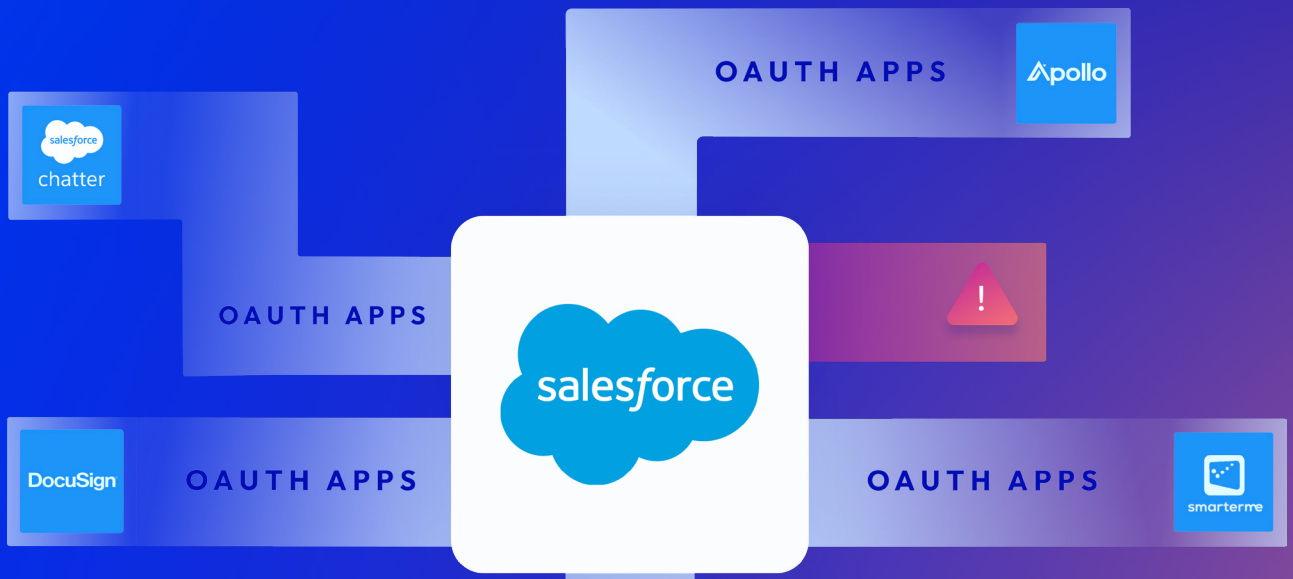
Astrix



Securing non-human identities in Salesforce

Salesforce environments across the world are connected to 11,225,724 AppExchange services, as well as countless other non-exchange services that can be integrated into Salesforce environments via API keys, OAuth tokens, service accounts and more. All these non-human connections accessing sensitive Salesforce environments significantly expand the attack surface, exposing companies to supply chain attacks, data breaches and compliance violations.

Salesforce is one of your organization's most critical core systems, holding crucial business processes and sensitive information. To automate processes and increase productivity, employees regularly connect third party apps and services to their corporate Salesforce, often without the knowledge of the security team.

The risks of unmonitored connections and non-human access to Salesforce environments

Salesforce app-to-app connections can often be made by anyone within the organization without any vetting from the security teams. While not all Salesforce users can use the app exchange, every single one is able to connect non-marketplace apps in multiple ways such as webhooks, SSH keys, OAuth tokens and more.

Everything from the Salesforce interface to accounts, contacts, calendars, Salesforce Flow, documents and more can be breached through third party non-human access. All it takes is just one of your connected apps or services to be breached, and your organization's most closely guarded assets, along with vital customer information, could be stolen or leaked.

For example, in recent years, sales intelligence solution Apollo fell victim to a breach that exposed some 9 billion data points. Salesforce users were affected by the breach because Apollo is an extremely common third party Salesforce integration, and the hackers who infiltrated Apollo were able to score some 7 million pieces of internal data regarding customers within Salesforce environments.

Your Salesforce environment could be more exposed than you think

Using the Astrix Security platform, we discovered that Salesforce environments are far more exposed to non-human connections than originally thought.

