Chrome Enterprise Recommended

okta

Chrome Enterprise Recommended Solution Overview with **Okta**

Establish security requirements to gate access to protected resources with Okta's Device Assurance

The hybrid work model and remote work are here to stay. As a result, endpoints such as laptops, phones, and other devices, can be located from anywhere in the world as potential points of enterprise vulnerability. In today's digital world, it's critical that organizations have a strong security posture and an agile workforce that can easily and securely access their resources.

Okta's **Device Assurance** allows admins to check sets of security-related device attributes as part of authentication policies before that device can be used to access Okta-protected resources. This includes support for signals from managed Chrome browsers and managed ChromeOS devices, to inform policies and gate access to protected applications.

Discover the benefits

Identity-driven approach to Zero Trust for robust defense in depth

Strengthen your posture with contextual access

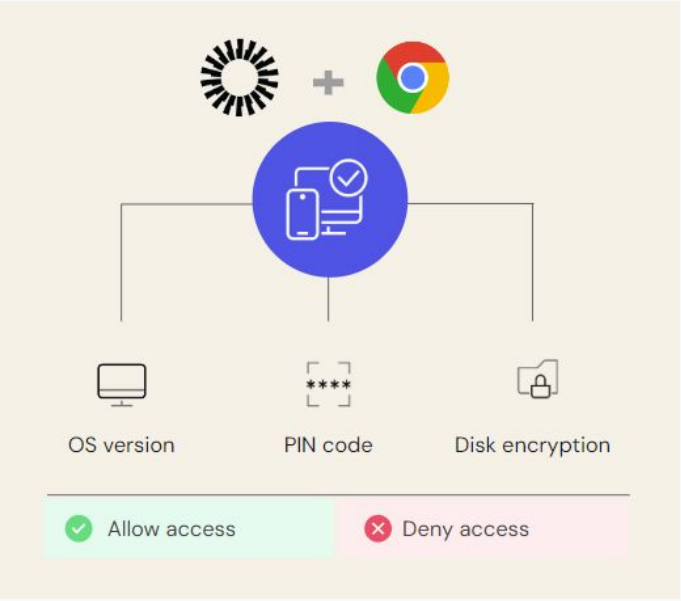
Enhance your security policies with a wide range of device signals that block or deny access to applications and resources.

Balance security and user experience

Provide your workforce with the tools they need to remain productive without sacrificing security.

Maintain security compliance standards

Meet internal device standards and other security requirements through policies with minimal setup.



Learn more