AppOmni

SaaS Security 101 Workshop

Securing Salesforce

Prevent SaaS Data Breaches

Agenda/Format

Topics to teach and questions to get answered

SaaS Security Overview

- *Transition to SaaS and related security challenges.*

Salesforce Security Deep Dive

- *Common Salesforce security challenges and misconfigurations*
- *Demos shown mixed into content*

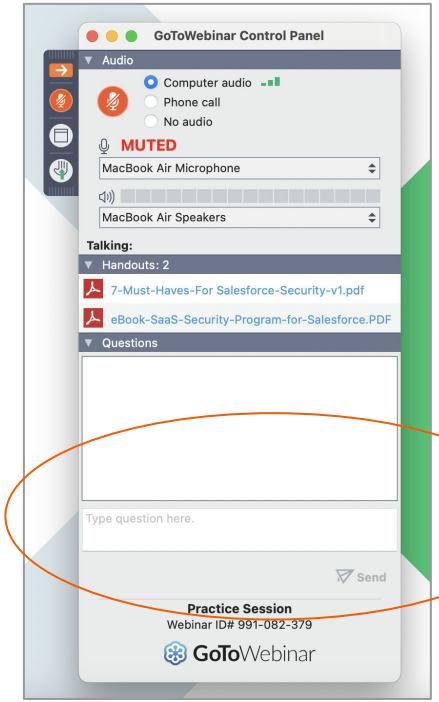
Q&A

- *Throughout the workshop we have time for questions and clarifications.*
  Please put questions into the questions panel and we will address them along the way.

Recap & Next Steps

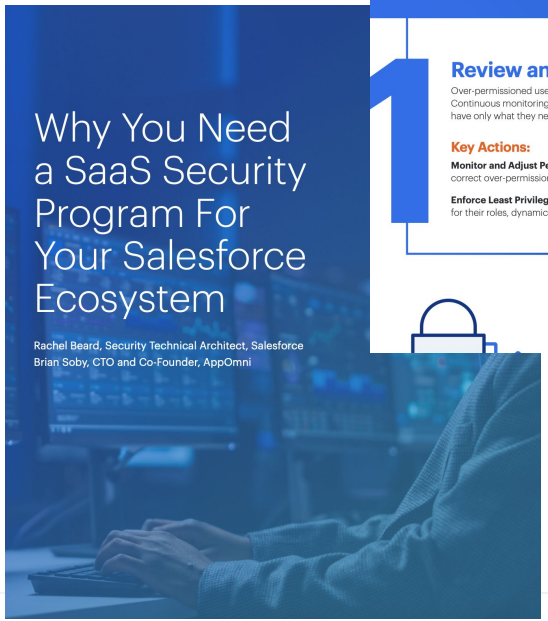
- *Recap of the essentials and what's on the horizon for skill-building.*
  Invite to join another workshop or share with a colleague

GotoMeeting navigation



Handouts

?



Where Does Your Most Critical Data Live?

In Your Laptop?

In a Cloud Database?

Or In SaaS Apps?

78% | Organizations storing sensitive data in SaaS[1]

1. DevSquad - SaaS Statistics and Trends for 2024

Business has Moved to SaaS

Modern organizations have shifted **(70-90%) of their business processes** to SaaS platforms to enhance agility, scalability, and security.

SaaS Usage Growth:

