Databricks Elevates Security and User Experience with **Integrated Okta and Palo Alto Networks Solutions**

okta

paloalto NETWORKS

Challenge: Disparate Security and User Experience Issues

Prior to implementing the integrated solutions, Databricks faced challenges with a disparate tech stack as their zero trust strategy wasn't fully implemented. The sign on process for VPN connectivity was also a less than optimal experience for end users, and the team wanted to strike a balance between convenience for their end-users while not compromising on security.

Solution: Okta + Palo Alto Networks GlobalProtect Integration

Databricks significantly evolved its security strategy by leaning into a comprehensive zero trust model, rolling out integrations between Okta and Palo Alto Networks GlobalProtect VPN and Cloud Identity Engine (CIE).

The integrations enabled Databricks to:

Extend granular Adaptive Multi-Factor Authentication (MFA) from Okta into user sessions, allowing for different authentication paths based on the trust level of an individual.

Implement certificate-based authentication leveraging CIE, allowing them to move to a passwordless experience that drastically improved the user experience by creating much less friction in their day.

Maintain strong security, as their system leverages multipe risk signals being ingested into Okta that only prompts the user for authentication when necessary. This provides security assurance for each individual session even without passwords.

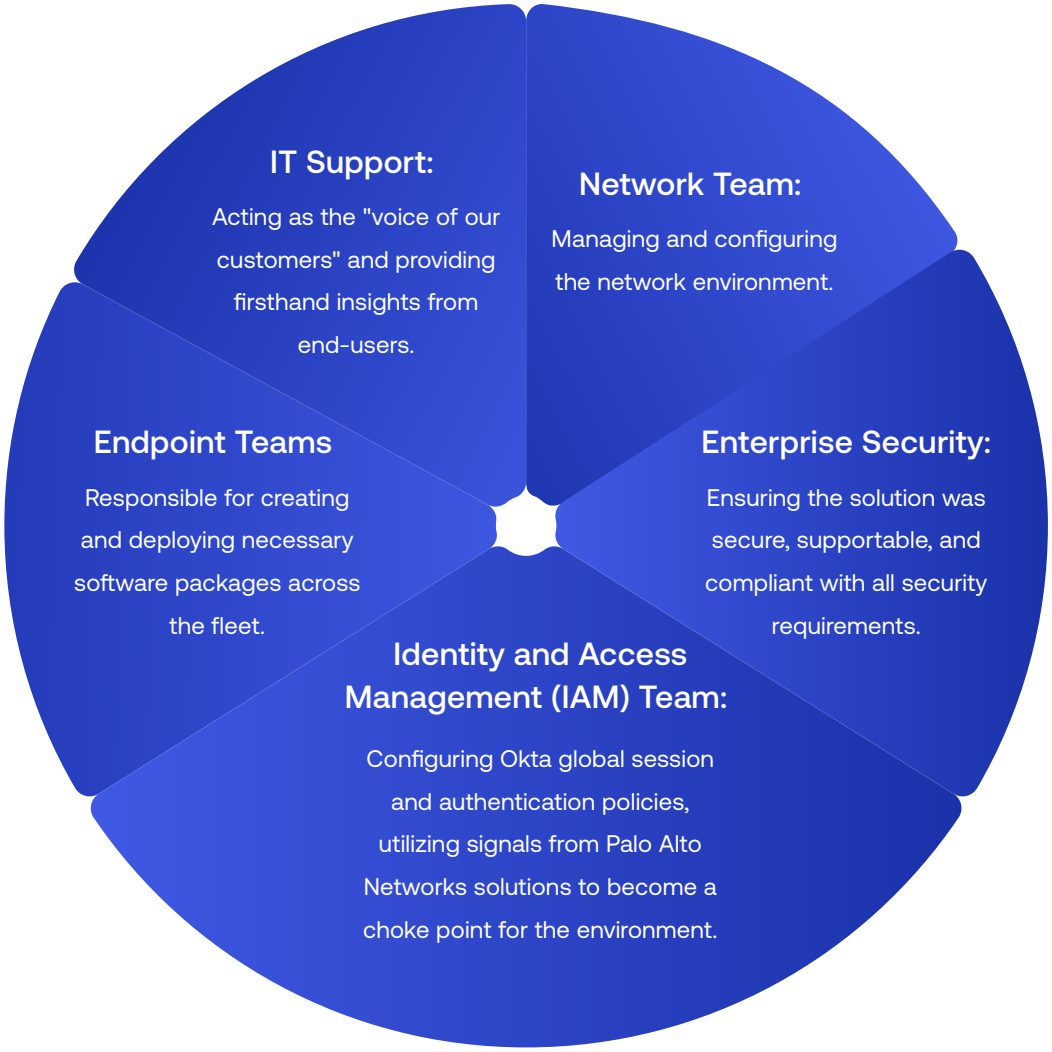
> “The integration has made for a much better experience for our end users, leading to much less friction in their day. They are very thankful for the passwordless experience and we worked very closely with our security departments to make sure that everything remains secure in our environment.”

Jack Zaldivar

Staff Systems Engineer, Databricks

Achieving Buy-in for Integrated Deployments

Rolling out such comprehensive integrations required collaboration across various internal teams at Databricks. This was a combined effort involving:



Databricks found that having strong leadership with a north star was crucial for aligning all teams towards a shared objective. Their collective goal was to balance end user experience as well as heightened security, prioritizing user convenience without compromising security. This collaborative approach, where different teams contributed their expertise, ultimately led to a smooth transition to their passwordless GlobalProtect journey.

Measurable Outcomes and Benefits

The integrated solutions yielded significant positive outcomes for Databricks:

Enhanced Default Security Posture: Implementing an always-on VPN and passwordless authentication established a "secure by default" environment, significantly shrinking the attack surface.

Improved User Experience and Productivity: End users had fewer interruptions, such as unnecessary reauthentication prompts, and more intelligent risk signals now prompt authentication only when necessary, making users much happier and much more productive.

Operational Efficiencies: Streamlined authentication meant IT spent less time fielding support requests, and automated access management cut down on manual updates.

> "We've lowered our attack surface by implementing our always-on VPN solution and removing passwords from the environment. That's no longer a factor that can be exploited."
>
> **Jack Zaldivar**
>
> Staff Systems Engineer, Databricks