

CrowdStrike and Okta

Combine best-in-class solutions for identity management and endpoint security

Challenges

Businesses today face a multifaceted challenge in safeguarding operations. With the evolving threat landscape, enterprise teams must ensure the security of web, cloud and on-premises access and activities. The proliferation of remote and hybrid workforces adds complexity, demanding secure access from both managed and unmanaged devices. To navigate these challenges, companies require proactive solutions that provide real-time threat assessment and fine-grained access management.

A wide variety of solutions have sprung up to help enterprise teams secure pieces of their enterprise. But different teams managing different solutions can lead to a lot of manual work, friction and — when data and intelligence are not shared across solutions — blind spots in your security.

Solution

Okta and CrowdStrike have deeply integrated joint solutions that centralize visibility, supply critical user and device context to access requests, and monitor and mitigate cybersecurity threats. You get the data-driven insights you need to support reliable, automated access decisions so your teams can support hybrid work productivity while keeping the enterprise safe.

Organizations need to provide safe access to their applications and data, whether stored in the cloud or on-premises. Remote work has made this significantly more challenging by expanding the attack surface. Adding user login context (delivered by Okta) and device security posture (delivered by CrowdStrike) can give enterprises a more holistic look at access activity and provide contextual insights that enable a true Zero Trust security posture. Your enterprise can safely protect remote and on-premises work through seamless, intuitive authentication into network resources from any device — including passwordless authentication — while maintaining security and supporting compliance requirements.

Key benefits

- Provide your workforce with simple, seamless access into any enterprise resource, hosted on-premises or in the cloud
- Give your IT and security teams a consolidated view into enterprise activity to help them maintain security and support compliance
- Use insights from user identities and host security posture to add context to access requests and intelligently evaluate login risk
- Deliver automated access decisions — allow/deny, prompt for multifactor authentication, permit passwordless — that keep enterprise resources safe

Business value

Use Case/Challenge	Solution	Benefits
Keeping up with the ever-evolving threat landscape	Deliver a great end-user experience by authorizing fast, context-aware, risk-based access to enterprise resources without compromising on security	Authorize fast, context-aware access
Expansion of remote and hybrid workforce	Get a holistic understanding of the security gaps in authentication policies, user roles, access privileges, and human and service accounts across on-premises and cloud environments	Provide safe access for your workforce
New tools are needed for real-time threat assessment	Leverage powerful insights into identities, user behavior, risks and device context that feed into a unified dashboard, eliminating security blind spots	Evaluate device data in real time

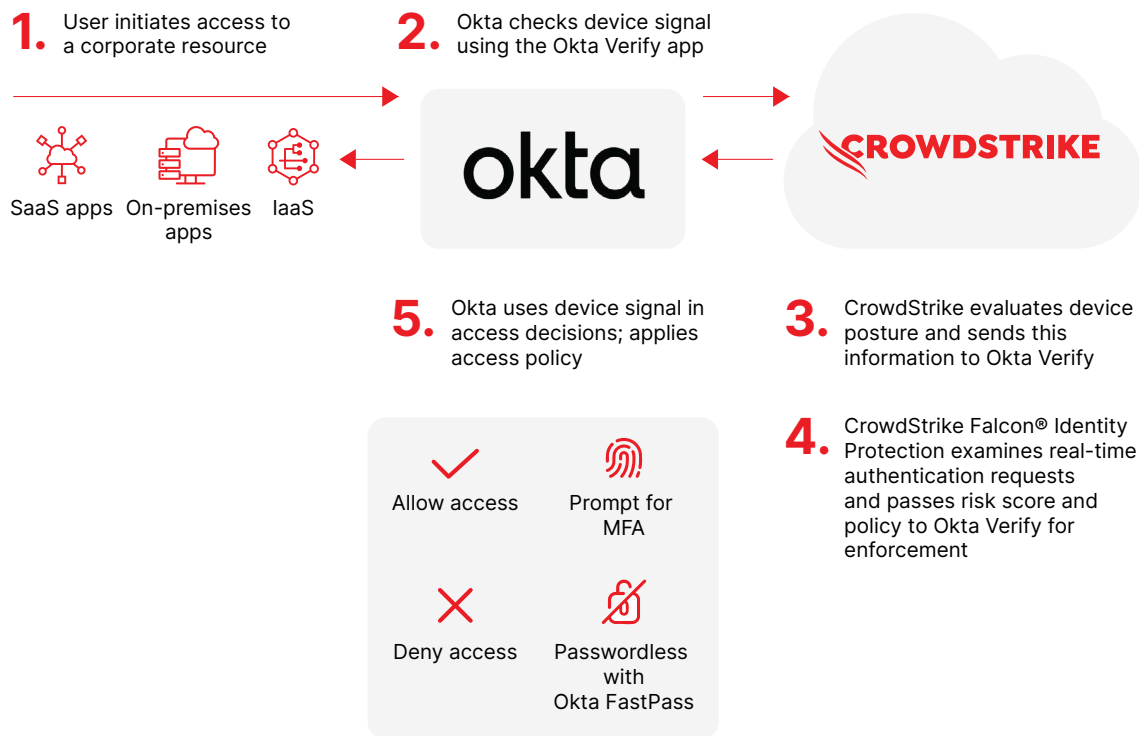
Technical solution

CrowdStrike extends the capabilities of Okta Verify and Okta Devices Platform Service so you can make smarter access decisions based on host security posture assessment, in correlation with user identities.

First, Okta Verify captures device posture signals collected by CrowdStrike's endpoint detection and response (EDR) solution, even when those devices are unmanaged. Okta's policy engine then compares these signals against the app sign-on policies defined by your administrators so access decisions can be adjusted accordingly. If the CrowdStrike Falcon® Zero Trust Assessment doesn't meet the defined security threshold requirements as defined by admins, access can be denied, or the user might be prompted for Okta multifactor authentication. An acceptable device score, on the other hand, might allow Okta FastPass passwordless authentication. Your workforce gets quick and appropriate access to everything it needs, even in today's chaotic bring-your-own device (BYOD) environments.

CrowdStrike and Okta also help unify your security data and enable response actions across endpoint and identity domains to enhance your team's detection and response of modern threats.

With CrowdStrike Falcon® Next-Gen SIEM, you can easily ingest and view Okta identity and authentication (single sign-on and multifactor authentication) data within the CrowdStrike Falcon® console, alongside additional threat indicators from other domains, to minimize context-switching and speed up threat detection. You can also trigger Okta response actions directly from the relevant detection manually or automatically through CrowdStrike Falcon® Fusion SOAR, including forcing a password reset and resetting authentication factors. By enabling Okta data ingestion and response actions with Falcon Next-Gen SIEM, your team is empowered to effectively secure your entire organization and identities, stopping advanced attacks before they cause damage.



Okta is a trusted **CrowdStrike Technology Alliance Partner**, offering innovative integrated solutions that help companies of any size access data and apps in the cloud, allowing them to secure their business without hassle.

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology — anywhere, on any device or app.

The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you.

Learn more at okta.com.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.



Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>