paloalto NETWORKS

Project Aerial

Team PANW
Minimum Viable Product

December 6, 2021

Note

(For Grading Purposes)

Fully **orange** slides denote the start of multi-slide sections of the rubric (ie. “Prototype”).

On most slides, a **green box** will indicate which part of the rubric the slide intends to address.

Some green boxes (e.g., the 3 parts of the MVP Summary Statement) span multiple non-contiguous slides. We suggest reading linearly.

Glossary of Key Cybersecurity Terms (Part 1)

- **EDR: Endpoint Detection & Response**
  - Managing the doors/windows of the castle (resolving attacks on individual assets)
- **XDR: Extended Detection & Response**
  - EDR, but with ML and extended features - PANW sells this
- **EASM: External Attack Surface Management**
  - Tools that help a company discover assets they don’t know they own (cloud machines, IAM roles, laptops of employees who left, etc)
  - Finding "doors / windows" (in our castle analogy)
- **SecOps: Security Operations**
- **CAASM: Cyber Asset Attack Surface Management**
  - Combines the functionality of EDR, EASM, and SecOps tools

Glossary of Key Cybersecurity Terms (Part 2)

- **ITSM: IT Service Management (ticketing systems for issues, like Jira)**
  - ServiceNow sells this
- **SOAR: Security Orchestration, Automation, and Response (serves as a dashboard for incidents)**
  - Unlike CAASM, SOAR tools do not help you with assets you don't know about
  - PANW sells this as XSOAR
- **CMDB: Content Management Database (keeps track of servers, datacenters, etc)**
  - ServiceNow also sells this
- **VA: Vulnerability Assessment**
  - Assesses a device (asset) to find vulnerabilities
- **NAC: Network Access Control**
  - Keeps track of which devices (assets) have access to which networks, and which IP addresses are allowed through which firewalls

Our Team

Ruta Joshi
Computer Science

Joshua Tan
Management Science & Engineering

Sharan Ramjee
Computer Science

Andy Jin
Computer Science

Ben Ditchfield
Management Science & Engineering

Zheng Lian
Computer Science

Our Mentors

Fred Gibbons
Stanford EE Professor

Greg Heon
Palo Alto Networks Director of PM

Anand Lalwani
EE PhD, TA

Context & Objectives

Presentation Context

- Stanford's **EE 205 Course** pairs student teams with Corporate Partners to explore a **new product concept**
- The product concept is based on a combination of **customer, market and desktop research** using core product management tools and techniques
- The project has **two key deliverables**: a product opportunity assessment and MVP

Today's Objectives

To present a **minimum viable product** based on analysis of Palo Alto Networks, including:

- Prototype
- User & Customer Experience
- Key Functionality
- Technical Feasibility and Risks
- Product Development
- Business Model

Project Journal Link:
https://www.notion.so/EE-205-PANW-d54b789b69af44fa9e20f9429c618afc

Motivation: The POA Identified a $300-400m Opportunity, with significant upside

Motivation to pursue Project Aerial

$300-400m NPV over 5 years assuming 16% market share and >$70k annual price

Increase value of existing products by facilitating wholesale integration with other security providers

Upsell existing customers by highlighting gaps in their Security portfolio

Access new segments by exploiting a different cost structure

POA Summary

Sources: PANW EE 205 POA Presentation

Problem

What problem are we trying to solve? For whom?

Our MVP is motivated by user pain points

User Story

User Story

Wrentaro Howell

Engineer in the Customer Security Incident Response Team at Target

Responsible for responding to security incidents including stolen passwords, computer viruses, firewall vulnerabilities among others

Sources: Customer Interviews

Our MVP is motivated by user pain points

User Story

User Story

“The most challenging things are to combine different [data sources] into [one source of truth] for [asset discovery] and automating incident response”

Sources: Customer Interviews

Wren Uses 6 Steps for Incident Response

User Story

Step	1 Prepare	2 Identify	3 Contain	4 Eradicate	5 Recover	6 Learn
Description	Set up asset discovery, coverage, etc.	Identify which asset, which alert, and incident details	Minimize threat/risk	Resolve threat (shut down host, etc.)	Reset credentials, restart services, etc.	Educate staff to avoid vulnerability in the future

Example Tools

SIEM

servicenow

stackoverflow

SSH

Sources: Customer Interviews

Wren Uses 6 Steps for Incident Response

User Story

Step	1 Prepare	2 Identify	3 Contain	4 Eradicate	5 Recover	6 Learn
Example Tools		SIEM	servicenow stackoverflow		O W	SSH

Takeaway

The Incident Response Process has too many tools and too much wasted time

Sources: Customer Interviews

These pain points were verified by multiple users

User Story

LIONBRIDGE

“the data was all there in **various different systems**”

GEM

“[We] found it really **difficult to correlate** [data] with a high degree of accuracy”

poly

“**you can’t manage what you can’t see**. If you don’t know what you have on the network, you can’t manage it – and **it’s almost surely vulnerable.**”

cimpress

“It’s extremely **hard to find** an asset management solution that can cover **11 distinct businesses**”

Censys

“The tech industry in moving into **Cloud Asset management**, which introduced **a lot of unknowns**” ~ Zakir Durumeric

“In relation to Netflix, it is **more difficult to protect Stanford due to large variations in machines, owners, and users**” ~ Michael Duff

Sources: Team Interviews, Public Statements

3 Jobs To Be Done are in scope for the MVP

POA Recap

Job to be done	In Scope?	Rationale
Track Assets on a Consolidated Source of Truth	✓	Most common customer pain points with no current best-in-class solution
Discover Gaps In Security Coverage	✓	High-value problem with relatively low-complexity solution based on API integrations
Resolve Gaps In Security Coverage	✓	High synergies to resolve all 3 JTBD in a single product
Automate Resolution to Vulnerabilities		Security teams remain wary of automated solutions with a human-in-the-loop
Validate and Enforce Security Policies Across Providers		Relies on other JTBD and product functionality to be feasible
Educate Employees About Best Practices		Relatively low synergies with other JTBD and existing PANW products

Sources: Team Analysis, PANW and Customer Interviews

3 Jobs To Be Done Hypotheses for MVP (Expanded)

User Story

JTBD	Description	Indicative Customer Quote	Interested Interviewees
Track Assets on a Consolidated Source of Truth	Combine varying information about all organizational assets (IP addresses, device IDS, locations, accounts, etc.	*"Our company did not have a way to easily know what data we have, where it is, and who has access to it"* ~ Henry Bagdasarian, former CISO of JD Power	Australian Electronic Medical Record, NIH / NIDA, Anthem Blue Cross, JD Power, Target, Skyworks, Stanford
Discover Gaps In Security Coverage	Identify which elements of an asset / the organization are insecure despite despite existing security protocols	*"Look at how data breaches happen - when they happen, that's an indicator of where the vulnerabilities are, and which things people missed"* ~ Zakir, Censys	Australian Electronic Medical Record, NIH / NIDA, Anthem Blue Cross, JD Power, Target, Skyworks, Stanford
Validate and Enforce Security Policies Across all Assets	Ensure all assets are compliant to organizational, federal, and other security standards	*"We want to protect sensitive customer information, so it is important that our systems are compliant with the newest security standards."* ~ CMIO of Australian Electronic Medical Record	Australian Electronic Medical Record, NIH / NIDA, JD Power, Skyworks

Sources: Team Interviews and Analysis

Solution

What can we build to solve the problem?

Strategic Fit with Corporate Partner

Provided by **PANW**

A core **value proposition...**

1. EDR
2. SecOps Center Automation
3. EASM
4. Everything else

...across ~24 **separate** products

- Cortex
- Firewalls
- XSOAR
- Prisma Cloud
- Prisma SASE
- Xpanse

...

Provided by **Competitors**

CAASM
EDR + EASM + SecOps Automation

- Integrates across SecOps tools, by consolidating **multiple products** and tools into a **single source**
- Discovers **gaps** in security coverage to **mitigate threats**
- Poses a competitive threat to PANW by threatening to **become the interface** customers use to access PANW products

CAASM would integrate many products in the PANW cybersecurity ecosystem

Minimum Viable Product

Project Aerial

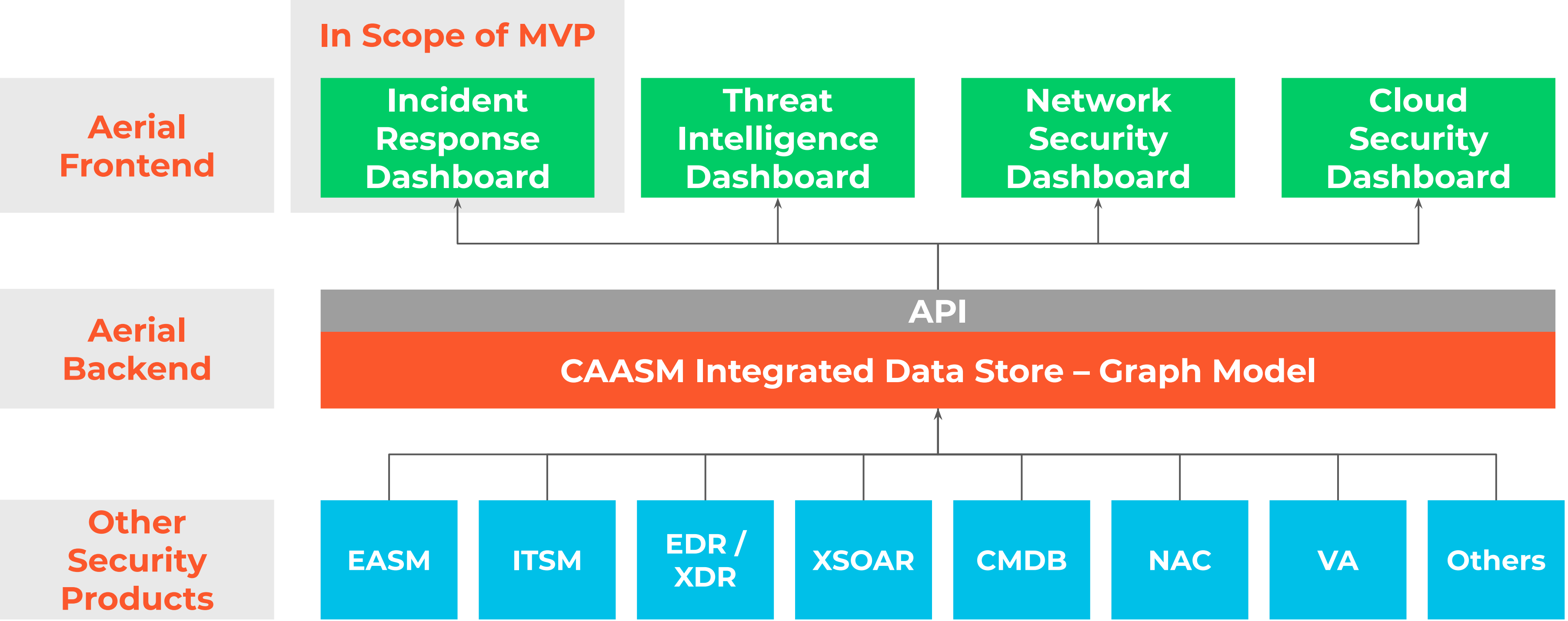
CAASM-enabled incident response dashboard

which integrates cyber asset information to identify, respond faster to, and manage security incidents

Key Features

- Asset graph backend
- Incident response frontend

Project Aerial integrates cyber asset information to identify, respond faster to, and manage security incidents

