

# SaaS Security 101 Workshop

Securing Salesforce

The Salesforce logo, which consists of a teal cloud shape with the word "salesforce" in white lowercase letters inside it.

salesforce

Prevent SaaS Data Breaches

---



But first! A quick poll.....

# Agenda

Topics to teach and questions to get answered

## SaaS Security Overview

- Mass adoption of SaaS and the key security challenges that come with it.

## Salesforce Security Deep Dive

- Common Salesforce security challenges and misconfigurations
- Integrated demos during this session.

## Q&A

- Questions welcome throughout - please use the Q&A panel 😊

## Recap & Next Steps

- Key takeaways
- Invitation to join or share our next workshop (ServiceNow, M365)

# SaaS is the OS of Business



1. AppOmni - [State of SSPM](#)

2. Fortune Business Insights - [SaaS market size and growth](#)

# SaaS Incidents And Breaches Are On The Rise

## 2024 State of SaaS Security Report

26%  31%  
2023 2024

### Breaches

Increased by 5 points  
from last year

71%  75%  
2023 2024

### Incidents

4 points from last year. Exposed  
data or compromised security



# Widespread Data Leak Across Salesforce Sites

THE IRISH TIMES

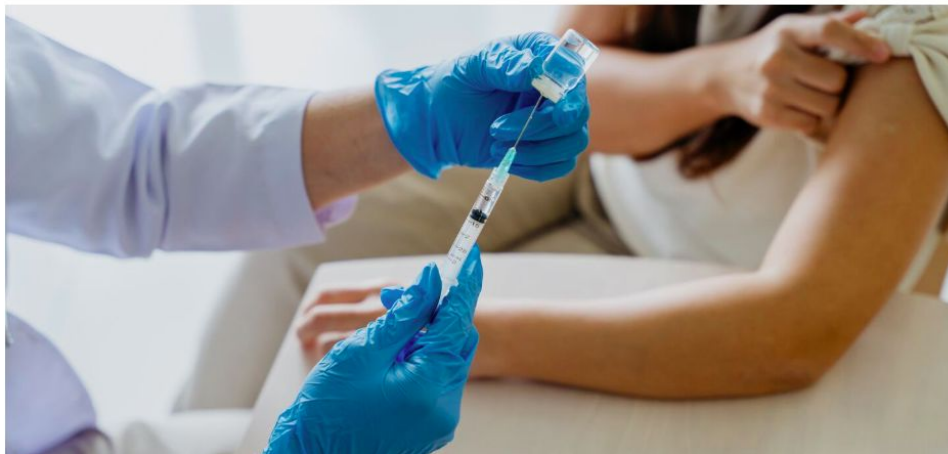
7°

Data & Security

## HSE glitch: Full names and vaccination status among data of up to 1 million people at risk

Covid jab status details available to unauthorised users, according to security researcher who discovered the issue

Expand



### LATEST STORIES >

Author Neil Gaiman dropped by US comics publisher after sexual misconduct allegations

