Beyond Identity Secure Work

The Strongest Authentication On The Planet

BEYOND IDENTITY

Trusted By Customers Like:

snowflake taulia VERTEX KYMERA LAMAR CLOUDplus

Eliminate Passwords To Protect Access To Critical SaaS Resources

Modern workforces are demanding access to critical resources from anywhere in the world, at any time, and across platforms. They're working beyond the confines of the traditional network perimeter. Security vulnerabilities like insecure passwords and weak authentication can no longer be tolerated.

Beyond Identity eliminates passwords and their vulnerabilities. We ensure organizations can verify the identity of every user and device using strong cryptography; force adherence to your organization's device security policies so all devices, including unmanaged devices, meet your security posture; and evaluate fresh contextual data to evaluate trustworthiness and reduce risk at every login attempt.

Beyond Identity is the only way to completely eliminate passwords and cryptographically bind identity and device.

Key Benefits:

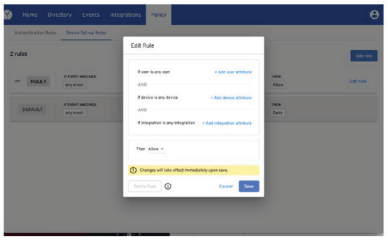
✓ No More Password Liabilities

Replace passwords with the same proven and scalable cryptography that you trust to protect online transactions every day and remove the most significant threat to digital security, obviating password use across your organization.

✓ MFA Users Love

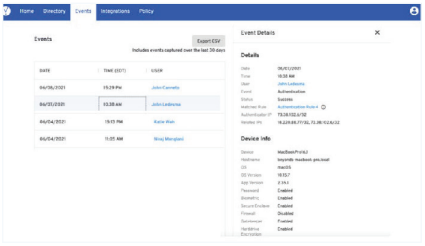
Implement the strongest MFA and a streamlined authentication experience that does not require users to pick up a second device or type in a one-time code at each authentication event.

Cryptographically Bind Identity And Device To Securely Authenticate Users:



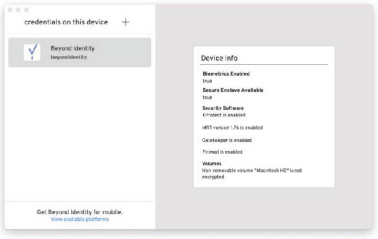
Risk-Based Access Controls

Restrict access to organizationally owned cloud resources in real-time, with customizable policies within the Beyond Identity cloud and risk-based access powered by constant contextual analysis.



Ensure Compliance

Enforce and prove compliance to regulations by capturing immutable records of device security metadata at the exact time of authentication for every user and every device requesting access to your resources.



Trust Your Endpoints

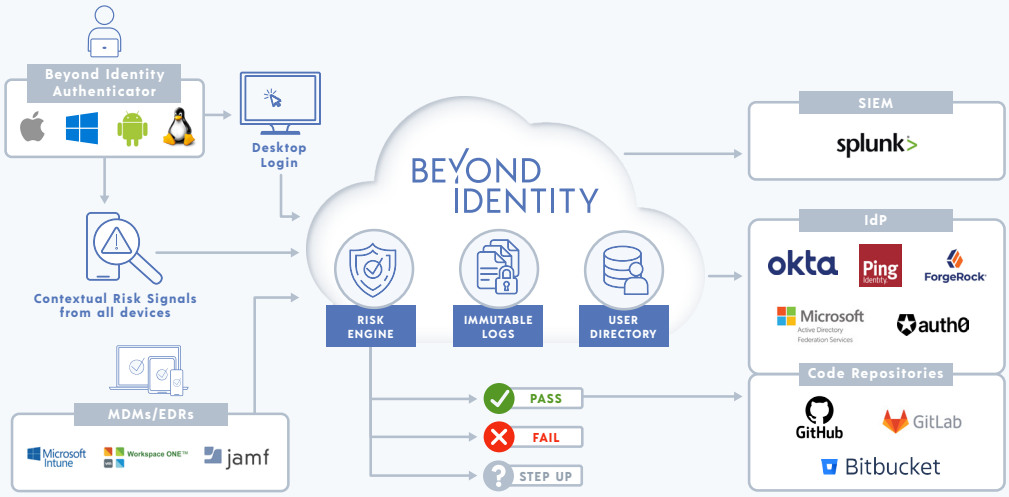
Verify device trustworthiness of managed and unmanaged devices across operating platforms and inform granular level policies that protect your resources from unauthorized access by unsecured devices.

How It Works

Beyond Identity uses the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily.

Beyond Identity eliminates passwords and replaces them with private keys stored on the TPM, binding identity to your users' primary devices, enforcing device security policy at every access attempt, replacing passwords with cryptographic proof of identity, contextual analysis, and rule-based access management. For the user, that all takes place within seconds; after one click on their primary device, they are seamlessly and securely granted access.

