



WELCOME

How enterprise SaaS apps may be leaking your data to 3rd parties—and how to get it under control



Boris Sieklik (borisinfosec@proton.me)

Senior Director, Information Security

MongoDB

16 June 2023



Agenda

Different Risk levels for SaaS applications

How can SaaS applications interconnect

Interconnected mesh = new supply chain headache

Custom integrations and example data leakage

SaaS clouds



Large SaaS providers





Google Security spend

2 Billion a year

These can be considered really mature companies

Salesforce Customers

150 000+

Spending large resources on security

Key point - there is lot of TRUST in their security

Slack security certificates

15+

Medium Size SaaS



Little bit lesser known but used by many corporations, e.g. payroll provider

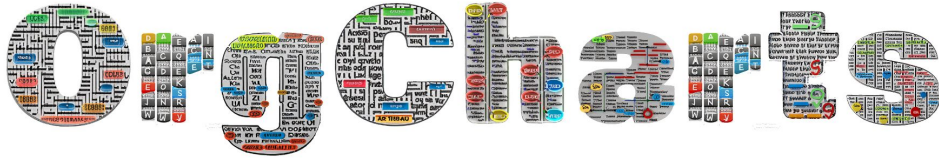
Decided not to name :-)

Is it fair to assume they spend less on security?

I think we can assume so



Small scale SaaS providers



Cool open source CI/CD tool



Security spend

Unknown (~Low)

These companies may not have mature security processes

Number of employees

Low (~50)

Questionable security spend

Lack of security certifications

Security certificates

Minimal (~1)

Key point - higher risk that top tier SaaS apps



Takeaway

Level of Risk

Not all SaaS clouds are equal in maturity
and associated risk



Why do we care?
Surely data in
these clouds is
isolated?



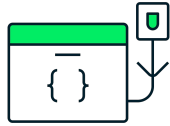
Integrations / Network of SaaS Clouds



These SaaS Clouds connect to each other



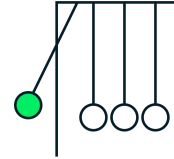
API integrations
(OAuth)



