

COVER YOUR SAAS

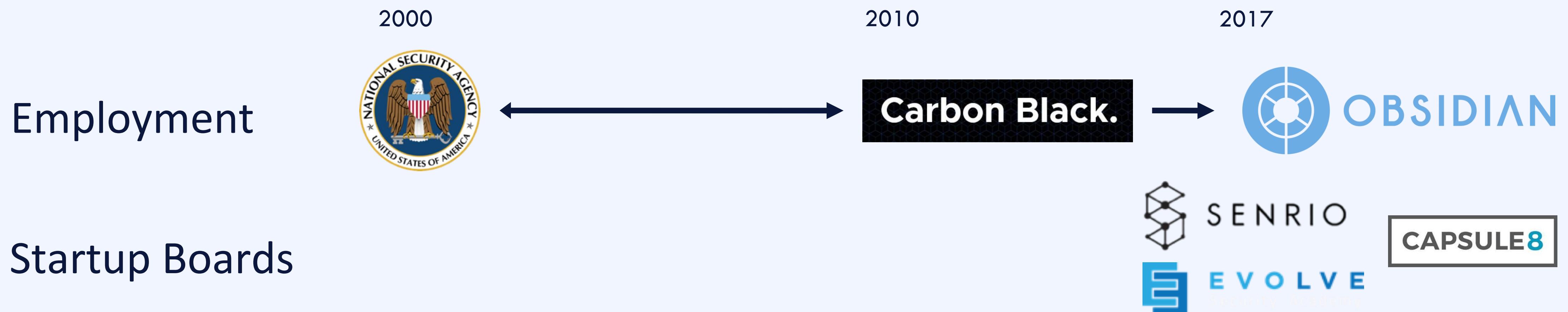
BEN JOHNSON
CTO & COFOUNDER, OBSIDIAN
SANS CLOUD SUMMIT 2020

BACKGROUND CHECK // BEN JOHNSON

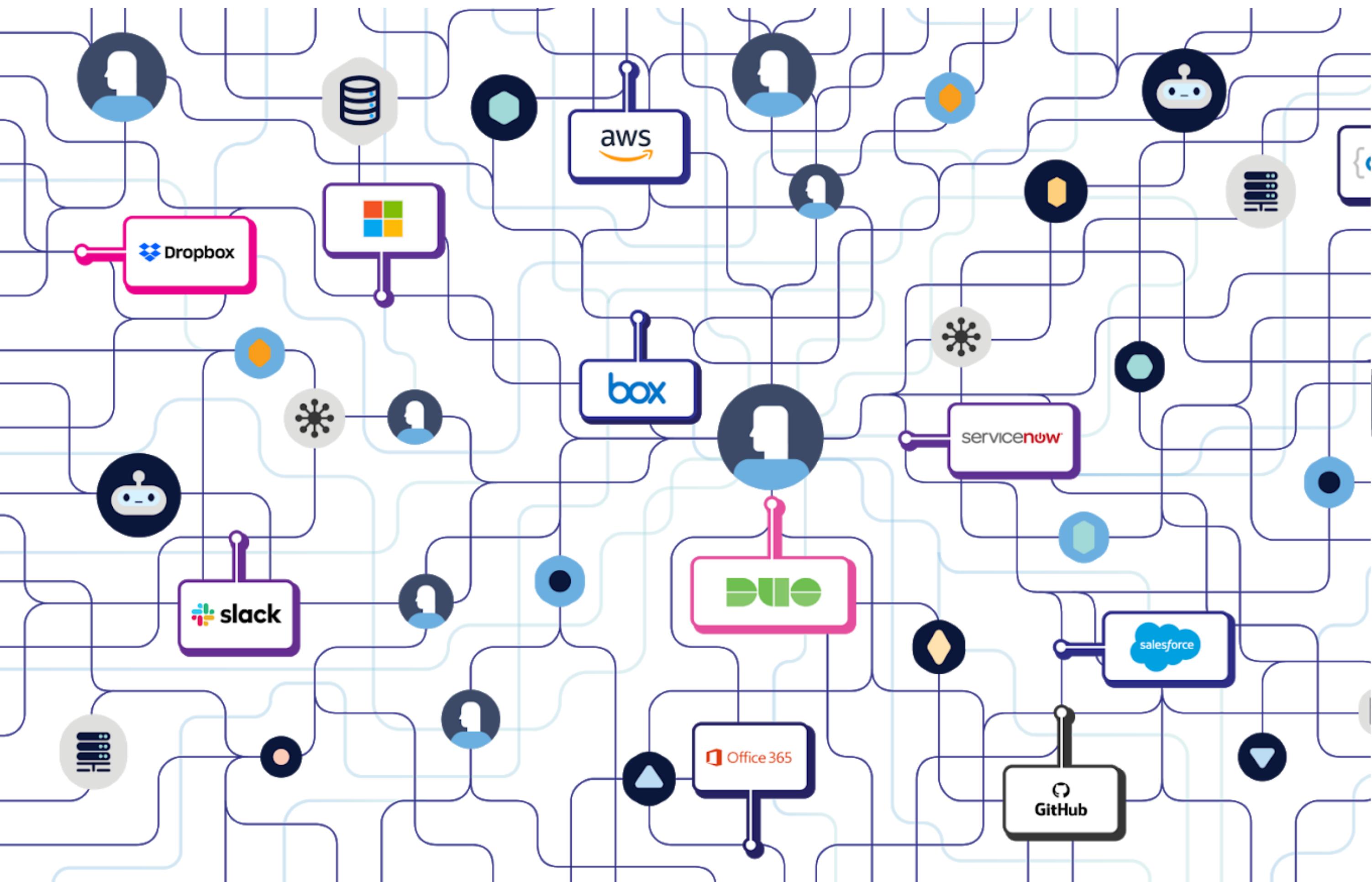
Co-Founder and CTO, Obsidian Security

Co-founder and former CTO of Carbon Black, built the first EDR product.
Previously NSA CNO and AI Lab

1st Technical Advisor (Amicus Curiae) to US FISA Court



CLOUD IS ACCELERATING BUSINESS

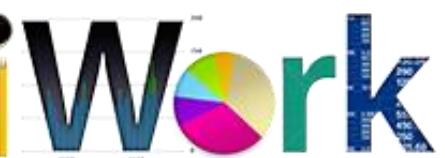


SECURITY IMPERATIVE:
ENABLE BUSINESS TO ADVANCE ITS
MISSION ... SAFELY!

