Salesforce Account Takeover Protection

Analyze human behavior to better protect your Sales Cloud CRM from threats.

Sales Cloud is awash with confidential customer info

The Sales Cloud CRM is the primary customer database in most organizations with sensitive contact information, financial data, confidential details about customers and products, and more that all must be protected.

Attackers are targeting Sales Cloud to execute attacks

While the data in Salesforce is a target for attackers looking to execute ransomware or conduct espionage, recent attacks have seen attackers attempt to compromise Salesforce CRM’s email function to use it to launch phishing campaigns.

Security teams lack visibility and access to Sales Cloud

As Salesforce is typically owned by the sales operations team, security teams often lack necessary visibility into the platform. CRMs are complex, so being able to understand the behavior of humans accessing Sales Cloud is critical.

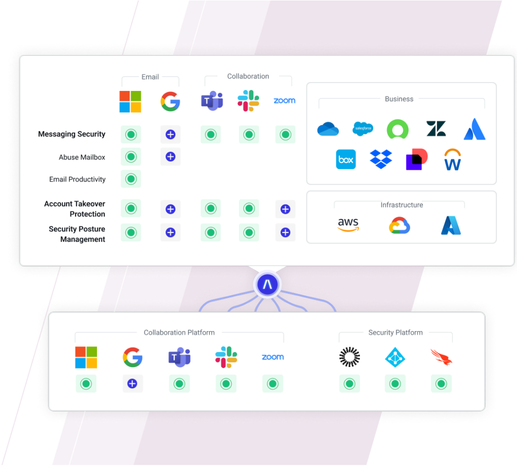
Extend Abnormal Protection Across All Platforms

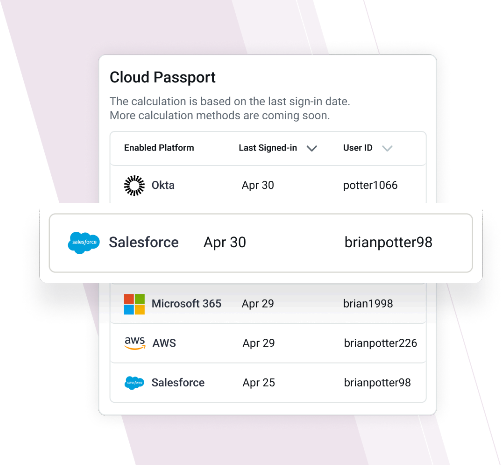
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. Of all the apps normally targeted in a breach, the Sales Cloud CRM tops the list. Outside of HR and finance tools, few platforms house more sensitive and confidential data—and in this case, data about customers. To stop these breaches security teams need a platform that provides consistent visibility and security automation that extends across not only Salesforce but all cloud apps and services. Abnormal provides that platform.

How Abnormal Secures Sales Cloud

Simple API Integration

Connect directly to the Salesforce APIs with Abnormal's cloud-native API architecture—automatically ingesting and normalizing sign-in signals related to every human in your organization that accesses Sales Cloud.





Cloud Passport

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

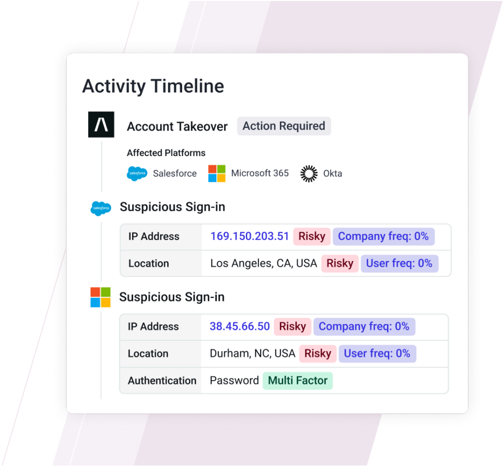
Enabled Platform	Last Signed-in	User ID
Okta	Apr 30	potter1066
Salesforce	Apr 30	brianpotter98
Microsoft 365	Apr 29	brian1998
AWS	Apr 29	brianpotter226
Salesforce	Apr 25	brianpotter98

Continuous Monitoring of Human Behavior in Sales Cloud

Build dynamic behavioral profiles for every human on Sales Cloud, develop a behavioral baseline, then automatically detect and analyze any notable deviations from that baseline behavior.

AI Account Takeover and Response

When suspicious activity occurs, Abnormal Human Behavior AI automatically triggers the creation of a contextual Case populated with Sales 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

Salesforce 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