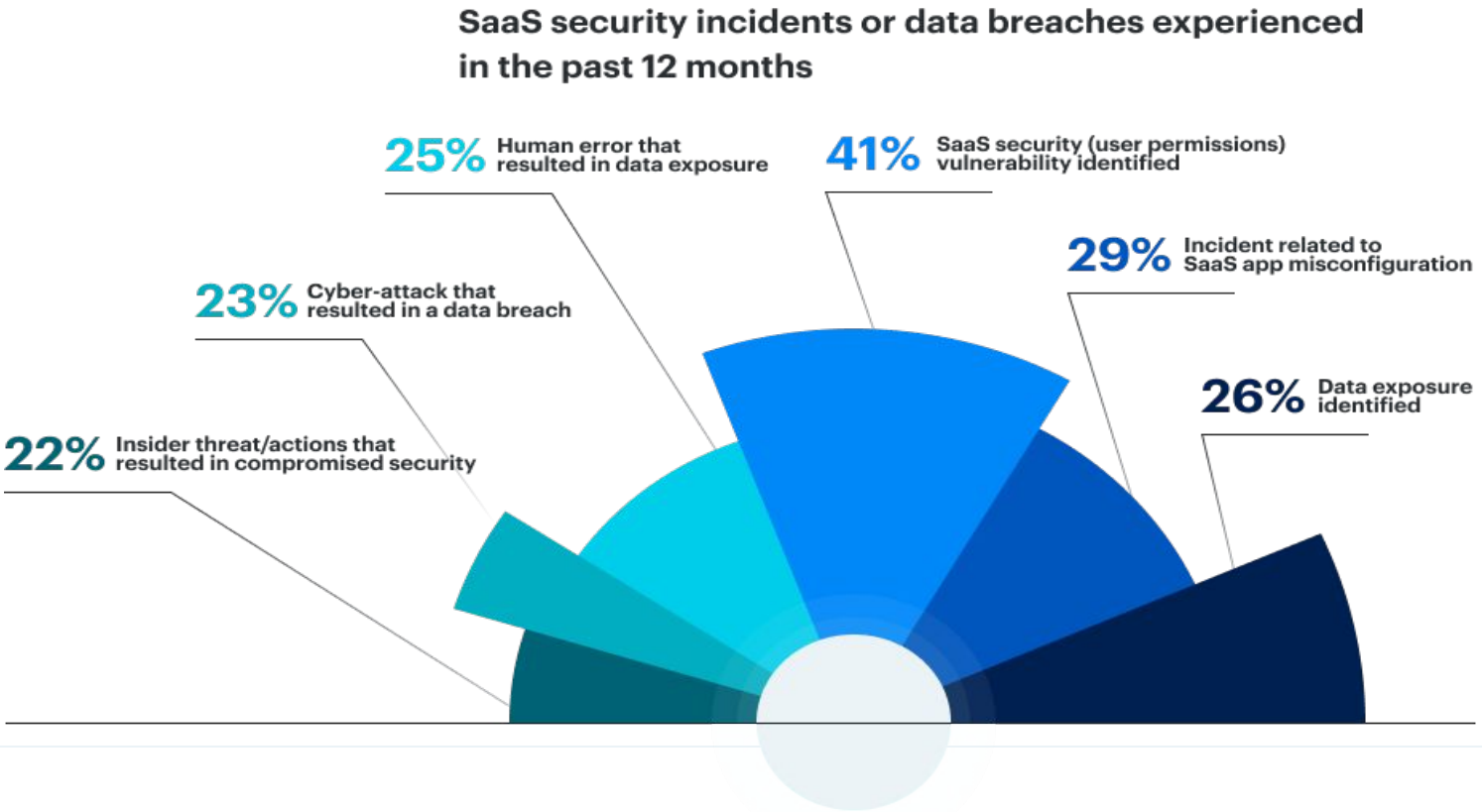
- The average company now uses **200 to 600 SaaS applications**, up from **16 in 2017**.
- Large enterprises may manage thousands of SaaS applications across business units.

