okta

Leveraging Okta's Identity cloud as the first line of defense against fraud, waste and abuse

okta Identity Cloud

As more government organizations move their citizen services to mobile and cloud-based platforms, ensuring the validity of those benefits claims is more important than ever. Many are adopting an identity centric security model as a framework for prevention of risk and fraud.

Why start with identity?

A unified identity layer sets the foundation for building modern citizen application access, building security policies and allowing your systems to get smarter and smarter. Access is given based on trust, and trust is determined by context. An effective identity strategy can reduce fraud at registration (synthetic identity fraud), authentication (account takeover fraud) and transactional risk.

Align trust to context

Step 1: Authentication. Enforce primary authentication assurance coupled with effective password and threat policies. This includes secure password and account recovery capability. Leverage Okta's pre-authorization risk policies to detect risk before primary authentication. Stop known bad actors, stop access from tor and proxies, stop access from regions outside your normal jurisdiction etc.

1 IDP Platform	2 Adaptive Authentication	3 MFA
Pre-Auth Policies	User Context	MFA
Password Policy	Application	MFA Policy
Password & Account Recovery	Device	Factor Management
Passwordless Auth	Network	
Threat	Location	
	Risk Engine/ML	

Pre-Authorization Risk Policies:

- ✓ **Threat Insights**: Global IP database used to analyze login patterns and ensure secure access decisions
- ✓ **Anonymous Proxy Detection**: Identify and block Tor anonymizer proxies
- ✓ **Dynamic Network Zones**: Leverage factors such as geolocation, IP type or ASN to deny authentication or enforce higher level of assurance
- ✓ **Behavior Detection**: Detect user behavior changes, such as new location, to drive authentication policies
- ✓ **Risk Scoring**: Real-time intelligence used to gain a holistic view of context behind each login.

Step 2: Automatically assess log in risk based on normal user login patterns. Variables include user context, device, network, location, and threats. Understand the risk associated for each request and layer that with Artificial Intelligence/Machine Learning and Heuristics based rules engines.

Step 3. Enforce additional strong customer authentication as and when required using a range of factor options including knowledge, possession and biometric factors. This includes self-serve factor management options.

SMS, Voice, and Email

One-time passwords like Okta Verify and Verify Push, and third-party solutions

Physical tokens including support for RSA, Symantec, and Yubikey tokens

Biometric factors including Windows Hello and Apple Touch ID

If implemented correctly, you'll achieve an identity centric security model. The goal, of course, is to achieve this with the least amount of friction possible. Security should be an enabler, not a blocker forcing users to hop around to different networks or enter different passwords.

Pain points

Identity attacks: Identity driven attacks such as citizen account takeover, synthetic identities are the leading causes of fraud and abuse across your citizen services.

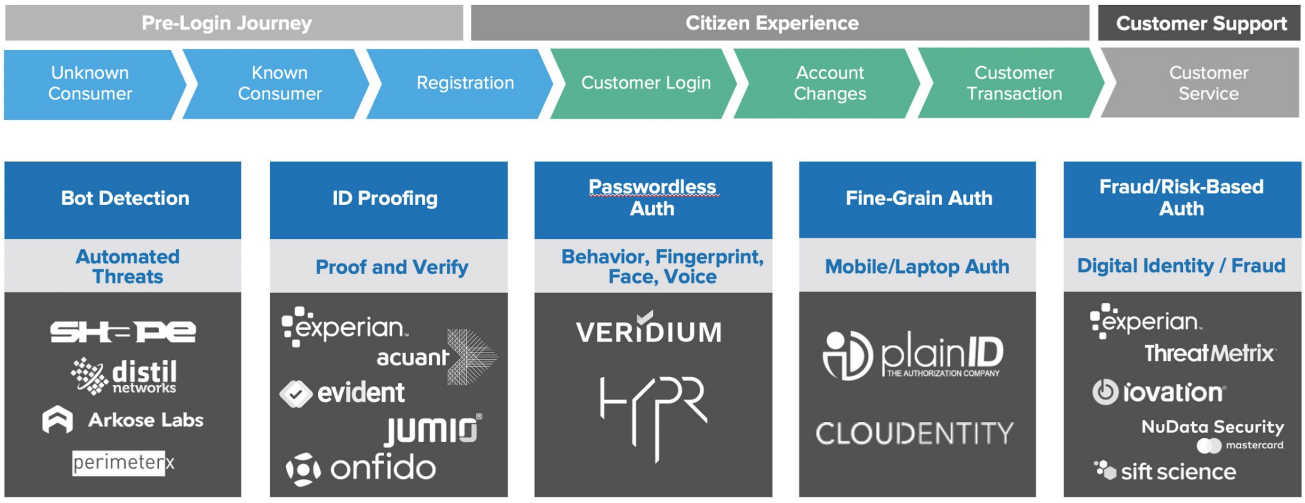
Password policies: Password driven security policies have limited efficacy in protecting a user account. User's reshare passwords across sites and insecure recovery flows are also leading causes of account takeover.

Existing fraud solutions: Miss a large number of fraudulent claims. These solutions often take time to detect an incident and have poor ROI. Different solutions of the stack do not often talk to each other causing abuse blind spots. These solutions increase insult rates and false positives.

Why Okta?

Okta's industry leading Identity Cloud platform provides all the tools needed to store user identities, deploy simple and secure sign-on policies and automate complete lifecycle management for all your users.

As an independent Identity Management platform, Okta can also integrate with a countless number of third-party enterprise fraud management (EFM) providers, whether it's improving your security posture with tools that perform identity proofing or bot detection, or if you need to deploy tools to help with functions such as analytics/reporting and consent management to adhere to stringent data and privacy policies. With close to 7,000 pre-built integrations in our Integration Network, and limitless others with our support for any open standard, Okta can connect you and your users to all of your applications.



The journey to secure citizens and build trust starts with Identity: A modern cloud based Customer Identity Solution lays the groundwork for security, and delightful citizen experiences while keep fraudsters and abusers at bay. With a solid identity layer, users earn trust based on a context that is continuously assessed and Okta is your modern identity and security platform to lay the foundation of trust and fight fraud and abuse.

Customer Success Story

One of the nation's largest state unemployment agencies turned to Okta to help manage the security and sign-on policies for their users. Within the first 30 days, Okta was managing and authenticating almost 1.6 million active users. More importantly, Okta sign-on policies successfully blocked over 40,000 fraudulent logon attempts to access the system, resulting in millions of dollars in savings from fraudulent claims.