Privacy-First Security: Prioritizing Device Security While Respecting User Privacy

At Beyond Identity, we understand the importance of balancing device security with user privacy. Our passwordless authentication solution is designed to ensure the highest level of security for your organization without compromising the privacy of your employees. Here's how we achieve this:

No Administrative Privileges Required: Beyond Identity does not require administrative privileges to operate on user devices. This means that we cannot and do not change the state of your device, ensuring that your employees maintain full control over their devices.

Collecting Only Essential Security Context: We only collect the device security context needed to support your organization's administrative policy configuration. This information is directly related to ensuring device security and proper possession. We do not collect any unnecessary data that could infringe on user privacy.

Our Guiding Principles:

Alignment with Organizational Values: We believe your organization's values should be well-represented in your security program. Our solution is designed to support your values and foster a positive working relationship between the end-user and the security team.

Informed Consent and Transparency: Trust is the foundation of our relationship with your organization and your employees. We prioritize informed consent and transparency in all our data collection practices, ensuring that your employees understand what data is being collected and why.

Respect for Personal Use: We understand that employees often use their company-owned devices for personal activities. Our detection capabilities are designed with this in mind, focusing on device security rather than invasive monitoring of personal activities.

Empowering Informed Decisions: We believe that end-users are capable of making rational and informed decisions about security risks when educated and honestly motivated. Our solution provides the necessary information and tools to empower your employees to make informed decisions about device security.

No Invasive Oversight: Beyond Identity will never be used for onerous levels of oversight, such as screen tracking, keyboard usage monitoring, or camera roll access. We respect the privacy of your employees and focus solely on device security.

The attributes we collect are focused on ensuring device security and are not privacy concerns. Additionally, as the administrator, you can choose what attributes you'd like to collect based on your own guidelines. These attributes include:

Attribute	Reason for Attribute	Privacy Sensitivity
Device platform	Ensures compatibility and supports platform-specific security policies	Low
Device security status	Detects rooted/jailbroken devices and enforces security policies	Low
Installed security software	Verifies the presence of required security software (e.g., antivirus, firewall)	Low
Operating system version	Ensures devices are running up-to-date and secure OS versions	Low
Presence of secure hardware	Verifies the availability of secure hardware (e.g., TPM, Secure Enclave) for enhanced security	Low
Disk encryption status	Ensures sensitive data is protected at rest through disk encryption	Low
Authenticator version	Ensures the Beyond Identity Authenticator is up-to-date and secure	Low
User group	Supports group-based access policies and permissions	Low
Has registered device(s)	Verifies that the user has registered devices associated with their account	Low
Authentication method enabled	Ensures appropriate authentication methods are enabled (e.g., biometric, PIN)	Low
Specific files, processes, or registry keys	Verifies the presence or absence of specific files, processes, or registry keys related to security	Low
Integrations (e.g., CrowdStrike, Intune)	Collects relevant security data from integrated third-party solutions to enforce comprehensive security policies	Low to Medium
Location (based on IP address)	Supports location-based access policies and detects unusual authentication patterns (e.g., impossible travel)	Medium
Authentication behavior	Detects and prevents suspicious authentication patterns (e.g., high frequency, impossible travel)	Medium

By collecting this essential security context, we can support your organization's security policies without compromising user privacy. Our solution enables you to strike the right balance between security and privacy, fostering a positive relationship between your security team and end-users.

