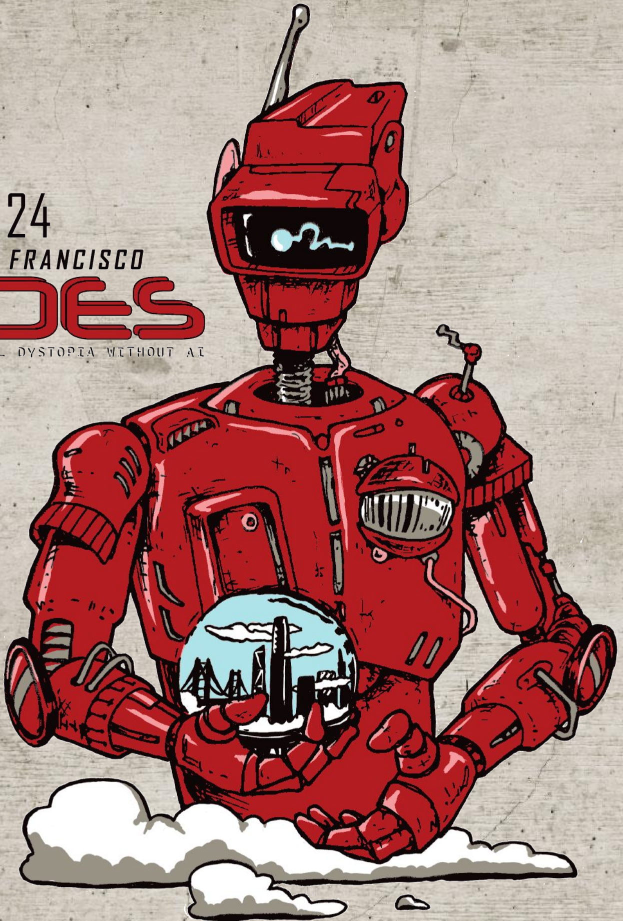
2024

SAN FRANCISCO

BSIDES

YOU CAN'T SPELL DYSTOPIA WITHOUT AI

2024
SAN FRANCISCO
BSIDES
YOU CAN'T SPELL DYSTOPIA WITHOUT AI



5 security startup pitches to raise money and eyebrows

Maya Kaczorowski
BSides SF 2024 | May 5 2024

I’m not a VC

This is not financial advice

Only hot takes here

About me

Maya Kaczorowski

@MayaKaczorowski

Previously

- CPO @ Tailscale
- Sr Director Software Supply Chain Security @ GitHub
- PM container security @ Google
- PM encryption at rest @ Google

Angel

TRUFFLE SECURITY Chainguard runreveal uno.ai

Indent RED QUEEN ensignia CloudQuery

My personal investment hypothesis

The most valuable thing I have to invest is my own time

Agenda

- What’s a ‘good’ idea to work on?
- Sources of potential ideas
- ✨ 5 fake company pitches ✨ and 🔥 feedback 🔥
- An idea isn’t a startup

What is a ‘good’ idea to work on?

What is a ‘good’ idea to work on?

Solve an actual problem for a clear user that they’re willing to pay for

Solve an actual problem for a clear user that they're willing to pay for

- Build something people actually need
- Focus on the problem, not a cool technology
- Have a really crisp definition of the problem
    - What it is
    - What the alternative is
    - Why now
    - How much people will pay

Solve an actual problem for a clear user that they’re willing to pay for

- Clear definition of the user
- Understand how they find and buy things
  - Which roles are buyers vs influencers vs users
  - IT and security have very different buying journeys
- Easier to work on what you know

Solve an actual problem for a clear user that they're willing to pay for

- How much does the alternative solution cost
- How much value does this provide
- How critical is the issue
- The only way to really know is to try

Inspiration for finding a 'good' idea

Source of inspiration

Ask your user what their top issues are!

What you're looking for

- A problem so critical they will pay anything to solve it
- A problem you can materially impact

What are the top problems CISOs have today?

- Limiting sensitive data leaks to LLMs ("LLM firewall")
- Prompt injection attacks / data phishing leaking private or sensitive information
- Workload isolation
- Abuse detection for cryptomining or training
- LLM review or validation
- Patching dependencies… for models

… so it's AI/ML/GPTs/LLMs for ~everyone

Inspiration for finding a ‘good’ idea

Source of inspiration

Stagnant market leader

What you’re looking for

- Lack of innovation or poor experience
- Large, still growing market
- Small subset of users with limited needs that you can satisfy

What security market leaders are not loved?