3rd party
marketplaces

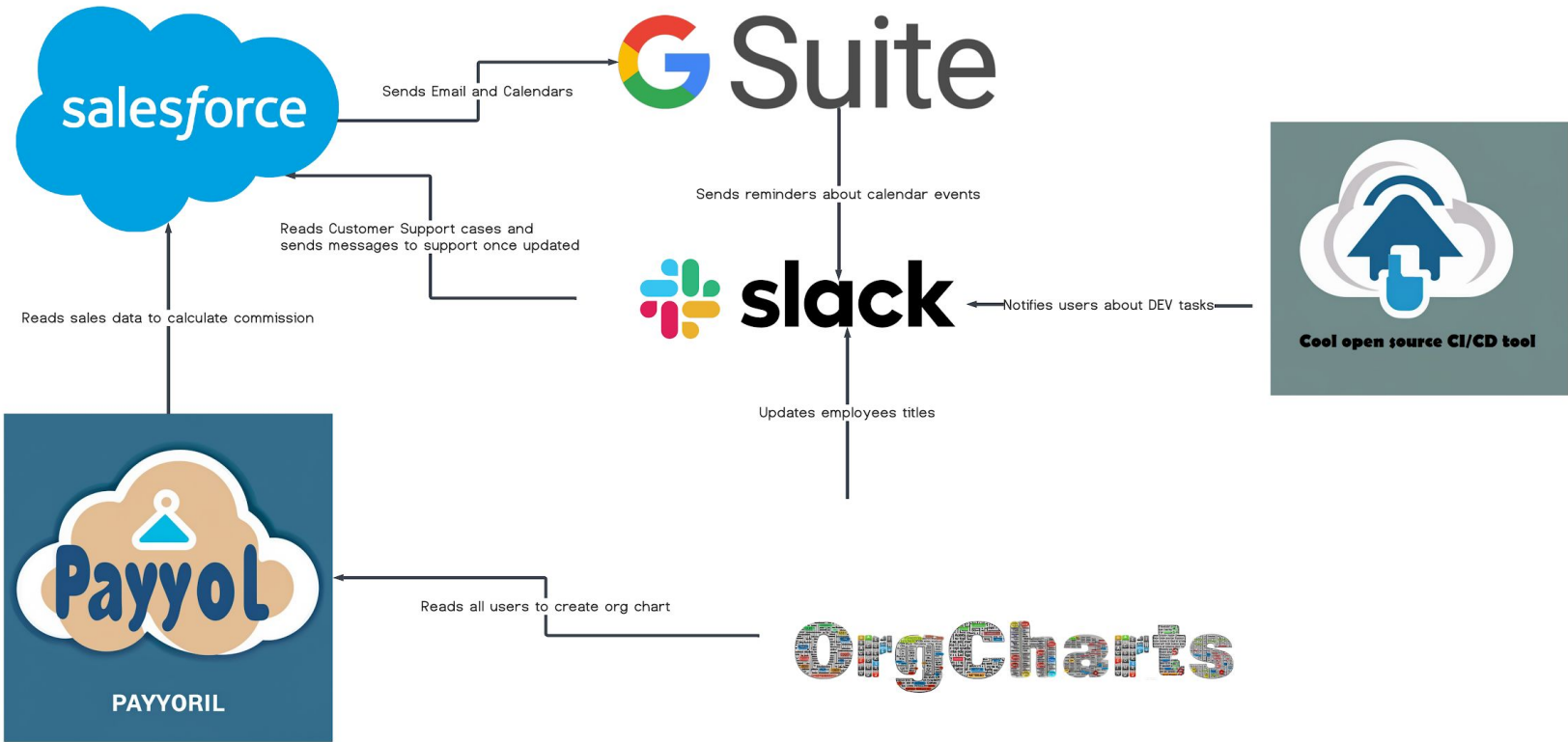


Webhooks

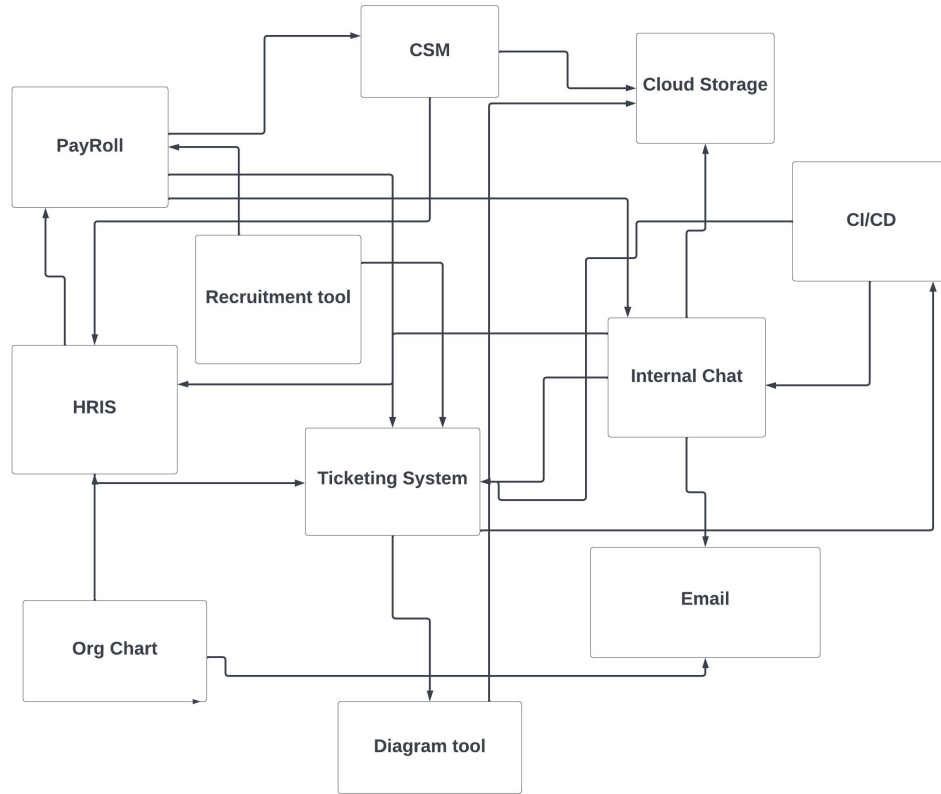