Appendix - Detailed Policy Attributes from Q1 2024

Type	Platform	Name	Reason for Collection	Privacy Sensitivity
User	--	User Group	Supports group-based access policies and permissions	Low
User	--	Has Registered Device(s)	Verifies that the user has registered devices associated with their account	Low
Device	--	Platform	Ensures compatibility and supports platform-specific security policies	Low
Device	Android	Device Root Is	Detects rooted devices and enforces security policies	Low
Device	Android	Device Has Authentication	Ensures devices have authentication enabled for security	Low
Device	Android	Authentication Method Enabled	Ensures appropriate authentication methods are enabled (e.g., biometric, PIN)	Low
Device	Android	API Level	Ensures devices are running up-to-date and secure Android versions	Low
Device	iOS	Device Jailbreak Is	Detects jailbroken devices and enforces security policies	Low
Device	iOS	Device Has Authentication	Ensures devices have authentication enabled for security	Low
Device	iOS	Authentication Method Enabled	Ensures appropriate authentication methods are enabled (e.g., biometric, PIN)	Low
Device	iOS	Version	Ensures devices are running up-to-date and secure iOS versions	Low
Device	macOS	Antivirus Is	Verifies the presence of antivirus software for enhanced security	Low
Device	macOS	Firewall Is	Verifies the presence of firewall for network security	Low

Type	Platform	Name	Reason for Collection	Privacy Sensitivity
Device	macOS	Installed Security Software Contains	Verifies the presence of required security software for comprehensive protection	Low
Device	macOS	Apps Installed Contains/Does Not Contain And App Version	Ensures the presence or absence of specific apps and their versions for security and compatibility	Low
Device	macOS	File Exists	Verifies the presence or absence of specific files related to security	Low
Device	macOS	Plist Key Value Contains	Checks configuration settings in plist files for security-related preferences	Low
Device	macOS	Process Running Contains	Verifies the presence or absence of specific processes related to security	Low
Device	macOS	User FileVault Is	Ensures sensitive data is protected at rest through disk encryption	Low
Device	macOS	OS Version: Build Is Within Last	Ensures devices are running up-to-date and secure macOS build versions	Low
Device	macOS	OS Version: Build Release Date Is Within Last	Ensures devices are running macOS builds released within a specific timeframe for security	Low
Device	macOS	OS Version	Ensures devices are running up-to-date and secure macOS versions	Low
Device	macOS	Secure Enclave Is	Verifies the availability of Secure Enclave for enhanced hardware security	Low
Device	Windows	Antivirus Is	Verifies the presence of antivirus software for enhanced security	Low
Device	Windows	Firewall Is	Verifies the presence of firewall for network security	Low
Device	Windows	Installed Security Software Contains	Verifies the presence of required security software for comprehensive protection	Low
Device	Windows	Domain Name Contains	Ensures devices are connected to the organization’s domain for centralized management and security	Low
Device	Windows	File Exists	Verifies the presence or absence of specific files related to security	Low
Device	Windows	Application Installed Contains And Application Version	Ensures the presence or absence of specific applications and their versions for security and compatibility	Low

Type	Platform	Name	Reason for Collection	Privacy Sensitivity
Device	Windows	Process Running Contains /	Verifies the presence of specific processes related to security	Low
Device	Windows	Process Running Does Not Contain	Verifies the absence of specific processes that may pose security risks	Low
Device	Windows	Registry Key	Checks the existence or absence of specific registry keys related to security settings	Low
Device	Windows	Registry Key Value	Verifies the values of specific registry keys to ensure secure configuration	Low
Device	Windows	Service Installed Contains	Verifies the presence of specific security-related services	Low
Device	Windows	Service Running Contains	Ensures required security services are running on the device	Low
Device	Windows	System Disks BitLocker Is	Ensures sensitive data is protected at rest through disk encryption	Low
Device	Windows	OS Version	Ensures devices are running up-to-date and secure Windows versions	Low
Device	Windows	OS Version: Revision Is Within Last	Ensures devices are running Windows versions released within a specific timeframe for security	Low
Device	Windows	OS Version: Revision Release Date Is in the Last	Ensures devices are running Windows versions released within a specific timeframe for security	Low
Device	Windows	TPM Is	Verifies the presence of TPM (Trusted Platform Module) for enhanced hardware security	Low
Device	Windows	TPM Version	Ensures the device has a compatible and secure version of TPM	Low
Device	Linux	Installed Security Software Contains	Verifies the presence of required security software for comprehensive protection	Low
Device	Linux	Process Running Contains	Verifies the presence of specific processes related to security	Low
Device	Linux	Process Running Does Not Contain	Verifies the absence of specific processes that may pose security risks	Low
Device	Linux	System Disks Encrypted Is	Ensures sensitive data is protected at rest through disk encryption	Low