- HashiCorp 💔 (now part of IBM)
- Splunk (now part of Cisco)
- Okta
- Anything Salesforce, IBM, etc. acquire

Inspiration for finding a ‘good’ idea

Source of inspiration

New technological innovation / technology trends

What you’re looking for

- Makes something previously hard or expensive possible

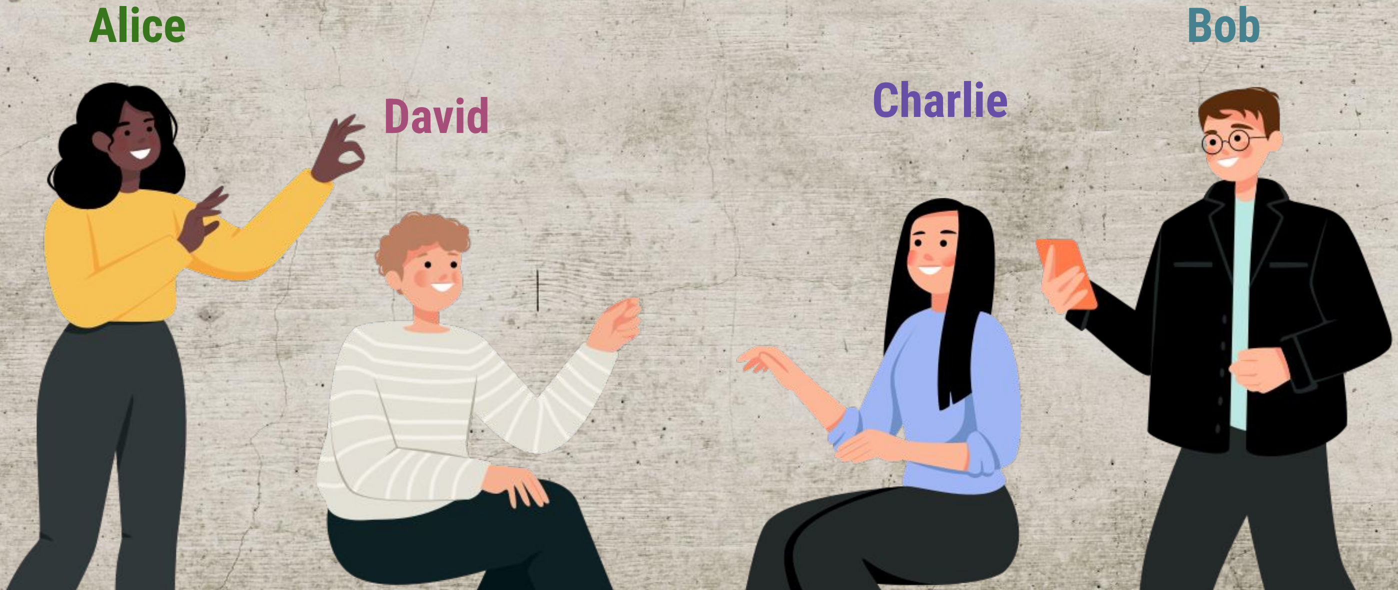
- Nix
- Deno + WASM
- WireGuard
- Passkeys
- eBPF
- LLMs

Broader trends

- LLMs
- Defragmentation of cloud
- PLG
- Likely military / defense spending

✨ Pitch time ✨

I pitched to VCs who do Seed or A security / infra investments



TrustVerify

Scalable vendor security reviews

THE PROBLEM

Vendor security reviews aren't working

- Companies have thousands of vendors and dozens of sub processors to review every year
- Hundred of questions in vendor security assessments make it difficult to find the real issues
- Security assessments block deal close, delaying the business

Yet **62%** of data breaches happen via vendors

OUR PRODUCT

TrustVerify

Scalable vendor security reviews

- AI-assisted solution to identify and prioritize the top risks in a vendor review
- Trained on publicly identifiable information such as breach disclosures, augmented with RAG to include vendor-specific information like questionnaires and policies
- Identifies missing or inconsistent information
- Allows for incremental reviews

#1 LLM for vendor security reviews

Overview

- Problem: security reviews
- Current solutions: SecurityScorecard
- Why now: LLM makes this much easier, increasing volume of vendors
- Target buyer: CISO

Why not do this?