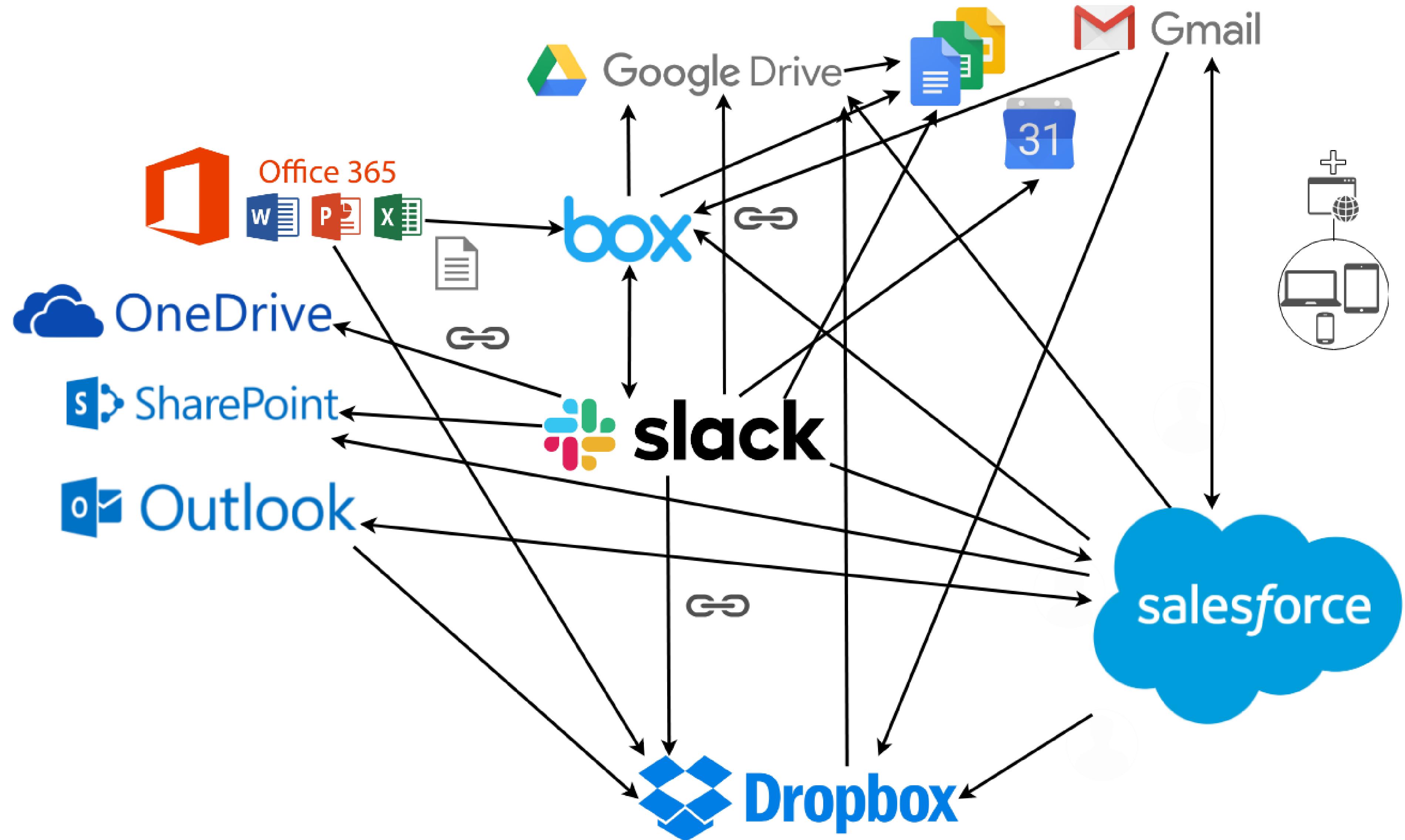
"75% OF THE CLOUD IS SAAS"
- DAVE SHACKLEFORD

AND IF YOU DON'T HAVE SAAS YET, IT'S COMING

Companies are picking a “cloud stack” of business services...the difference being these new technologies are cloud-based and designed for

collaboration.	EMAIL	    
	WORD PROCESSOR	     
	COMMUNICATION	    
	CONTENT MANAGEMENT	    
	INFORMATION TECHNOLOGY	    
	SALES & MARKETING	    
	FINANCE	   
	HUMAN RESOURCES	    
	SECURITY	    

CLOUDS TALK TO CLOUDS



WHO PROTECTS CLOUD? (HINT: YOU)

Shared responsibility model



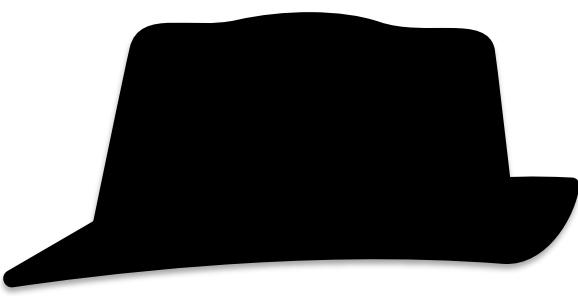
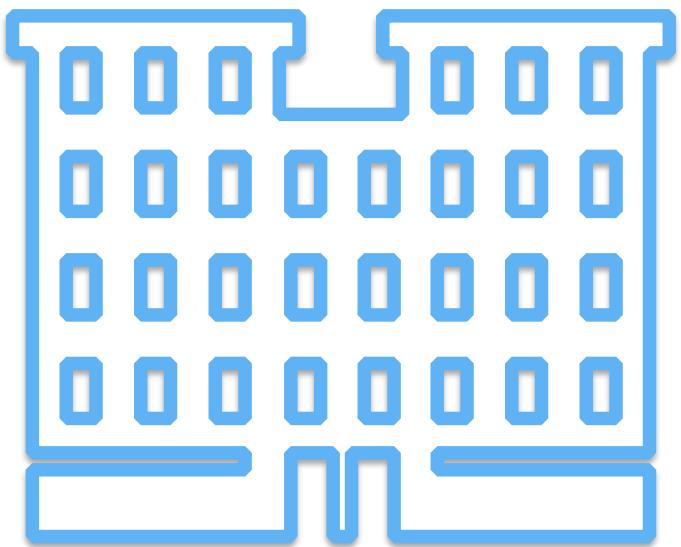
—● SAAS IS YOUR RESPONSIBILITY