Uniphar continues growth in 2024

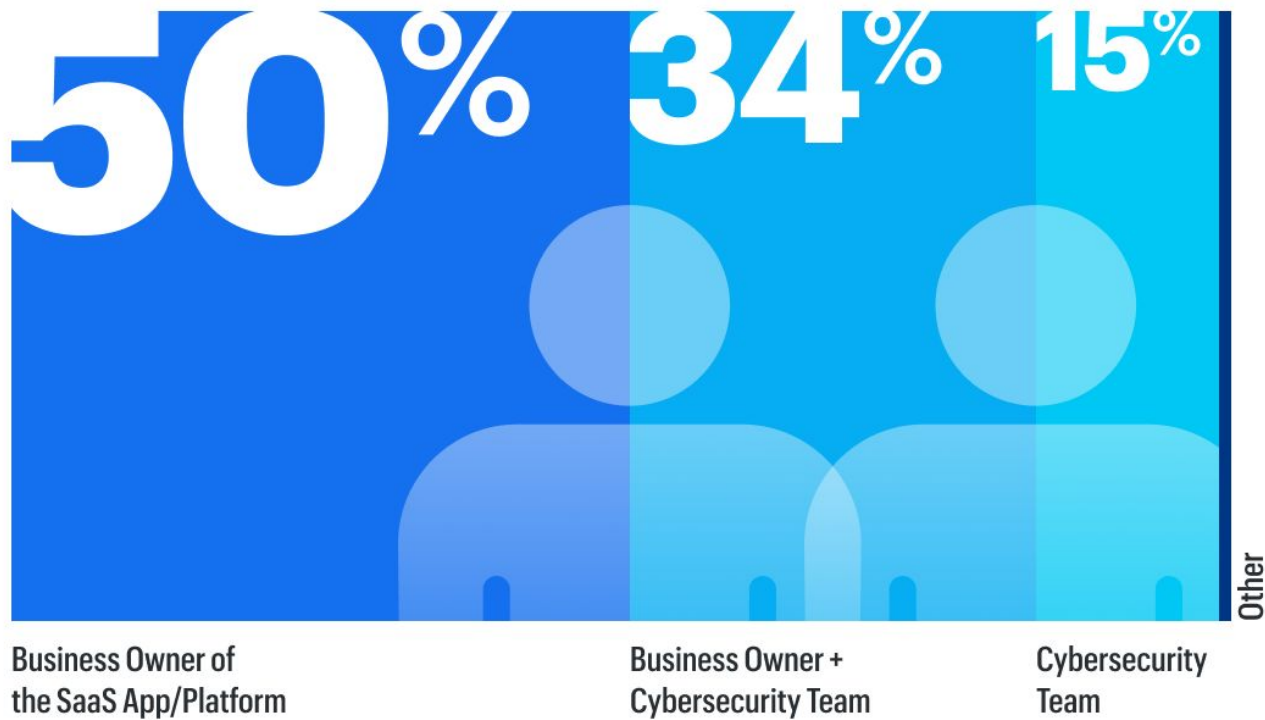
Is there any issue with driving an electric car through a flood?

State sells more AIB shares as bailout recovery reaches €17.9bn, with full exit in sight

OpenAI's Sam Altman vows 'better models' as China's DeepSeek disrupts global AI race

# Responsibility for SaaS Security is Distributed

2024 State of SaaS Security Report





# Time for a poll!

# Securing Salesforce



salesforce



## What's Inside a SaaS App?



App  
Server



Database  
Server



Web  
Server



Indexing  
Server



XML



Mail  
Server



Content  
Rendering



Load  
Balancer



Indexing &  
Reporting

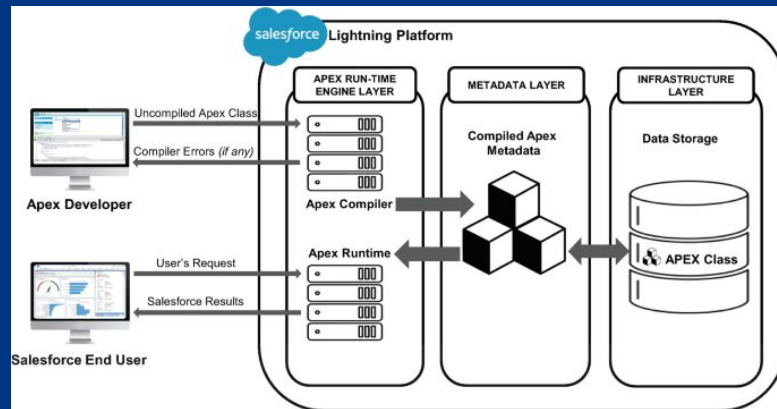
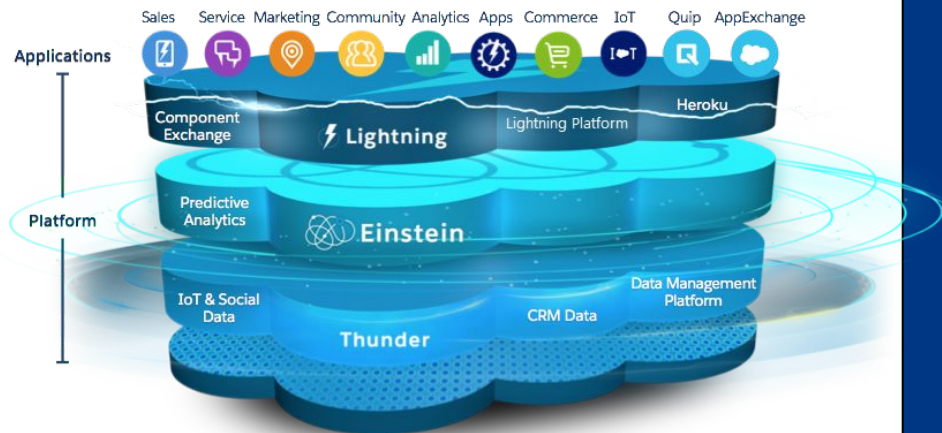


