

SHADOW IT

doesn't have to be

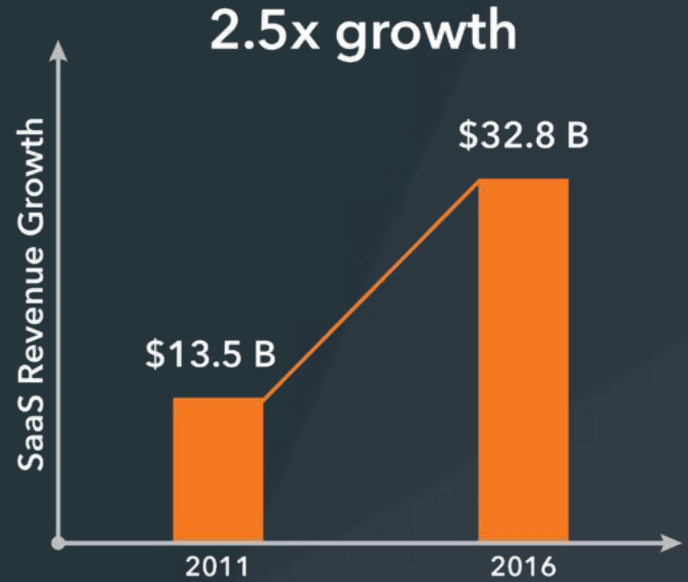
SHADY

Joey Peloquin

Standing in for Netskope



Cloud app revenue explosion



Source: Gartner

Cloud app projects double in 12 months



There are **5,000** enterprise apps today (and growing).



A close-up photograph of a hand with fingers touching a screen, overlaid with a dark grey semi-transparent rectangle containing white text.

People love their cloud apps, and for good reason

Productivity

**Anywhere
Access**

Collaboration

IT estimate:

40–50



Actual:

461

Business
underestimates
cloud app usage by

90%

IT estimate:

40–50

Actual:

461

App redundancy

41 HR

27 Storage

27 Finance

This *was* controlled
by IT in the past

61%


Of those surveyed
don't have a or don't
know about their
cloud app policy.



17%
don't know



44%
don't have



People love their cloud apps,
and for good reason
**Love doesn't have
to be blind**



STEP 1:

Discover the cloud
apps running in
your enterprise



STEP 1:

Discover the cloud apps running in your enterprise

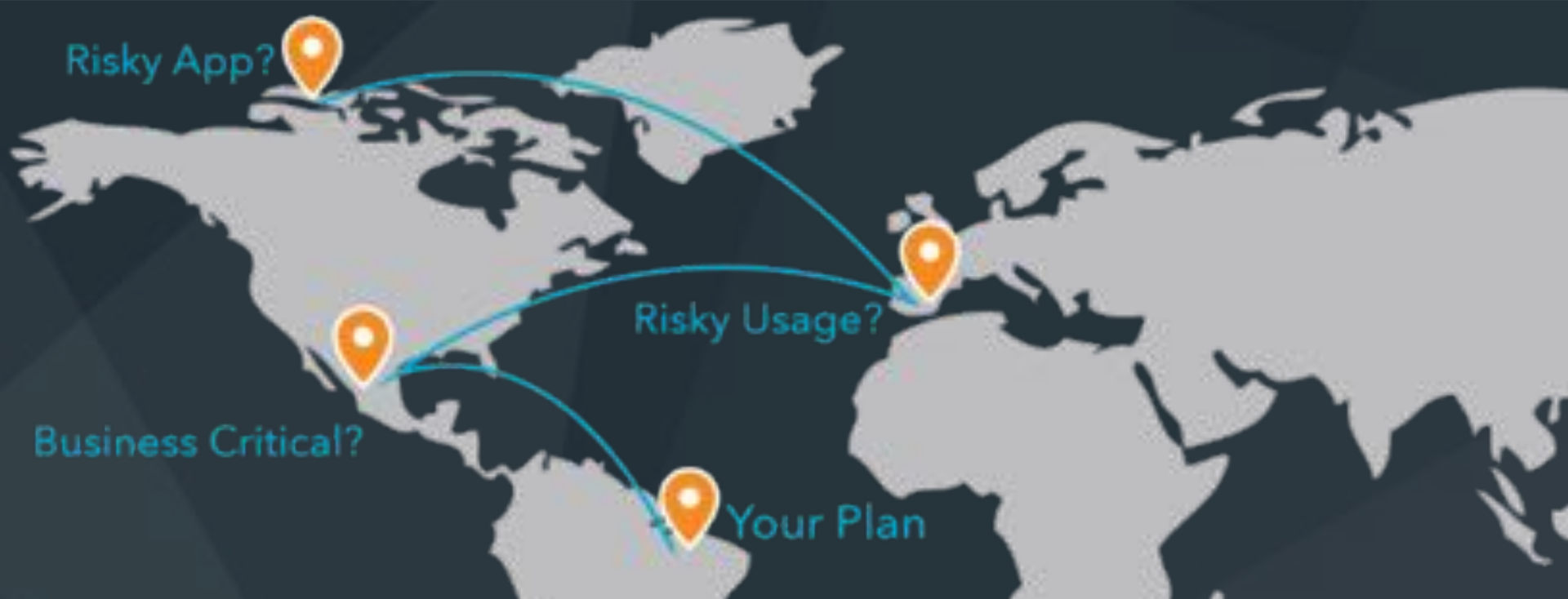
- 3rd party tools like Netskope can analyze firewall logs (and others) for this information
- Resist the urge to immediately blacklist unsanctioned apps

STEP 2:

Understand the context of



usage at a deeper level



STEP 3: Plot a course of action based on risk, usage criticality

STEP 3: Plot a course of action based on risk, usage criticality

- Use an objective criteria for assessing app. The Cloud Controls Matrix from CSA is good start and vendors have taken this to a whole new level.
- After risk, look at usage, including the nature of the content. This will help triage next steps, especially when hundreds of apps are in play.
- Risky usage can be more important than app risk.