The SaaS Provider handles all aspects **except for identity and access management, client devices controls, and data accountability.**

The Customer (you), therefore, must **understand users, devices & data related to that service.**

CLOUD SECURITY NEEDS TO BE A PRIORITY

"89% of companies use SaaS" *



"Up to 95% of cloud breaches occur due to human errors." **

"...someone in your organization should do regular audits to detect potential abuse" - Salesforce



ALWAYS ON, ALWAYS REACHABLE TARGETS

USERS OVERSHARE AND AUTHORIZE APPS

LACK OF EXPERTISE IN CLOUD DETECTION

OVER-ACCESS INCREASES INSIDER RISK

POORLY UNDERSTOOD, DISPARATE AUDIT LOGS

● CLOUD SECURITY IS THE SAME ... AND DIFFERENT

- Enable the business to advance its mission ... SAFELY.
- Protect the business but also allow for the business — productivity, cost savings, and innovation are largely why organizations are going to SaaS/PaaS/IaaS. If you (as security) hurt these, you will not be popular.
 - Review and monitor access
 - Review and monitor privileges
 - Review and monitor configurations
 - Review and monitor behavior

So not that different from on-premise?

Yet the networks, assets, applications might not be under any of your control.

● WHAT'S SECURITY'S AIM FOR CLOUD?

- Protect account access
- Enable responsible use
- Enable responsible collaboration
- Detect misuse, compromise, and other unwanted behavior
- Investigate and cleanup when there's a problem

PROTECT DETECT RESPOND

“The absence of disease does not mean health.”

INTRO TO SAAS DETECTION

- Often, the primary goal for SaaS is to keep the adversaries out. This is a smart primary goal.
- Then you likely want to understand privileged activity, and any changes to privileged users.
- From here, understanding how your information might be exposed, such as sharing files broadly or buckets created.
- Then, observing any increases to the surface area by adding third party apps and/or new user accounts.
- Finally, insider threats, especially in IP-heavy companies and industries.

DETECTION: LOGINS (O365)

Search Clear

Activities User logged in

Start date 2020-01-08 00:00

End date 2020-01-16 00:00

Users Show results for all users

File, folder, or site Add all or part of a file name, folder name, or URL.

Search

+ New alert policy

+ New Retention Policy

Results 300 results found (More items available, scroll down to see more.)

Date	IP address	User	Activity
2020-01-15 14:42:08	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 14:42:08	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 11:41:54	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 11:41:54	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 11:41:54	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 08:41:55	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 08:41:55	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 05:41:49	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 05:41:48	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 02:41:46	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 02:41:46	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-14 23:41:50	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-14 23:41:50	34.200.8.251	macewindu@hyenacapitalorg.onmicr...	User logged in
2020-01-15 15:29:05	104.183.139.113	nancy.admin@hyenacapital.org	User logged in
2020-01-15 15:27:26	104.183.139.113	nancy.admin@hyenacapital.org	User logged in
2020-01-15 15:24:03	104.183.139.113	nancy.admin@hyenacapital.org	User logged in
2020-01-15 15:19:05	104.183.139.113	nancy.admin@hyenacapital.org	User logged in

Timestamps, IP-addresses, user, results; some search capabilities

DETECTION: LOGINS (GSUITE)

Event Description	IP Address	Date	Login Type
Nancy Admin logged in	104.183.139.113	Jan 15, 2020, 2:45:05 PM PST	Google Password
Nancy Admin logged in	104.183.139.113	Jan 15, 2020, 9:19:39 AM PST	Google Password
Nancy Admin failed to login	104.183.139.113	Jan 15, 2020, 9:19:19 AM PST	Google Password
John User logged in	104.183.139.113	Jan 14, 2020, 11:45:22 AM PST	Google Password
John User logged in	104.183.139.113	Jan 14, 2020, 11:44:45 AM PST	Google Password
Nancy Admin logged in	104.183.139.113	Jan 10, 2020, 9:15:07 AM PST	Google Password
Mike Smith failed to login	104.183.139.113	Jan 9, 2020, 8:32:52 AM PST	Unknown
Mike Smith failed to login	104.183.139.113	Jan 9, 2020, 8:32:35 AM PST	Google Password
Mike Smith failed to login	104.183.139.113	Jan 9, 2020, 8:32:31 AM PST	Google Password
Nancy Admin logged in	2600:8802:2000:2360:dd83:4539:da9f:ec	Jan 9, 2020, 12:41:36 AM PST	Google Password
Nancy Admin logged in	104.183.139.113	Jan 8, 2020, 2:12:50 PM PST	Google Password

Some useful information but lacking a lot of context

DETECTION: LOGINS (SALESFORCE)

Login Time ↓	Username	Source IP	Subdivision	City	Country	Login Type	Status	Browser	Platform	Application	Login URL
1/15/2020 5:28:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:27:30 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:26:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:25:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:24:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:24:26 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:24:26 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:23:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:22:30 PM PST	[REDACTED]@obsidiansecurity.com	52.26.111.111	Oregon	Boardman	United States	Remote Access 2.0	Success	Unknown	Unknown	Demisto	login.salesforce.com
1/15/2020 5:22:15 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:15 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:14 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:14 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com
1/15/2020 5:22:14 PM PST	[REDACTED]on@obsidiansecurity.com	54.174.174.174	Virginia	Ashburn	United States	Remote Access 2.0	Success	Unknown	Unknown	HubSpot	login.salesforce.com

Show me [fewer](#) ▲ / ▼ [more](#) records per list page

Providing more context than some other systems

● DETECTION: LOGINS SUMMARY

- What should you care about when it comes to logins?
 - Admin login times, locations
 - Unusual login locations across user population
 - Spikes in failed logins for a particular user
 - IP or Geo targeting many users (password sprays, credential stuffing, etc)

DETECTION: ACCESS / PRIVILEGE CHANGES (O365)

Date ▾	IP address	User	Activity	Item
2019-12-02 15:11:02	<null>	nancy.admin@hyenacapital....	Added member to Role	ben.johnson@hyenacapital....
2019-11-13 08:07:33	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-13 08:07:32	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-13 08:07:32	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-13 08:07:32	<null>	nancy.admin@hyenacapital....	Added member to Role	mmyers@hyenacapital.org
2019-11-06 20:37:50	<null>	nancy.admin@hyenacapital....	Added member to Role	macewindu@hyenacapitalo...
2019-11-04 14:55:44	<null>	john.user@hyenacapital.org	Added member to group	john.user@hyenacapital.org
2019-10-23 12:16:31	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:30	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:30	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:29	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:29	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:29	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:28	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-23 12:16:28	<null>	nancy.admin@hyenacapital....	Added member to Role	se-demo@hyenacapital.org
2019-10-22 20:29:26	<null>	nancy.admin@hyenacapital....	Added member to group	ben.johnson@hyenacapital....