API  
Server



JSON

# What's Inside Salesforce



# What are we seeing?

- Authentication control in SFDC does not work in the way people think....
- Controlling user access and permissioning is hard
- Data Record Exposures, however, are super easy!
- Shield logs are powerful, but difficult to work with

# Authentication control in SFDC does not work in the way people think....



- Profile setting overrules org wide setting for SSO
- Profiles settings overrule org wide setting for password complexity
- SSO can be enabled org wide, but not enforced allowing easy bypassing
- IP restrictions are surprisingly easy to misconfigure

IP Restrict Request range overly permissive

[Summary](#) Remediation Feed

### Occurrence Details

|                                    |                                                       |
|------------------------------------|-------------------------------------------------------|
| <b>Status</b><br>Open              | <b>Last Found</b><br>An hour ago<br>24/01/2025, 10:46 |
| <b>Monitored Service</b>           | SFDC - Prod                                           |
| <b>Profile</b>                     | Global System Administrator                           |
| <b>Number of allowed IP ranges</b> | 3,204,382,462                                         |

Profile configured with

[Occurrences](#) Occurrence Summary High Severity Low Severity

Occurrences 1 - 6 of 6 < 1 > Export

Search admin Monitored Service Threads Environment

Status Open

Applied Filters: Search admin Status Open Clear (2)

| <input type="checkbox"/> | Risk | Monitored Service         | Profile                     | Status | Last Found                       | Due                              |
|--------------------------|------|---------------------------|-----------------------------|--------|----------------------------------|----------------------------------|
| <input type="checkbox"/> | High | SFDC - Prod<br>Salesforce | System Administrator        | Open   | An hour ago<br>24/01/2025, 10:46 | 2 years ago<br>14/11/2022, 09:33 |
| <input type="checkbox"/> | High | SFDC - Prod<br>Salesforce | Global System Administrator | Open   | An hour ago<br>24/01/2025, 10:46 | 2 years ago<br>10/05/2022, 05:27 |

## Why does this matter?

Weak authentication controls increase the risk of unauthorised access to critical business data, making it difficult to secure and verify user access effectively.

Let me see.

The background features a blue gradient with large, semi-transparent gear shapes. On the right side, there is a target graphic consisting of concentric circles and a central bullseye.

Time for a poll.....