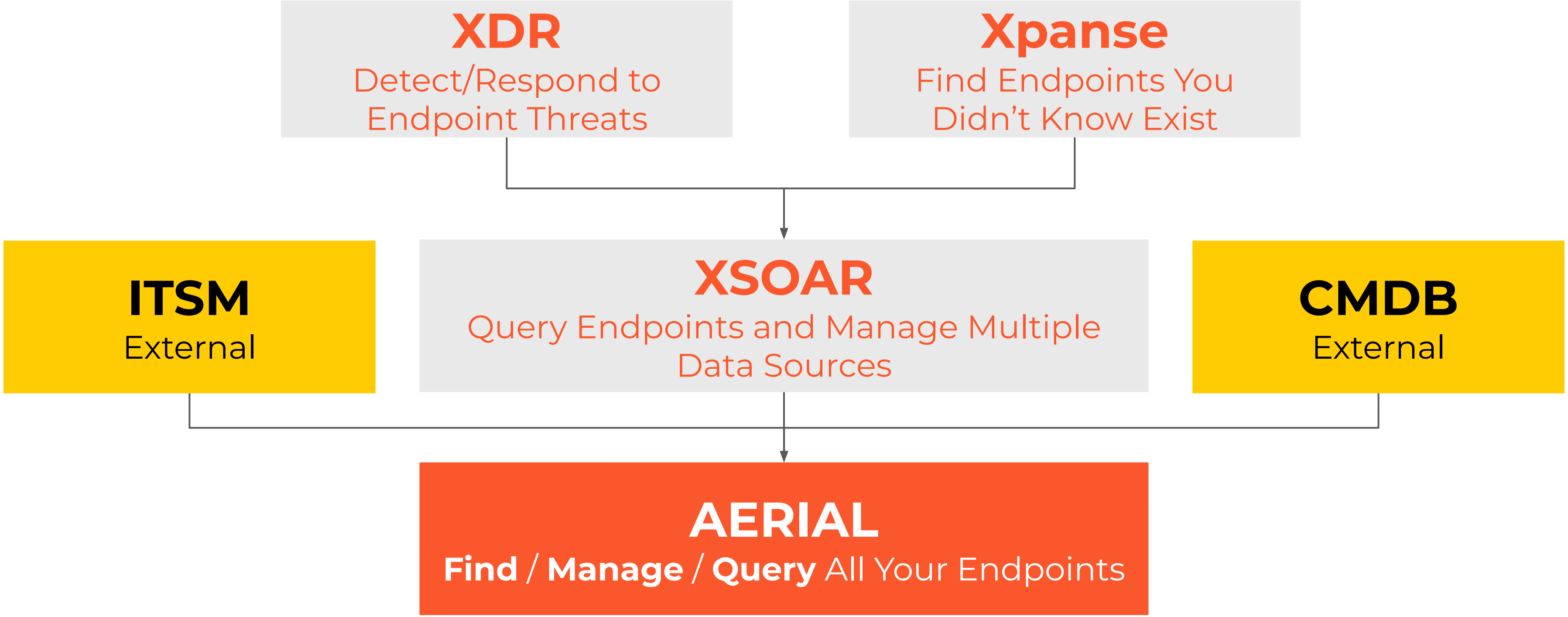


Sources: Team Interviews and Analysis

Aerial - A PANW CAASM Built On Top of Cortex

Proposed Integration

🟨 External Products ⬜ PANW Products 🟧 Aerial



XDR

Detect/Respond to Endpoint Threats

Xpanse

Find Endpoints You Didn’t Know Exist

ITSM

External

XSOAR

Query Endpoints and Manage Multiple Data Sources

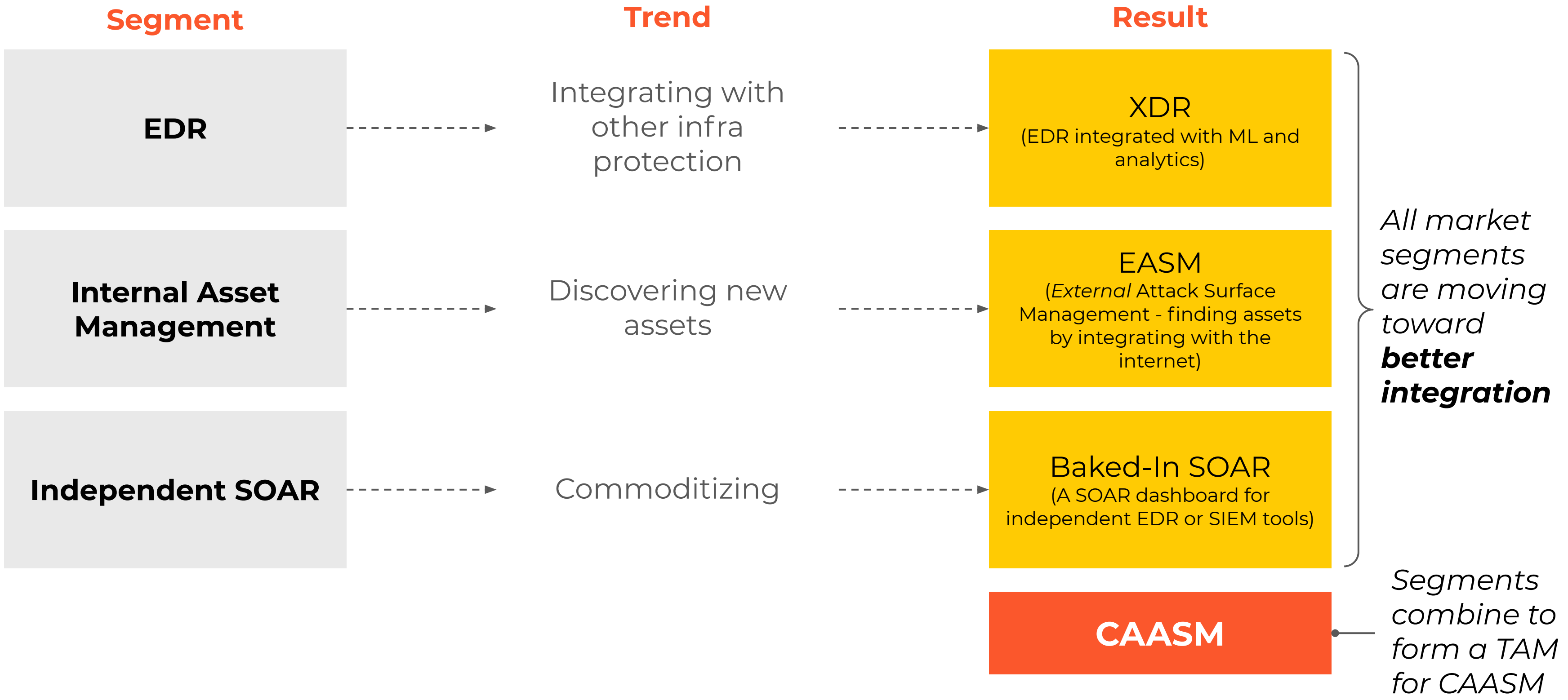
CMDB

External

AERIAL

Find / **Manage** / **Query** All Your Endpoints

The trends in each market segment are naturally driving CAASM Penetration



Segment	Trend	Result
EDR	Integrating with other infra protection	XDR (EDR integrated with ML and analytics)
Internal Asset Management	Discovering new assets	EASM (*External* Attack Surface Management - finding assets by integrating with the internet)
Independent SOAR	Commoditizing	Baked-In SOAR (A SOAR dashboard for independent EDR or SIEM tools)

All market segments are moving toward ***better integration***

CAASM

Segments combine to form a TAM for CAASM

There are 3 primary market segments that combine to form a $9 billion TAM

EDR Segment

14-25% CAGR

$2 billion now to **$6.72 billion in 2026**

SOAR Segment

9-16% CAGR

$1 billion now to **$2 billion in 2026**

EASM Segment

Unknown CAGR

Extrapolate PANW **18.9% market share**

Global Securities & Vulnerabilities Market - 6.3% CAGR
13.8 billion now to 18.7 billion in 2026

$8.72 billion
Total Addressable Market

Serviceable Available Market

Counting just the customers we already have in these segments:

$70 million revenue in 5 years

Assuming $50k per customer annual SaaS price

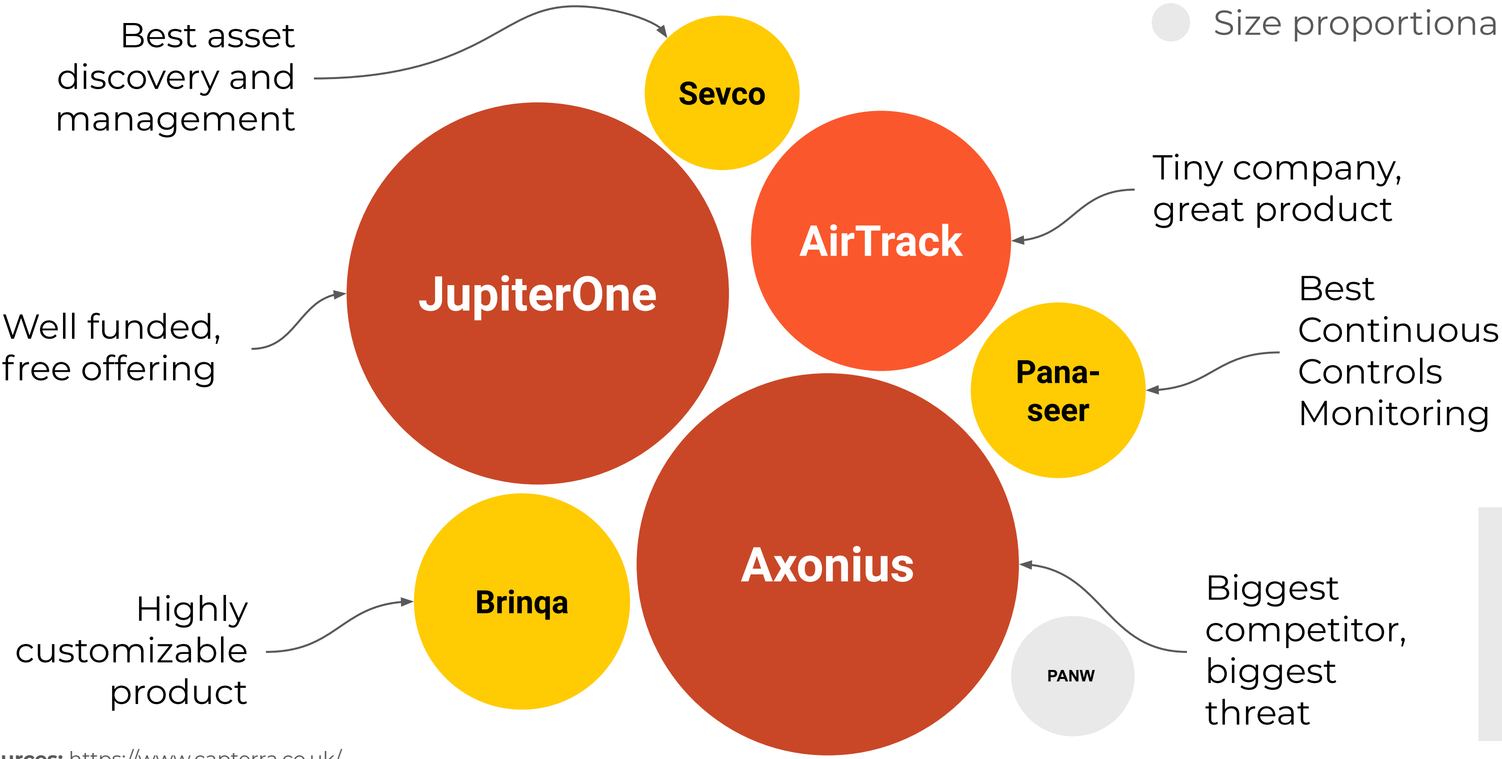
Sources: MarketsAndMarkets, MarketWatch

Most of Project Aerial's Competitors are Startups

Map of PANW CAASM Competitors

High threat — Low threat

Size proportional to maturity



Best asset discovery and management

Tiny company, great product

Well funded, free offering

Best Continuous Controls Monitoring

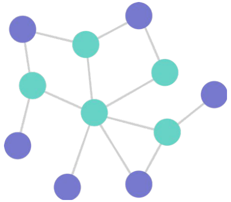
Highly customizable product

Biggest competitor, biggest threat

Detailed competitor profiles in appendix

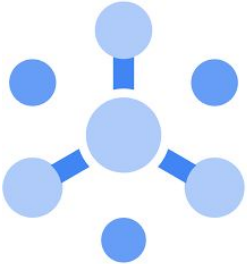
Sources: https://www.capterra.co.uk/

Now: **Leverage** PANW's big **sales** team → make **customization** easy



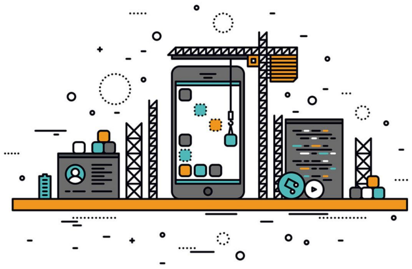
Build one great backend: **single source of truth**