ExtendedProperties:

```
[{"Name": "resultType", "Value": "Success"}, {"Name": "auditEventCategory", "Value": "RoleManagement"}, {"Name": "nCloud", "Value": "<null>"}, {"Name": "actorContextId", "Value": "fccf267d-8661-42ed-8bd7-8a34a7cf8646"}, {"Name": "actorObjectId", "Value": "f901fa8c-b955-469a-ad49-d960d742867c"}, {"Name": "actorObjectClass", "Value": "User"}, {"Name": "actorUPN", "Value": "nancy.admin@hyenacapital.org"}, {"Name": "actorUID", "Value": "10037FFEA677314"}, {"Name": "teamName", "Value": "MSODS."}, {"Name": "targetContextId", "Value": "fccf267d-8661-42ed-8bd7-8a34a7cf8646"}, {"Name": "targetObjectId", "Value": "6dec3fe0-9127-458d-84d1-ae75b950a3b9"}, {"Name": "extendedAuditEventCategory", "Value": "Role"}, {"Name": "targetUPN", "Value": "mmyers@hyenacapital.org"}]
```

DETECTION: ACCESS / PRIVILEGE CHANGES (G SUITE)

Role Assign	Role Threat Hunter assigned to user threat.hunter@hyenacapital.net	Nancy Admin	Sep 11, 2019, 2:25:06 PM PDT	104.183.139.113
Role Creation	New role Threat Hunter created (role_id: {25916594752323600})	Nancy Admin	Sep 11, 2019, 2:24:43 PM PDT	104.183.139.113
Assign User License	A license for G Suite product and G Suite Enterprise sku was assigned to the user threat.hunter@hyenacapital.net	Google System	Sep 11, 2019, 2:23:40 PM PDT	
User Creation	threat.hunter@hyenacapital.net created	Nancy Admin	Sep 11, 2019, 2:23:30 PM PDT	104.183.139.113

User Suspension	rchavali@hyenacapital.net suspended	Nancy Admin	Oct 29, 2019, 2:28:48 PM PDT	104.183.139.113
Assign User License	A license for G Suite product and G Suite Enterprise sku was assigned to the user rchavali@hyenacapital.net	Google System	Oct 29, 2019, 2:23:48 PM PDT	
User Creation	rchavali@hyenacapital.net created	Nancy Admin	Oct 29, 2019, 2:23:38 PM PDT	104.183.139.113
Revoke User License	A license for G Suite product and G Suite Enterprise sku was revoked from user rchavali@hyenacapital.net	Google System	Oct 29, 2019, 1:25:30 PM PDT	
User Deletion	rchavali@hyenacapital.net deleted	Nancy Admin	Oct 29, 2019, 1:25:19 PM PDT	

New user added A new user has been added to the domain.	Active	Send Notification	--	System defined	1/30/19 7:40 PM
--	--------	-------------------	----	----------------	-----------------

User granted Admin privilege A user is granted an admin privilege.	Active	Send Notification	--	System defined	1/30/19 7:39 PM
---	--------	-------------------	----	----------------	-----------------

● DETECTION: ACCESS / PRIVILEGE SUMMARY

- What should you care about when it comes to access / privilege changes?
 - New privileges granted! (New admins, additional roles, etc)
 - Removal of privileged access (should be rare, want to scrutinize)
 - Specific grants, like Mailbox delegation
 - If possible, correlate new accounts to a source of truth (HR system)
 - Keep an eye on those contractors, consultants, and service providers

DETECTION: ADMIN ACTIVITY (GSUITE)

Audit log

Organization filter Date range

Admin

+ Add a filter

Event Name	Event Description	Admin	Date	IP Address	⚙️
Revoke User License	A license for G Suite product and G Suite Enterprise sku was revoked from user rchavali@hyenacapital.net	Google System	Oct 29, 2019, 2:29:03 PM PDT		
User Deletion	rchavali@hyenacapital.net deleted	Nancy Admin	Oct 29, 2019, 2:28:52 PM PDT		
Data transfer request created	Data transfer request created from rchavali@hyenacapital.net to nancy.admin@hyenacapital.net for apps Drive and Docs [include private data], Calendar [release calendar resources], Google+	Nancy Admin	Oct 29, 2019, 2:28:48 PM PDT	104.183.139.113	
User Suspension	rchavali@hyenacapital.net suspended	Nancy Admin	Oct 29, 2019, 2:28:48 PM PDT	104.183.139.113	
Assign User License	A license for G Suite product and G Suite Enterprise sku was assigned to the user rchavali@hyenacapital.net	Google System	Oct 29, 2019, 2:23:48 PM PDT		
User Creation	rchavali@hyenacapital.net created	Nancy Admin	Oct 29, 2019, 2:23:38 PM PDT	104.183.139.113	
Revoke User License	A license for G Suite product and G Suite Enterprise sku was revoked from user rchavali@hyenacapital.net	Google System	Oct 29, 2019, 1:25:30 PM PDT		
User Deletion	rchavali@hyenacapital.net deleted	Nancy Admin	Oct 29, 2019, 1:25:19 PM PDT		
Data transfer request created	Data transfer request created from rchavali@hyenacapital.net to ben.johnson@hyenacapital.net for apps Drive and Docs , Calendar , Google+	Nancy Admin	Oct 29, 2019, 1:25:07 PM PDT	104.183.139.113	
User Suspension	rchavali@hyenacapital.net suspended	Nancy Admin	Oct 29, 2019, 1:25:07 PM PDT	104.183.139.113	

