potentially malicious, or more likely error prone code is cryptographically bound to the user who committed - thus reducing the likelihood of an insider threat.

The solution provides strong control about the code in Git repositories and thus helps in securing the CI/CD pipeline. It delivers the link between code, device, and identities, allowing to track who has altered which piece of code, by binding GPG keys to identities. Based on their policies, customers can limit or open up the environment according to their needs. Further capabilities for additional DevOps support such as support for private Git repositories are on the roadmap.

Strengths

- Wide support for Git repositories including GitHub, GitLab and BitBucket, Azure DevOps, AWS Code Commit and Jenkins
- Full support for policy-controlled GPG generation and secure storage in TPM (secure enclave)
- During CI/CD pipeline run, code commit signatures are verified by the Git by making API calls to the BeyondIdentity cloud
- Simple to install, use and manage from an admin dashboard
- Goes some way to balancing the Convenience Security Authentication (CSA) parameters for DevOps environments
- Device agnostic application ensures good fit for today's WFH and remote working trends
- Keys are managed and generated by the app running on the individual device

Challenges

- Does not yet support access to private Git servers, which often depend on SSH tools for access and authentication
- Administration tools are relatively basic at present, but improving
- Allowing multiple credentials on a single device could be a potential vulnerability

Related Research

Leadership Compass: Privileged Access Management for DevOps
Advisory Note: Integrating Security Into an Agile DevOps Paradigm
Leadership Compass: CIEM & DREAM Platforms
Leadership Compass: Access Management
Leadership Compass: Container Security

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, 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.