From our research, we discovered:

1.
Hundreds of connections to third-party applications and cloud services.

2.
New connections are seen on a weekly basis.

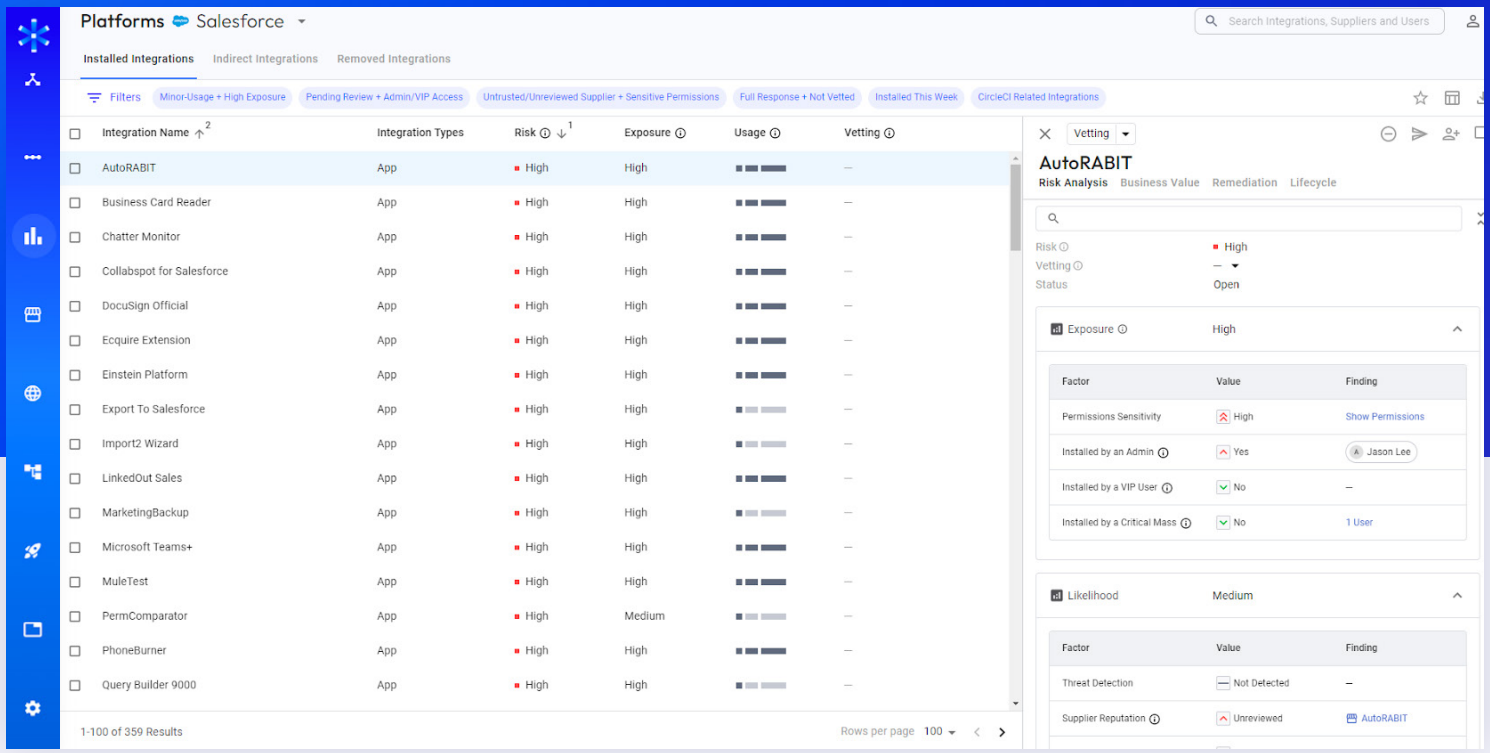
3.
Access granted between Salesforce and other apps was no longer used.