DETECTION: ADMIN ACTIVITY (DROPBOX, BOX)

Activity

Date range: 9/1/2019 to 1/15/2020

People: One or more names or emails

Content: Name of file, folder, Paper doc, or showcase

Activities:

- Changed team member admin ...
- Started trusted team admin se...
- Ended trusted team admin ses...
- Ended admin sign-in-as session
- Started admin sign-in-as sessi...
- Granted/revoked option to ena...
- Approved user's request to join...
- Declined user's request to join ...
- Verified team domain

No results found

Participants: Any

Filter Action Type: Select All

Application

- Application created
- Added public key to application
- Deleted public key from application
- Enterprise App Authorization Created
- Enterprise App Authorization Updated
- Enterprise App Authorization Deleted

Automations

- Created Automation
- Deleted Automation
- Edited Automation

Collaboration

Admin Login

Added Device Association

Accepted Terms of Service

Failed login

Login

Rejected Terms of Service

Add login app

Removed login activity application

Removed Device Association

Login verification enabled

Login verification disabled

Failed Device Trust Check

User	Action	Affected	Details	Date
Ben Johnson ben.johnson@hyenacapital.net	Add login app	Mac Chrome	--	Jan 15, 2020 8:11 PM
Ben Johnson ben.johnson@hyenacapital.net	Add login app	Mac Chrome	--	Jan 15, 2020 8:11 PM
Nancy Admin nancy.admin@hyenacapital.net	Add login app	Obsidian-QE	Service: Obsidian-QE	Jan 15, 2020 9:20 AM

Policies

Shared Links

Tasks

Users

Developer Sandboxes



DETECTION: BROADLY SHARED FILES (GSUITE)

Drive

Item Visibility Change: Internal to External × + Add a filter

Item name	Event Description	User	Date	Event Name	Item Id	Item Type	Owner	Prior Visibility	Visibility
 DO_NOT_GET_LIST	Nancy Admin changed link sharing visibility from Anyone with the link within the domain to Private for hyenacapital.net	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing visibility change	1L2VfsYE_XkwUBgw9U80SLyjznfJrgyugl9SBYy iGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web
 DO_NOT_GET_LIST	Nancy Admin changed link sharing access type from Can view to None for hyenacapital.net	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing Access Type Change	1L2VfsYE_XkwUBgw9U80SLyjznfJrgyugl9SBYy iGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web
 DO_NOT_GET_LIST	Nancy Admin changed link sharing visibility from Private to Public on the web for all	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing visibility change	1L2VfsYE_XkwUBgw9U80SLyjznfJrgyugl9SBYy iGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web
 DO_NOT_GET_LIST	Nancy Admin changed link sharing access type from None to Can view for all	Nancy Admin	Oct 29, 2019, 3:25:28 PM PDT	Link Sharing Access Type Change	1L2VfsYE_XkwUBgw9U80SLyjznfJrgyugl9SBYy iGmM	Google Docs	nancy.admin@hyenacapital.net	Anyone with the link within the domain	Public on the web

DETECTION: OAUTH / THIRD-PARTY APPLICATIONS

APP	SCOPE	USER		
OAuth grant activity by user				
Jan 9, 2020 - Jan 15, 2020				
<input type="button" value="Select filter"/> ? 				
User	Grants	Grant change	Scopes Granted	Scope change
nancy.admin@hyenacapital.net	6,661	7% ↑	25	19% ↑
ben.johnson@hyenacapital.net	107	-6% ↓	25	25% ↑
jondoe@hyenacapital.net	103	-8% ↓	20	0%
emilyevernote@hyenacapital.net	103	-9% ↓	20	0%
george.harrison@hyenacapital.net	103	-9% ↓	20	0%
john.user@hyenacapital.net				
eddie.nimda@hyenacapital.net				
mickjagger@hyenacapital.net				
mike.smith@hyenacapital.net				

Privileged OAuth apps ...

20 privileged OAuth ...

Apps that users gave permissions to. Discovered by Cloud App Security



High Medium Low

App	Permission level
pwnauth	High
DROPBOX	High
Obsidian Security MS Graph [te...	High
My Python App	High

<input type="checkbox"/> App name	Type	ID	Users	Requested services	Access
<input type="checkbox"/> Box	Web Application	371608620635-lsbr3prap4hae8kl0netf6r...	3	Other	Limited
<input type="checkbox"/> Google APIs Explorer	Web Application	292824132082.apps.googleusercontent....	2	Drive, Gmail, +4	Limited
<input type="checkbox"/> Evernote	Web Application	447407681759.apps.googleusercontent....	2	Drive, Calendar, +2	Limited
<input type="checkbox"/> GSuite SA Extended POC	Web Application	1092078371667-9a3vpnib3pajvqbqcj8nh...	1	G Suite Admin, Other	Limited
<input type="checkbox"/> Slack	Web Application	19570130570-tfuuvh6hutjd09bq64is5sa...	1	Drive, Other	Limited
<input type="checkbox"/> GAM Project Creation	Unknown Applicat...	297408095146-fug707qsjv4ikron0hugpe...	1	Cloud Platform	Limited



DETECTION: SHARING SUMMARY

- What should you care about when it comes to sharing and third-party apps?
 - Sensitive scopes/grants (i.e. full GMail access)
 - Sharing externally with no expiration
 - Sharing externally with no password or restrictions
 - System-level apps that grant access to all accounts
 - Apps granted sensitive access that are only installed by 1 user (or a few users)

● WHAT DOES OBSIDIAN DO (INTERNALLY)?

- SaaS and IaaS heavy
- Worry about threats and excessive risk but try to always say YES to the business
- Enable auditing on SaaS applications, pull telemetry into our own product connect up to Splunk, Snowflake, Elasticsearch, datalake, etc.)
- Enable cloudtrail, similar to SaaS ^^
- IP-Geo enrichment (IPs often mean very little but countries or states DO mean something)
- Send alerts to slack- GuardDuty, Marcie, Obsidian, Carbon Black, etc.
- Operators see alerts in Slack and pivot to domain specific tools
- We correlate either on Identity or IP
- Operators don't need production access if the right data is flowing to the right place
- Turn review tasks into alert tasks (get to good state and alert on drift/violation)!!!