# Controlling user access and permissioning is hard



Key recommendations to mitigate risk include

- Identify your most sensitive data objects. They're your crown jewels!
- Identify the RBAC elements with access to sensitive data and risky permissions, then monitor them for new user additions
- Make sure you understand exactly what perceived low privilege users (eg, digital experience portal members, junior staff members, external contractors) can see and do
- Continuously monitor access for these high risk users

**Access Explorer**  
Role: External One Prod Authenticated (testdrive+external1-prod-authenticated@appomni.com)  
Service: SFDC - Prod (Contains PHI, [+1 more](#))  
Scanned: 03/20/2024 at 03:44 PM  
[Choose Another Role](#)

Objects 22 Classifications 1 Permissions 22 Apex 402 SaaS-to-SaaS Apps 7

☒ Show System Objects ☐ Detail View

SEARCH FILTER BY SOURCE FILTER BY OBJECT TYPE

| Target Object                        | Field Access         | Accessible Records | Percent Accessible | Create | Read | Edit | Delete |
|--------------------------------------|----------------------|--------------------|--------------------|--------|------|------|--------|
| Account<br>account                   | <a href="#">View</a> | 202                | 100%               | —      | ✓    | —    | —      |
| Email Template<br>emailtemplate      |                      | 18                 | 100%               | —      | ✓    | ✓    | ✓      |
| Product<br>product2                  |                      |                    |                    | —      | ✓    | ✓    | ✓      |
| Document<br>document                 |                      |                    |                    | —      | ✓    | ✓    | ✓      |
| Achievement<br>redwing_achievement_c |                      |                    |                    | —      | ✓    | ✓    | ✓      |
| Attachment<br>attachment             |                      |                    |                    | —      | ✓    | ✓    | ✓      |