→



Build an **API** to that single source of truth

→



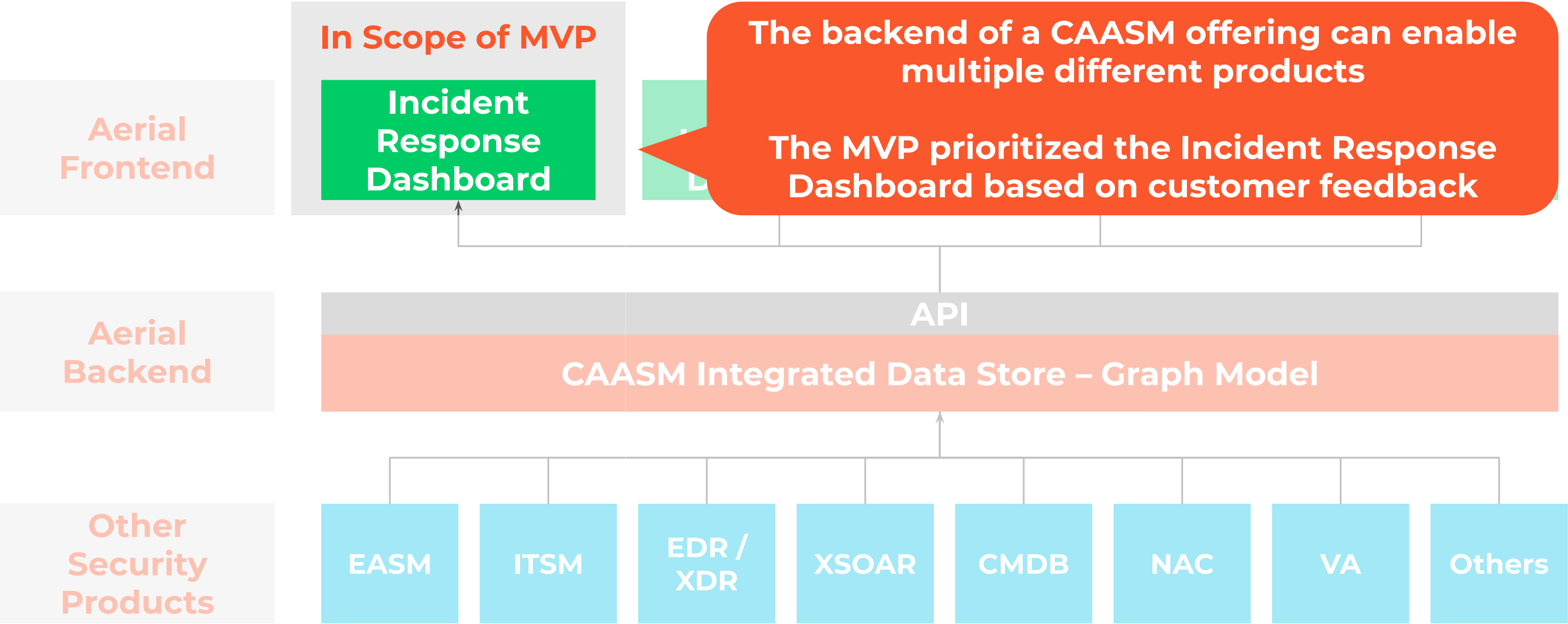
Make **app development** easier.

→

Sell **customized apps** to clients.

Product Vision

Project Aerial integrates cyber asset information to identify, respond faster to, and manage security incidents

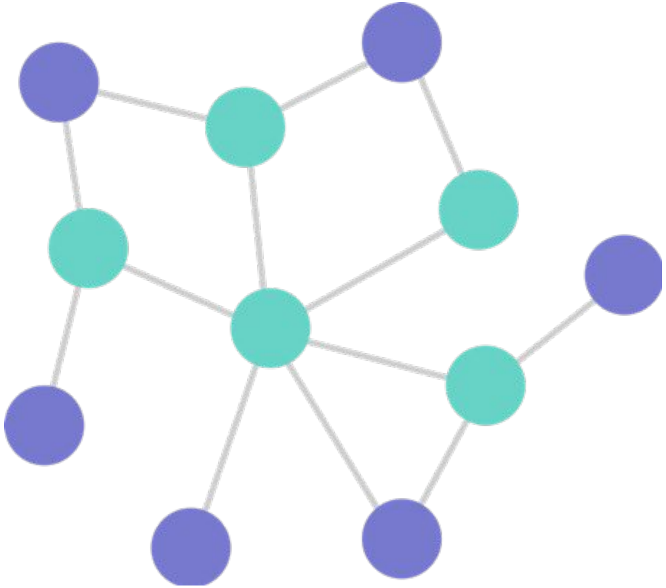


The backend of a CAASM offering can enable multiple different products

The MVP prioritized the Incident Response Dashboard based on customer feedback

Sources: Team Interviews and Analysis

Why PANW’s **Asset Graph is Better:** Technical Perspective



Node: Asset or Incident

Edge: Relationship (e.g., “exposed to”, “belongs to”)

Bigger Graph → **Better Imputation**

PANW tracks:

- More **types** of assets
- More **quantity** of assets
- More **comprehensive** information about assets

Simplifies the problem of **imputing missing links** in a graph with new nodes.

Prototype

Designing an MVP

Design Principles - General

Design Principles

1. Address the JTBD
2. Each feature should solve a user problem
3. Simpler is better
4. Don’t build for problems that do not exist: test before iteration

Design Principles - Cybersecurity-Specific

Design Principles

1. Ease of use by security operators
2. Consolidate data across PANW and external systems that may have different definitions of an asset

Main User Workflows - Operators

Prioritized Features

Part of Mockup: ***Prioritized based on user feedback, feasibility, and relevance to JTBD***

Identify What to Do Next

Resolve Security Attacks and Vulnerabilities

Task Management Interface

Not Part of Mockup (but needed in MVP)

Test and Configure Integrations

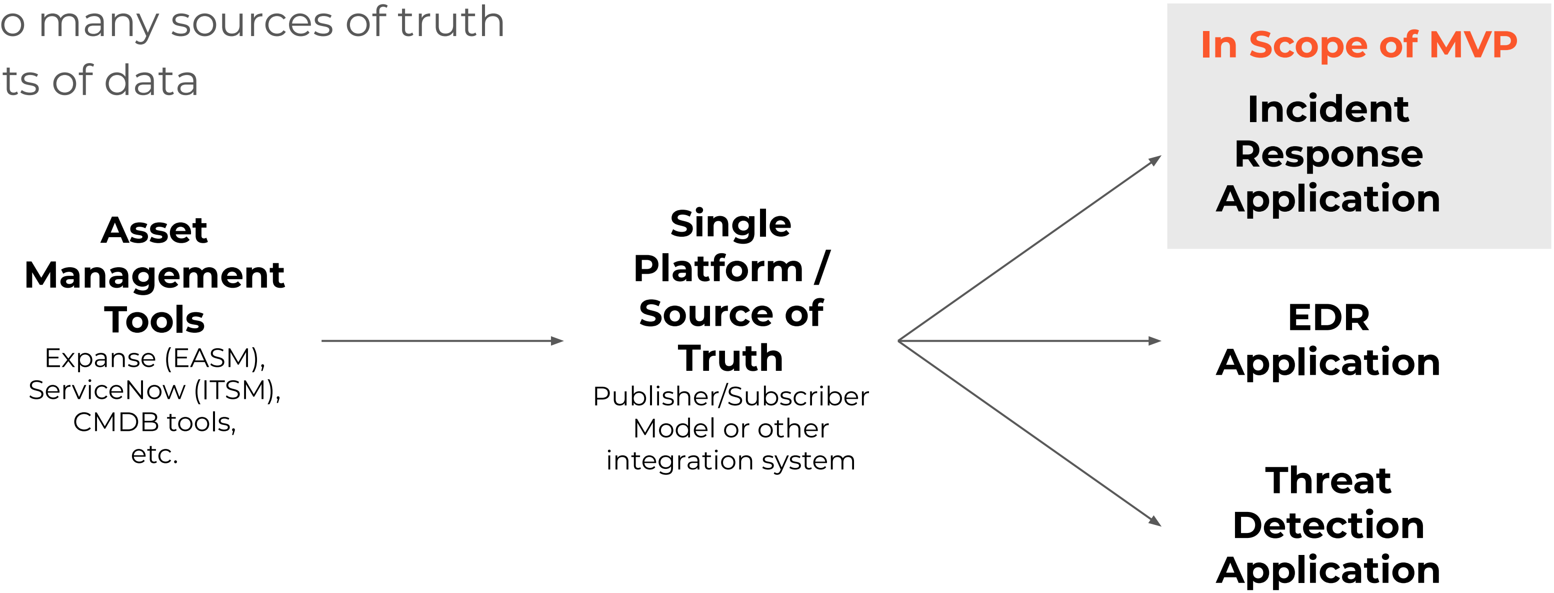
Correct/Change Risk Assessment and Priority

Audit Compliance Report Automation

Why build an Incident Response Dashboard?

Asset management is a *poorly, but diversely* solved problem

- Too many sources of truth
- Lots of data



Asset Management Tools
Expanse (EASM),
ServiceNow (ITSM),
CMDB tools,
etc.

Single Platform / Source of Truth
Publisher/Subscriber
Model or other
integration system

In Scope of MVP

Incident Response Application

EDR Application

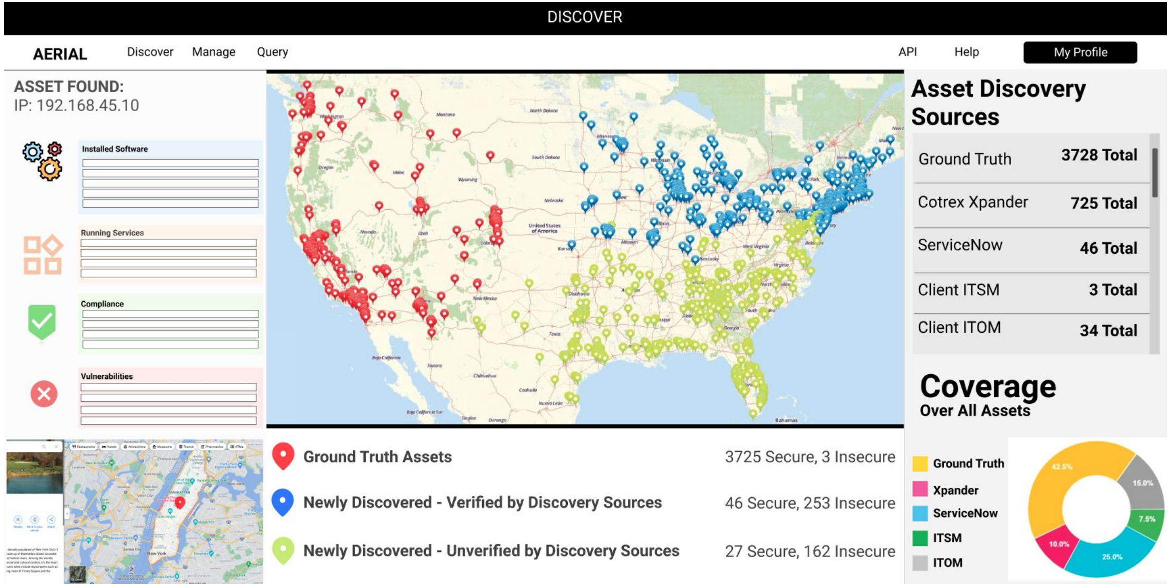
Threat Detection Application

Create a backend for an internal Cortex/CAASM-based *application ecosystem.*

First prototype

Prototype User Story

Visual Representation


DISCOVER

ASSET FOUND:
IP: 192.168.45.10

Asset Discovery Sources

Ground Truth	3728 Total
Cotrex Xpander	725 Total
ServiceNow	46 Total
Client ITSM	3 Total
Client ITOM	34 Total

