What to Do About Unknown Devices Attempting to Access Accounts

BEYOND IDENTITY

Are unknown devices a risk to your applications? Short answer, yes. Allowing unverified devices to access your applications increases your risk for attacks. You need to mitigate that risk, but you also need your customers and users to be able to frictionlessly access your product and services, with the understanding they may not always use the same device.

Assessing risk is the first step in protecting your applications. You don't want to set off alarms for every unknown device attempting to access your application. But you don't want to let your guard down either. Your risk assessment policies must be able to discern levels of risk and step up defenses as needed.

How to assess risk

Your organization needs a way to judge appropriate security responses for unknown devices that try to access your applications. This process is known as risk-based authentication.

You can assess risk signals during authentication (such as location, time of day, or lack of security updates) and determine what is an acceptable level of risk via access policies. Access is granted, denied, or prompted for additional verification based on the risk signals. You determine what risk you're willing to accept. For instance, financial institutions may deny access to a jailbroken or rooted device seeking access. It may also call for step-up authentication if that is deemed necessary.

In addition to determining your risk signals, assessment of those signals must happen continuously. Users can reconfigure security settings, disable endpoint management software, or (God forbid) download malware. If they are compromised after they are authenticated, the attacker can use that connection to access your network. By continuously monitoring security posture, you are able to respond to new risk signals and deny access.

How to authenticate unknown devices the right way

Many companies try to remember "trusted devices" via session cookies but this is neither secure nor reliable. Users can bypass cookies with blockers and VPNs while attackers can intercept. The more secure solution is establishing identity by utilizing cryptographic credentials tied to both the user and their device.

Cryptographic credentials:

- Are immutable and cannot be removed or used on another device, so you can be certain the user is who they say they are.
- Accelerate onboarding and logins by eliminating knowledge factors. This means no more passwords!
- Allows you to perform a device posture check to ensure the authenticating device meets policy requirements before allowing access.
- Make it possible for you to customize authentication policies with unlimited, granular security attributes.

With cryptographic credentials, it lets you allow any device to access an account while keeping things secure, which is a great experience for your users and stops bad actors.

Better security doesn't need to be disruptive

Cybersecurity is important to you. Ease of access is important to your users. The authentication process is often difficult or disruptive and any friction in the login or purchasing process leads to lost sales or lost productivity. For example, a quarter of eCommerce shoppers will abandon a high-value cart ($100+) if a password reset is necessary.

So how do you deny access to bad actors and prevent account takeover without making your customers jump through hoops? Beyond Identity's Secure Customers and Secure Workforce makes the login process frictionless while allowing you to implement risk-based access policies that protect your business. Every authentication leverages unphishable factors by default without requiring the user to pick up a second device, check for codes, or click push notifications.

See Beyond Identity risk-based authentication in action. Ask for a demo today.