# Amazon Web Services Account Takeover Protection

Analyze human behavior across the AWS environment to detect risks to your critical infrastructure.


## AWS Environments House Critical Business Processes

AWS is a sprawling ecosystem of cloud services, and in the last five years alone, attackers have targeted and stolen everything from customer names and social security numbers to airline navigation information and proprietary software.

## Attackers Are Targeting AWS With Sophisticated Tactics

Session hijacking, credential stuffing, and other sophisticated tactics are being used by attackers to attempt to compromise AWS environments to steal sensitive data, steal proprietary software, or take down entire services.

## Complex AWS Environments Impact Security Visibility

Security teams are tasked with protecting AWS environments but may have incomplete visibility across all objects and stores. And even with the security tools provided by Amazon, there is a need for centralized cloud visibility not afforded by point solutions.

## Extend Abnormal Protection Across All Platforms

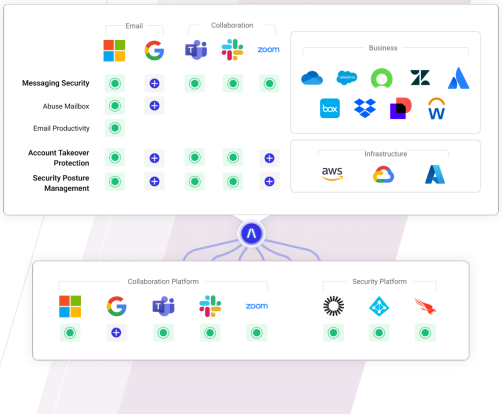
Cloud phishing breaches—breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are on the rise. And since AWS *is* "the cloud" in most organizations, keeping attackers out of AWS is a top concern.

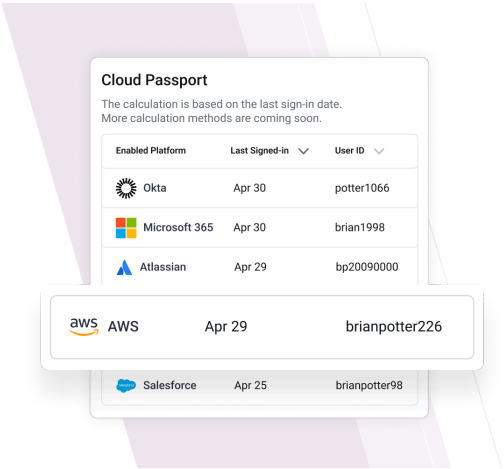
The key to stopping these breaches is consistent visibility and security automation across the AWS environment through an extensible AI platform. Abnormal protects not only AWS, but all of your most important cloud services.

# How Abnormal Secures Amazon Web Services

## Simple API Integration

Connects to AWS Cloudtrail through cloud-native API architecture to automatically ingest and normalize sign-in signals from across your AWS environment—analyzing humans accessing everything from Lambda to S3 and beyond.



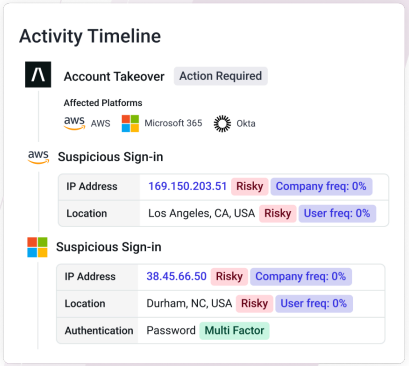




## Continuous Monitoring of Human Behavior in AWS

Learns what normal behavior looks like for every human with access to AWS, develops a dynamic behavioral baseline, then automatically detects and analyzes deviations from the norm.

## AI Account Takeover and Response

When a deviation appears suspicious, Abnormal Human Behavior AI automatically creates a contextual Case for that suspicious human populated with their cross-AWS activity. Each Case is scored based on detection confidence and continually enriched with activity from all platforms integrated into your Abnormal Portal.




## 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