Beyond Identity collects and analyzes dozens of user and device risk signals at the exact time of login - enabling customers to enforce continuous, risk-based access control.



Unique Benefits:

Leverage Primary Devices

Turn primary devices into multi-factor cryptographic software and device authenticators. End the need for second devices, one-time passwords, 2-step processes for authentication, and the friction and vulnerabilities that go with them.

Force Policy Adherence

End unauthorized device access to SaaS resources - force adherence to device security policies via contextual analysis of the device and its security state at the exact time of each access request. Devices that are unidentified or unsecured have no avenue for access.

Continuously Analyze Risk

Employ rule-based access via customizable policies and constantly evaluate the risk and trustworthiness of each user and the device requesting access to your SaaS resources.

Create Immovable Identities

Ensure the strong authentication of users with immovable, inimitable, cryptographically proven device-bound identities mounted to the TPM. There are no credentials to steal, effectively securing SaaS resources against all unauthorized users and credential-based intrusions.

okta Ping Identity ForgeRock Microsoft Active Directory Federation Services auth0 jamf Workspace ONE™ Microsoft Intune

Beyond Identity Secure Customers

BEYOND IDENTITY

Convert and secure customers with cross-platform, zero-friction passwordless authentication.

Eliminate authentication friction and build trusted customer relationships

Customers have rising demands for frictionless experiences while attackers are exploiting the move to digital with increasingly frequent phishing, credential stuffing, and brute force attacks.

The problem is, existing methods of customer authentication don't eliminate the root cause of friction and security issues -- the password.

Beyond Identity Secure Customers delivers the fastest authentication across all your applications with no second devices required and eliminates the password for customers and from your database. 1

Streamline registration, login, and recovery to drive conversions. Secure customers against account takeover fraud by deprecating passwords completely. Precisely control access with adaptive risk-based policies based on granular user and device risk signals captured in real time.

Key Benefits:

- ✓ Completely eliminate account takeover fraud
- ✓ Passwordless MFA with two strong factors in one transaction
- ✓ Privacy-preserving credentials customers own and control
- ✓ Zero-friction with no second devices, OTP, or push notifications

Use Cases

Accelerate customer conversions

Prevent drop-offs by eliminating passwords, one-time codes, push notifications, and second devices on native and web applications.

Eliminate account takeover fraud

Make account takeover impossible by removing passwords from the customer experience and database. Instead, secure accounts with passwordless MFA that validates two strong factors in one transaction.

Modernize your application

Simplify your application stack with a cross-platform authentication product built on proven open standards for extensibility, scalability, and reliability.

Implement adaptive access control

Evaluate user and device risk prior to login and implement dynamic step-up authentication for higher risk behaviors according to your security policies.

How It Works

Beyond Identity leverages an innovative implementation of asymmetric cryptography that underpins TLS to completely eliminate passwords from the customer experience and your database.

Instead of passwords, Beyond Identity authenticates customers with two strong factors -- something you are from the device biometric and something you own from the private key -- without requiring a second device.

During authentication, Beyond Identity issues a challenge signed by the private keys in the device's secure hardware (TPM), evaluates user and device security risk in real-time, and makes a risk-based authentication decision based on your security requirements.

Unique Benefits:

Zero-friction authentication

Drive faster conversions by removing passwords and the need for second devices across native and web apps.

Privacy-preserving credentials

Preserve privacy with tamper-resistant credentials backed by private keys that are only owned by the customer and can't ever leave hardware TPMs.

Cryptographic identity verification

Only allow the right customers to access the right account with immutable, device-bound identity attestation for each access request.

Adaptive access controls

Configure dynamic access policies and step-up authentication using granular user and device risk signals captured in real time.

auth0 KEYCLOAK ForgeRock

Secure DevOps

BEYOND IDENTITY

Verify every piece of source code was committed from a corporate identity and authorized device to stop software supply chain attacks before they start.

Protect source code from malicious attacks and deter insider threats

Attackers continue to exploit vulnerabilities in modern DevOps environments. Recent attacks ranging from Solarwinds and Kaseya to one of the most expensive in history - NotPetya - have shown the real exposure and massive cost of these attacks.

Companies have moved their agile software development life cycle (SDLC) to the cloud. Today, source code is one of a company's most valuable assets. In distributed cloud-based development environments, engineers can access and update source code anywhere from any device.

The only way to know your source code has not been compromised is to track every source code commit. Who made what changes from what device?

