Dynamic access for AWS

Eliminate standing access to your AWS environments.

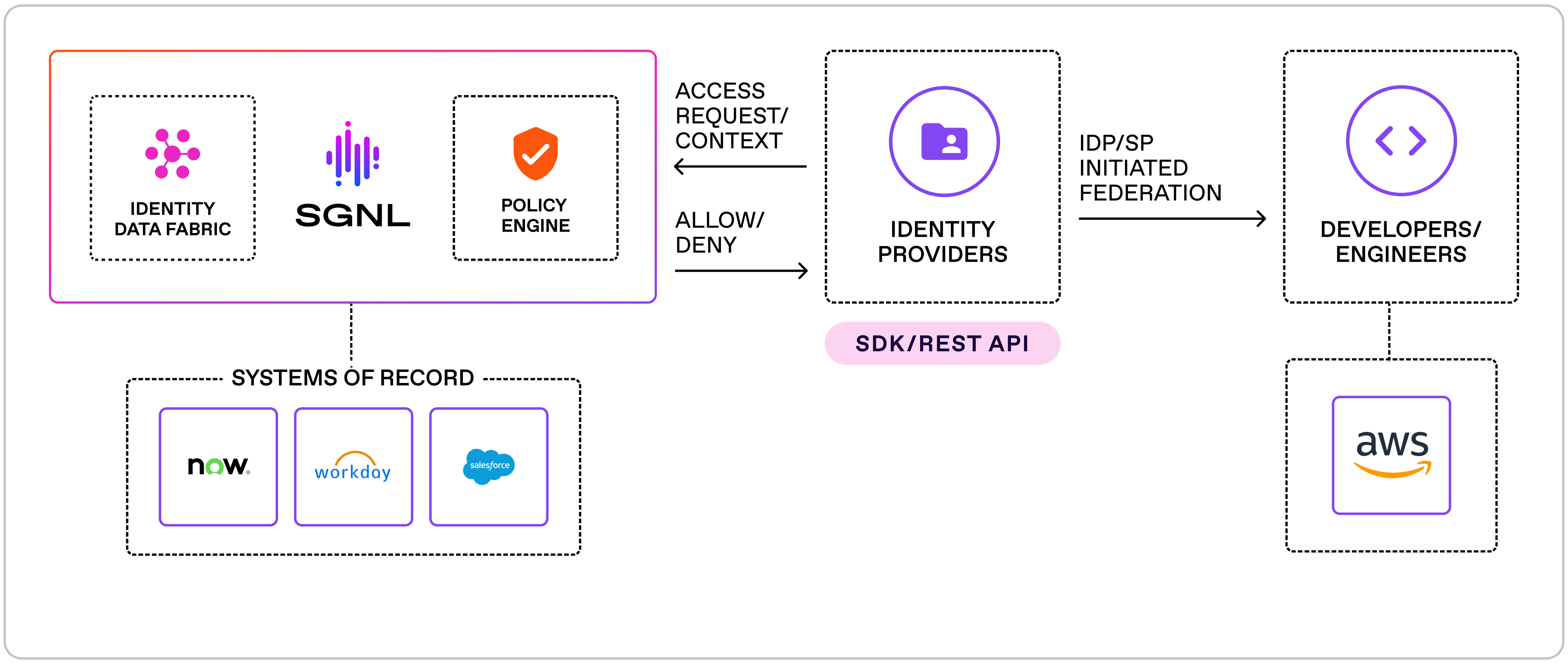
Organizations depend on Amazon Web Services (AWS) for their production environments. This makes AWS an ideal target for malicious actors. Unfortunately, most organizations still grant standing access to AWS which can lead to a dangerously large blast radius in the event of an identity breach.

SGNL enables companies to achieve Zero Standing Privilege for AWS, limiting their workforce to only the access they need, when they need it. This approach drastically reduces the potential blast radius.

> "By 2026, 70% of identity-first security strategies will fail unless organizations adopt context-based access policies that are continuous and consistent."
>
> GARTNER, IDENTITY-FIRST SECURITY MAXIMIZES CYBERSECURITY EFFECTIVENESS
>
> BY REBECCA ARCHAMBAULT, FELIX GAEHTGENS, JAMES HOOVER, ANT ALLAN, DECEMBER 7, 2022

How does it work?