● PLAYBOOK

Some places for you to .



● MAKE ACCESS HAVE A HALF-LIFE

Stop thinking of accounts as binary.

When possible, set an end-date to
FORCE review.

When not possible, force review
through culture and process. “Use it
or lose it.”

Invite Single-Channel Guests

These guests will only have access to messages and files in a single channel.

Email Address	Full Name (optional)	Remove
slee@cfr.org	Simon Lee	X
name@example.com	Optional	X
name@example.com	Optional	X

[⊕ Add another or add many at once](#)

Invite to

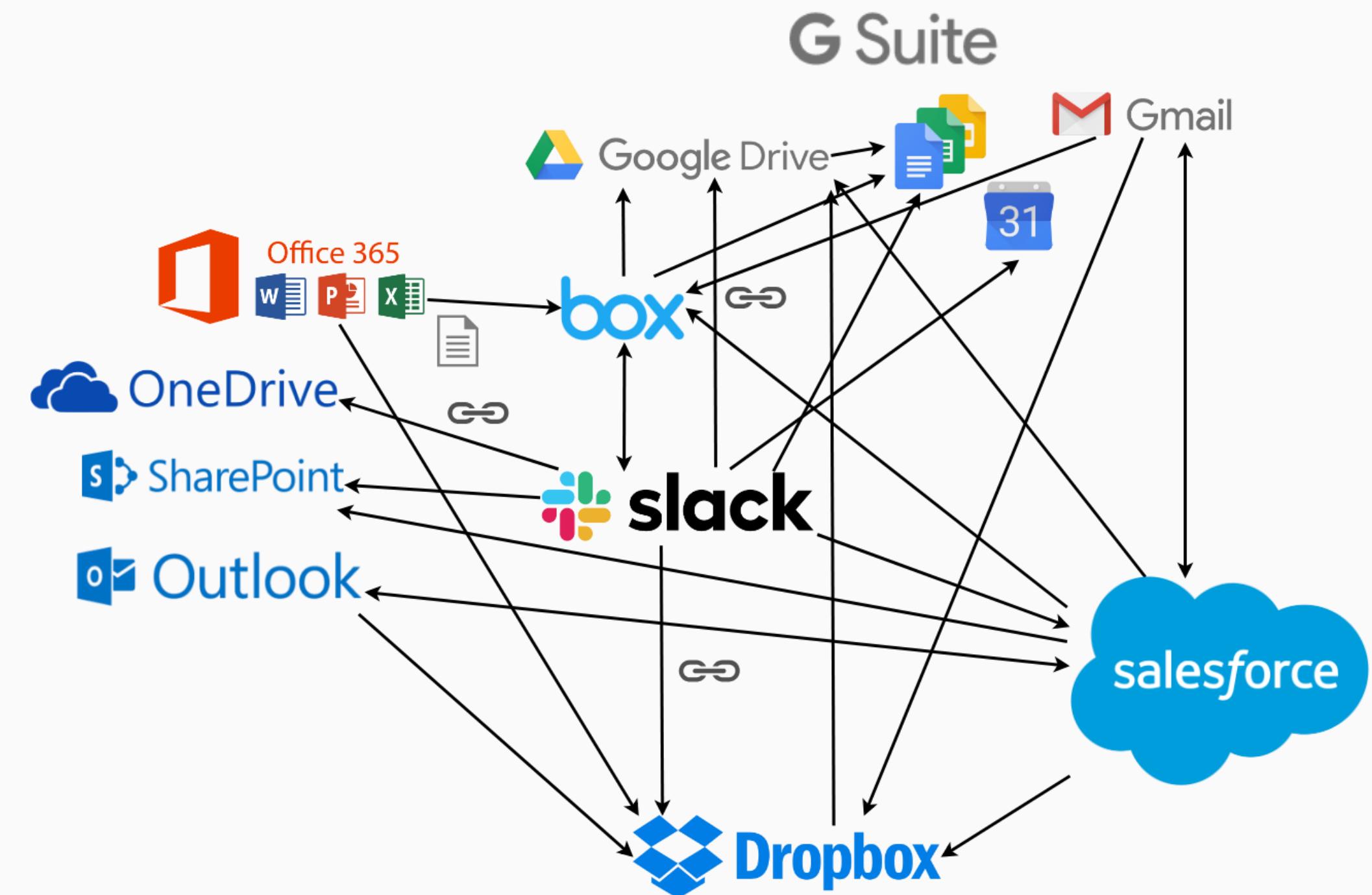
Choose an option...

Time Limit

These accounts will be deactivated on **July 28th at 11:59 PM**. [Change](#)

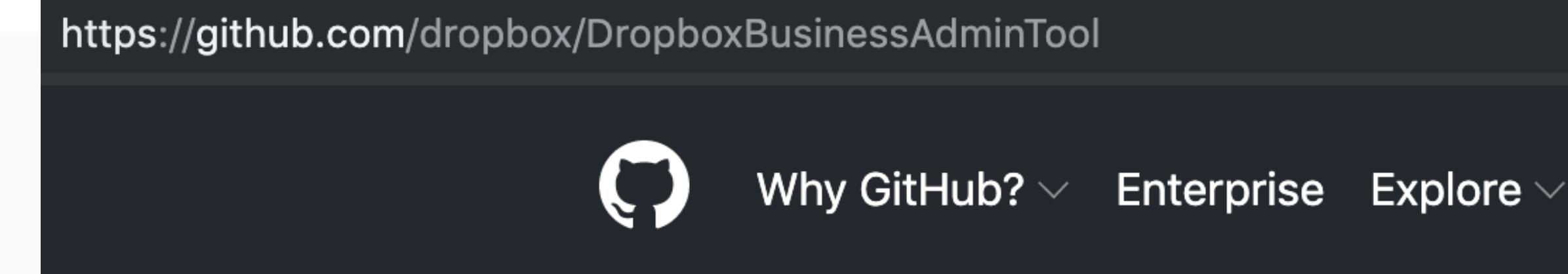
LOCK DOWN WHAT YOU CAN

- Single Sign-On; create choke point
- Create separate Admin accounts
- Use built-in settings to disable forwarding, require passwords on invites, allow maximum number of devices, conditional access, etc.
- Watch out for OAuth, Linking Accounts, and API attacks



