AppOmni

SaaS Security 101 Workshop

Securing 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

Maturity

Shadow IT → Critical Infrastructure

Usage

100+

SaaS apps per organization[1]

Growth

18.7%

CAGR[2]

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% (2023) ↗ **31%** (2024)

Breaches

Increased by 5 points
from last year

71% (2023) ↗ **75%** (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

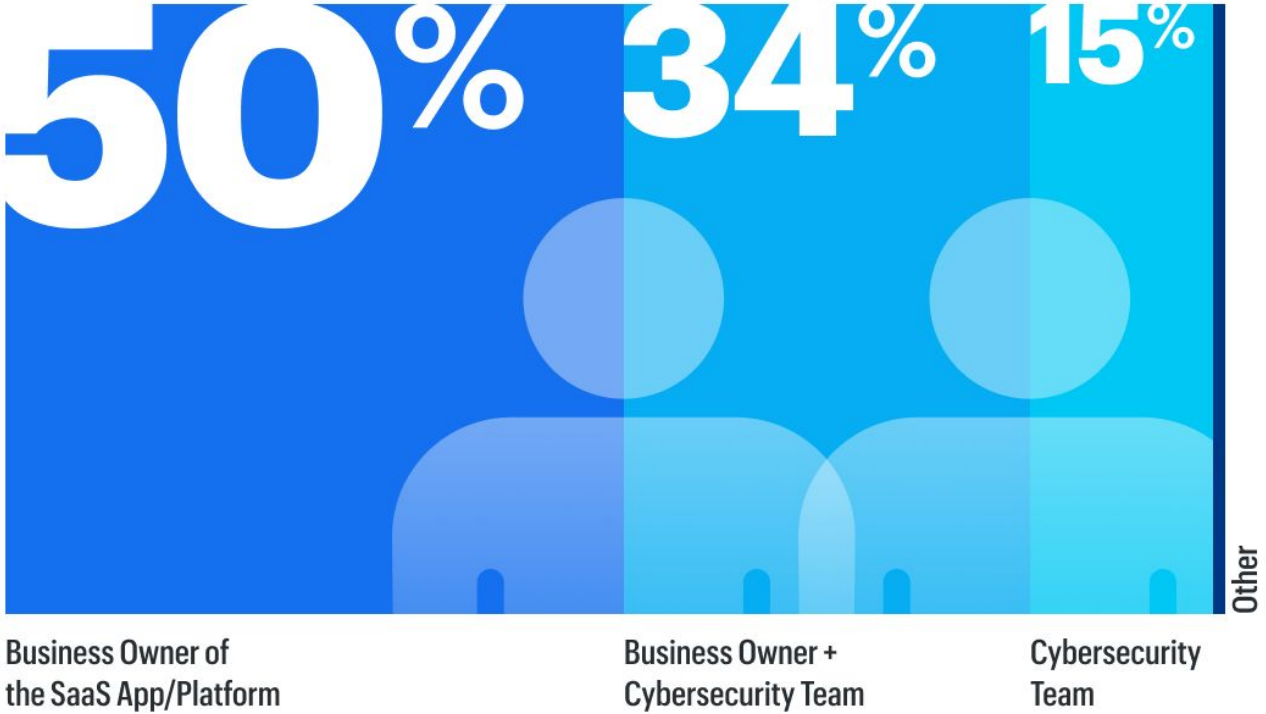
Expand

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



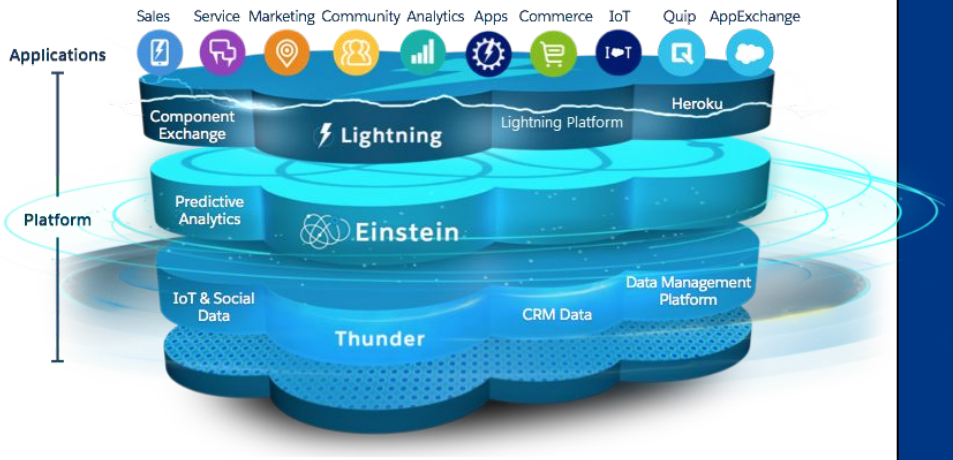
Time for a poll!