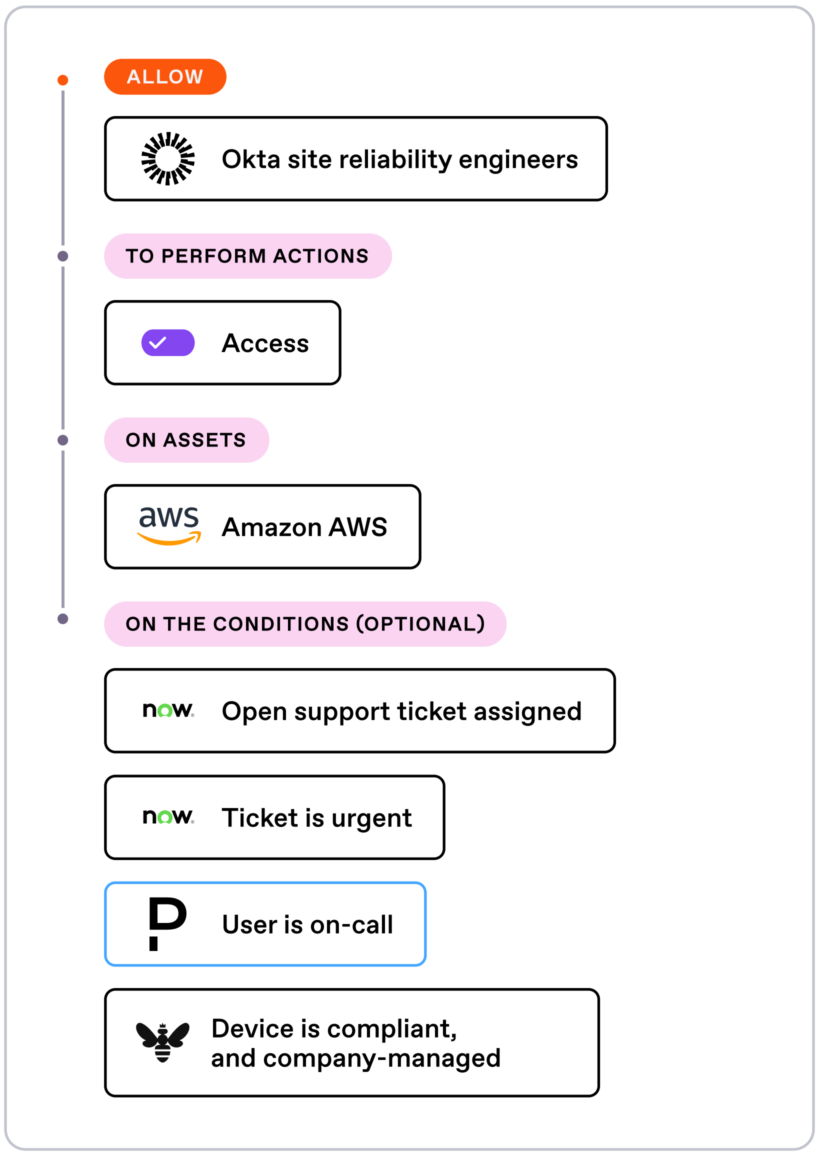
SGNL for AWS allows enterprises to create context-based policies that grant dynamic access to production environments only when required, and rescind that access when the work is complete.



Sample use case:

For example, a site reliability engineer is assigned a bug or outage that requires investigation in a production environment. The engineer only has access while all of the following remain true:

- A ServiceNow ticket is open and assigned to them
- They are the on-call engineer in PagerDuty
- Kandji shows their company-managed laptop is compliant



ALLOW

Okta site reliability engineers

TO PERFORM ACTIONS

Access

ON ASSETS

Amazon AWS

ON THE CONDITIONS (OPTIONAL)