COLLECT TELEMETRY

- Activity drives access needs (and pruning)
- Incident Response and compliance need telemetry (enable audit logs!!!)
- Lots of APIs out there ...
<https://marketplace.zoom.us/docs/api-reference/>
<https://api.slack.com/>
<https://developers.google.com/admin-sdk/>
<https://developer.salesforce.com/docs/api-explorer>
- And so on... (and some tools ->)



The screenshot shows the GitHub repository page for the "DropboxBusinessAdminTool". The URL in the address bar is <https://github.com/dropbox/DropboxBusinessAdminTool>. The page includes the GitHub logo, navigation links for "Why GitHub?", "Enterprise", and "Explore", and a link to the repository's profile: [dropbox / DropboxBusinessAdminTool](#). Below the header, it says "Release 6.1" and "Features". A bulleted list of features is provided, each preceded by a checked checkbox.

Features

- ✓ Search for content across the entire Dropbox Business team by name or full text search
- ✓ Download and save content from any team members Dropbox for holding or audit purposes while taking action on their account (suspend, delete)
- ✓ Quickly access CSV templates from file menu
- ✓ Expediently provision, deprovision in bulk from CSV
- ✓ View accurate Dropbox usage numbers for the entire team while exporting member users, status and member type
- ✓ Create group(s) and provision multiple members to a single group
- ✓ Bulk provision groups and bulk provision members to groups
- ✓ Export group relationships by user, folder, and team folder
- ✓ Downgrade user to basic type, and remove access / shares for any content where user was a member**
- ✓ Export team folder membership to CSV
- ✓ Bulk create team folder(s) or view your existing team folders and their state
- ✓ Bulk recover users, in case of accidental deletion*
- ✓ Report (and search) on Device usage associated Dropbox
- ✓ Take actions on Devices attached to your Dropbox team (remote wipe)
- ✓ Export list of Devices on your Dropbox team
- ✓ Report on all files in your Dropbox team
- ✓ Export full team member list with status

● MAKE IT EASY TO DO THE RIGHT THING

Make it easy to do the right thing:

1. Give users what they need (and sometimes want)
2. Have a (low-pain) process to approve new stuff

If you're a user/engineer/individual contributor, go through the proper channels:

1. Consider Security
2. Consider Privacy
3. Consider Productivity
4. Go through process from above!

● MAKE IT INTEGRATED INTO THE BUSINESS

- Make them own it, with your reviews and oversight
- Enable the teams that own various applications to integrate into your authentication mechanisms
- Provide guidance on privileged access and security controls
- Monitor, pen-test, etc.

● CLOUD: OPPORTUNITY TO UNIFY IT & SECURITY

IT

Enablement

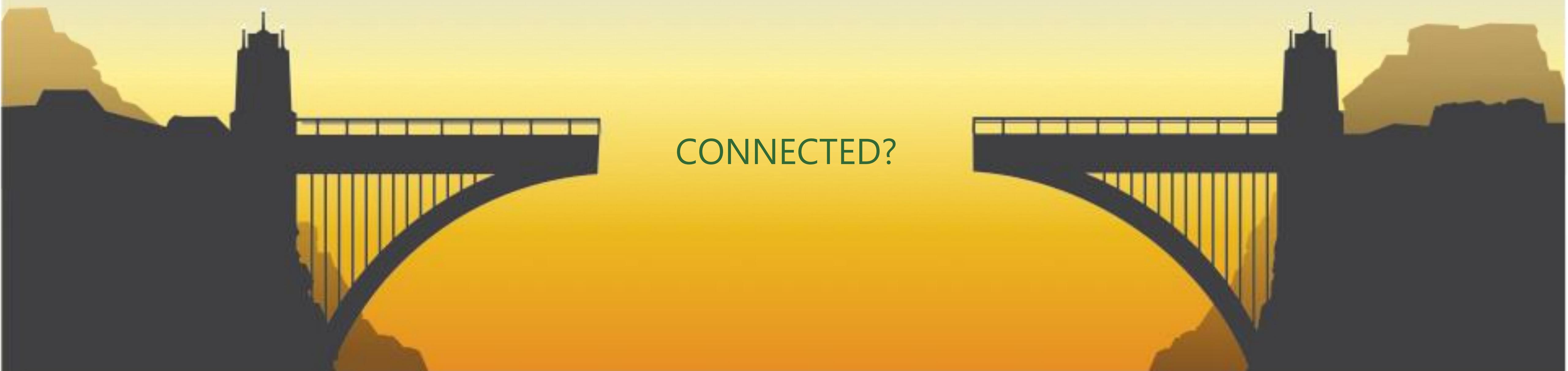
Provides Appropriate Tech

Security

Enablement

Provides Appropriate Risk

CONNECTED?



WHERE WILL YOU FOCUS?

SLOW
ATTACKERS
DOWN

ENCOURAGE
GOOD
CHOICES
& BEHAVIOR

DISCOURAGE
BAD
CHOICES
& BEHAVIOR

SPEED
DEFENDERS
UP



COVER YOUR (GROWING) SAAS

The SaaS Graph™

The SaaS Graph™ shows the relationship between people and SaaS apps in an organization. Each line represents an app-to-person connection.

Actual data from an anonymous company's SaaS usage, as of January 2019.

