ACP

Alpin

What Risks Lurk In The Cloud? Ways Things Can Go Badly And How You Can Prepare

Mitchel Forney | mitchel.forney@alpin.io | 520-477-6952

Agenda

Our theme today: SaaS can be scary and few people know the extent of the problem. So what can you do to be prepared?

Statistics, Trends, and Context

The ACP Game Show:

On
Horrors in
Shadow /
Hidden
Information
Technology

Expect discussion questions and interactivity

How Cloud Software Spreads

1

Fred: this app will help me be so productive!

Sign up with Google

2

Fred to @Team: Check out this AMAZING App!

+20 Users

3

6 months later...

4

$$$

1,000+ Paid Users

5

APPROVED

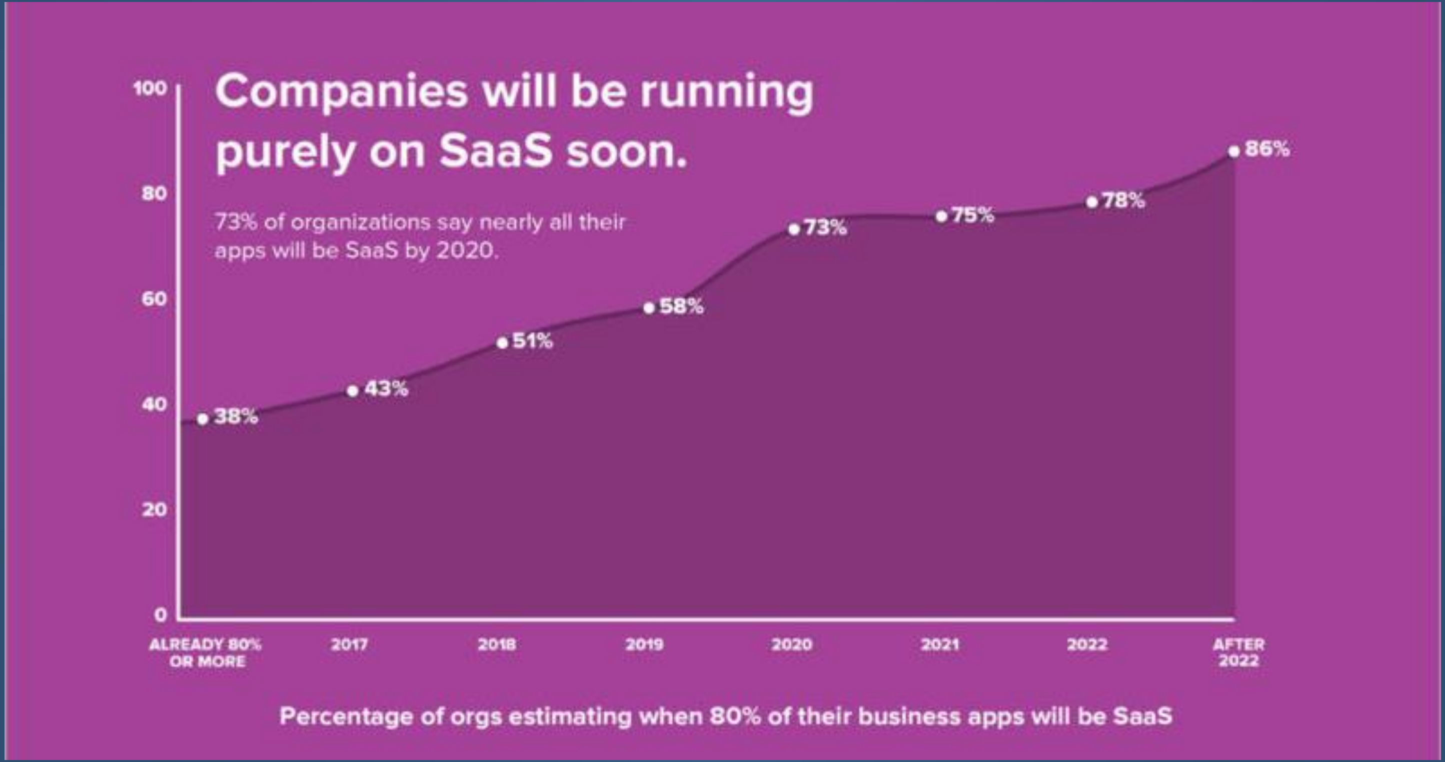
AP Dept: "This is fine"

6

Fred to @Team: Check out this OTHER AMAZING App!

Rinse and repeat.