Custom methods

It's an interconnected Mesh

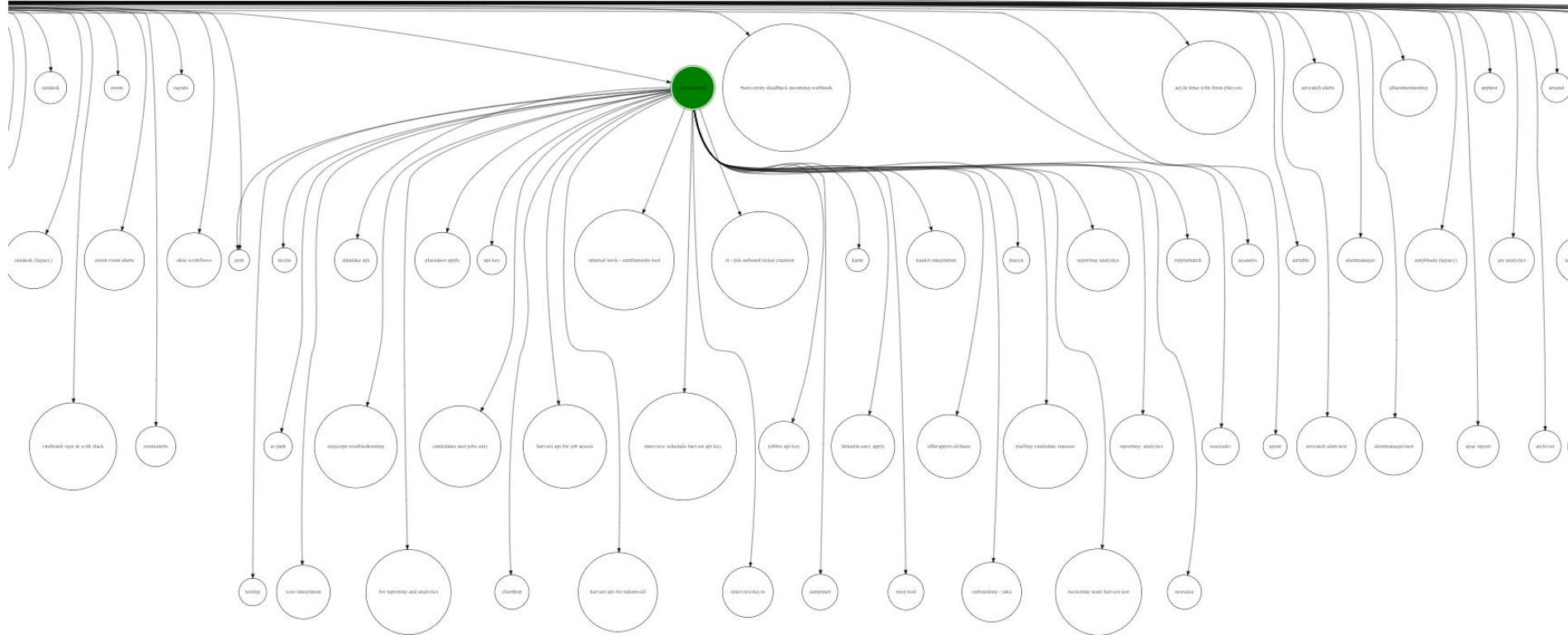


What if we add few more SaaS clouds?

