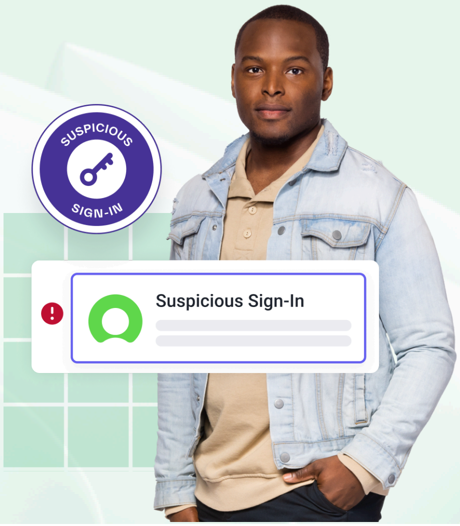
ServiceNow Account Takeover Protection

Analyze human behavior on ServiceNow to detect risk to your ticketing platform.



ServiceNow contains confidential data

ServiceNow is not just for IT tickets. While those tickets themselves contain sensitive information such as internal or customer vulnerabilities, the confidential data stored in ServiceNow's knowledge bases are a valuable target if the platform is compromised.

Native protections in ServiceNow are just one layer

Session hijacking, credential stuffing, and other sophisticated tactics allow attackers to break traditional authentication protections. ServiceNow's native security tools are effective, but authentication security is still primarily the responsibility of the customer.

Security teams lack visibility into platforms like ServiceNow

Security teams are tasked with protecting ServiceNow but often require additional visibility and access to do so effectively—lacking the ability to analyze the rich telemetry data related to ServiceNow users that can help to better secure the platform.

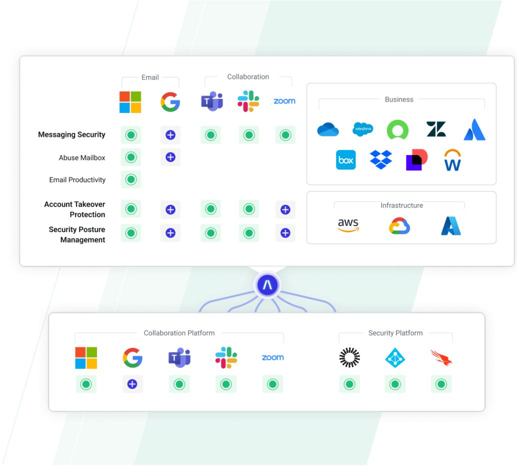
Extend Abnormal Protection Across All Platforms

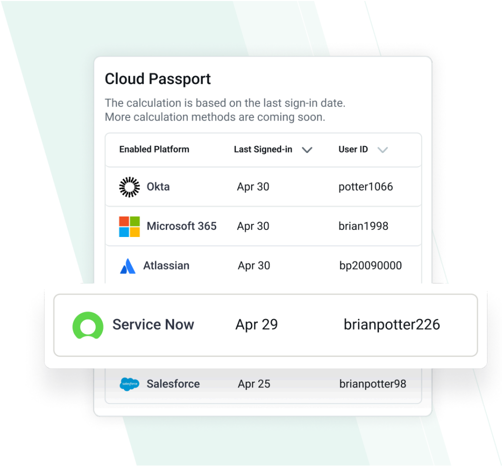
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are on the rise. Platforms like ServiceNow are the helpdesk for the cloud, requiring greater protection from breaches to not only secure the data within but to maintain a positive employee experience. The key to defending against these breaches is visibility and security automation delivered via an extensible AI platform. Abnormal is that platform, providing higher fidelity threat detection to ServiceNow and across all of your most important cloud services.

How Abnormal Secures ServiceNow

Simple API Integration

Connect to ServiceNow with Abnormal's cloud-native API architecture to automatically ingest and normalize ServiceNow sign-in signals—analyzing humans accessing any of the ServiceNow products that you own.





Cloud Passport

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

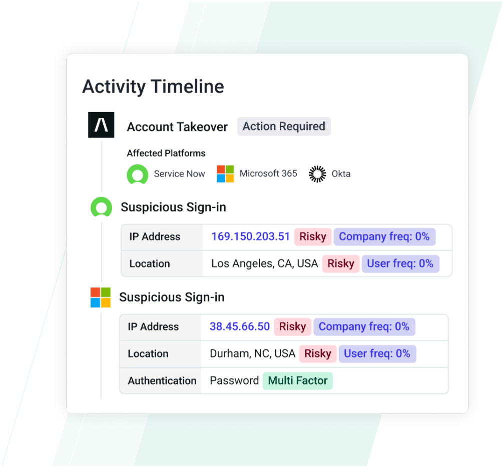
Enabled Platform	Last Signed-in	User ID
Okta	Apr 30	potter1066
Microsoft 365	Apr 30	brian1998
Atlassian	Apr 30	bp20090000
Service Now	Apr 29	brianpotter226
Salesforce	Apr 25	brianpotter98

Continuous Monitoring of Human Behavior in ServiceNow

Abnormal learns what normal ServiceNow access behavior looks like, develops a dynamic behavioral baseline and profile for each human, then automatically detects and analyzes anomalous activities.

AI Account Takeover and Response

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



Activity Timeline

Account Takeover Action Required

Affected Platforms

Service Now 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