18

EMPLOYEES

81

APPS

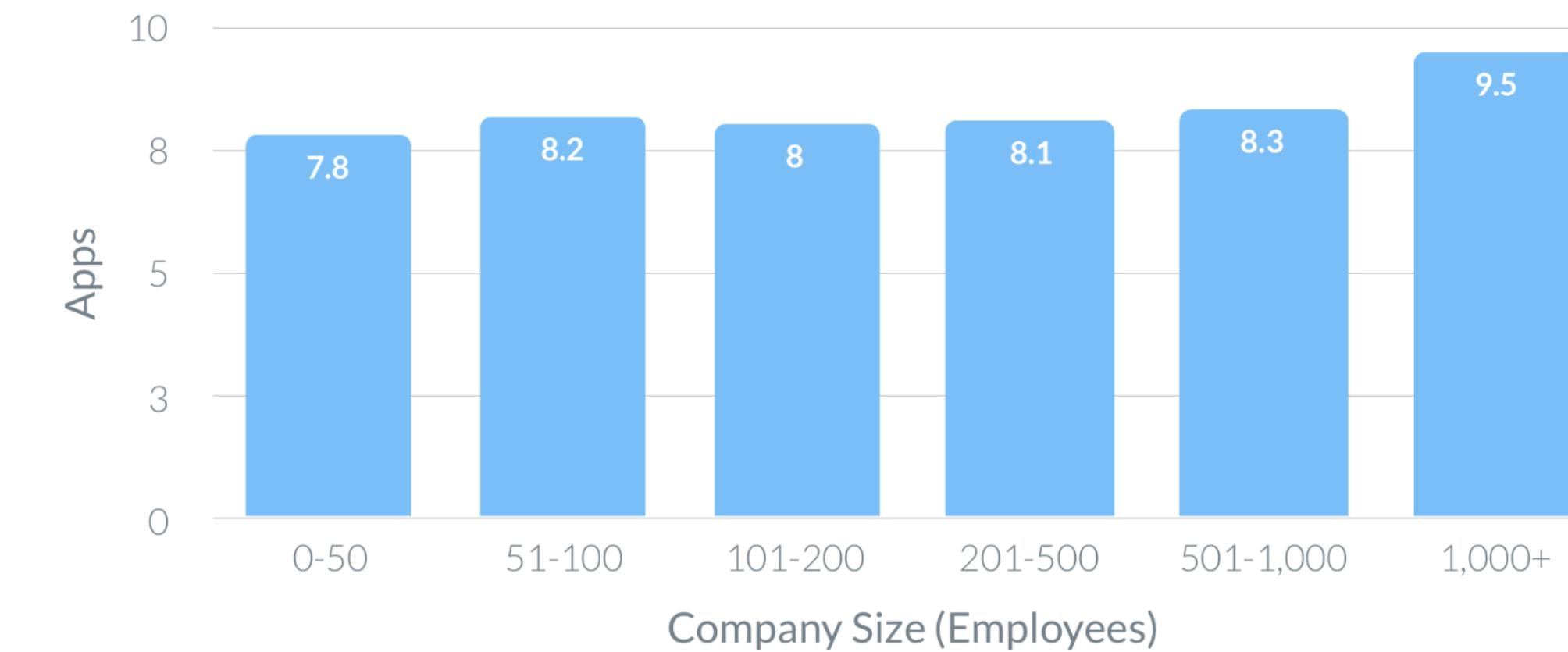
400

CONNECTIONS

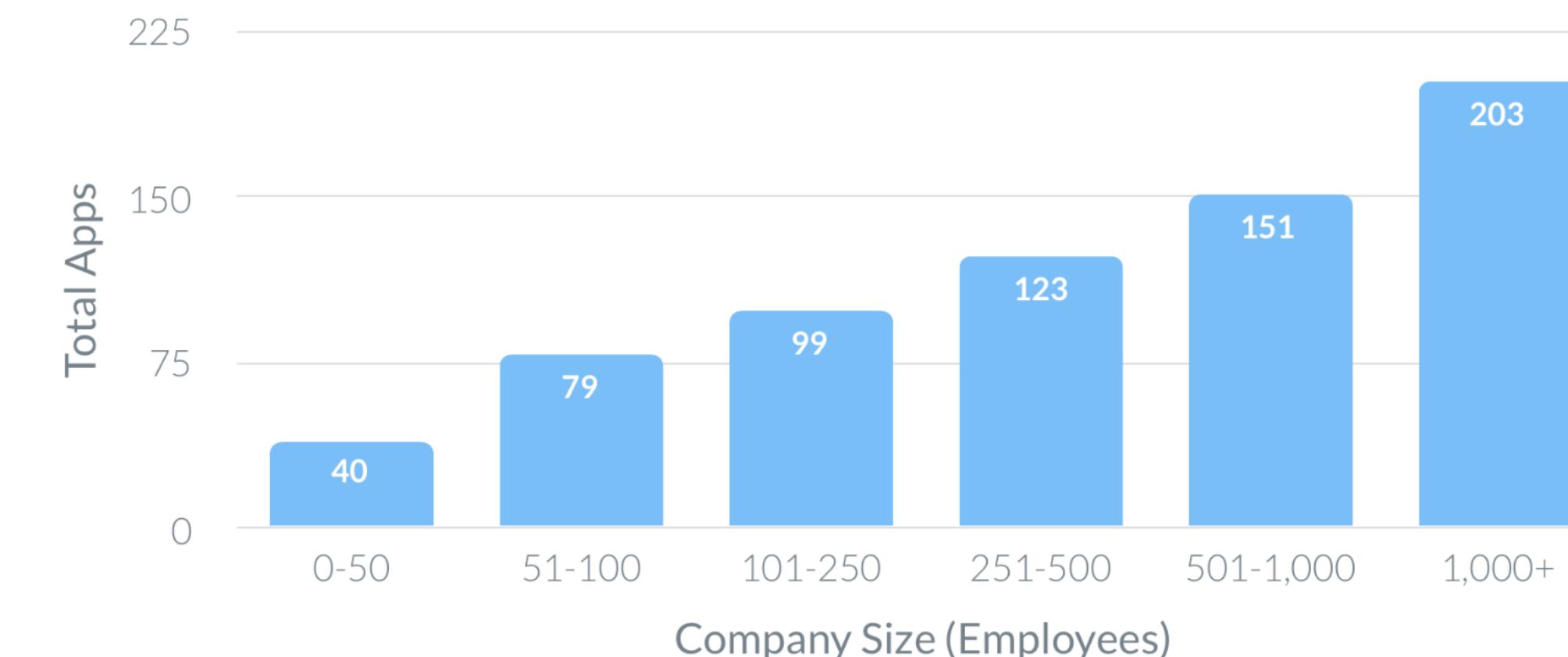
Growing Complexity

Company Size (Employees)	Average Connections
0-10	47
11-50	189
51-100	584
101-200	1,120
201-500	2,478
501-1,000	5,671

Number of Apps per Employee



Number of Apps per Company



"The journey is going to end in SaaS"
- CISO, major athletics company

Thank you & be well.

BEN JOHNSON | BEN@OBSIDIANSECURITY.COM | @CHICAGOBEN