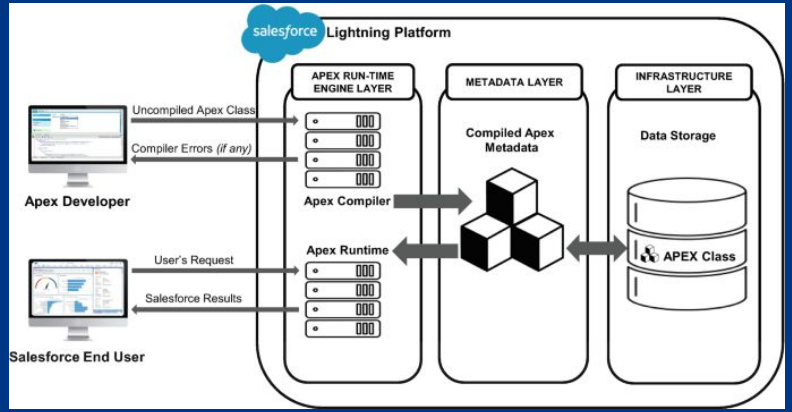
Securing Salesforce

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



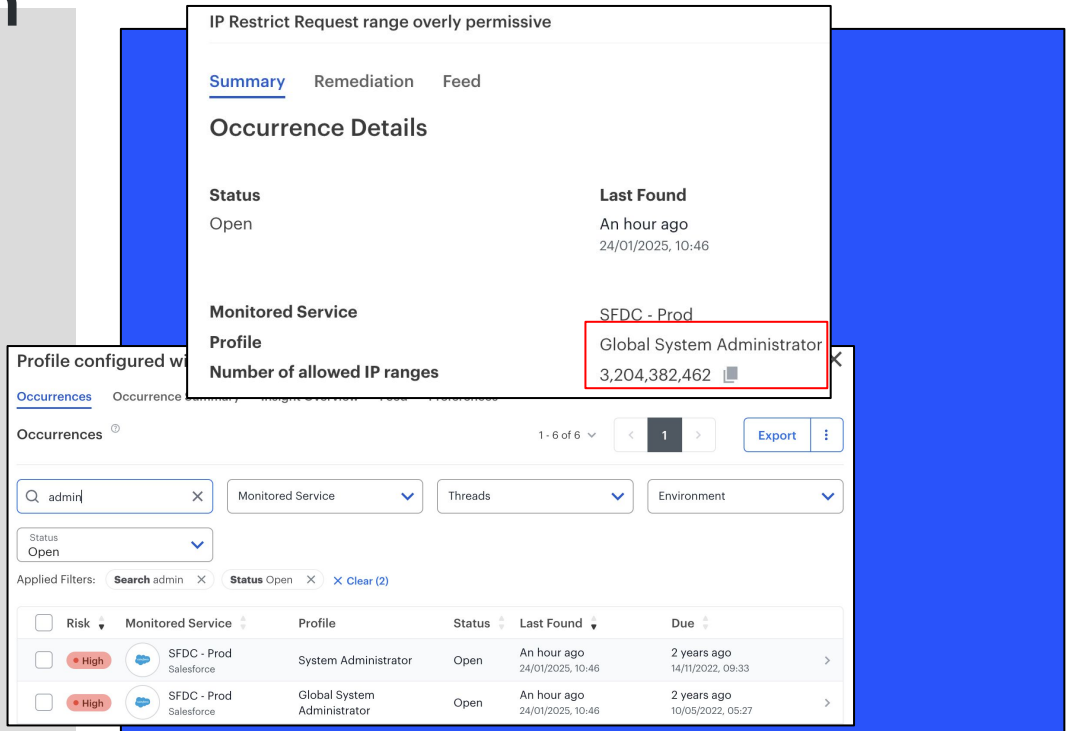


What are we seeing?

