One-Minute Webinar: Identity and Access Management Insights from Analyst Firm ESG

Too busy to watch the ESG + Okta Webinar: How Identity Fits Into a Security-First Approach? Don't worry. We've got you covered.

IT analyst firm Enterprise Strategy Group (ESG) recently conducted a study into identity and access management, and the challenges presented by the cloud and mobile computing wave. Spoiler alert: Identity can reduce complexity and enhance security in both hybrid environments and cloud-first organizations.

Here's what ESG found:

- Cloud and mobile initiatives are creating chaos in IT organizations who have to manage authentication and access across a **scattered application landscape and a new, undefined perimeter.**
- **No clear owners for IAM:** Sometimes IAM projects are owned by IT (50%), other times the security team is in charge (31%).
- **But interest for IAM is rising:** 66% of respondents indicated that their security group had gotten more involved in IAM over the previous two years.
- **Security groups are increasing engagement in IAM:** Security teams are now getting involved in day-to-day IAM operations, defining IAM policies and monitoring privileged accounts.
- **Lack of education is still a major threat vector:** Credential theft, remote system access, and account provisioning are problems that when not properly managed and employees are not properly trained, lead to data breaches.
- MFA is often not implemented because **teams have a difficult time deciding which assets need MFA** and which don't.

Okta's take:

- Authentication with **a username and password is simply no longer secure enough.** This is an authentication technique that was invented in the 1960s and is now ready to be retired. With most data breaches occurring through the use of weak or stolen credentials, the need for a better form of authentication is clear.
- Teams need to realize that **all assets should be protected by MFA**. The good news, though, is that MFA doesn't need to degrade the user experience or complicate access management.
- **Adaptive MFA offers the ability to understand context of a login into account**, which makes it the obvious solution in an era where the security perimeter has moved to the user. When a user logs in from a well-known network and device, the authentication process can be streamlined. When a login occurs under unusual circumstances, however, additional authentication factors can (and should!) be introduced.
- Thanks to the contextual nature of Adaptive MFA, **we're close to doing away with passwords completely**. The passwordless future is upon us.

How Okta can help:

- Okta solutions were born and built in the cloud, making them easy to implement and manage. We offer a complete, integrated service for every type of user, and allow users to connect securely to over 5,500 pre-built and supported integrations. This allows authentication data to be shared throughout your IT and security ecosystems, increasing your team's visibility and allowing them to make more informed decisions, while reducing response time.
- Okta's identity-driven security approach extends beyond your network and firewall, and focuses on the new security perimeter: people. Adaptive MFA examines where users are, what devices they're on, what networks they're using, and what their relationship is to your business.
- Passwordless auth is coming soon!

If you're interested in more from ESG and Okta, you can find the full webinar here: How Identity Fits Into a Security-First Approach. Check out the product page for more details on Okta Adaptive Multi-Factor Authentication and how Okta can help provide secure access for your entire business.