Function-Specific SaaS Adoption:

- **Collaboration & Communication**: (Slack, Microsoft 365, Google Workspace)
- **HR & Payroll**: (Workday, ADP, Rippling, BambooHR)
- **Finance & ERP**: (NetSuite, SAP, Bill, QuickBooks Online)
- **CRM & Sales**: (Salesforce, HubSpot)
- **Security & Identity**: (Okta, Microsoft Entra ID, Ping, 1Password, Crowdstrike)

AppOmni State of SaaS Security 2025 Report

AppOmni State of SaaS Security 2025 Report



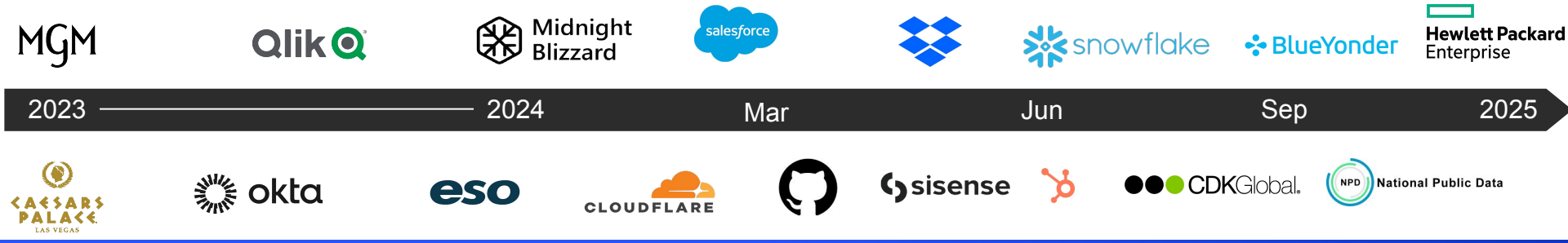
Legacy Attack Surface & Kill Chain

- Recon Target
- Check perimeter for vulnerabilities
- Recon / Spearphish weak users
- Drop foothold / establish C2
- Upgrade foothold to full malware kit
- Recon internal network
- Move lateral / privilege escalate
- Repeat as needed
- Action on objectives

Modern Attack Surface & Kill Chain

- Acquire IdP account
  - Cred Spray / Stuff / Buy, Phish, AiTM, MFA Push bomb, Steal tokens, Misconfigured SaaS
- Post Auth SaaS Recon
  - Doc Repo, Chat, PassVault, SaaS apps, Directories, Meetings, etc...
- Privilege Escalate
- IaaS, PaaS, Legacy Network
- Action on objectives

More data than ever stolen from SaaS



1B+ individuals impacted by major SaaS breaches in 2024[1]

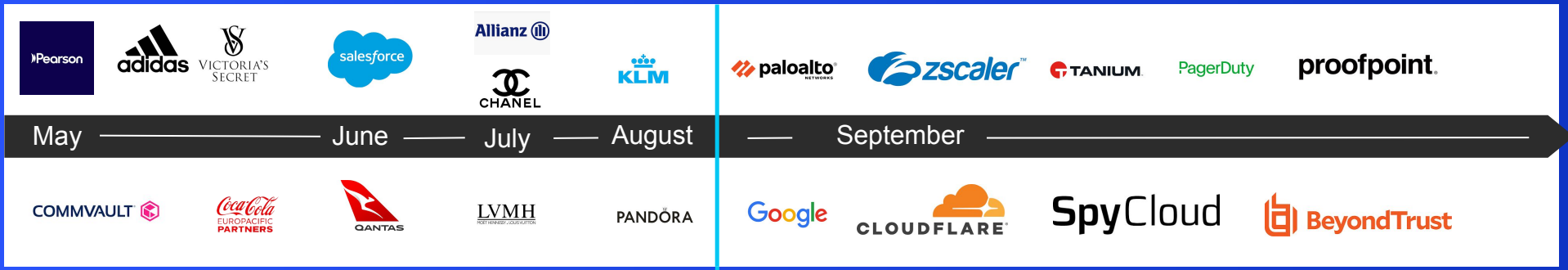
49% of organizations don't have full visibility into their SaaS applications[2]

7B+ Records exposed from data breaches in the first half of 2024[3]

UNC6040 & UNC3944

1. Anonyme Labs 2024 Data breaches.
2. AppOmni - State of SaaS Security Report
3. Jumpcloud - 2024 Cyber Trends

In the 2025 ‘Summer of breaches’, they exploded



At the heart of this initial surge were two prolific threat groups:

ShinyHunters (UNC6040)
Scattered Spider (UNC3944)

Despite distinct playbooks, both groups exploit the same systemic SaaS weaknesses

The result? Organizations across all industries suffered SaaS breaches

700+

Companies affected

A new bad guy in town - **UNC6395**

Using nation-state sophistication to automate a widespread attack affecting over 700 companies worldwide.