Ground Truth Assets	3725 Secure, 3 Insecure
Newly Discovered - Verified by Discovery Sources	46 Secure, 253 Insecure
Newly Discovered - Unverified by Discovery Sources	27 Secure, 162 Insecure

Coverage
Over All Assets

Prototype User Feedback:

- Ping: the geographic view is overwhelming; operators would prefer a stack ranking of actionable tasks
- Wren: when there is a vulnerability, the first thing we do is look for who owns the asset

Our Users

Wrentaro Howell

Engineer in the Customer Security Incident Response Team at Target

Ping Wei

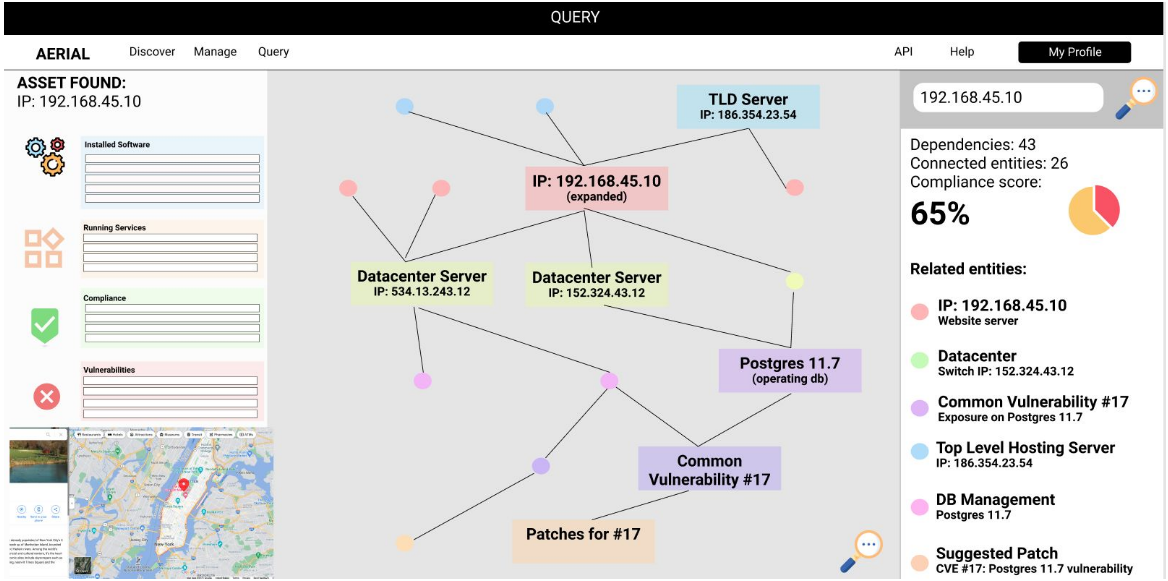
Senior Director of Information Security Operations at Stanford University

paloalto NETWORKS

First prototype

Prototype User Story

Visual Representation



ASSET FOUND:
IP: 192.168.45.10

Dependencies: 43
Connected entities: 26
Compliance score:
65%

Related entities:

- **IP: 192.168.45.10** Website server
- **Datacenter** Switch IP: 152.324.43.12
- **Common Vulnerability #17** Exposure on Postgres 11.7
- **Top Level Hosting Server** IP: 186.354.23.54
- **DB Management** Postgres 11.7
- **Suggested Patch** CVE #17: Postgres 11.7 vulnerability

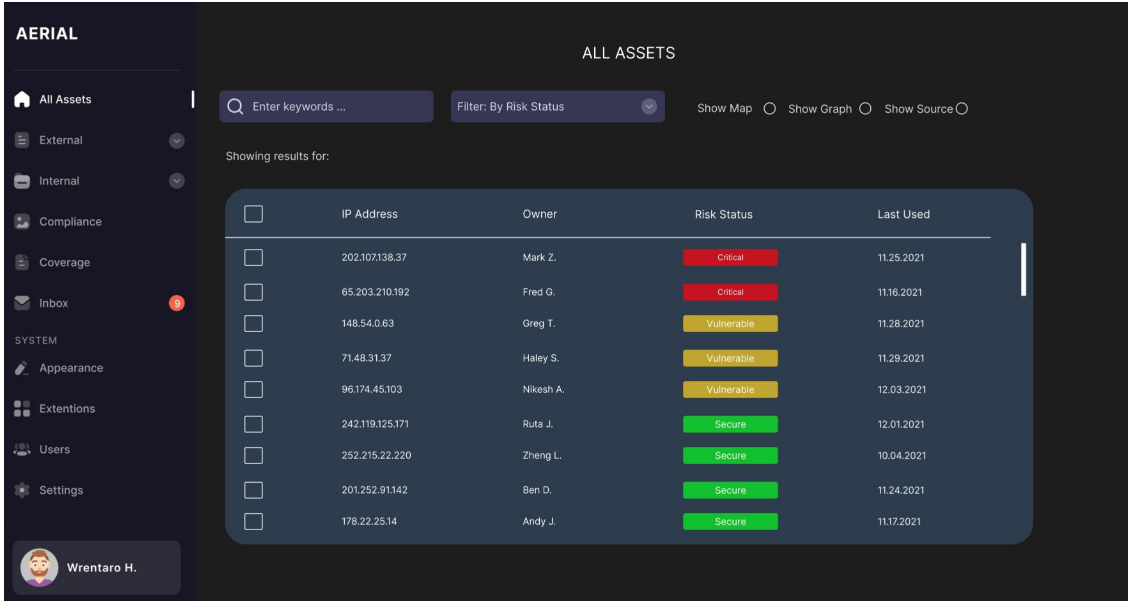
Prototype User Feedback:

- Ping: asset graph is fascinating but distracts from the critical path

Second Prototype

Prototype User Story

Visual Representation



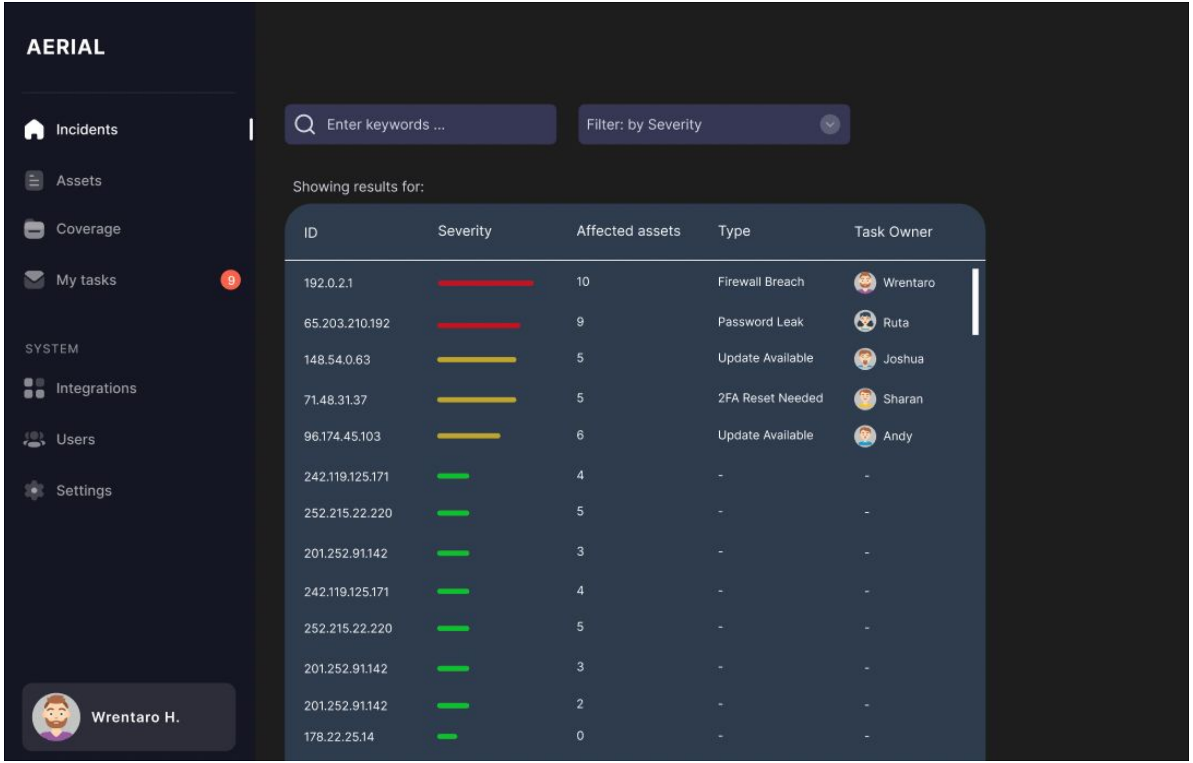
□	IP Address	Owner	Risk Status	Last Used
□	202.107.138.37	Mark Z.	Critical	11.25.2021
□	65.203.210.192	Fred G.	Critical	11.16.2021
□	148.54.0.63	Greg T.	Vulnerable	11.28.2021
□	71.48.31.37	Haley S.	Vulnerable	11.29.2021
□	96.174.45.103	Nikesh A.	Vulnerable	12.03.2021
□	242.119.125.171	Ruta J.	Secure	12.01.2021
□	252.215.22.220	Zheng L.	Secure	10.04.2021
□	201.252.91.142	Ben D.	Secure	11.24.2021
□	178.22.25.14	Andy J.	Secure	11.17.2021

Prototype User Feedback (Greg):

- What does risk status mean?
- Confusing: is each row an asset or incident? Which did you prioritize and why?
- Want to know the data source of each aset

MVP: incident dashboard (final prototype)

Visual Representation



Showing results for:

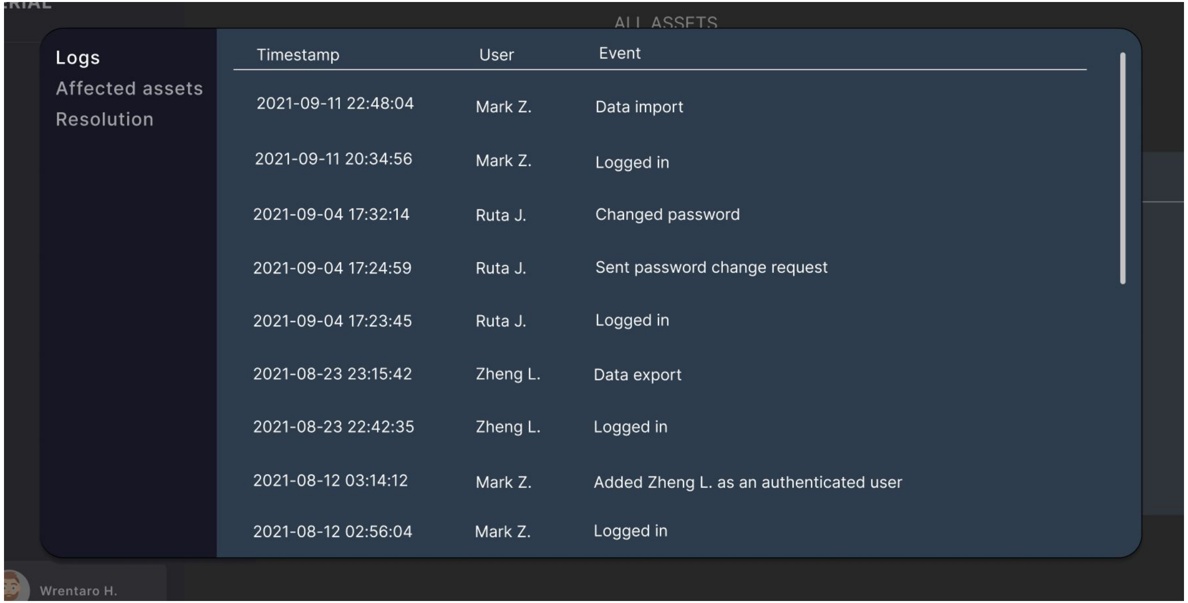
ID	Severity	Affected assets	Type	Task Owner
192.0.2.1	🟥	10	Firewall Breach	Wrentaro
65.203.210.192	🟥	9	Password Leak	Ruta
148.54.0.63	🟨	5	Update Available	Joshua
71.48.31.37	🟨	5	2FA Reset Needed	Sharan
96.174.45.103	🟨	6	Update Available	Andy
242.119.125.171	🟩	4	-	-
252.215.22.220	🟩	5	-	-
201.252.91.142	🟩	3	-	-
242.119.125.171	🟩	4	-	-
252.215.22.220	🟩	5	-	-
201.252.91.142	🟩	3	-	-
201.252.91.142	🟩	2	-	-
178.22.25.14	🟩	0	-	-