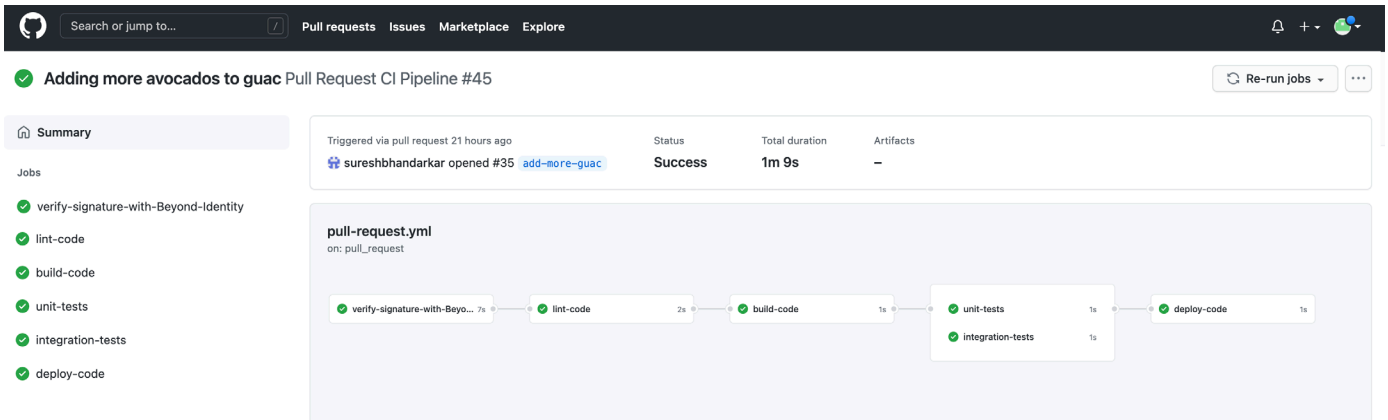
Beyond Identity Secure DevOps is the only product that secures the software supply chain at the developer level. Prevent malicious source code commits by cryptographically binding access and signing keys to a corporate identity and authorized device. Systematically inspect every commit so only source code that is signed by a valid corporate identity is built into the product.

Key Benefits:

- ✓ Eliminate key sprawl and stolen credentials
- ✓ Stop code injection at repo from non-authorized users
- ✓ Protect access to build enviornments, infrastructure, and 3rd party tooling
- ✓ Verifiable source code provenance for auditing and forensics

Verify source code is signed by a valid corporate identity

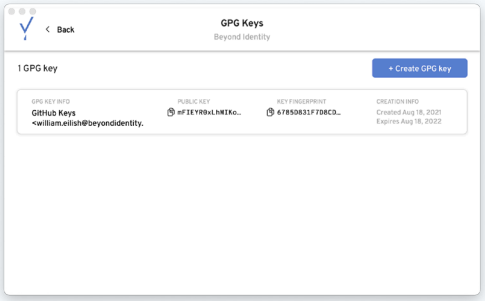
Secure your CI/CD pipeline. Place the Beyond Identity source code provenance check - a Git action or simple API call - at the beginning of your CI/CD pipeline to ensure that only source code that is cryptographically tied to a valid corporate identity makes it into your build.



How It Works

Beyond Identity is the only way to secure the software supply chain at the developer level.

Beyond Identity validates that every Git commit is signed by a verified corporate identity and trusted device. This is done by cryptographically binding a valid corporate identity to the device by minting GPG keys and storing the private keys in the TPM hardware on the developer's authorized device. The private key cannot be moved, and therefore can be trusted. Beyond Identity ensures compliance for all developers. It's an easy one time set up for developers, then Beyond Identity signs all Git Commits in the background without any ceremony to access the private key. Beyond Identity is the only source code signing product thats stops Git Commits from non-authorized devices.

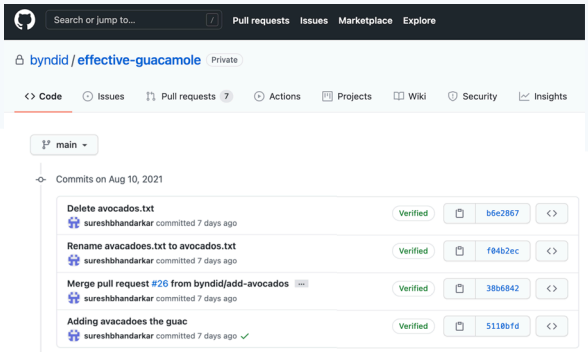


Signing keys are trustworthy

Developers mint their GPG keys using the Beyond Identity Authenticator, private keys are stored in the secure hardware and cannot leave the device. Key revocation is centralized and easy to manage. Beyond Identity's policies control which devices are authorized to create keys.

Restrict source code commit to corporate identites and devices

Only source code that is signed by a corporate identity using Beyond Identity is allowed in the build. There's a 1x set up for developers, then Beyond Identity signs source code behind the scenes for them without the need for a complex signing ceremony which ensures compliance.



GitHub GitLab Bitbucket

Integrates with leading code repositories and CI / CD tools

By integrating your CI automation tool (eg, Jenkins, Bamboo, Circle CI) with Beyond Identity's Identity Verification API, you can show alerts with the CI tool, flag a build or fail a build if there are code commits are not properly signed by a valid corporate identity.