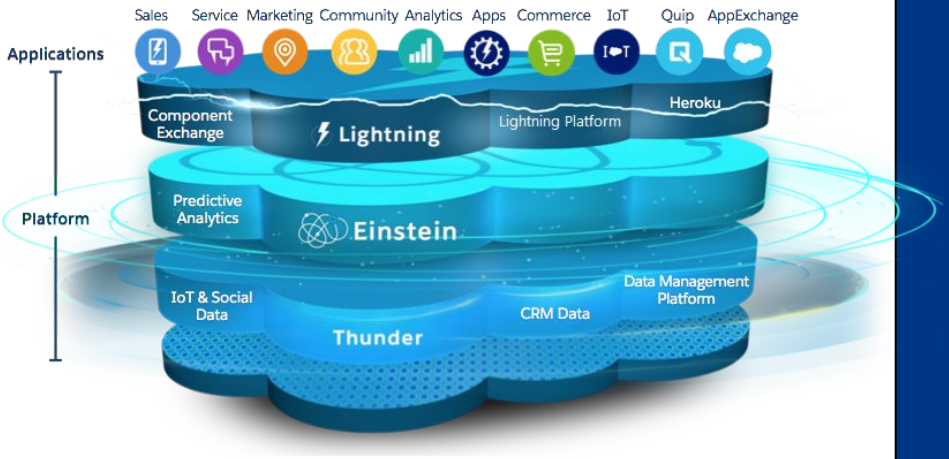
The latest example of SaaS supply chain attacks, where trust in one connected app can open the door to broader data exposure

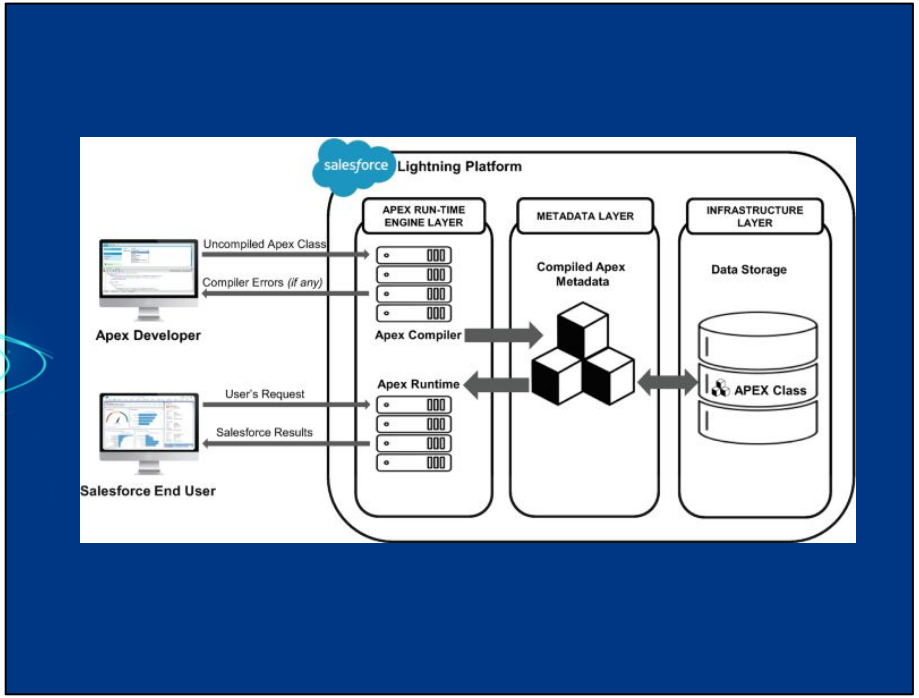
Securing Salesforce

What's Inside a SaaS App?