Target problems:

- How do we identify incidents that need resolution?
- How do operators prioritize what to do next?
- How can we consolidate all assets affected by an incident?
- Who is the point person for the resolution of an incident?
- Search, filter, and sort through these problems/properties according to specific need

MVP: incident logs (final prototype)

Visual Representation



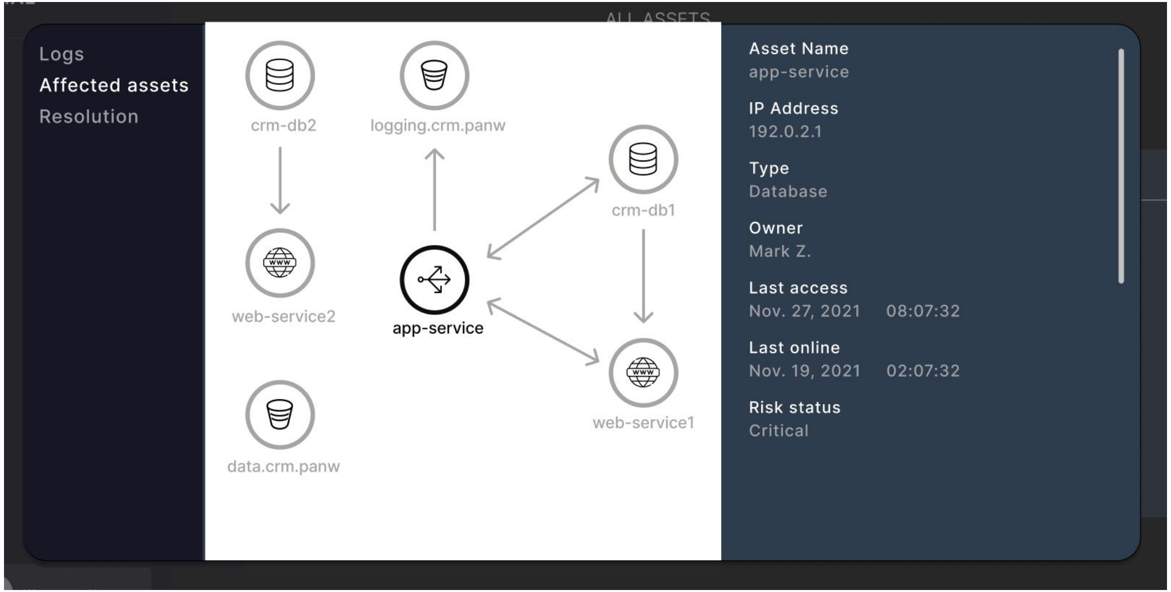
Timestamp	User	Event
2021-09-11 22:48:04	Mark Z.	Data import
2021-09-11 20:34:56	Mark Z.	Logged in
2021-09-04 17:32:14	Ruta J.	Changed password
2021-09-04 17:24:59	Ruta J.	Sent password change request
2021-09-04 17:23:45	Ruta J.	Logged in
2021-08-23 23:15:42	Zheng L.	Data export
2021-08-23 22:42:35	Zheng L.	Logged in
2021-08-12 03:14:12	Mark Z.	Added Zheng L. as an authenticated user
2021-08-12 02:56:04	Mark Z.	Logged in

Target problems:

- Collect and identify necessary information to resolve the vulnerabilities
- How was the vulnerability exposed and how do we prevent this in the future?
- Who are the stakeholders involved in exposing this asset?

MVP: incident affected assets (final prototype)

Visual Representation



Asset Name
app-service

IP Address
192.0.2.1

Type
Database

Owner
Mark Z.

Last access
Nov. 27, 2021 08:07:32

Last online
Nov. 19, 2021 02:07:32

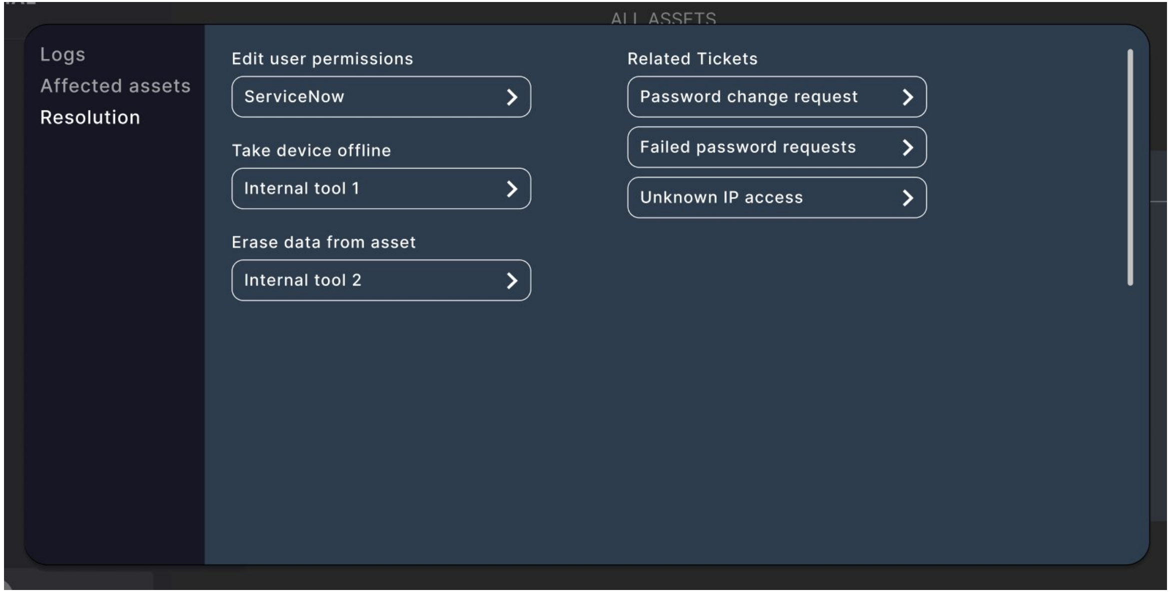
Risk status
Critical

Target problems:

- What are the assets affected by an incident?
- How are these assets related to one another?
- How does a vulnerability of one asset expose other assets?
- What is the critical path to resolving the vulnerability?

MVP: incident resolution (final prototype)

Visual Representation



ALL ASSETS

Logs
Affected assets
Resolution

Edit user permissions

ServiceNow

Take device offline

Internal tool 1

Erase data from asset

Internal tool 2

Related Tickets

Password change request

Failed password requests

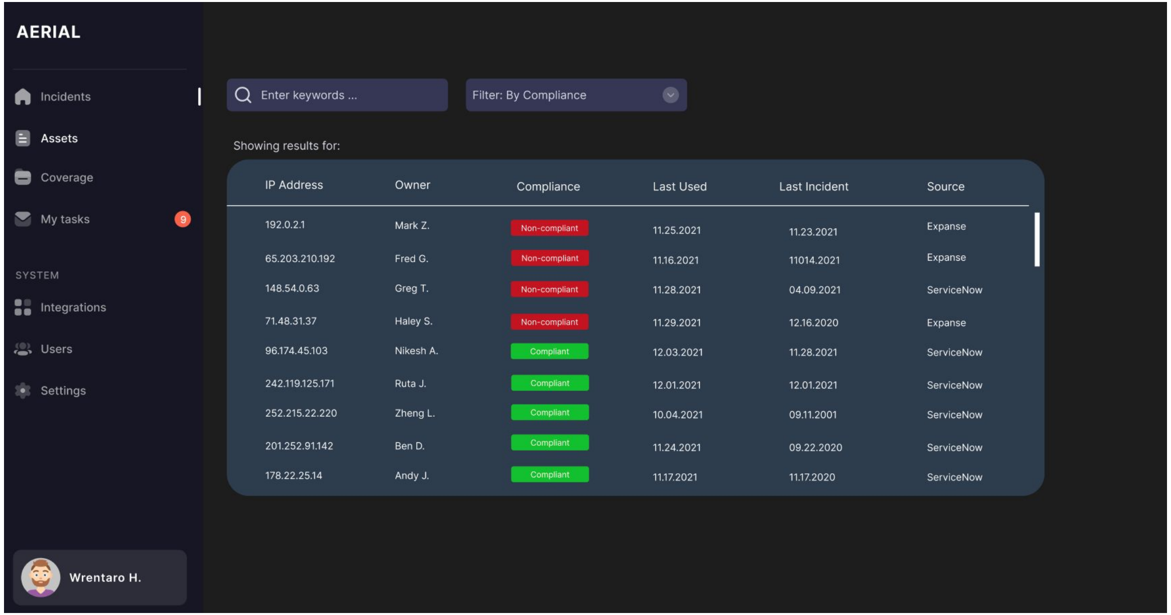
Unknown IP access

Target problems:

- How might I resolve this issue? What options do I have?
- How can I streamline and consolidate vulnerability resolution across multiple providers?

MVP: asset dashboard (final prototype)

Visual Representation



Enter keywords ...

Filter: By Compliance

Showing results for:

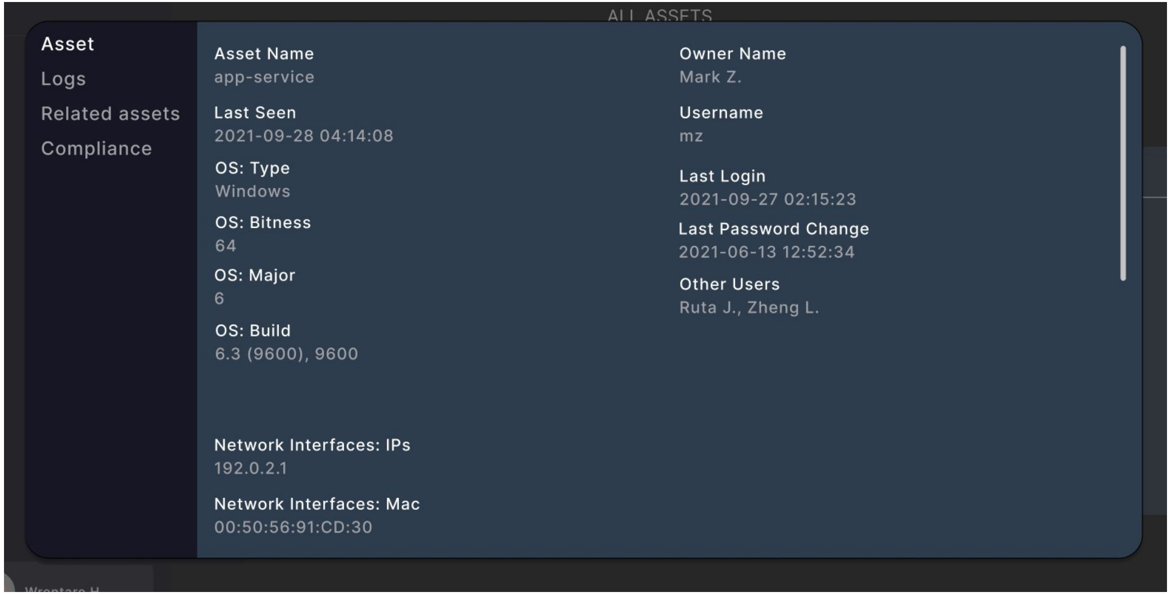
IP Address	Owner	Compliance	Last Used	Last Incident	Source
192.0.2.1	Mark Z.	Non-compliant	11.25.2021	11.23.2021	Expanse
65.203.210.192	Fred G.	Non-compliant	11.16.2021	11014.2021	Expanse
148.54.0.63	Greg T.	Non-compliant	11.28.2021	04.09.2021	ServiceNow
71.48.31.37	Haley S.	Non-compliant	11.29.2021	12.16.2020	Expanse
96.174.45.103	Nikesh A.	Compliant	12.03.2021	11.28.2021	ServiceNow
242.119.125.171	Ruta J.	Compliant	12.01.2021	12.01.2021	ServiceNow
252.215.22.220	Zheng L.	Compliant	10.04.2021	09.11.2001	ServiceNow
201.252.91.142	Ben D.	Compliant	11.24.2021	09.22.2020	ServiceNow
178.22.25.14	Andy J.	Compliant	11.17.2021	11.17.2020	ServiceNow

Target problems:

- Are all my assets compliant?
- How do I track the status and compliance of all assets to prevent vulnerabilities?
- Who is the point person for assets that need attention?
- What is the data source of each asset?
- When was the last incident for relevant assets?
- Search, filter, and sort through these problems/properties according to specific need

MVP: asset details (final prototype)

Visual Representation



ALL ASSETS

Asset

Logs

Related assets

Compliance

Asset Name
app-service

Last Seen
2021-09-28 04:14:08

OS: Type
Windows

OS: Bitness
64

OS: Major
6

OS: Build
6.3 (9600), 9600

Network Interfaces: IPs
192.0.2.1

Network Interfaces: Mac
00:50:56:91:CD:30

Owner Name
Mark Z.