4.
Connections with common cloud services were configured with complete (and unnecessary) admin permissions.

5.
The majority of these connections are applications originating from non-marketplace sources which are not vetted.

6.
Many of the connections were with third-party apps and services of low-reputation publishers.

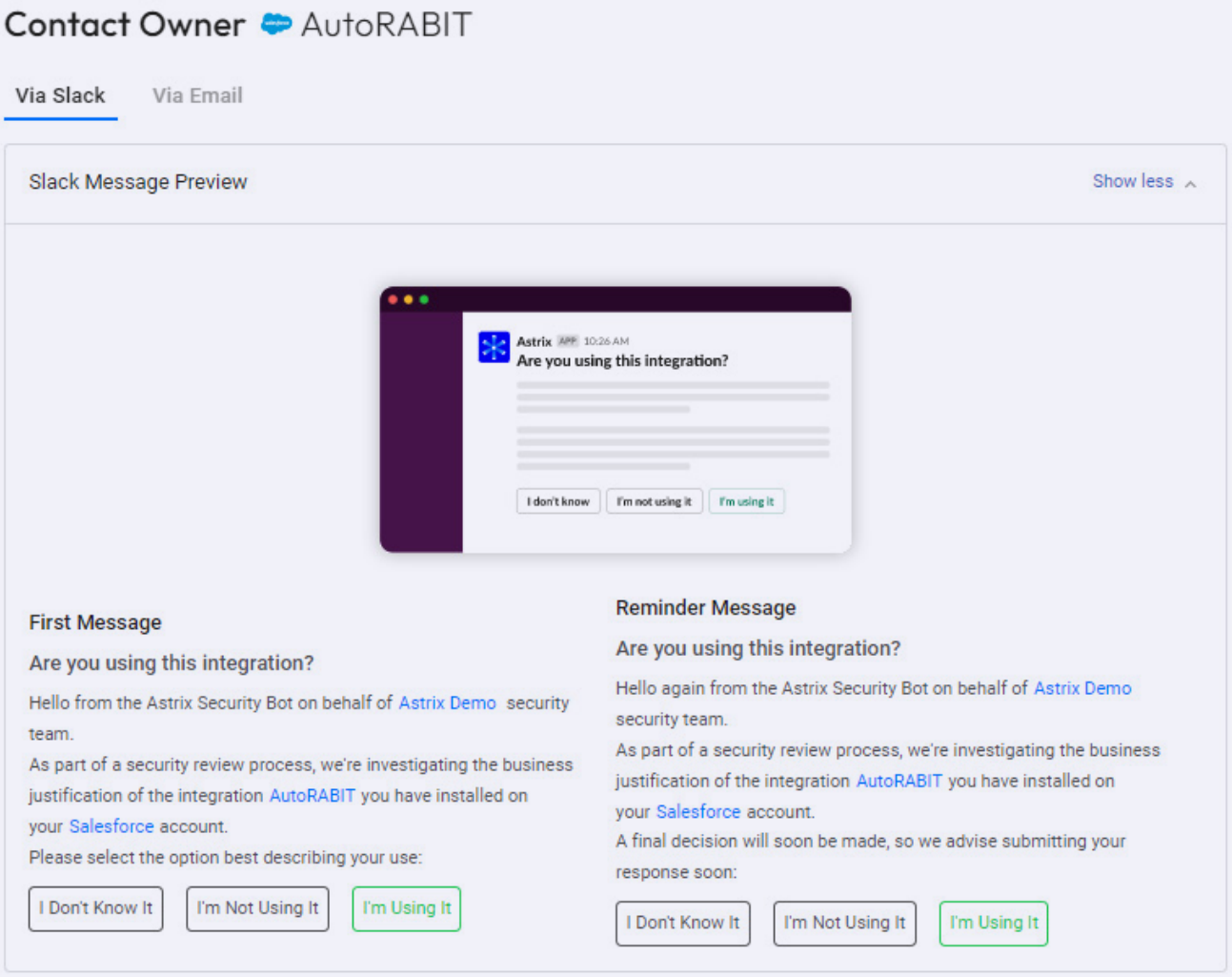
How Astrix helps secure your Salesforce environment



All integrations to a Salesforce environment sorted by risk, and a high risk integration details

Indirect integrations done through Salesforce automations:

1. Get a full inventory of all non-human access to your Salesforce environment, and understand the risks associated with them.
2. Get granular visibility into the OAuth permissions of your Salesforce environment. Salesforce OAuth tokens are usually very privileged and there is no easy way of knowing what access these tokens have without Astrix.
3. Ensure all non-human identities accessing your Salesforce environment have least privileged access, and remove unused connections.
4. Detect anomalous activity and remediate risks - Astrix's behavioral analysis looks into the app's access parameters such as geolocation, IP and user agent as well as advanced behavioral parameters such unusual usage, to detect misbehaving services and apps.
5. Get alerts only on risks that expose you to supply chain attacks, data breaches, and compliance violations, and easily remediate them through automated workflows.



Slack bot automation to verify the integration's business value with its owner

Astrix is the pioneer in securing non-human identities and is already trusted by leading enterprises such as

Rapyd workato Figma priceline agoda exabeam NETFLIX

bloomreach S&P 500 REIT Company Guesty FINTECH COMPANY hopper

Start using app-to-app connections safely

Book a demo