- RAG is a key part of this, and SecurityScorecard likely has a questionnaire bank
- It’s a small market: SecurityScorecard revenue estimated to be ~$100M

#1 LLM for vendor security reviews: *what VCs said*

This is very manual — **it's a great consulting business**.
I agree that **the market is too small**.

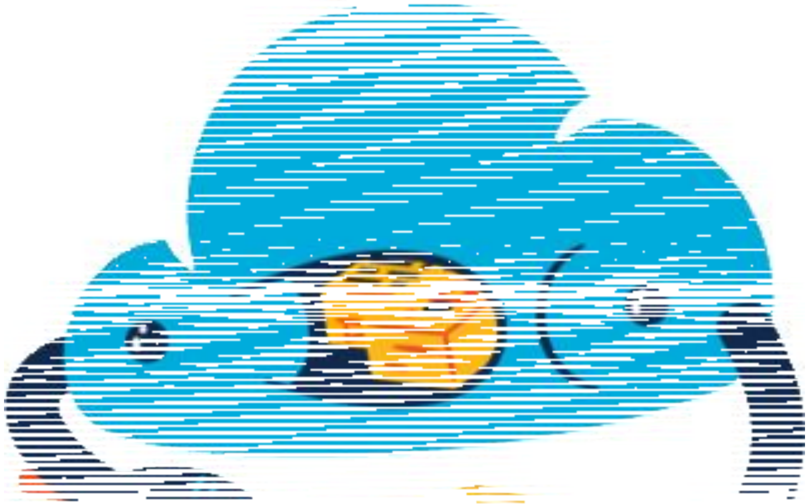
This is like the Moody's of vendors.
SOC2 isn't enough — SOC2 clearly isn't preventing breaches. I have an axe to grind with Drata / Vanta.
Why would I buy this? **Does spending on this have a measurable effect on improving security?**

Is the goal to reduce costs / move faster, or to be more secure?
The urgency is on the person making the sale, so the vendor side, not the buyer reviewing vendors.

You could say that you're SecurityScorecard but that you don't suck.
This is a **good ATM business** — it prints money.
The only people who will win in this market long term are the insurance companies. It's going to end with some single score to evaluate vendors, and the gap will be filled by buying insurance.