Username
mz

Last Login
2021-09-27 02:15:23

Last Password Change
2021-06-13 12:52:34

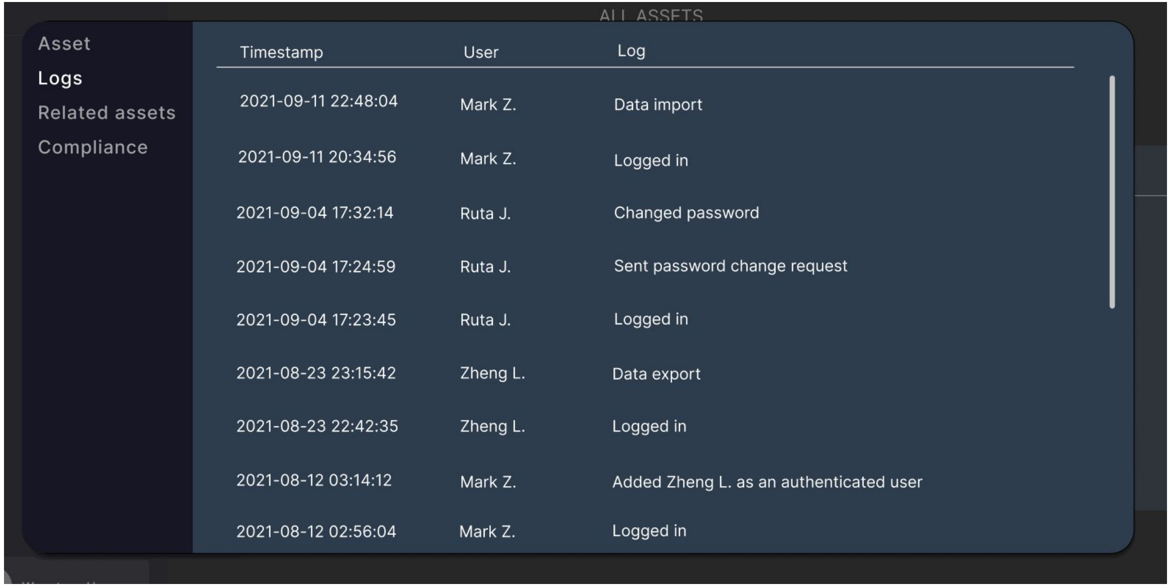
Other Users
Ruta J., Zheng L.

Target problems:

- What are the asset properties that could affect its vulnerability?
- If an asset is vulnerable, what information can I use to inform the resolution?

MVP: asset logs (final prototype)

Visual Representation



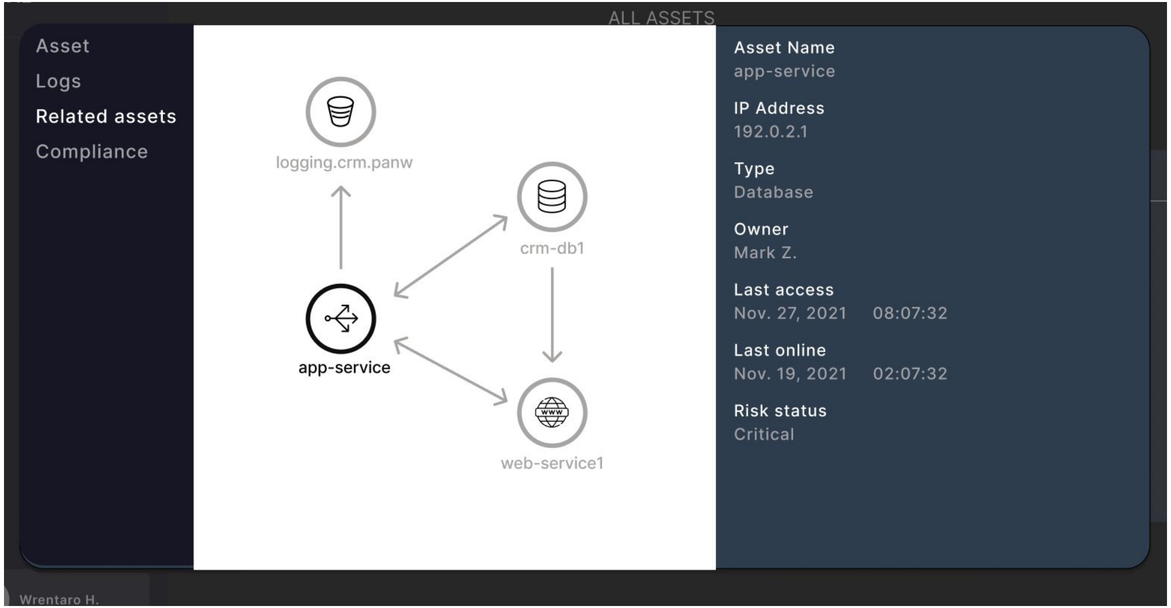
Timestamp	User	Log
2021-09-11 22:48:04	Mark Z.	Data import
2021-09-11 20:34:56	Mark Z.	Logged in
2021-09-04 17:32:14	Ruta J.	Changed password
2021-09-04 17:24:59	Ruta J.	Sent password change request
2021-09-04 17:23:45	Ruta J.	Logged in
2021-08-23 23:15:42	Zheng L.	Data export
2021-08-23 22:42:35	Zheng L.	Logged in
2021-08-12 03:14:12	Mark Z.	Added Zheng L. as an authenticated user
2021-08-12 02:56:04	Mark Z.	Logged in

Target problems:

- Identify suspicious events before a vulnerability is exposed
- Collect and identify necessary information to resolve the vulnerabilities
- How was the vulnerability exposed and how do we prevent this in the future?
- Who are the stakeholders involved in exposing this asset?

MVP: asset logs (final prototype)

Visual Representation



Asset Name
app-service

IP Address
192.0.2.1

Type
Database

Owner
Mark Z.

Last access
Nov. 27, 2021 08:07:32

Last online
Nov. 19, 2021 02:07:32

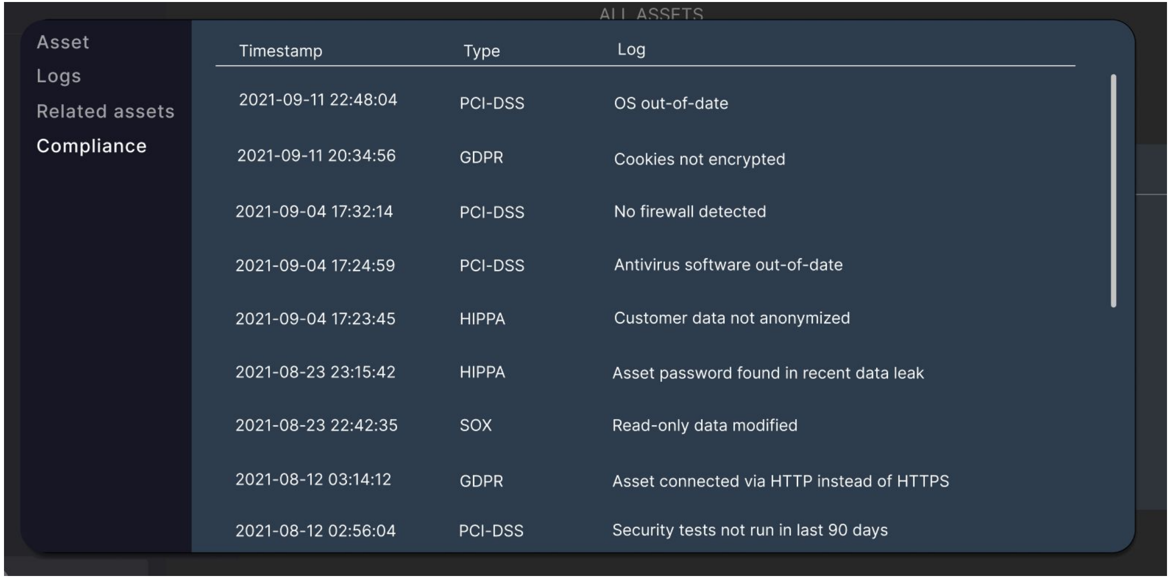
Risk status
Critical

Target problems:

- How are other assets related to this asset?
- Which assets are most important to protect/supervise?

MVP: compliance logs (final prototype)

Visual Representation



Timestamp	Type	Log
2021-09-11 22:48:04	PCI-DSS	OS out-of-date
2021-09-11 20:34:56	GDPR	Cookies not encrypted
2021-09-04 17:32:14	PCI-DSS	No firewall detected
2021-09-04 17:24:59	PCI-DSS	Antivirus software out-of-date
2021-09-04 17:23:45	HIPPA	Customer data not anonymized
2021-08-23 23:15:42	HIPPA	Asset password found in recent data leak
2021-08-23 22:42:35	SOX	Read-only data modified
2021-08-12 03:14:12	GDPR	Asset connected via HTTP instead of HTTPS
2021-08-12 02:56:04	PCI-DSS	Security tests not run in last 90 days

Target problems:

- How has this asset’s level of security changed with time?
- Are there specific gaps in time where this asset was particularly vulnerable?

Visual Representation

Please click on the video to open it in Google Drive

Prototype User Story: Wren’s Experience

Prototype User Story

Wren validated that he can:

- ✓ Quickly **find relevant information** about any asset (internal / external)
- ✓ **Check logs** to find out what went wrong during an incident
- ✓ **See similar/related assets** that might have similar problems now or in the past
- ✓ Quickly **resolve** incidents

> *I like having this one place to find everything I need and fix things*

> *Now I can resolve more issues faster*

Sources: Customer Interviews

Why

What value does this solution hold in the long term?