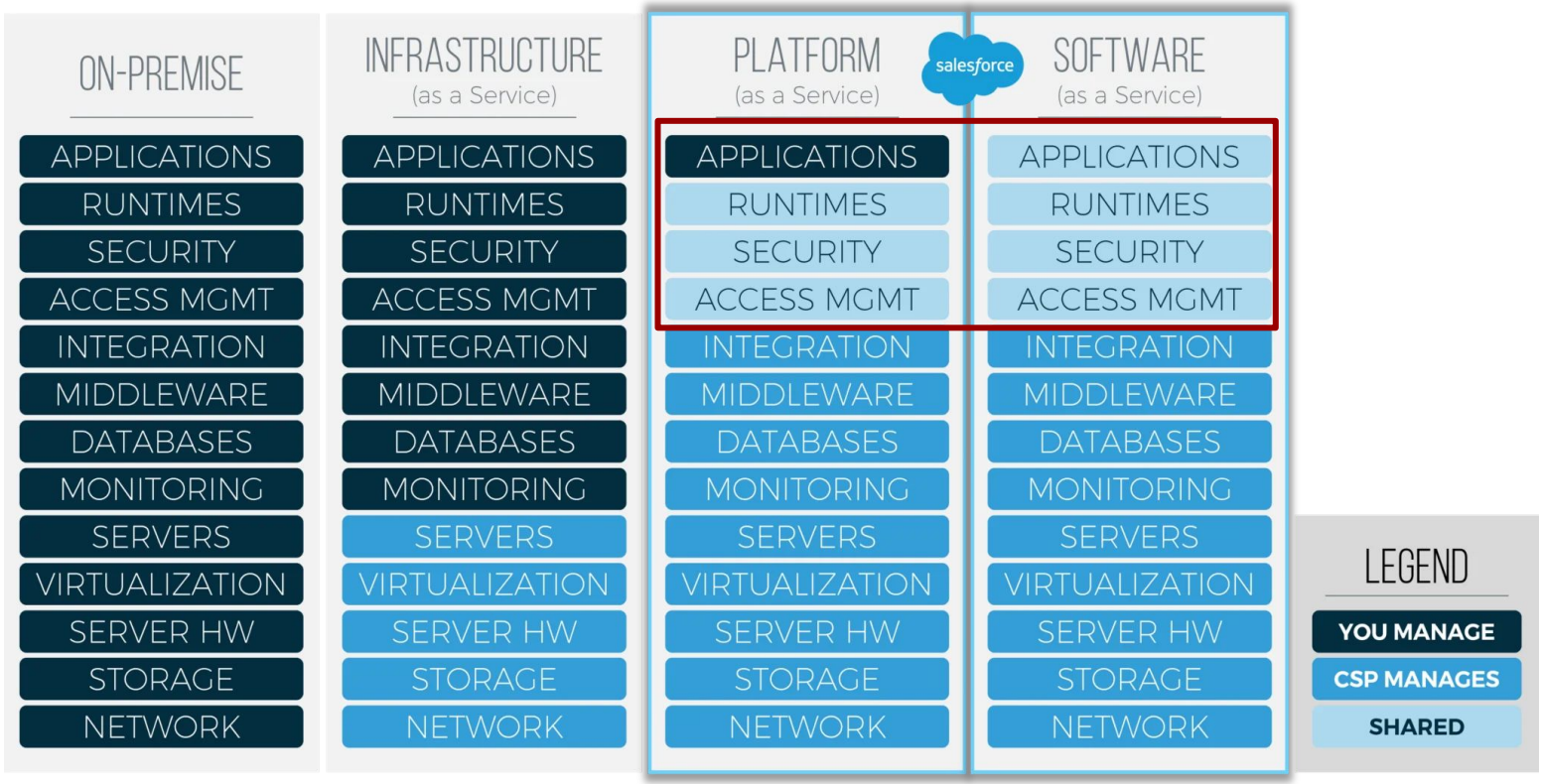
App Server
Database Server
Web Server
Indexing Server
XML
Mail Server
Content Rendering
Load Balancer
Indexing & Reporting
API Server
JSON