- **Authentication control in SFDC does not work in the way people think....**
- **Controlling user access and permissioning is 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 over rules 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



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.

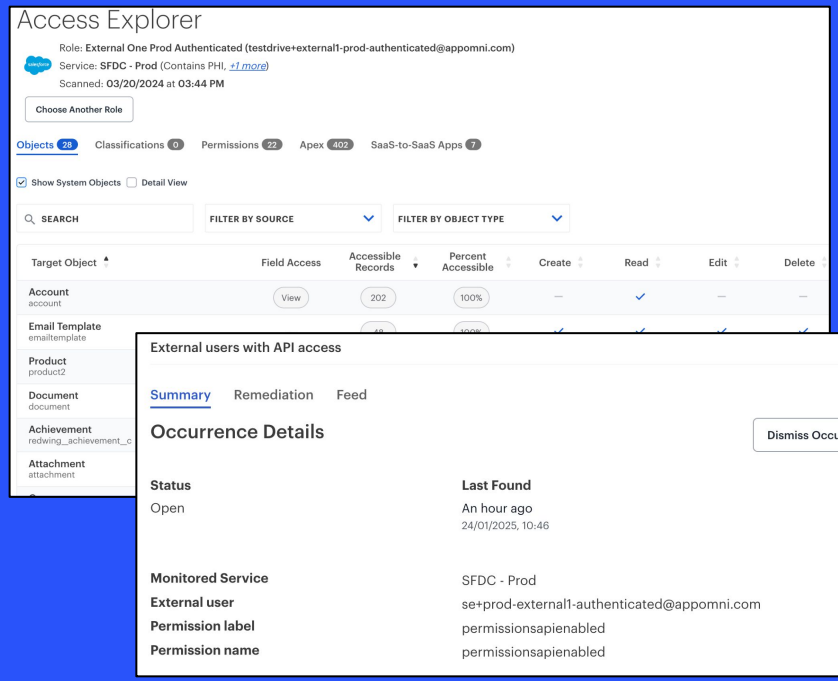
Time for a poll.....

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



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.

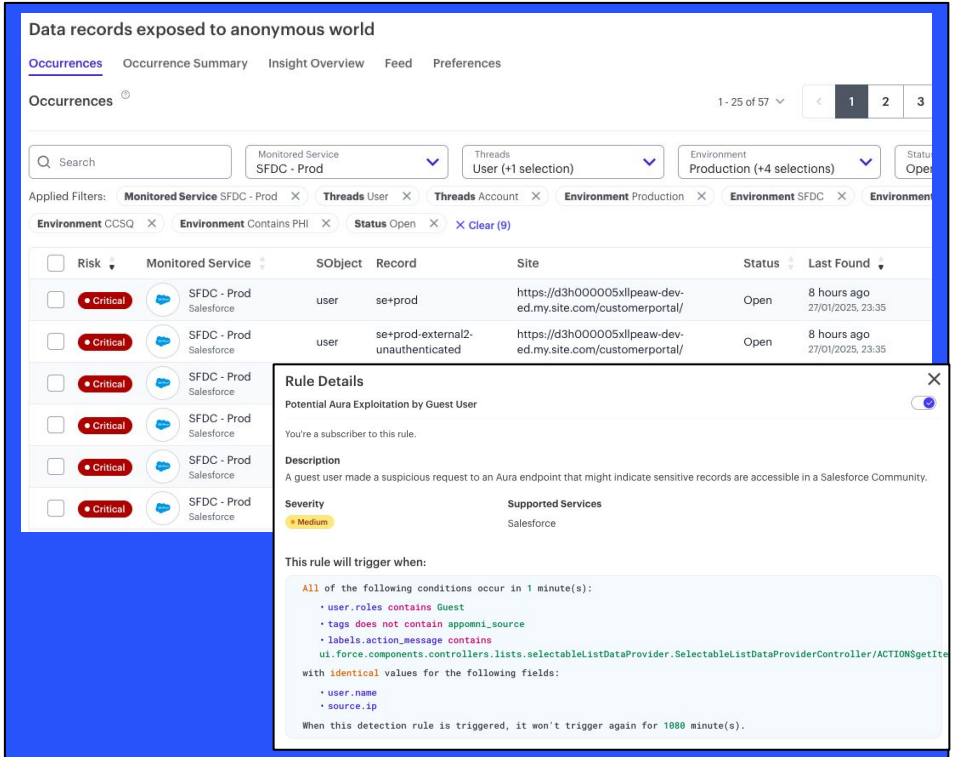
Ouch. Show me.