CAASM’s value proposition creates three additional sources of value for PANW

Project Aerial Value Proposition

Integrate cyber asset information to better identify, respond faster to, and manage security risks

Additional Sources of Value

Improve Value of Other PANW Products

- Combine the existing products into more than the sum of their parts

Upsell existing customers

- Integration can highlight the value of PANW products that customers don’t currently buy
- Aerial offers a new opportunities for product pricing and bundling

Access Small to Mid-Size Businesses

- A free CAASM trial offers a new customer acquisition opportunity for small growing companies with lower security budgets – which may not be targeted by existing PANW sales efforts

Business Model

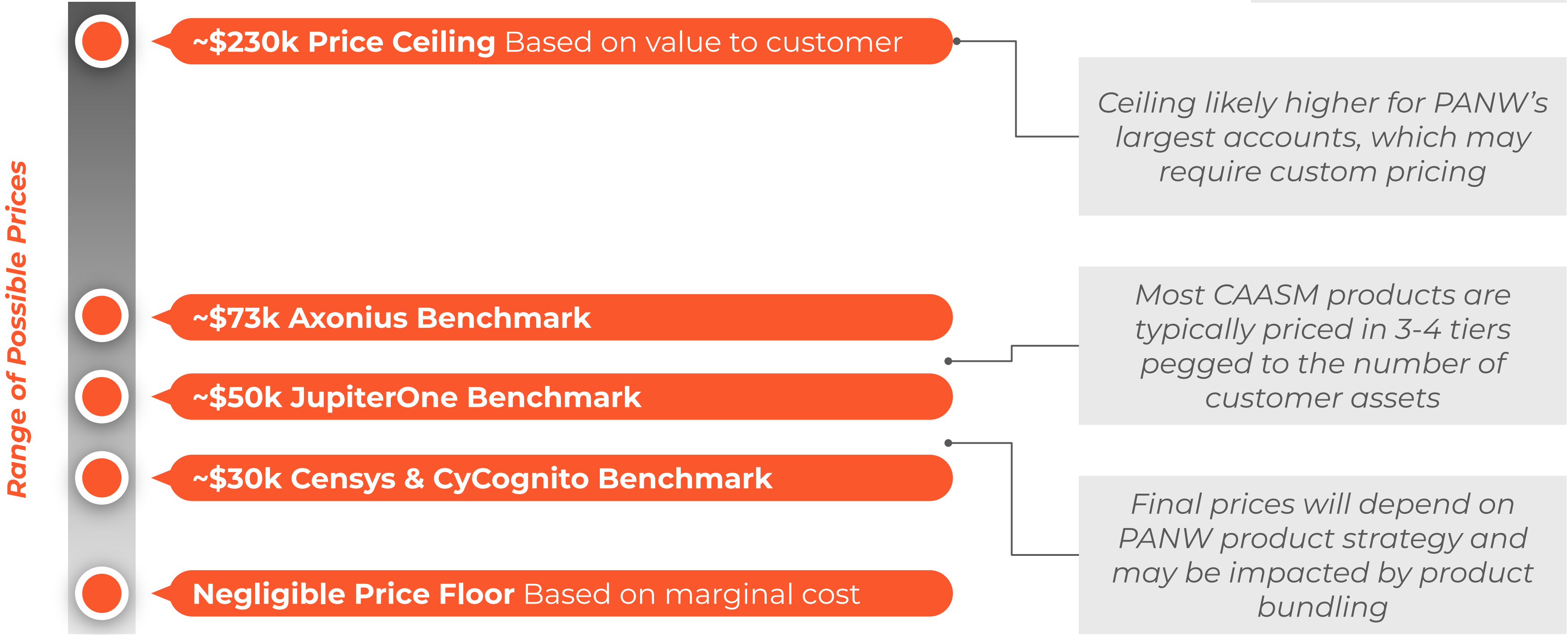
Sources: Team Analysis, PANW and Customer Interviews

Benchmarks suggest Aerial should be priced at $30-80k/yr

Proposed Approach To Pricing (Annual)

Business Model

INDICATIVE ONLY



Range of Possible Prices

~$230k Price Ceiling Based on value to customer

~$73k Axonius Benchmark

~$50k JupiterOne Benchmark

~$30k Censys & CyCognito Benchmark

Negligible Price Floor Based on marginal cost

Ceiling likely higher for PANW's largest accounts, which may require custom pricing

Most CAASM products are typically priced in 3-4 tiers pegged to the number of customer assets

Final prices will depend on PANW product strategy and may be impacted by product bundling

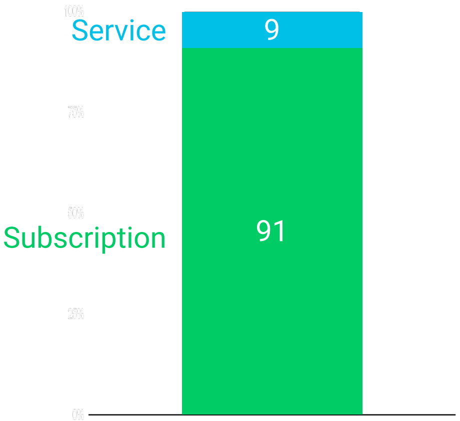
Sources: Team Analysis, PANW and Customer Interviews, Axonius Business Value Assessment, JupiterOne Blog, Censys Press Releases, AWS

Costs: Industry research indicates integrated products typically improve gross margin 10-15%

INDICATIVE ONLY

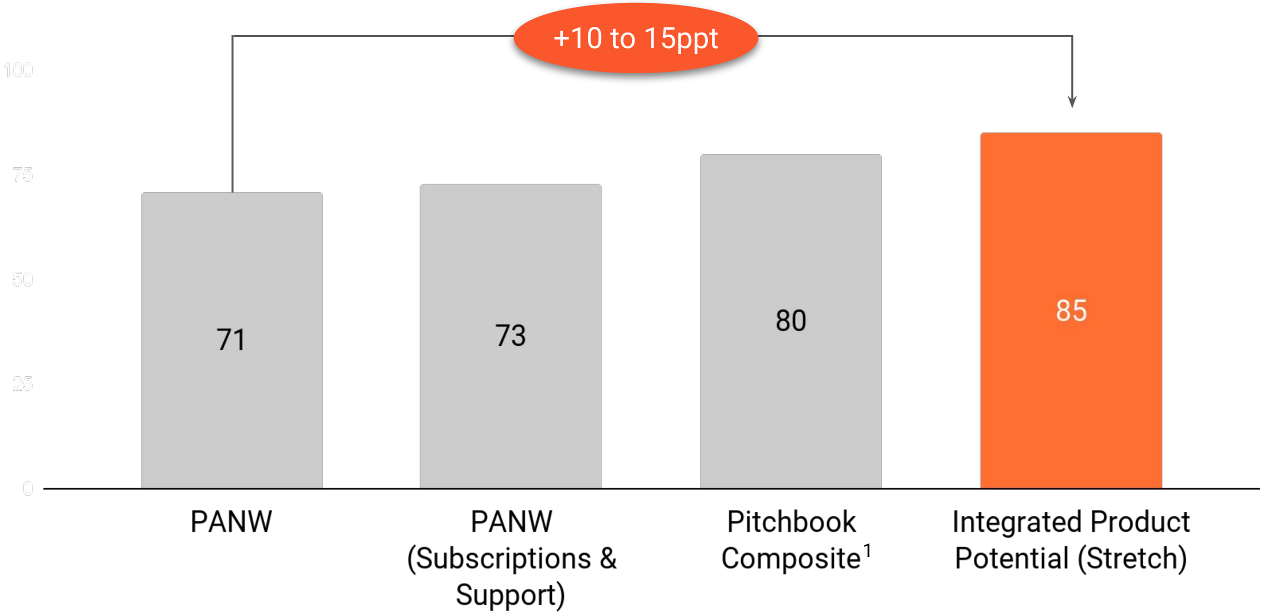
Business Model

Proposed Revenue Structure, %



Benchmarked Against Competitors

Gross Margin %



[1] Based on average margins from startups with high similarity scores to Axonius and JupiterOne

Sources: Team Analysis, PANW Annual report, Axonius Business Value Assessment, PitchBook, McKinsey IT Integration Report

Operationalizing Aerial requires PANW to stand up several new business processes

Business Model

Sales

- Set sales strategy in conjunction with other PANW products
- Develop relevant CAASM bundles, and approach to upselling
- Train sales force
- Adjust sales incentives

Support

- Develop triage process to route customers between PANW support and integrated API offerings
- Decide whether to stand up a new team or integrate support into existing org

Backend

- Establish team to build and maintain ML models
- Establish team to build and maintain integrations
- Establish team to build asset graph

SMBs

- Stand up small dedicated team
- Finalize tiered/freemium offer
- Launch acquisition effort

Sources: Team Analysis, PANW and Customer Interviews

Aerial is estimated to cost $1.5m to build over 5 months

DETAIL ON Next Slide

Dev Time Estimates

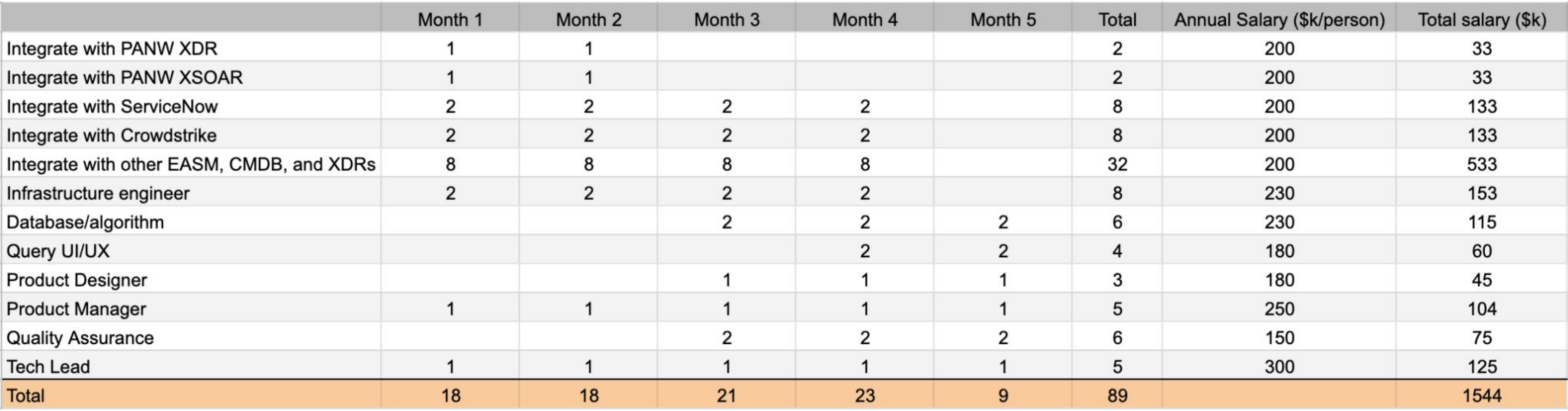
Dev Cost Estimates

Projected Development Costs	
Tech Lead + PM	**$229k**
Infrastructure + UI/UX	**$448k**
Integration with PANW products	**$66k**
Integration with external products (e.g. Crowdstrike EDR, ServiceNow)	**$800k**
Total	**$1.544 million**

*Allocated over **5 months of development***

Sources: Team Analysis and Interviews

Product Development: Team, Technologies, Time, and Cost



	Month 1	Month 2	Month 3	Month 4	Month 5	Total	Annual Salary ($k/person)	Total salary ($k)
Integrate with PANW XDR	1	1				2	200	33
Integrate with PANW XSOAR	1	1				2	200	33
Integrate with ServiceNow	2	2	2	2		8	200	133
Integrate with Crowdstrike	2	2	2	2		8	200	133
Integrate with other EASM, CMDB, and XDRs	8	8	8	8		32	200	533
Infrastructure engineer	2	2	2	2		8	230	153
Database/algorithm			2	2	2	6	230	115
Query UI/UX				2	2	4	180	60
Product Designer			1	1	1	3	180	45
Product Manager	1	1	1	1	1	5	250	104
Quality Assurance			2	2	2	6	150	75
Tech Lead	1	1	1	1	1	5	300	125
Total	18	18	21	23	9	89		1544

Skills Needed:

- Software Engineers specializing in:
  - Database management
  - Infrastructure, QA
  - UI / UX
- Product designers
- Managers

Timeline:

- Month 1: Integration/Infrastructure
- Month 2: Integration/Infrastructure
- Month 3: Integration/Predictive Modeling
- Month 4: Predictive Modeling/Audit Compliance Report Automation
- Month 5: Test and Deployment

Team

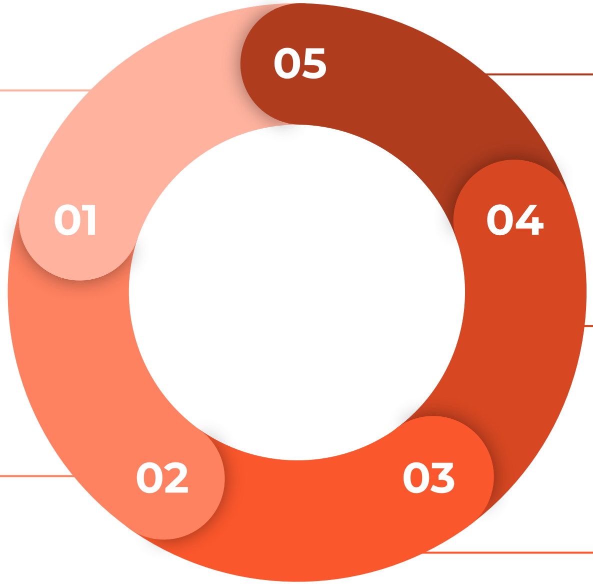
Size

Skills

Technical Roadmap

What does it look like to build CAASM?