What's Inside Salesforce





Shared Responsibility



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

Top 4 Salesforce Security Concerns

- **Data Record Exposures**
  - *Is there any data exposed to the Internet?*
- **Misconfigurations**
  - *Are we compliant with policy?*
- **Third-party Applications**
  - *Do we understand what integrations are installed and the risk they pose?*
- **Activity Anomaly Detection**
  - *Can we identify and respond to risky events?*

AppOmni

Live Demo

Prevent SaaS Data Breaches

AppOmni

SaaS Security Program Sample Workflow

Prevent SaaS Data Breaches

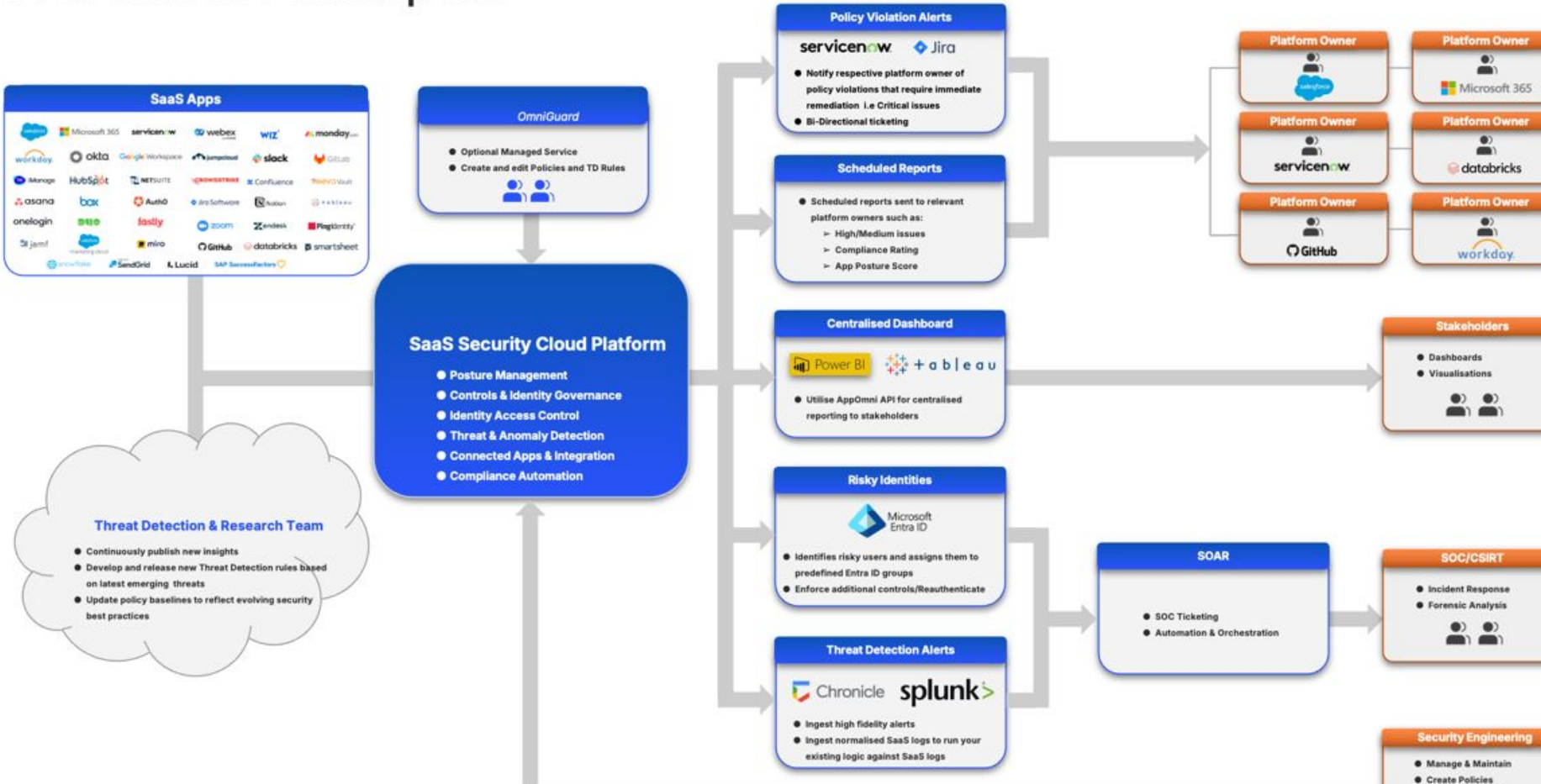
Typical Roles & Responsibilities

Persona	Primary Responsibilities	AppOmni Access Level	RBAC Permissions
Platform Owner	• Remediate Policy Violations & Misconfigurations • Receive Bi-directional tickets from ServiceNow including full remediation guidance	**Respective SaaS apps only**	**View**
SOC/CSIRT	• Investigate threat detection alerts within SIEM/SOC • Investigate risky identities • View, create and edit detection rules within AppOmni platform if required	**Threat Detection and Identities**	**View, Edit, Create**
Security Engineer	• Manage and maintain AppOmni platform • Access all findings, policies and insights • View, create and edit policies and rules	**Full AppOmni Platform**	**View, Edit, Create**
Stakeholders	• Metrics, reports and dashboards to be accessed within PowerBI, Tableau etc. • Optional access to AppOmni platform if required	**None** **(Optional Access if required)**	**View** **(Optional)**

Alerting & Notification Examples

Recipient	Alert Type	Alert Examples	Method Received	Suggested Frequency