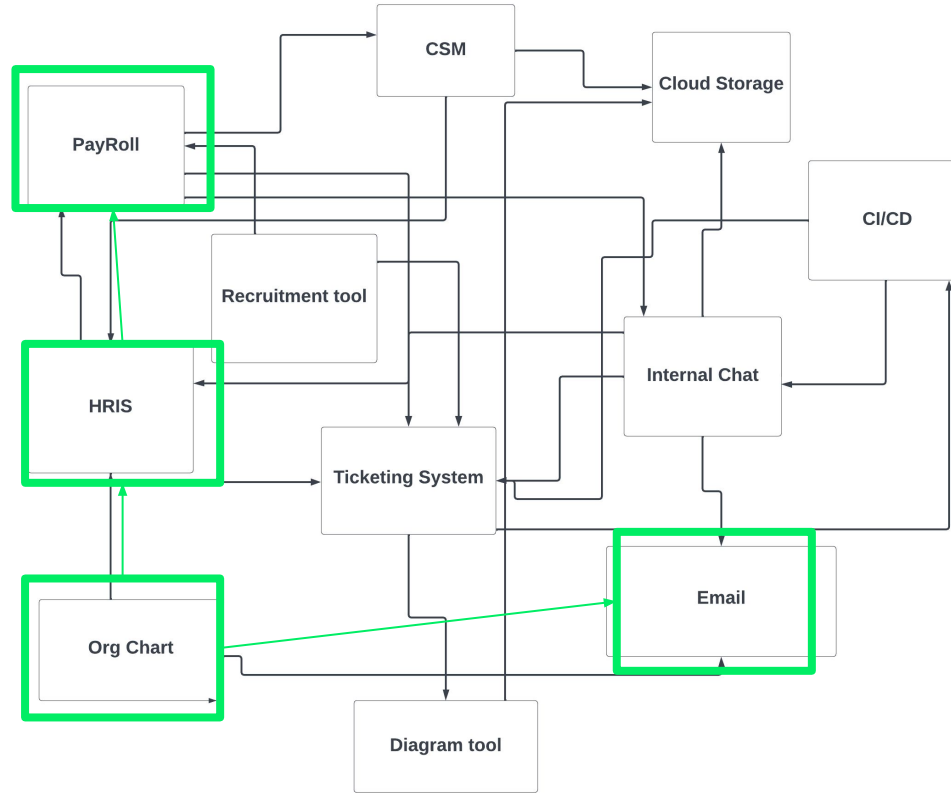




What does it look like when you have 200+ SaaS apps?



Example Attack Pattern





Takeaway

Complexity

Adding a few clouds rapidly increases complexity = more risk

Larger attack surface

How can security teams track these connections?



Takeaway

Interconnected
SaaS apps are a
supply chain risk
and a security
nightmare

Technical problems with integrations

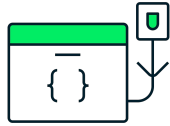




Technical problems with integrations



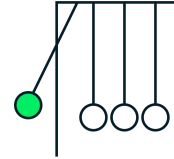
API integrations
(Oauth)



3rd party
marketplaces



Webhooks



Custom methods



Takeaway

Problems with Oauth

Permissions are approved as a bundle

You approve sets of permissions not individual scopes

Hard to know what permissions mean

Difference in access can be significant

<https://www.googleapis.com/auth/drive.file> vs
<https://www.googleapis.com/auth/drive>

No standard for permission categories

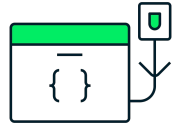
Each SaaS app has its own naming conventions and categories



These SaaS Clouds connect to each other



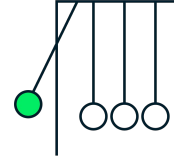
API integrations
(OAuth)



3rd party
marketplaces



Webhooks



Custom methods

So many Marketplaces



appexchange



Google Workspace Marketplace



MarketPlace examples

Reference:

<https://twosixtech.com/api-privacy-a-look-at-g-suite-marketplace-permissions-and-policies/>

Sign in with Google

ezShared Contacts wants to access your Google Account

This will allow **ezShared Contacts** to:

- Read, compose, send, and permanently delete all your email from Gmail
- See, edit, create, and delete all of your Google Drive files
- View users on your domain
- See, edit, download, and permanently delete your contacts
- See, edit, create, and delete your spreadsheets in Google Drive
- Connect to an external service
- Allow this application to run when you are not present
- View and manage data associated with the application
- Display and run third-party web content in prompts and sidebars inside Google applications

Make sure you trust ezShared Contacts

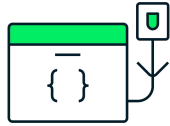
You may be sharing sensitive info with this site or app. Learn about how ezShared Contacts will handle your data by reviewing its [terms of service](#) and [privacy policies](#).



These SaaS Clouds connect to each other



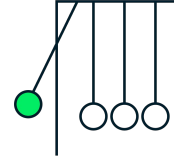
API integrations
(OAuth)



3rd party
marketplaces



Webhooks



Custom methods



Interconnected SaaS apps are a supply chain nightmare

Risk

If any part of mesh is compromised this significantly increases data leak risks and hacks

Limited visibility

Extremely hard to list all connections from all SaaS clouds - how do we secure what don't know?