Open support ticket assigned

Ticket is urgent

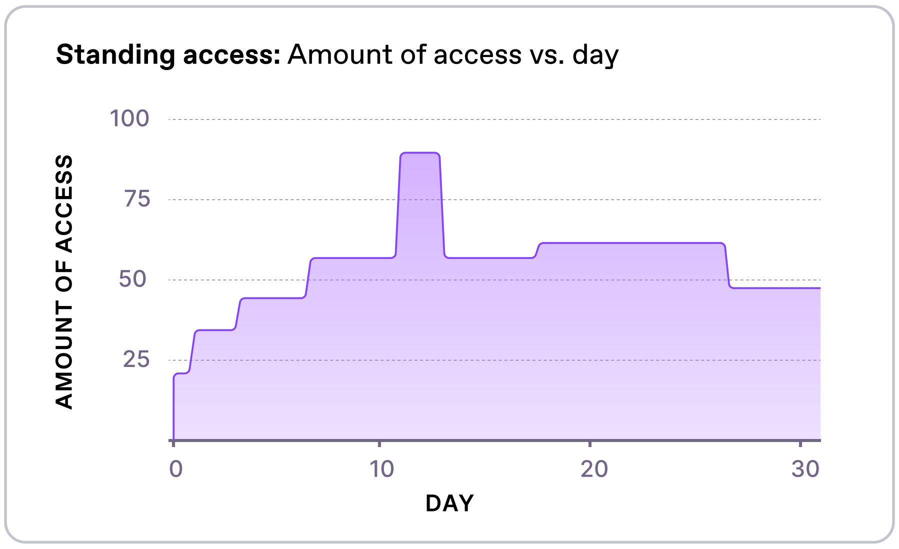
User is on-call

Device is compliant, and company-managed

The exploitability of standing access vs. Zero Standing Privilege

Standing access

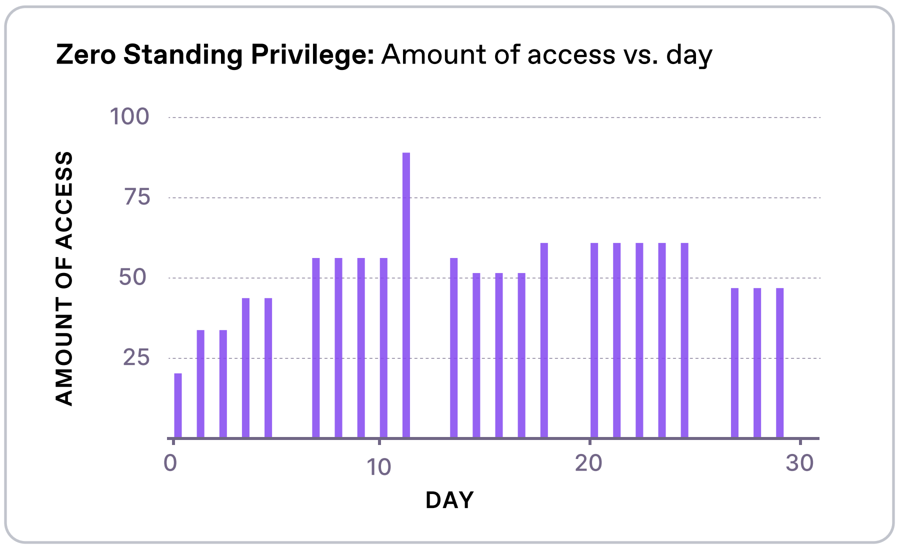
In a standing access environment, a spike in the charts represents a firefight incident in which the user got extraordinary access to fix a production issue. This additional access is typically granted for longer than necessary in a standing access environment versus a much faster return to normal with Zero Standing Privilege.



Standing access: Amount of access vs. day

Zero Standing Privilege

In a Zero Standing Privilege environment, the area under the graph is zero when a user doesn't have a session or access token. There are no access rights for threat actors to exploit or misuse. In a standing access environment, some level of access is always available using the user's credentials.



Zero Standing Privilege: Amount of access vs. day

ABOUT SGNL

SGNL's modern Privileged Identity Management system eliminates standing access to critical systems by granting and revoking contextual access in real time, drastically reducing the potential impact of a breach. By incorporating context-based intelligence, SGNL prevents attackers—leveraging compromised credentials or other means—from freely navigating cloud applications like Azure, AWS, GitHub, and Salesforce, as well as on-prem systems.

SGNL IS BACKED BY LEADING TECH INVESTORS

CISCO investments

M12 MICROSOFT'S VENTURE FUND