okta

Okta Devices

Okta embedded on every device to offer secure, device-based contextual access experiences.

Okta Devices is a platform service of the Okta Identity Cloud that embeds Okta on every device to collect and evaluate device identity and endpoint security posture signals. Using Okta Devices, organizations enable secure, device-based contextual access experiences.

How does Okta Devices help my organization?

Okta Devices addresses pain points organizations face with enabling device visibility, enforcing device-based access controls and device-based passwordless experiences, and enabling in-app access controls. Here's how Okta Devices can help:

Reduce data breaches as a result of weak passwords

Compromised credentials due to use of weak passwords continue to be a pain point in securing access to corporate apps and consumer-facing apps. Removing the requirement to enter passwords is a critical step in reducing data breaches.

Enable a consistent approach to passwordless auth

Each operating system (Windows, MacOS, iOS, Android) has its own nuances in how policies can be enforced on a device, which in turn affects the ability to deliver a "one fits all" solution to deliver passwordless auth. Okta Devices delivers a consistent passwordless auth experience on all major platforms.

Integrate identity with endpoint security tools to enforce access decisions

Many organizations use endpoint management/endpoint detection and response tools to enforce device security, but these tools do not directly tie into an identity service. This causes organizations to have to create separate policies for user-based risk and device-based risk. Use Okta Devices to integrate identity with endpoint management and detection.

Visibility into managed *and* unmanaged devices

As an influx of new devices enter the workforce, organizations require visibility into devices managed by an enterprise mobility management tool, as well as devices accessing corporate resources in Bring-Your-Own Device (BYOD) scenarios. Okta Devices enables visibility to any device registered with Okta.

Key Features

Okta FastPass

Users on devices that have been registered to Okta Universal Directory get a passwordless experience into any Okta-managed app (browser, native mobile app, desktop apps), from any location. Supported on Windows, MacOS, Android and iOS.

Remote Sign-out

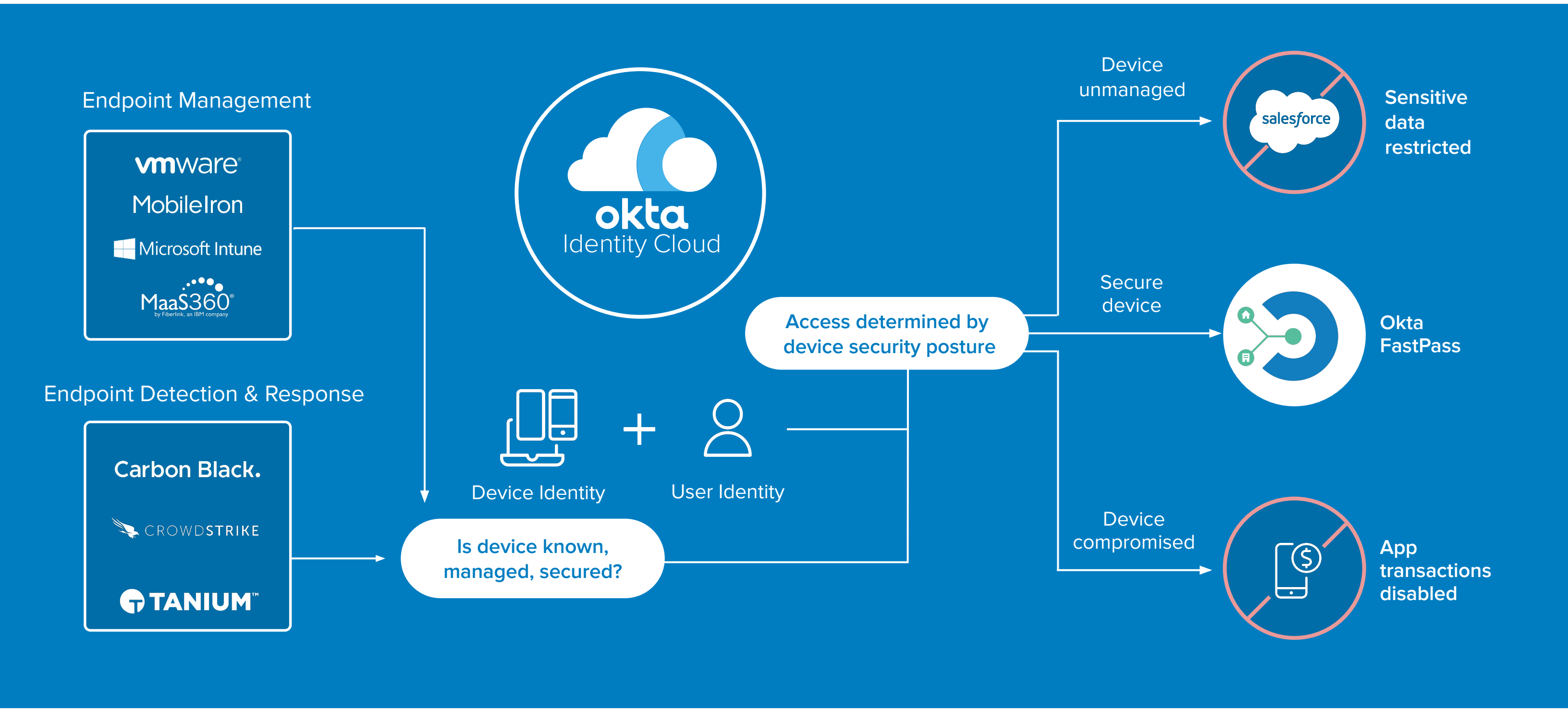
Admins can suspend access from individual devices or delete individual devices from Okta Universal Directory. This ensures that users are not logged out of Okta sessions across all their devices.

Device Visibility

View devices in Okta Universal Directory. Admins will be able to view user + device bindings, device attributes (serial number, OS version etc), and if a device is managed by an Enterprise Mobility Management (EMM) solution or just registered to Universal Directory.

Device context

Combine Okta FastPass with device context to enforce secure, device-based access decisions. For example, only enable Okta FastPass on managed devices, or integrate with endpoint detection and response (EDR) vendors to deny access to Okta when a device has malware, the firewall has been disabled, the disk is not encrypted etc.



How do I learn more?

Interested in understanding how you can use Okta Devices in your organization? Learn more at www.okta.com/platform/devices.