Permissions

No standard for permissions, hard for security teams to understand access levels



What can we do to lower the risk?

Discovery

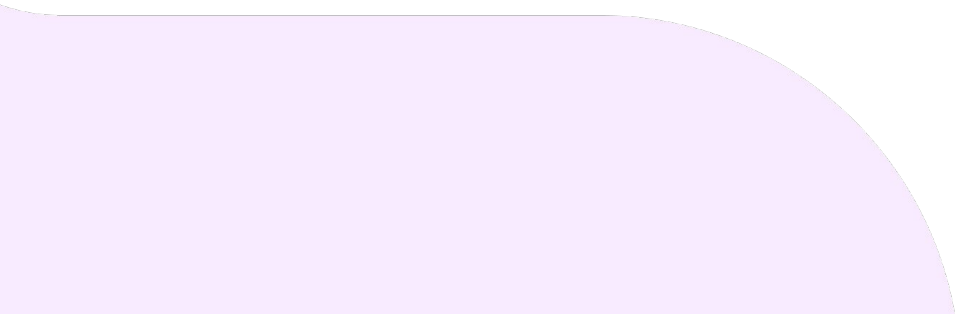
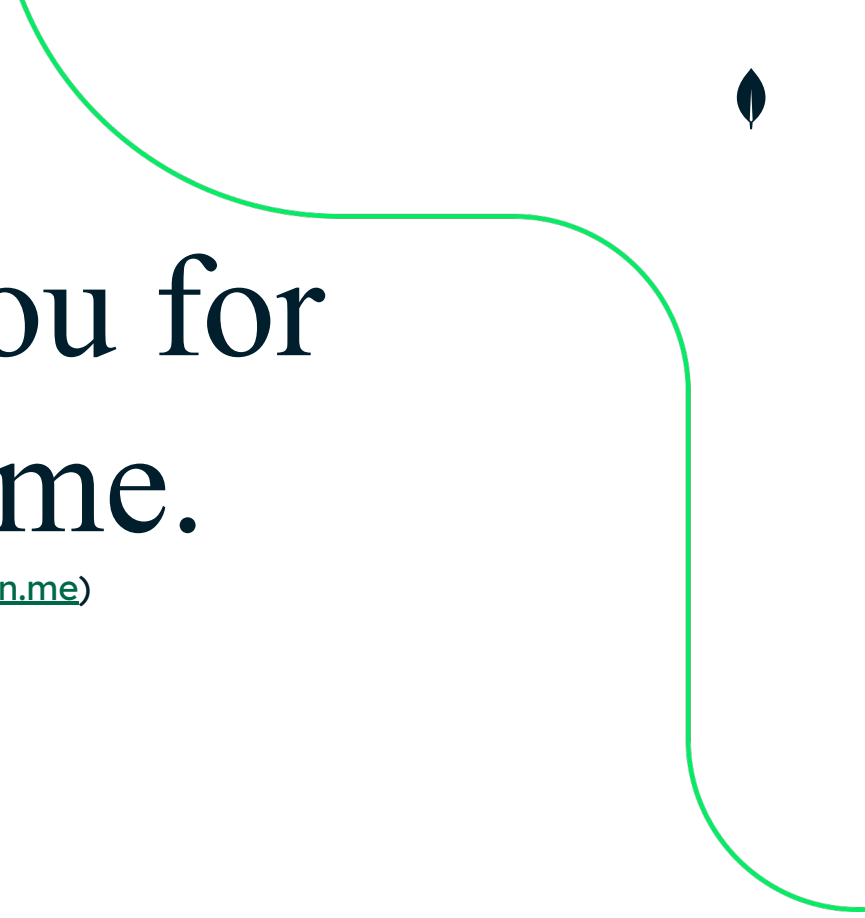
Know which SaaS apps you really have and how they connect to each other

Process

Have a process for approving and listing new connections. Make sure business understand the risk

New standard? (controversial)

We may need new standard to replace Oauth and these incoinstences



Thank you for
your time.

borisinfosec@proton.me