Closing the Gap: The Future of Access Management

A future-looking access management solution should extend the strengths of identity access management (IAM) and mobile device management (MDM) to unmanaged apps and devices, ensuring all access attempts are trusted and secure.

6 Critical Capabilities of a Future-Focused Solution

IDENTITY AUTHENTICATION

Validate the identities and permissions of the entire workforce and manage the full user life cycle from end to end.

SECURE SIGN-IN

Enable secure sign-in from any location on any device regardless of whether it involves single sign-on (SSO), passwords, multi-factor authentication, or passwordless/passkeys.

DEVICE HEALTH

Block access to corporate resources from unhealthy devices — including personal devices — to simplify and expand compliance.

EXTENDED ACCESS POLICIES

Apply to every device, granting or denying access to apps based on dozens of contextual signals, including the state of the device being used and credential strength.

EVERY APPLICATION SECURED

Provide secure access to every application, whether through SSO or managed by IT, as well as secure unmanaged apps, known as shadow IT.

EVERY CREDENTIAL SECURED

Provide security across managed and unmanaged apps and websites.