**External users with API access**

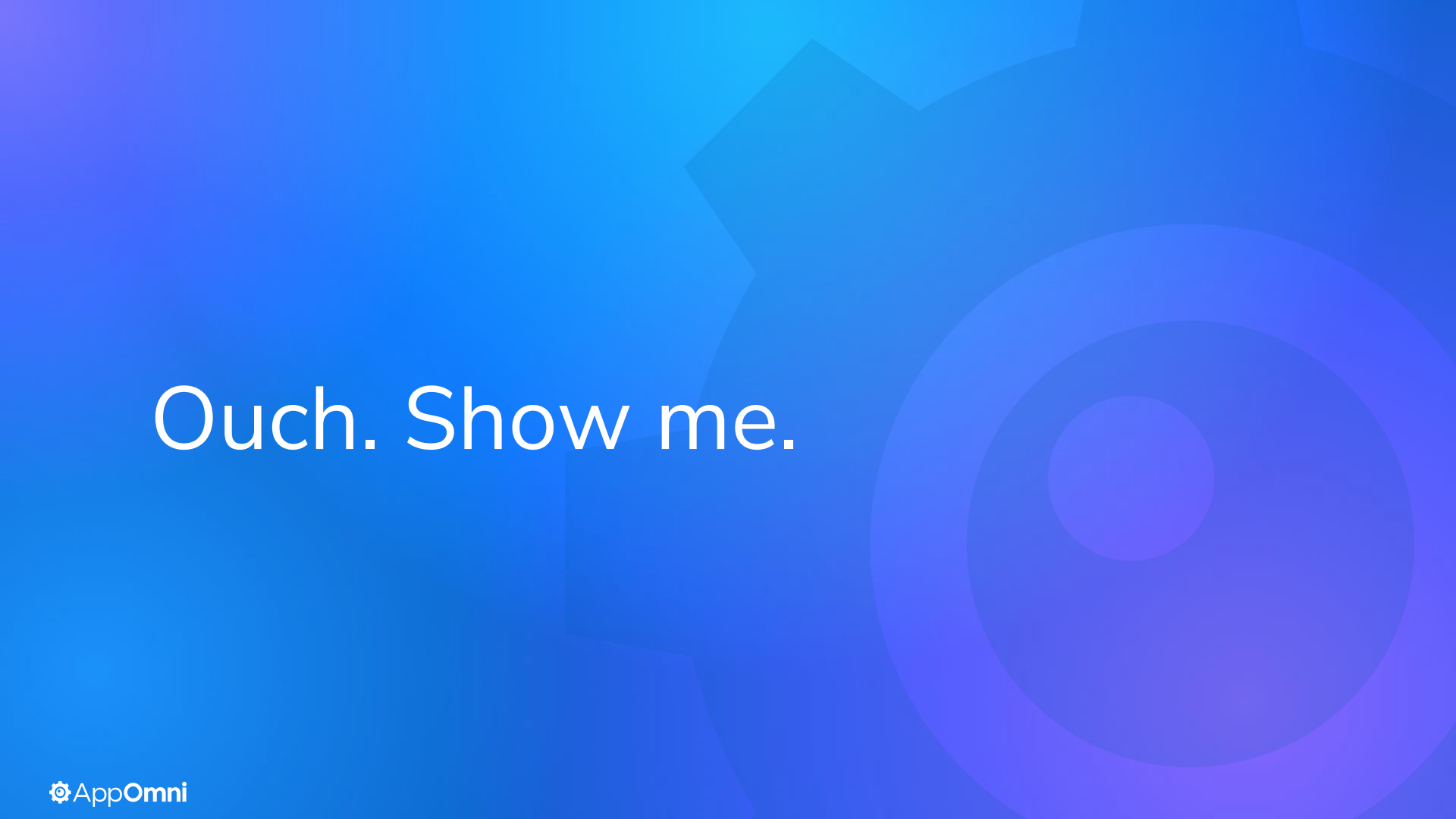
[Summary](#) Remediation Feed

**Occurrence Details** [Dismiss Occurrence](#)

|                          |                                             |
|--------------------------|---------------------------------------------|
| <b>Status</b>            | <b>Last Found</b>                           |
| Open                     | An hour ago<br>24/01/2025, 10:46            |
| <b>Monitored Service</b> | SFDC - Prod                                 |
| <b>External user</b>     | se+prod-external1-authenticated@appomni.com |
| <b>Permission label</b>  | permissionsapienabled                       |
| <b>Permission name</b>   | permissionsapienabled                       |

## Why does this matter?

Inefficient RBAC & Access Control management opens your tenant up to misuse, complicates compliance efforts and make it challenging to audit who has access to sensitive data.



Ouch. Show me.

The background features a blue gradient with large, semi-transparent gear shapes. On the right side, there is a target graphic consisting of concentric circles and a central bullseye.

Time for a poll.....

# Data Record Exposures, however, are super easy!

Key recommendations to mitigate risk include

- Make sure you are only exposing records you mean to expose from your digital experiences
- Monitor your logs for attempts to extract records by external actors
- Review external user access continuously to ensure it doesn't drift

The screenshot displays the 'Data records exposed to anonymous world' interface in Salesforce. It includes a navigation bar with 'Occurrences', 'Occurrence Summary', 'Insight Overview', 'Feed', and 'Preferences'. Below the navigation bar, there are filters for 'Monitored Service' (SFDC - Prod), 'Threads' (User (+1 selection)), and 'Environment' (Production (+4 selections)). A table lists occurrences with columns for Risk, Monitored Service, SObject, Record, Site, Status, and Last Found. A modal window titled 'Rule Details' is open, showing a rule for 'Potential Aura Exploitation by Guest User'. The rule description states: 'A guest user made a suspicious request to an Aura endpoint that might indicate sensitive records are accessible in a Salesforce Community.' The severity is 'Medium' and supported services include 'Salesforce'. The rule triggers when all of the following conditions occur in 1 minute(s): user.roles contains Guest, tags does not contain appomi\_source, labels.action\_message contains ui.force.components.controllers.lists.selectableListDataProvider.SelectableListDataProviderController/ACTION\$getItem, with identical values for the following fields: user.name, source.ip. When this detection rule is triggered, it won't trigger again for 1080 minute(s).

## Why does this matter?

Monitoring for data exposures in Salesforce is crucial to protect sensitive customer information, ensure compliance with regulations, and prevent potential security breaches.

The background of the slide features a blue gradient. On the right side, there are faint, semi-transparent graphics: a large gear and a target symbol with concentric circles. The text "Oh good! Let me see." is centered in a white, sans-serif font.

Oh good! Let me see.

The background features a blue gradient with large, semi-transparent gear shapes. On the right side, there is a target graphic consisting of concentric circles and a central bullseye.

