Google Cloud Account Takeover Protection

Analyze human behavior to protect Google Cloud workloads.

Cloud platforms like GCP are a top concern for CISOs

When asked which platforms give security leaders the most concern when it comes to protecting cloud applications and infrastructure from compromise, cloud platforms like GCP were in the top 2.

Sophisticated attackers have targeted cloud credentials

Threat groups have launched large-scale campaigns targeting cloud credentials, attempting to compromise Google Cloud, Azure, and AWS credentials due to the prevalence of multi-cloud environments.

Google Cloud Platform security is one layer

While Google BeyondCorp and other Google tools provide threat detection and access control, this—as is the case with email security for Gmail—it is one layer in a broader defense-in-depth strategy that spans the cloud.

Extend Abnormal Protection Across All Platforms

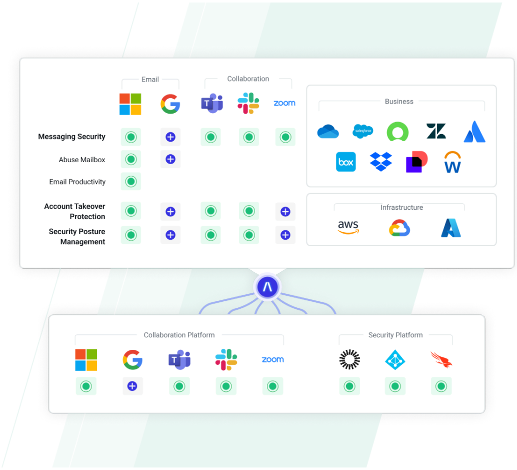
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. In many organizations, Google Cloud Platform is “the cloud,” necessitating a greater level of protection than Google’s own security tools alone can provide. To stop attackers from compromising Google Cloud environments, security teams need an extensible platform that provides consistent visibility and security automation across not only Google Cloud workloads but all cloud applications and infrastructure services for holistic, higher fidelity detection. Abnormal provides that platform.

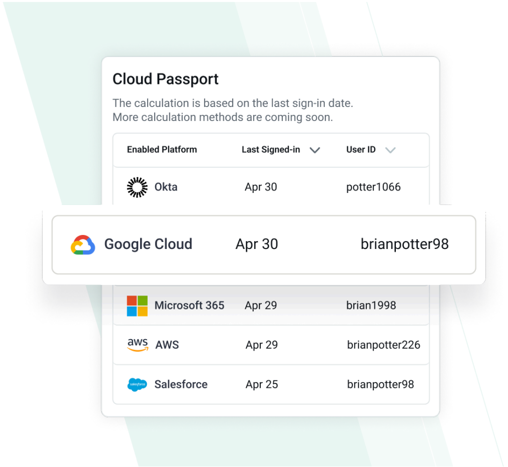
Abnormal

How Abnormal Secures Google Cloud Platform

Simple API Integration

Connect directly to Google Cloud with Abnormal's cloud-native API architecture—automatically ingesting and normalizing access data for every human that signs in to GCP.





Cloud Passport

The calculation is based on the last sign-in date.
More calculation methods are coming soon.

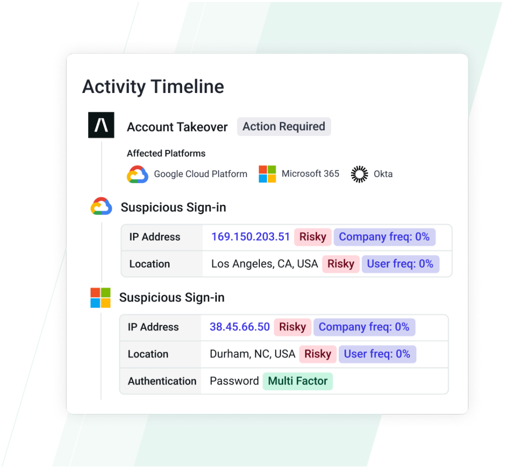
Enabled Platform	Last Signed-in	User ID
Okta	Apr 30	potter1066
Google Cloud	Apr 30	brianpotter98
Microsoft 365	Apr 29	brian1998
AWS	Apr 29	brianpotter226
Salesforce	Apr 25	brianpotter98

Continuous Monitoring of Human Behavior in GCP

Automatically learn and dynamically monitor Google Cloud access patterns, develop a behavioral baseline and profile for every human on the Google Cloud Platform, and automatically detect and analyze behavioral deviations.

AI Account Takeover and Response

When suspicious activity occurs, Abnormal Human Behavior AI automatically triggers the creation of a contextual Case populated with Google Cloud activity. Each Case is scored based on detection confidence and continually enriched with new activity across all platforms integrated with Abnormal.



Activity Timeline

Account Takeover Action Required

Affected Platforms

Google Cloud Platform Microsoft 365 Okta

Suspicious Sign-in

IP Address	169.150.203.51 Risky Company freq: 0%
Location	Los Angeles, CA, USA Risky User freq: 0%

Suspicious Sign-in

IP Address	38.45.66.50 Risky Company freq: 0%
Location	Durham, NC, USA Risky User freq: 0%
Authentication	Password Multi Factor

Try Abnormal Today

See how Abnormal can keep attacks out of your cloud email and connected platforms. Integrate in minutes via API.

abnormalsecurity.com/risk →

Abnormal