SECURE BRIDGE

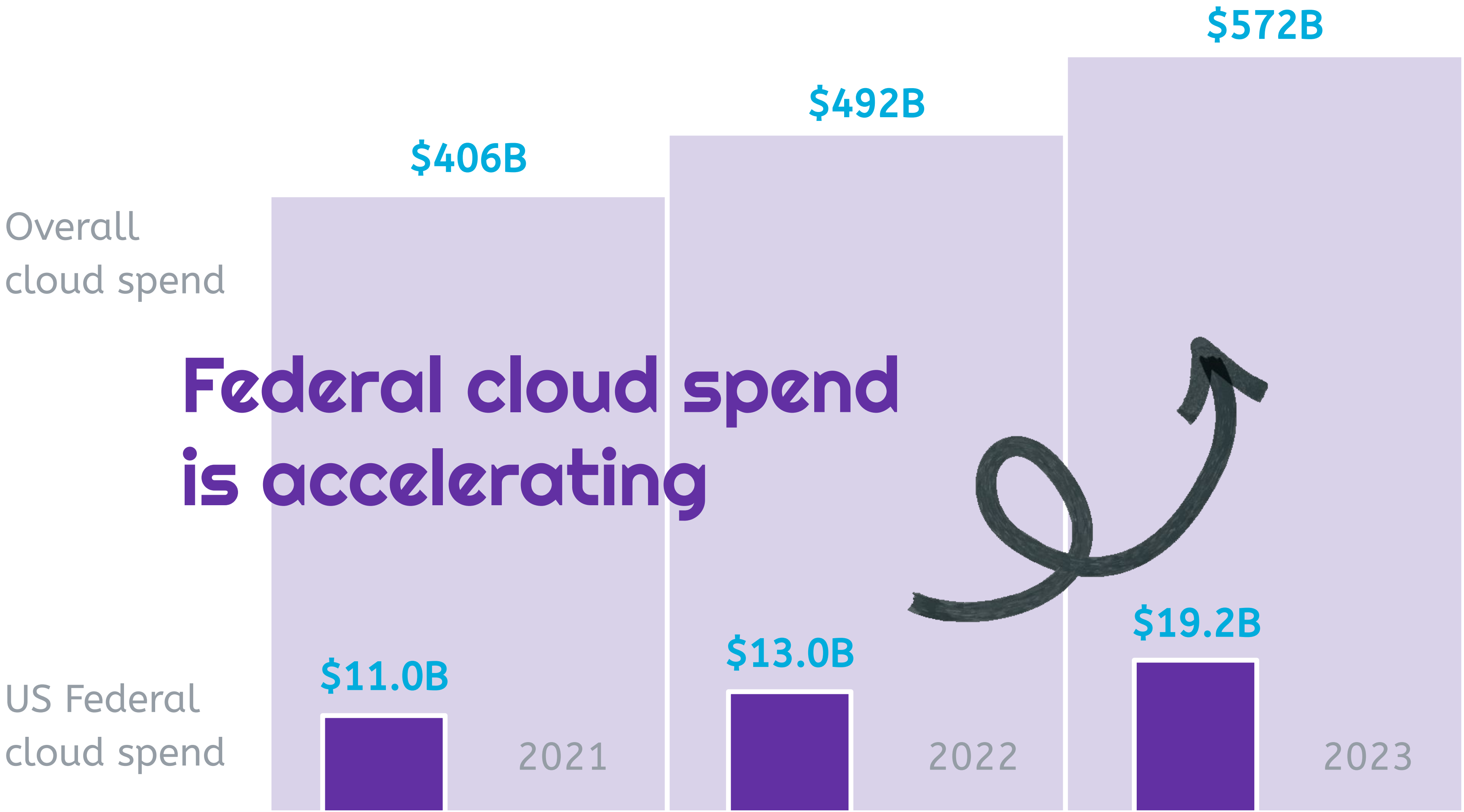
Compliance as a service

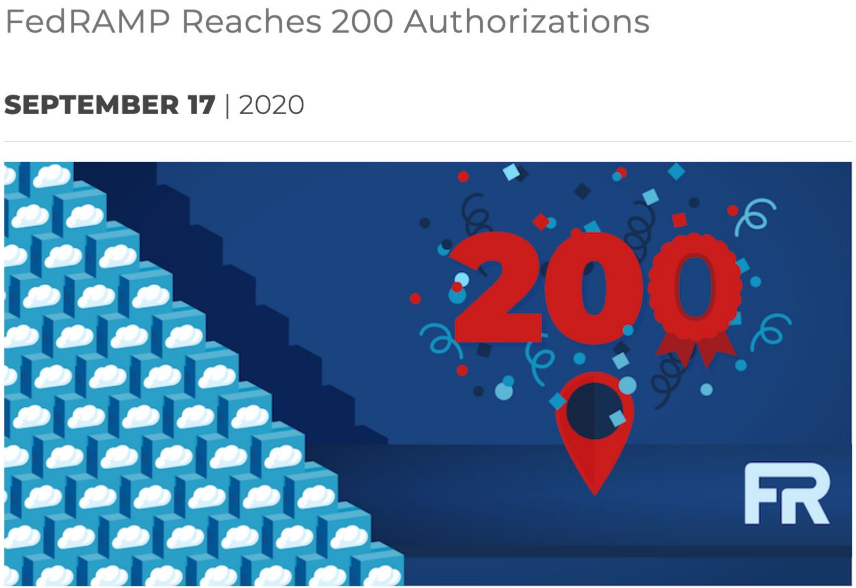


Cloud has eaten the world

94% of companies globally use cloud software

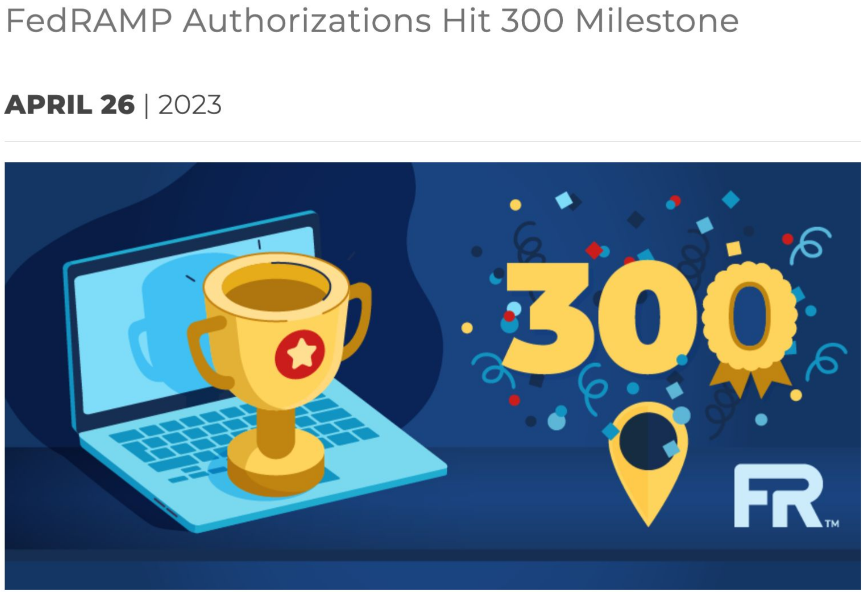
Federal cloud spend is accelerating





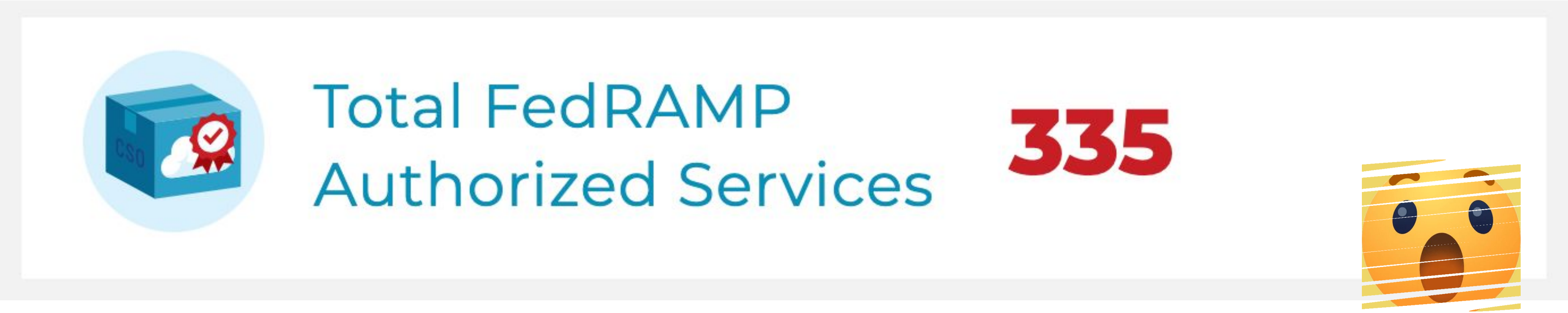
FedRAMP Reaches 200 Authorizations

SEPTEMBER 17 | 2020



FedRAMP Authorizations Hit 300 Milestone

APRIL 26 | 2023



Total FedRAMP Authorized Services

335

Our solution

A secure bridge to FedRAMP

Comprehensive

Controls, evidence automation, and starter documentation

Fast

Less than a year to FedRAMP Low, through either JAB or Agency authorization routes

How we're doing it

Your journey to FedRAMP

Automated pre-assessments

Pre-assessments based on your existing controls reviewed by a third-party assessment organization

Tenanted environments

AWS and other cloud tenant accounts that are part of our FedRAMP compliant cloud, managed by a team of US persons

Tracking of any gaps

Tracking and updating milestones to burn down the steps needed in your Security Assessment Report

#2 FedRAMP as a service

Overview

- Problem: offering a FedRAMP compliant SaaS service
- Current solutions: n/a - manual
- Why now: acceleration of SOC2 (Vanta, Drata, Secureframe), and somewhat on-prem (Replicated)
- Target buyer: CTO, CEO

Why not do this?

- This is a consultancy not a product
- Time to value is too long

#2 FedRAMP as a service: *what VCs said*

This only solves half the problem – compliance is one part, the other is go to market. **You (and your customers) need to build a federal go-to-market team**.
Your success relies on the end user, on selling a product to the government – you're a **channel**.

I like this one.
Right now, companies get FedRAMP closer to $100M ARR. **Do you get them at $50M ARR? $10M ARR?**
This is a TAM expander. However, the Federal budget dictates your total market size.
This would have to be a straight **top-down enterprise sale**.

Is Vanta not doing this? **How much of this is services oriented vs. how much is really tech**?
If your value prop is going twice as fast – at what cost? And, after an initial upfront cost, your customers don't want to talk to you. It's a bad NDR.

