Microsoft Azure Account Takeover Protection

Analyze human behavior to protect Azure cloud workloads.

Cloud platforms like Azure 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 Azure were in the top 2.

Nation-state attackers continually target Azure

Threat groups like Midnight Blizzard have targeted Microsoft's cloud environment with sophisticated tactics pointing to a need for greater protections in customer Azure deployments.

Microsoft security is strong but is one layer

While Microsoft provides active threat detection and access controls, this—as is the case with email security for Microsoft 365—is only one layer in an effective defense-in-depth strategy to protect the cloud.

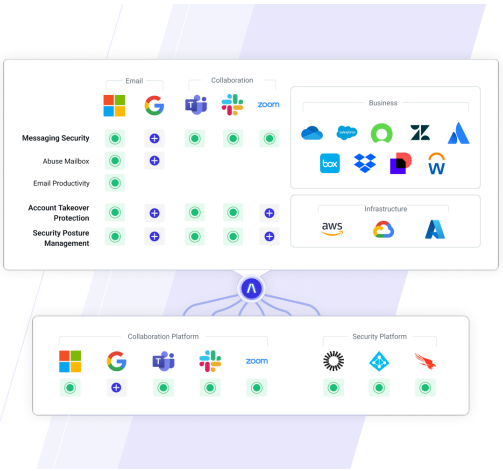
Extend Abnormal Protection Across All Platforms

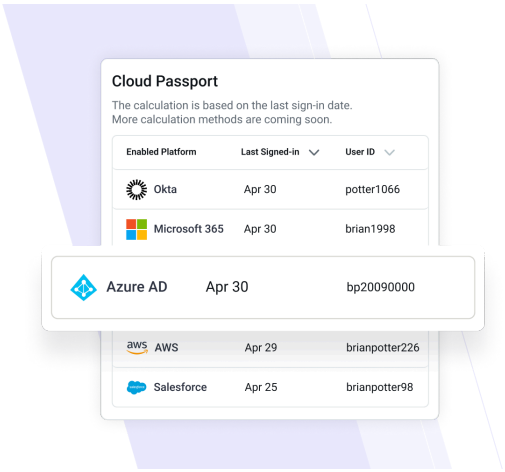
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. In most organizations, Azure is "the cloud," necessitating a greater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

How Abnormal Secures Azure

Simple API Integration

Connect directly to the Microsoft Graph API with Abnormal's cloud-native API architecture—automatically ingesting and normalizing access data for every human that signs in to Azure.



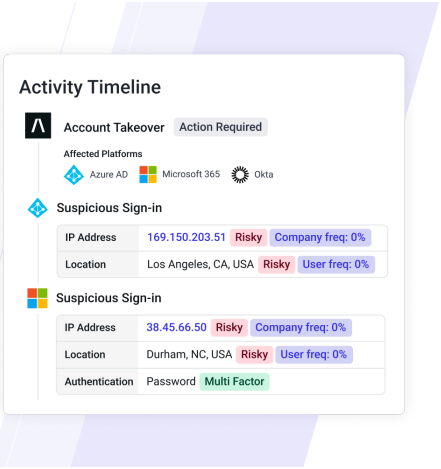


Continuous Monitoring of Human Behavior in Azure

Automatically learn and dynamically monitor Azure access patterns, develop a behavioral baseline and profile for every human on the Azure 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 Azure activity. Each Case is scored based on detection confidence and continually enriched with new activity across all platforms integrated with Abnormal.



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