Time for a poll.....

Data Record Exposures, however, are super easy!

Key recommendations to mitigate risk include

- Make sure you 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



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.

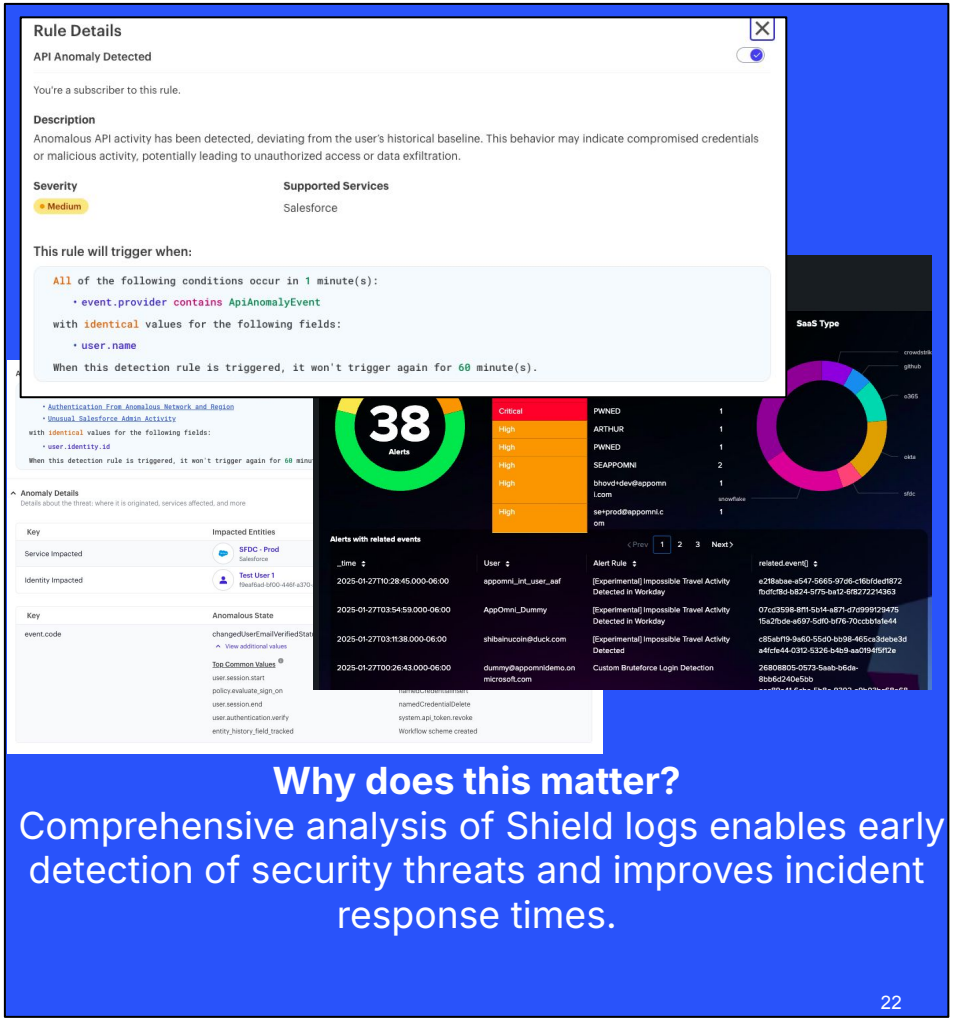
Oh good! Let me see.

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.

What does this look like?

Time for a poll.....

AppOmni

Questions

Prevent SaaS Data Breaches

AppOmni

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

https://www.turnberrysolutions.com/salesforce-and-the-shared-responsibility-model/

AppOmni

Join another workshop or share with a colleague

www.appomni.com/workshops

Prevent SaaS Data Breaches

AppOmni

Tim Gibbs

Sales Director
tgibbs@appomni.com

Rob Gregg

Senior Solutions Engineer
rgregg@appomni.com

Prevent SaaS Data Breaches