Cloud Software Growth



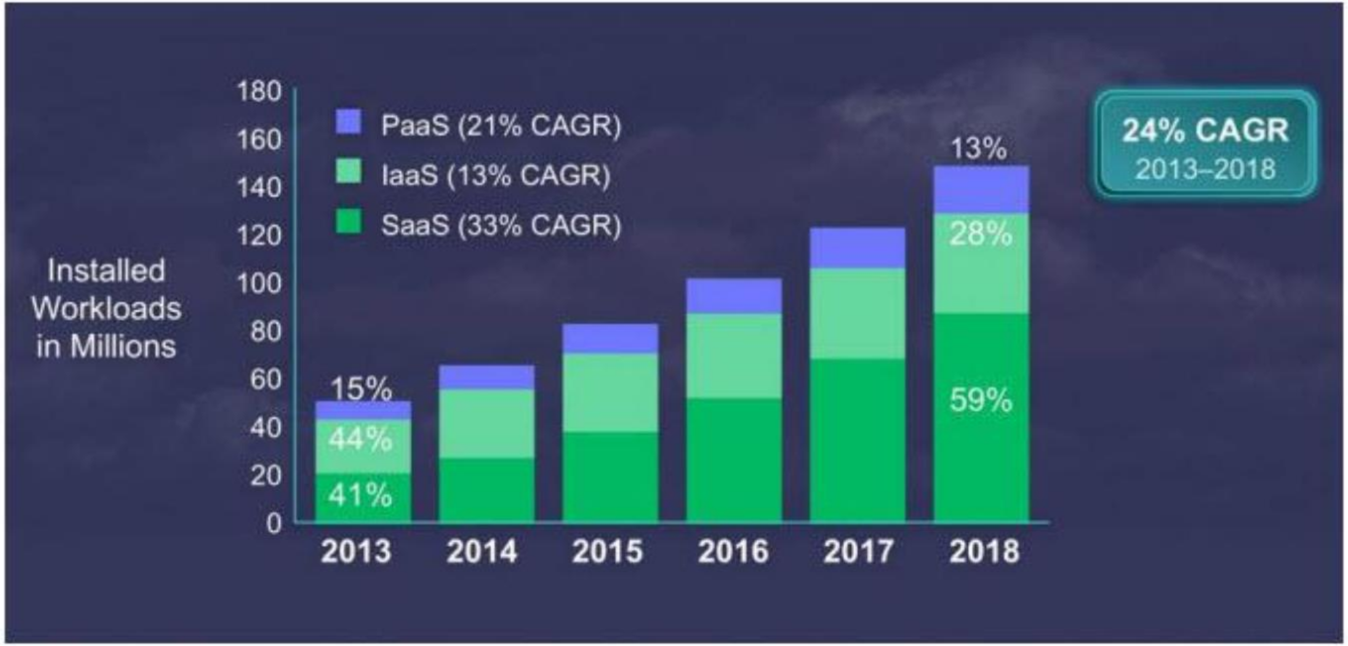
Companies will be running purely on SaaS soon.

73% of organizations say nearly all their apps will be SaaS by 2020.

Percentage of orgs estimating when 80% of their business apps will be SaaS

Cloud Software Growth

Figure 9. SaaS Most Highly Deployed Global Cloud Service by 2018



Source: Cisco Global Cloud Index, 2013–2018

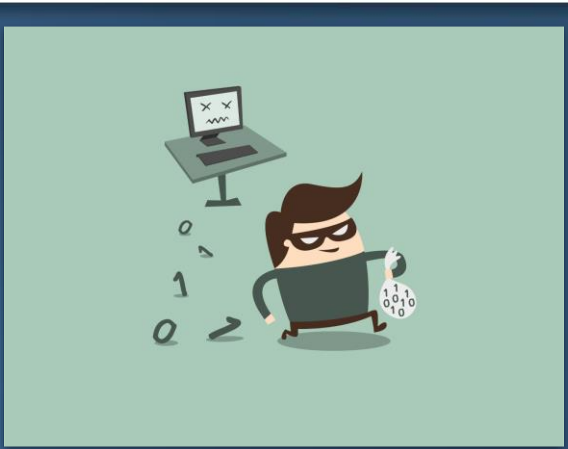
Cloud Software Growth

Growth: 54% of CIOs expect to use cloud software for **mission critical applications** within the next 3 years.

Budget: CIOs expected to double their spend on cloud-based services, from 22% to 44%, over the next 3 years

Motivations: According to CIOs **–**

Scalability and agility (over 70%)
Reducing costs (44%)
Enhancing security (34%)



Cloud Software Growth

A clickbait-ey Alpin ad on the topic

Cisco: large enterprises **use over 1,200 cloud services on average**, and fewer than 50 of those cloud services are known by IT.