Another nice ATM business, it's **not venture scale**.
You could build a marketplace with this, and effectively **become the channel / VAR partner** for government. But that's not building software.

FORT ALICE

secret management

Your organization has

1000s OF INFRASTRUCTURE SECRETS

HashiCorp Vault is not usable

Too much to configure

Difficult to add users

Doesn’t scale well

Defaults not sane for enterprise

Too burdensome to run

Too expensive

FORT ALICE

MAKES SECRETS DEVELOPER CENTRIC

Managed hosted secret store

Secret injection to your CI/CD tooling

Authenticate with your IdP

Manage policy as code

CLI for devs

#3 Secret management with better DevEx

Overview

- Problem: more usable secret management
- Current solutions: Vault Enterprise, HCP Vault, Vault OSS / OpenBao, Doppler
- Why now: forking of Vault, IBM acquisition of HashiCorp, increasing set of ML environments
- Target buyer: CTO

Why not do this?

- Doesn’t address secret exfil from CI/CD
- Requires trusting a startup with secrets
- Doesn’t address the underlying problem of workload identity

#3 Secret management with better DevEx: *what VCs said*

I like this more than the first two.
HashiCorp has taken the lion’s share of the market, at the top end.
You’re susceptible to Vault getting better.

Just saying you’re going to be a little bit better at developer experience… that’s not enough.
You **need to have some key compelling differentiation** that’s hard for competitors to go after.

I like this one — there’s a clear market. It’s believable that this company exists a few years from now.
The DevEx of Vault isn’t good. It’s not a secret that this is a problem, especially now that IBM has Vault.
It feels tech heavy (so good margins), and bottom-up go-to-market is plausible.

Enterprises sophisticated enough to use a secret manager don’t want to use a hosted solution — it’s **putting all of their eggs in one basket**.