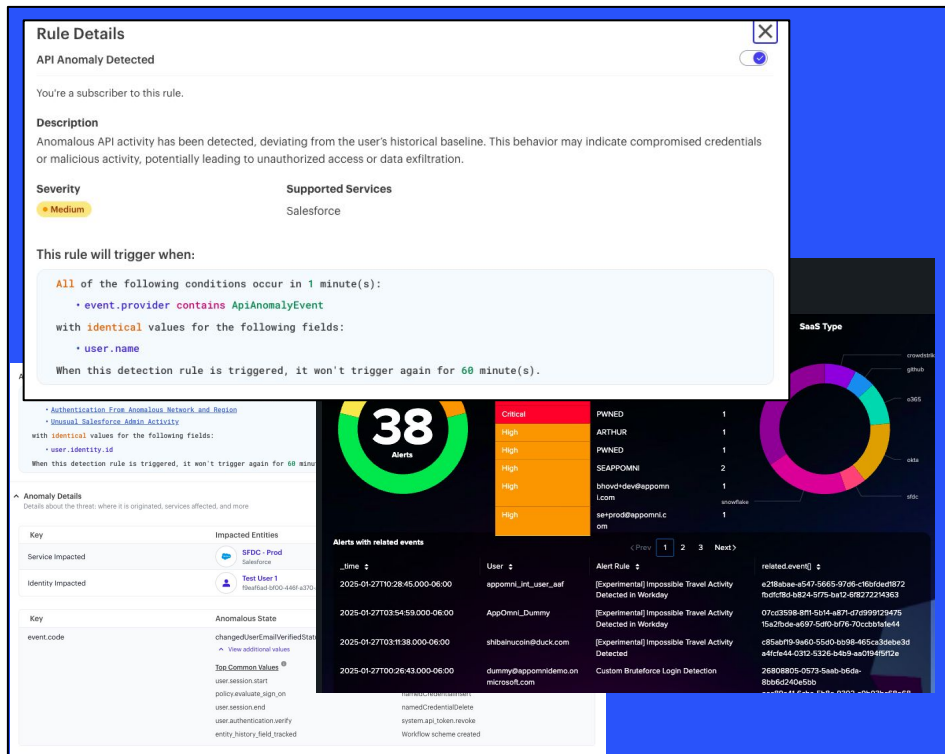
Time for a poll.....