Type	Platform	Name	Reason for Collection	Privacy Sensitivity
Device	Linux	File Exists	Verifies the presence or absence of specific files related to security	Low
Device	Linux	OS Version	Ensures devices are running up-to-date and secure Linux distributions	Low
Passkey	--	Passkey Tag Is	Allows for grouping and managing passkeys based on user-defined tags	Low
Integration	CrowdStrike Falcon	ZTA Score	Incorporates device security posture from CrowdStrike Falcon into access policies	Low
Integration	CrowdStrike Falcon	Device Found	Verifies the device is managed by CrowdStrike Falcon for comprehensive security	Low
Integration	CrowdStrike Falcon	Connection Is	Ensures the integration with CrowdStrike Falcon is functioning properly for continuous security monitoring	Low
Integration	Cybereason	Sensor Found	Verifies the device is managed by Cybereason for comprehensive security	Low
Integration	Cybereason	Prevention Status	Ensures the Cybereason prevention features are active on the device	Low
Integration	Google Workspace	Mobile Android Managed State is	Verifies the management status of Android devices in Google Workspace for consistent security policies	Low
Integration	Intune	Connection Is	Ensures the integration with Microsoft Intune is functioning properly for continuous device management	Low
Integration	Intune	Registration Is / Is Not	Verifies the registration status of devices in Microsoft Intune for comprehensive management	Low
Integration	JAMF	Connection Is	Ensures the integration with JAMF is functioning properly for continuous device management	Low
Integration	JAMF	Computer Managed State Is	Verifies the management status of macOS devices in JAMF for consistent security policies	Low
Integration	JAMF	Mobile Device Managed State Is	Verifies the management status of iOS devices in JAMF for consistent security policies	Low
Integration	Kandji	API Is	Ensures the integration with Kandji is functioning properly for continuous device management	Low

Type	Platform	Name	Reason for Collection	Privacy Sensitivity
Integration	Kandji	Device Is Managed Is / Is Not	Verifies the management status of devices in Kandji for comprehensive security	Low
Integration	SentinelOne	Agent Is Active	Ensures the SentinelOne agent is active on the device for continuous monitoring and protection	Low
Integration	SentinelOne	Agent Is Decomissioned	Verifies if the SentinelOne agent has been decommissioned on the device	Low
Integration	SentinelOne	Agent Operational State Is / Is Not	Ensures the SentinelOne agent is operating in a healthy state on the device	Low
Integration	SentinelOne	Connection Is	Ensures the integration with SentinelOne is functioning properly for continuous security monitoring	Low
Integration	SentinelOne	Device Found	Verifies the device is managed by SentinelOne for comprehensive security	Low
Integration	Workspace ONE	Connection Is	Ensures the integration with Workspace ONE is functioning properly for continuous device management	Low
Integration	Workspace ONE	UEM Is / Is Not	Verifies the enrollment status of devices in Workspace ONE UEM for comprehensive management	Low
Authenticator Version	--	If Authenticator Version Is	Ensures the Beyond Identity Authenticator is up-to-date and secure	Low
Location	--	If Location Is In / Not In	Supports location-based access policies and detects unusual authentication patterns (e.g., impossible travel)	Medium
Behavior	--	Impossible travel detected	Detects and prevents suspicious authentication patterns that may indicate compromised credentials or unauthorized access	Medium
Behavior	--	Number of user authentications in last minute	Detects and prevents suspicious authentication patterns that may indicate automated attacks or unauthorized access	Medium
Behavior	--	Days since last user authentication	Identifies dormant or inactive user accounts that may pose security risks	Medium