PO SECURITY

Splunk accelerates secure cloud access with PO Security

splunk> a CISCO company

About Splunk

Splunk helps organizations turn data into doing.

Their platform secures and delivers reliable performance for even the most complex digital ecosystems with complete visibility, flexible data management and federation, and fast response powered by AI.

Overview

Splunk is a global leader in cybersecurity and observability.

With 2,000+ developers and professional services engineers occasionally needing access to customer environments in Splunk Cloud, the team required a modern solution to manage privileged access without compromising security, productivity, or compliance.

As Splunk scaled, their legacy PAM solution—Okta ASA—introduced friction and overhead.

Developers needed better ways to securely access EC2s and cloud services across AWS, GCP and Azure, without standing SSH keys or single points of failure.

splunk> a CISCO company

Challenge

With customer environments hosted across AWS, GCP, and Azure, developers often needed SSH access to virtual machines—tasks considered highly privileged due to access to configurations, network controls, and sensitive customer data.

Splunk's previous PAM, Okta ASA, introduced multiple pain points:

- **Outdated architecture**—ASA relied on a network proxy model that couldn't govern cloud-native entitlements or fine-grained resource access.
- **Operational overhead**—Platform teams had to deploy agents on each EC2 instance, increasing complexity as infrastructure scaled.
- **Developer friction**—ASA lacked out-of-the-box support for just-in-time (JIT) access and didn't integrate easily with modern tooling like Slack or PagerDuty.
- **Single point of failure**—The proxy-based architecture posed risks if the proxy or agents failed.

Splunk needed a modern PAM that could scale with their cloud-native workflows.

> "P0's agentless PAM solution helps us govern access to EC2s in AWS, by providing our developers JIT access to production, and removing any standing access."

Adeel Khurshid,
Senior Director,
Security Engineering
Splunk

splunk> a CISCO company

Solution

Splunk selected P0 after evaluating other options including Teleport, StrongDM, and CyberArk. P0's agentless architecture, built to natively leverage cloud IAM APIs, stood out.

Using P0, Splunk now provides:

- **Agentless JIT access** to EC2s via AWS SSM, GCP IAP, and Azure Bastion—without network proxies.
- **Expanded coverage** across services like S3 and EKS, and for non-human identities such as IAM roles or service accounts.
- **Cloud-native governance** with workflows for secrets rotation and overprivileged role remediation.
- **Slack, JIRA and PagerDuty** integrations that enable seamless access requests and on-call automation.

Results

- Eliminated SSH keys and proxy dependencies
- Reduced operational complexity for platform teams
- Delivered instant, JIT access to production environments
- Laid foundation for future cloud access governance, including identity discovery and secrets management

Why it matters

Splunk eliminated the risk and friction of proxy-based PAM while expanding visibility and governance across their cloud infrastructure.

Developers now receive secure, just-in-time access without slowing down operations, helping the organization meet stringent compliance standards like SOC 2 and ISO 27001.