# Shield logs are powerful, but difficult to work with



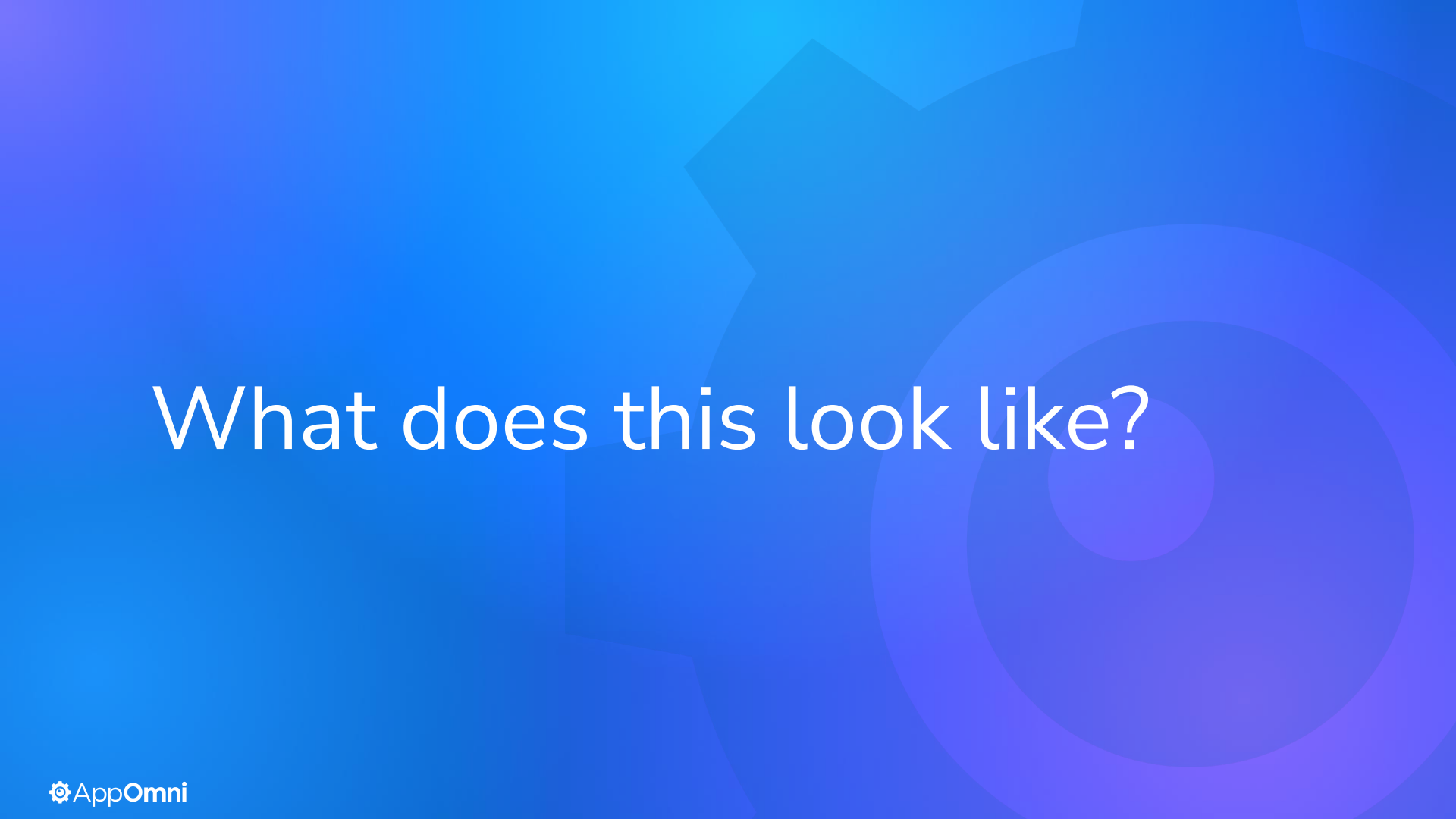
Key recommendations to mitigate risk include

- Monitor for excessive Workbench downloads
- Baseline your users then monitor for anomalous API usage
- Monitor for credentials stuffing attacks for profiles without SSO
- Pull your Salesforce logs in to your SOC tools for enrichment



## Why does this matter?

Comprehensive analysis of Shield logs enables early detection of security threats and improves incident response times.

The background features a blue gradient with large, semi-transparent gear shapes. One gear is prominent in the upper right, and another is partially visible in the lower left. A series of concentric circles is also visible on the right side of the image.

# What does this look like?

The background features a blue gradient with large, semi-transparent gear shapes. On the right side, there is a target graphic consisting of concentric circles and a central bullseye.

Time for a poll.....

# Questions

Prevent SaaS Data Breaches

---

# Recap & Next Steps

Prevent SaaS Data Breaches

---

# Recap & Next Steps

- **SaaS has introduced new security challenges**
  - Traditional tools and techniques aren't effective or available
  - This is no longer a human solvable problem
- **Salesforce Security Takeaways**
  - Data leakage is widespread and over provisioned access is everywhere
  - Authentication is hard and needs constant attention
  - Shield Logs are invaluable, but difficult to work with out of the box
- **Upcoming Workshops**
  - 13th February - ServiceNow

# Join another workshop or share with a colleague

[www.appomni.com/workshops](https://www.appomni.com/workshops)



**Tim Gibbs**

Sales Director  
tgibbs@appomni.com



**Rob Gregg**

Senior Solutions Engineer  
rgregg@appomni.com