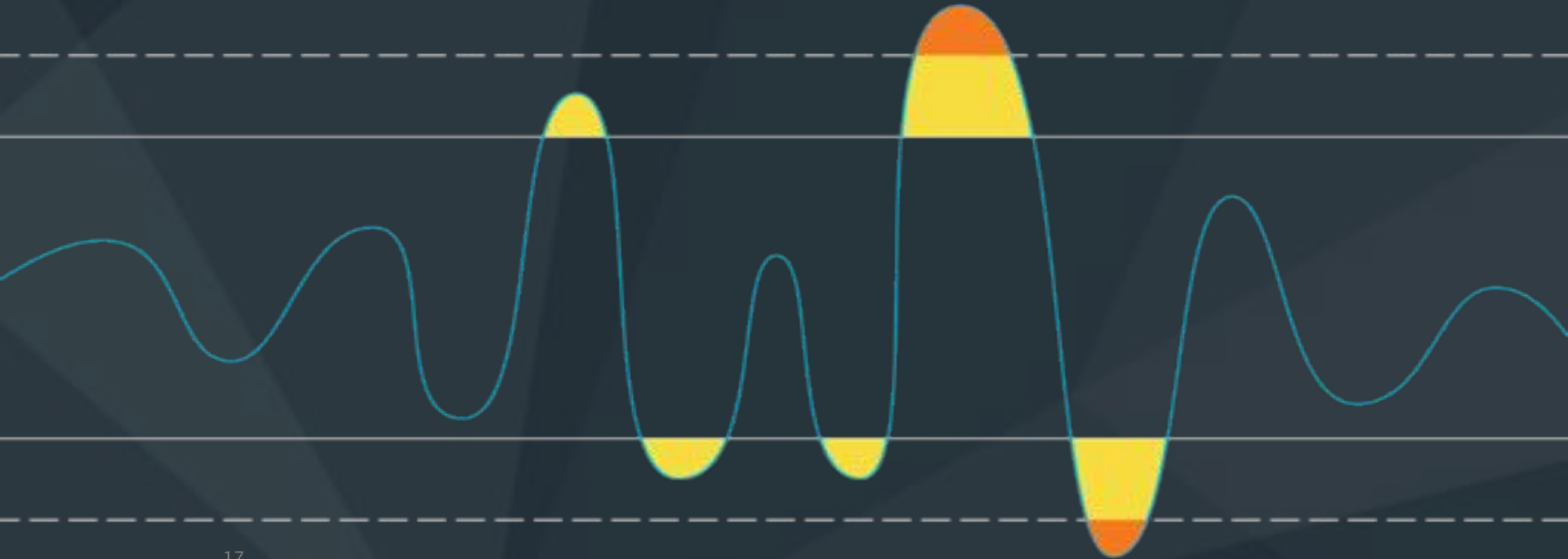
STEP 4: Enact a cloud app policy that people can get behind



- Consumerization is a strong force — being too heavy-handed with policy is a recipe for revolt
- Consider what other policies need to be modified
- Be transparent about how you'll treat unsanctioned apps
- Create an amnesty program for cloud app admins that are embedded in business units

STEP 4: Enact a cloud app policy that people can get behind

STEP 5: Monitor usage, detect anomalies, conduct forensics



- Use machine learning tools to establish baselines and monitor anomalous behavior in real-time
- Use context to reduce false positives and false negatives
- Establish clear rules for forensic analysis to maintain user privacy while protecting data

STEP 5: Monitor usage, detect anomalies, conduct forensics



STEP 6: Identify and prevent the loss of sensitive data

STEP 6: Identify and prevent the loss of sensitive data


- Rely on tools that are built for analysis of content in the cloud (don't backhaul data on-premises for analysis)
- Leverage rich context around app, user, time, etc. before you look at the data to help reduce unnecessary analysis



STEP 7: Implement security without breaking business process

STEP 7: Implement security without breaking business process

- Understand app usage and dependencies. Talk to users and find out what they're doing with these apps
- Stop blocking by default. Think about how stopping a specific behavior (i.e., sharing outside of the company) might be enough



You're using a risky app. How about using a safer app instead?

STEP 8:

Don't leave users in the dark.
Coach them on safe usage.

STEP 8: Don't leave users in the dark. Coach them on safe usage.

- Users are acutely aware of how an app *should* work. If you're doing something that changes that experience, let them know.
- A little coaching goes a long ways. You're buying good will.
- Tell them what you'd *like* them to do instead. Offer alternatives if you're going to stop something.

1: Discover the cloud apps running in your enterprise

2: Understand the context of usage at a deeper level

3: Plot your course of action based on risk, usage, criticality

4: Enact a cloud app policy that people can get behind

5: Monitor usage, detect anomalies, conduct forensics

6: Identify and prevent the loss of sensitive data

7: Implement security without breaking business process

8: Don't leave users in the dark. Coach them on safe usage.

The real face of shadow IT is you and me.



Ultimately, this is simply
unmanaged risk.

ALLOW
is the new
BLOCK