Platform Owner 	**Policy Violations & Misconfigurations**	• SSO disabled • MFA disabled • Data Records Exposed • IP range restrictions include IP's outside of configured global trusted networks • Too many users with admin permissions	servicenow Jira Microsoft Teams slack	**Fully automated and customisable alert notifications** Critical - Immediate High - Daily Medium - Weekly Low - Never
SOC/CSIRT 	**Threat Detection & Risky Identities**	• Unusual Admin activity from an anomalous location • Admin MFA modified from an anomalous network location • Successful login from newly observed IP address after many failures • Activity from known Tor IP address	Microsoft Sentinel Chronicle splunk>	Critical - Immediate High - Daily Medium - Weekly Low - Never

Workflow Examples



AppOmni

Questions

Prevent SaaS Data Breaches

AppOmni

Recap & Next Steps

Prevent SaaS Data Breaches

Key Takeaways

Identify

- Know all SaaS in use
- Know the interconnects
- Know the users
- Know the data
- Know their criticality

Protect

- Conduct VRA
- Understand your current risk
- Harden tenant posture
- Maintain posture state

Detect

- Posture change
- Config drift
- New Interconnects
- Anomalous behavior
- Threat Intel Matches
- New Unsanctioned SaaS
- New Connected Apps

Respond

- Integrate into SIEM
- Integrate into XDR
- Integrate into MDR
- Integrate IR Process

Recap & Next Steps

- **SaaS Security has introduced new challenges**
  - Traditional tools and techniques aren't effective or available
  - Condensed kill chain
- **Salesforce Security Takeaways**
  - Common data leakage and over provisioned access
  - Compliance Challenges
  - Effective detection of threat activity
- **Upcoming Workshops**
  - 01/21/2026 - ServiceNow

AppOmni

Join another workshop or share with a colleague

www.appomni.com/workshops

Prevent SaaS Data Breaches