INCIDENT INSIGHT

Assisted incident response

INCIDENT RESPONSE IS HIGHLY MANUAL

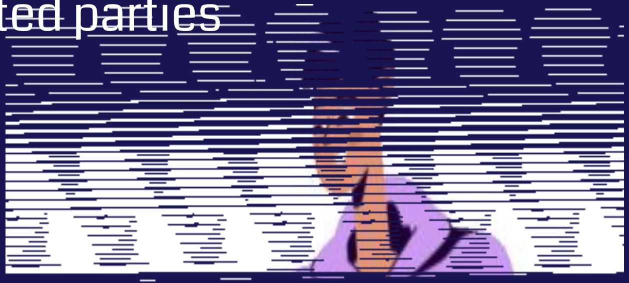
Understanding & reproducing the issue

Ensuring sufficient investigation

Delegating remediation

Communicating to affected parties

Coordinating disclosure



INCIDENT INSIGHT

HELPS INCIDENT COMMANDERS

Summarizes the issue

Gives status updates

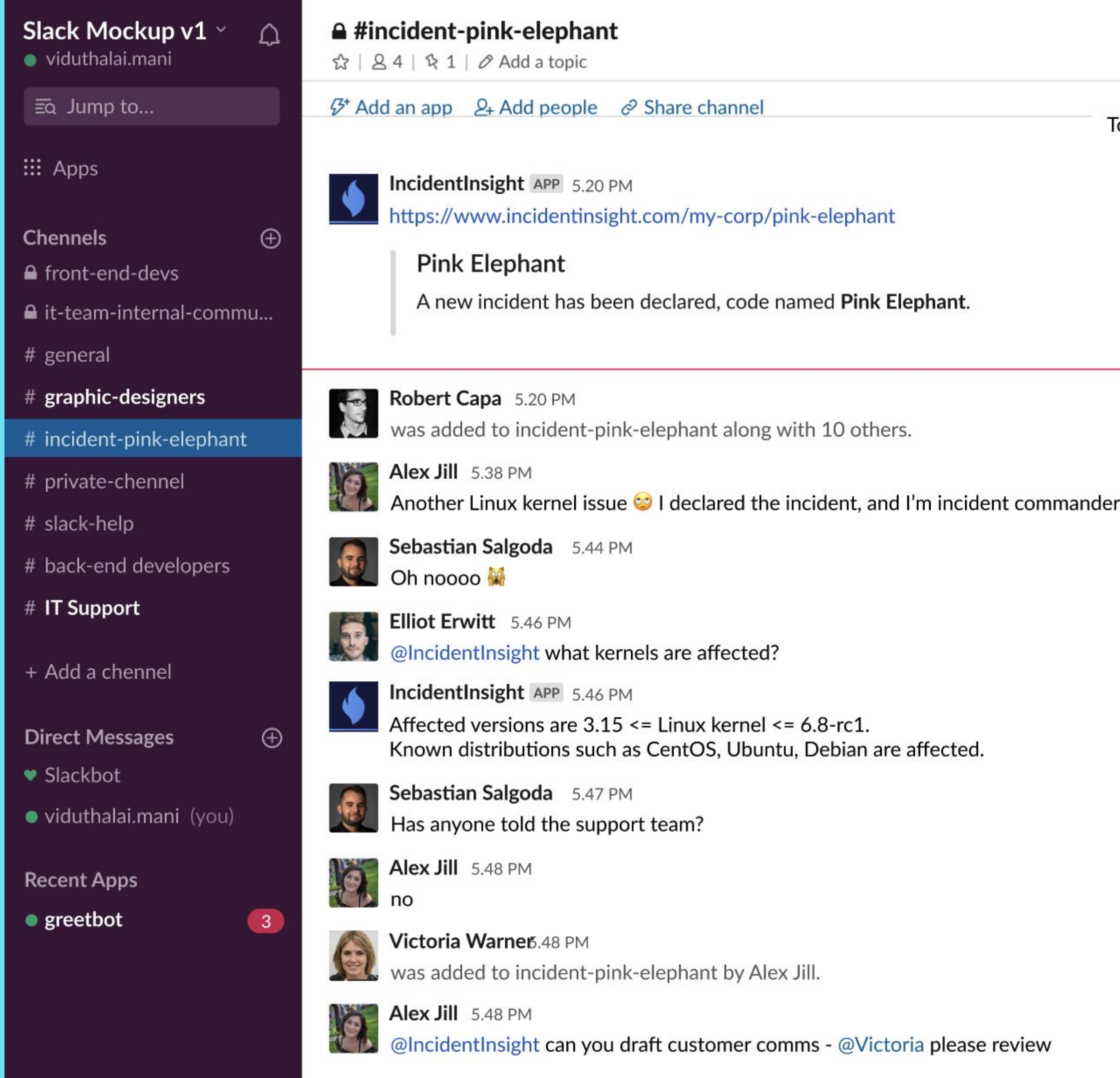
Handles handover

Steps you through the process

Drafts customer communications

Auto generates post mortems

Tracks remediations



IncidentInsight APP 5.20 PM
https://www.incidentinsight.com/my-corp/pink-elephant

Pink Elephant

A new incident has been declared, code named **Pink Elephant**.

Robert Capa 5.20 PM
was added to incident-pink-elephant along with 10 others.

Alex Jill 5.38 PM
Another Linux kernel issue 😳 I declared the incident, and I'm incident commander

Sebastian Salgoda 5.44 PM
Oh noooo 🙀

Elliot Erwitt 5.46 PM
@IncidentInsight what kernels are affected?

IncidentInsight APP 5.46 PM
Affected versions are 3.15 <= Linux kernel <= 6.8-rc1.
Known distributions such as CentOS, Ubuntu, Debian are affected.

Sebastian Salgoda 5.47 PM
Has anyone told the support team?

Alex Jill 5.48 PM
no

Victoria Warner 5.48 PM
was added to incident-pink-elephant by Alex Jill.

Alex Jill 5.48 PM
@IncidentInsight can you draft customer comms - @Victoria please review

#4 Incident response support bot

Overview

- Problem: understanding and responding to increasing volume of complex, long-lived incidents
- Current solutions: mostly homegrown, manual processes
- Why now: RAG makes this possible beyond just a simple chatbot
- Target buyer: SecOps lead

Why not do this?

- Bigger companies will build this in-house, and smaller companies don’t need this

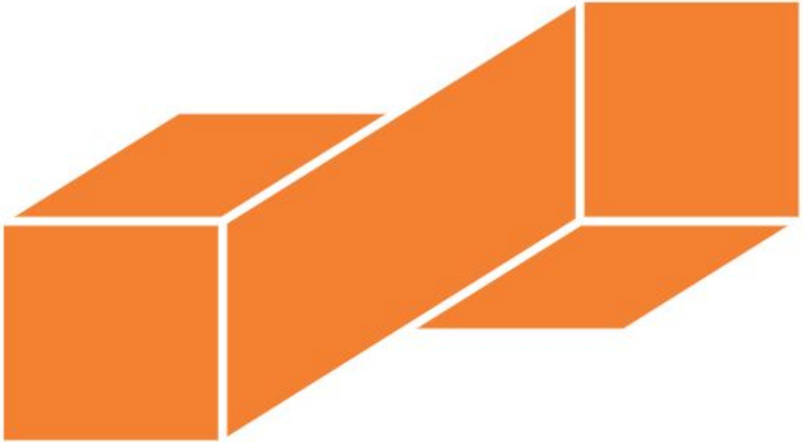
#4 Incident response support bot: *what VCs said*