CIOs estimated 51 cloud services; had 15-22 times that amount.

Gartner found that **shadow IT is 30-40% of IT spend**; Everest group says it's 50% or more.

In Sum…

Cloud Software Stats (warm up)

For every employee….

0.5 - 1

a. Security breaches, big or small
b. File containing PII uploaded to SaaS app
c. Unique SaaS applications

Cloud Software Stats (warm up)

ACP | Alpin

For every employee….

0.5 - 1

a. Security breaches, big or small

b. File containing PII uploaded to SaaS app

c. Unique SaaS applications

Cloud Software Stats (warm up)

ACP | Alpin

Alpin Tracks….

_ _ _ _ _ _ _

a. 3,000 apps
b. 7,000 apps
c. 20,000 apps
d. 40,000 apps

Cloud Software Stats (warm up)

Alpin Tracks….

_ _ _ _ _ _ _

a. 3,000 apps
b. 7,000 apps
c. 20,000 apps
d. 40,000 apps

Cloud Software Stats (warm up)

Companies have 99 _______, 9 _______, and 6 ________ subscriptions on average

a. Game, project management, file sharing
b. NSFW, project management, file sharing
c. Slack, project management, file sharing

Cloud Software Stats (warm up)

Companies have 99 _______, 9 _______, and 6 ________ subscriptions on average

a. Game, project management, file sharing
b. NSFW, project management, file sharing
c. Slack, project management, file sharing

Game: Shadow IT Horror Stories

Many employees, including the CEO and CFO, granted full access to their inboxes (and all sensitive content) to

____

a. A dating app owned by Iranian entities
b. A Russian-owned gaming site
c. A calendar tool owned by a well-known hacktivist group

Game: Shadow IT Horror Stories

ACP | Alpin

Many employees, including the CEO and CFO, granted full access to their inboxes (and all sensitive content) to

____

a. A dating app owned by Iranian entities

b. A Russian-owned gaming site

c. A calendar tool owned by a well-known hacktivist group

Game: Shadow IT Horror Stories

ACP | Alpin

Users were known for storing sensitive information in a project management app, which they were advised against. That was OK until management discovered:

b. 4 additional project management apps
b. 5 different Slack accounts, each containing important passwords, PII, and more
c. 5 duplicate versions of the same project management app, unsupervised

Game: Shadow IT Horror Stories

Users were known for storing sensitive information in a project management app, which they were advised against. That was OK until management discovered:

b. 4 additional project management apps

b. 5 different Slack accounts, each containing important passwords, PII, and more

c. 5 duplicate versions of the same project management app, unsupervised

Game: Shadow IT Horror Stories

Upon scanning a cloud storage vendor, the CFO was discovered having switched the following to a “public” share setting:

a. Lurid and inappropriate conversation through a plain text file shared with a vendor rep.
b. The entire root-level Finance folder used by their entire department and the company at large.
c. A list of their most important passwords.

Game: Shadow IT Horror Stories

Upon scanning a cloud storage vendor, the CFO was discovered having switched the following to a “public” share setting:

a. Lurid and inappropriate conversation through a plain text file shared with a vendor rep.
b. The entire root-level Finance folder used by their entire department and the company at large.
c. A list of their most important passwords.

Game: Shadow IT Horror Stories

“Wait, they’ve been gone ___________ and not only could they access all of our CRM data but we’ve been paying for the privilege?”

a. 3 days
b. 3 weeks
c. 3 months
d. 3 years

Game: Shadow IT Horror Stories

“Wait, they’ve been gone ___________ and not only could they access all of our CRM data but we’ve been paying for the privilege?”

a. 3 days
b. 3 weeks
c. 3 months
d. 3 years

Game: Shadow IT Horror Stories

A SaaS provider experienced a major data breach. How do you know if any current or former employees have an account?

a. Ask department heads
b. Ask someone in IT to scan firewall, agent, or proxy logs
c. Panic
d. Log in to a single tool and check in a few clicks

Discussion Questions

How has your organization handled SaaS, in policy and practice?

What would you expect to find in your organization?

What's important in a system of record for SaaS, from a DR perspective?

If you could pull one report on all SaaS vendors today, what would it include?

Discussion Questions

How are you handling continuity discussions around mission-critical SaaS applications?

How could some non-critical SaaS subscriptions create continuity issues?

What would be the worst part of suddenly discovering you have several hundred or thousand more vendors to deal with?

What Risks Lurk In The Cloud? Ways Things Can Go Badly And How You Can Prepare

Mitchel Forney | mitchel.forney@alpin.io | 520-477-6952