Just because big tech companies are building this in-house, **doesn't mean other big companies are**. Are banks doing this right now too? Do they need it too? Ask people from non big tech companies to engage and see what they think.
Also, see if there's deeper stuff that the big tech companies are building here.

This ends up being a **hard sell outside of very forward thinking organizations**. Most people just want to check a box.
I would expect someone like Blameless, FireHydrant, or Incident.io to build this.
Some of these companies were already building workflows — **how much more is possible with LLMs**?

It's not crazy.
This is kind of like an incident Copilot. You could even generate a runbook from past incidents.
This sits right next to SOAR.
Big teams will have their own bespoke solutions they want to hold onto.

We already invested in two companies doing this.
There's much **more interest in this space given the SEC guidelines** on reporting incidents.



build stack

reproducible packages

No one loves their build tooling

Not reproducible

Security is added on

Poor multi environment support

Hard to maintain

that's where **build stack** comes in

Nix-based packaged builder

Reproducible packages, not just images

Makes point patches possible

Configurable as code

Ecosystem agnostic

Infrastructure agnostic

#5 Nix-based package builder

Overview

- Problem: securely and reproducibly building packages and SBOMs
- Current solutions: GitHub Actions, CircleCI, Jenkins, …
- Why now: Nix has sufficient popularity to make this reasonable, ongoing interest in supply chain security and SBOMs
- Target buyer: CTO, DevOps lead

Why not do this?

- Hard to get companies to move off their current build system
- High learning curve for Nix
- Not significantly different value than just “adopt nix” for servers
- Not necessarily the most pressing CI/CD security problem right now

#5 Nix-based package builder: *what VCs said*

I don't know enough about Nix, beyond **the drama**, to understand what the tech enables.

Hasn't there been some **drama in the Nix community** recently?
Having an angle around how CI works with SBOM is important.
We periodically get pitches on package managers — **I just don't see how you make money**.
This is the idea that interests me the most, but prior art suggests I'm not going to like the outcome.

Mrrrrrmmmmh.
The **CI space is a race to the bottom**.
Changing anything in the configuration of how software is built is almost impossible. It's too risky.
Hiring for this would be really hard.

This seems pretty narrow? **I don't know** how to get a good read on how big the opportunity will be.

What would you fund?

TrustVerify
Scalable vendor security reviews

SECURE BRIDGE
Compliance as a service

FORT ALICE
secret management

INCIDENT INSIGHT
Assisted incident response

build stack
reproducible packages

slido

Join at slido.com
#4804129

ⓘ Click **Present with Slido** or install our Chrome extension to display joining instructions for participants while presenting.

A smattering of other ideas

- Privacy-preserving analytics
- RAG to understand compliance requirements
- RAG for CVE summaries, patch updates
- Enterprise requirements (SCIM, audit logs) for SaaS
- XDR with a locally run ML model
- Fuzzing for ML models
- Prompt injection protections, e.g., filtering, firewalls, guardrails
- LLM identity

What would you fund?

ⓘ Click **Present with Slido** or install our Chrome extension to activate this poll while presenting.

What would you fund? *what VCs said*

TrustVerify

Scalable vendor security reviews

SECURE BRIDGE

Compliance as a service

FORT ALICE

secret management

INCIDENT INSIGHT

Assisted incident response

build stack

reproducible packages

A startup isn’t just an idea

- The right problem & solution
- The right market & time
- The right people

A startup is a lot of work

Please start some of these companies!

I’m planning on starting something, but I’m not sure exactly what yet 🤷‍♀️

I would personally be excited to see these companies

The subtitle of your talk should be “**I love these ideas for you**”.

Steal my slides: https://tinyurl.com/3k2vszap

Thanks!

2024
SAN FRANCISCO
BSIDES
YOU CAN'T SPELL DYSTOPIA WITHOUT AI