Development Methodology



Create API's for each input system to CAASM

Build GraphQL + neo4j infrastructure to support querying security data from XDR, Xpanse, XSOAR, ServiceNow, and CMDB.

Unify Asset Schema Definition

Create a shared schema that captures key attributes of assets, and enforce on each input system to CAASM

Develop Aerial Platform

Establish the core CAASM platform that periodically calls the API's or uses a publisher subscriber model to "listen" for updates on each input system

Build Incident Response Use Case

Build and sell the first use case of CAASM to SecOps teams.

Predict Threats and Automate Compliance

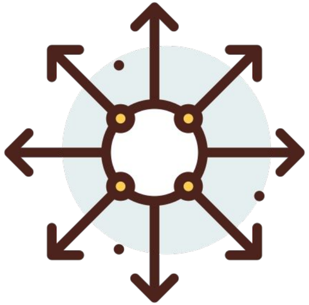
Train machine learning models to predict and prioritize threats, and create visualizations to support explainability. Automate security reports generation for faster audit compliance

Technology Solution Overview

Competitor Products

- Patchwork APIs
- No consolidated definition of an asset
- Inflexible

Project Aerial



- Only outward-facing APIs
- ONE definition of Asset
- Flexible to new asset classes
- Built on a single source of truth that can be used for other applications

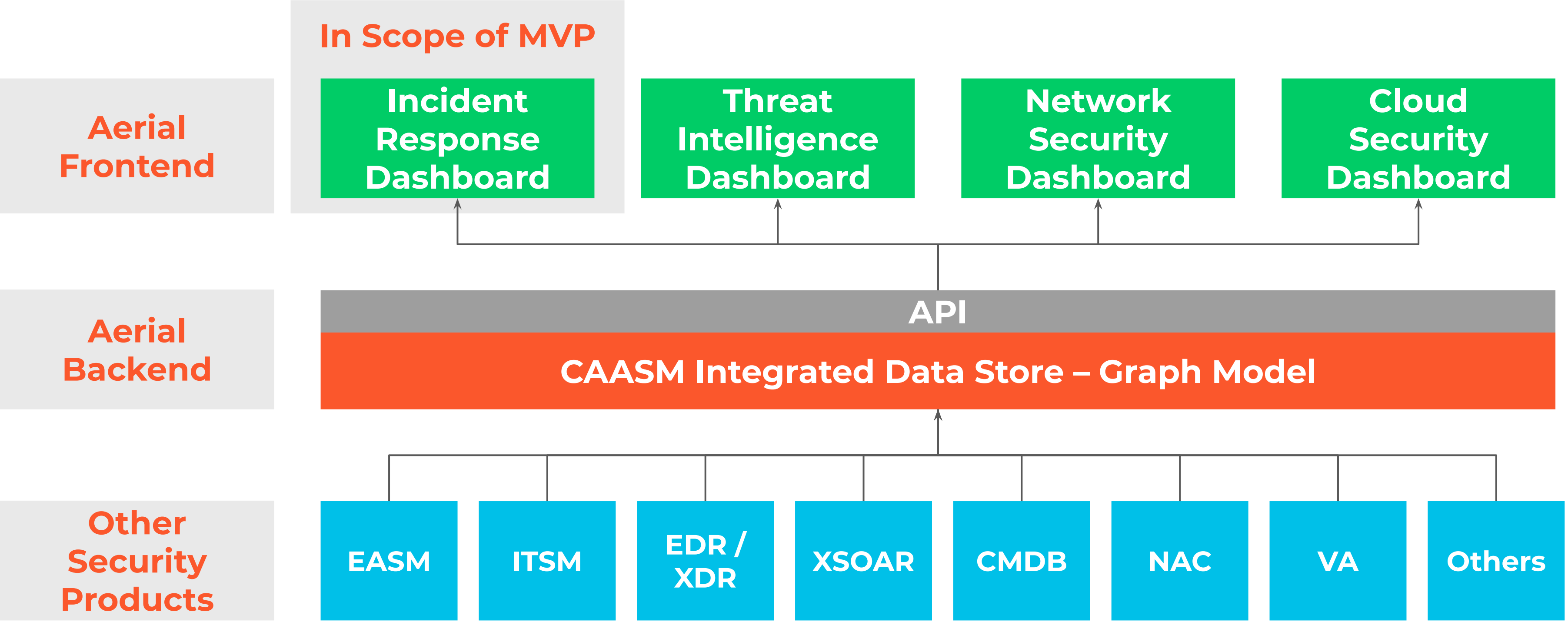
Long Term Trends in Tech Platforms have made Project Aerial Technically Feasible

*In light of the rapid **growth in the number of assets** (both known and unknown), industry trends that favor CAASM development, as reported by the 2021 Gartner Hype Cycle include:*

- Greater **API** Interactivity + Availability
- Prevalent desire for a platform that **consolidates** lots of security capabilities
- Desire for **full visibility** into all assets under an organization's control
- Quicker **audit compliance reporting** through comprehensive asset security reports

Sources: Gartner Hype Cycle for Security Operations (July 23, 2021)

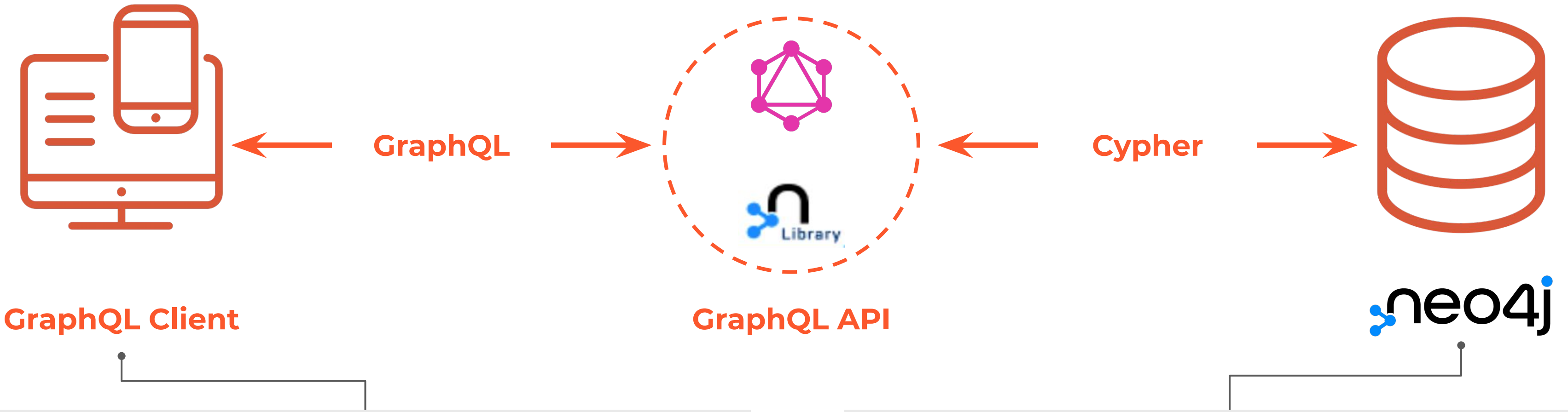
Project Aerial integrates cyber asset information to identify, respond faster to, and manage security incidents



Sources: Team Interviews and Analysis

Long Term Trends in Tech Platforms have made Project Aerial Technically Feasible

There is a shift toward availability of **graph-inspired technologies like GraphQL and Neo4j** to store and query large-scale data, as well as **integrations** between API and database layers



API structure allows clients to flexibly define structure of data required (reduces need for endless REST endpoints to cater to different query structures)

Graph database management system — graph storage and processing. ACID-compliant transactional database accessible via Cypher query language via HTTP endpoint

Sources: Announcing the Neo4j GraphQL Library (April 27, 2021)

Technical Feasibility: Dependencies and Risks

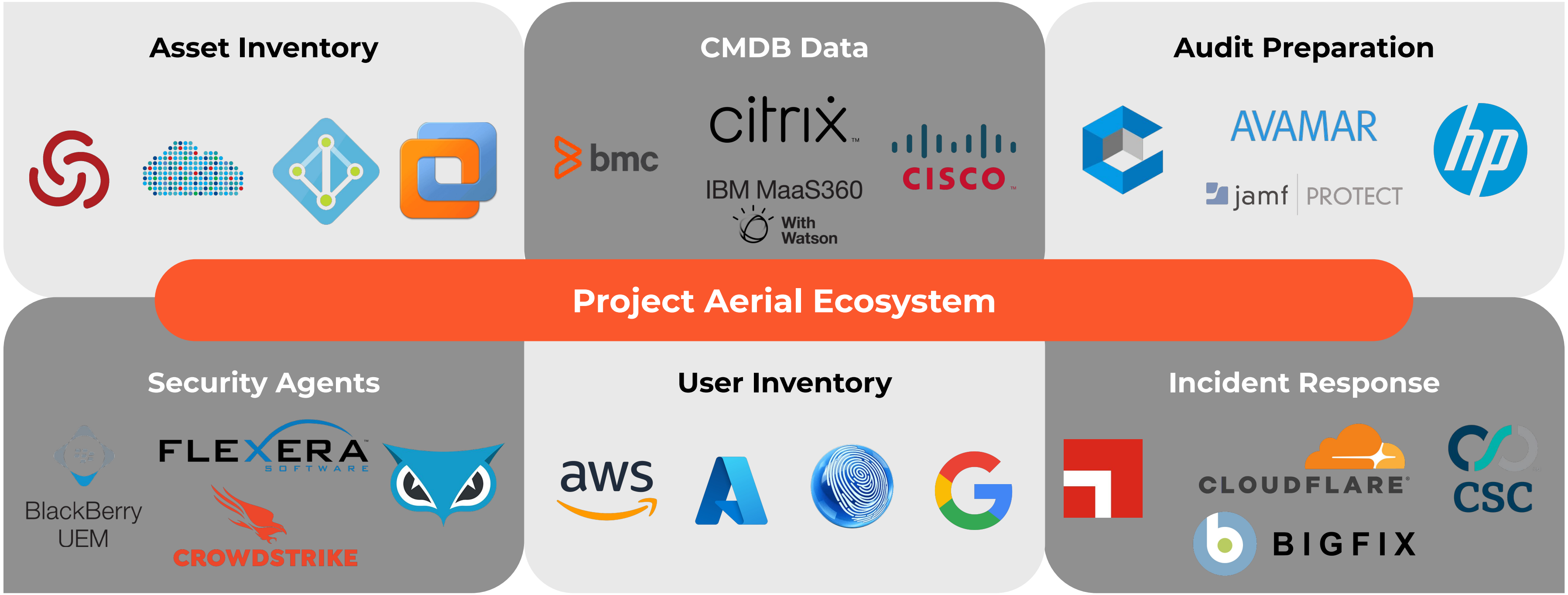
🟥 High risk 🟨 Medium risk 🟩 Low risk

	Dependencies	Risks	Severity
Incident Prioritization *(ensure customer satisfaction)*	Aerial depends on AI/ML models to prioritize incidents, preventing information overload to security officers	Need to **mitigate risks of false precision**. Must also ensure the **model is explainable** when justifying recommendations to SecOps teams.	🟥 False precision may impose legal liability and customer dissatisfaction
Inter-Asset Relationship Graph *(key competitive advantage)*	Aerial depends on supporting robust user question answering and data imputation via an inter-asset graph	May require **restructuring asset data as a graph** (e.g., assets/incidents as nodes and relationships as edges) and **ensuring schema consistency** across inputs to CAASM.	🟥 Asset definitions currently inconsistent across security providers
API Integration *(necessary for product existence)*	Aerial depends on clients' assets being able to integrate into CAASM discovery APIs	May not have readily available endpoints (e.g., GET APIs) for PANW products and **external products**	🟨 Competitors demonstrate integration feasibility

Aerial requires API integration with the security ecosystem

Example Aerial Adapters / Integration in non-PANW Ecosystem

INDICATIVE ONLY – MORE DETAIL IN A FEW SLIDES



Project Aerial Ecosystem

Asset Inventory

CMDB Data

bmc

citrix

IBM MaaS360 With Watson

cisco

Audit Preparation

AVAMAR

jamf PROTECT

hp

Security Agents

BlackBerry UEM

FLEXERA SOFTWARE

CROWDSTRIKE

User Inventory

aws

G

Incident Response

CLOUDFLARE

CSC

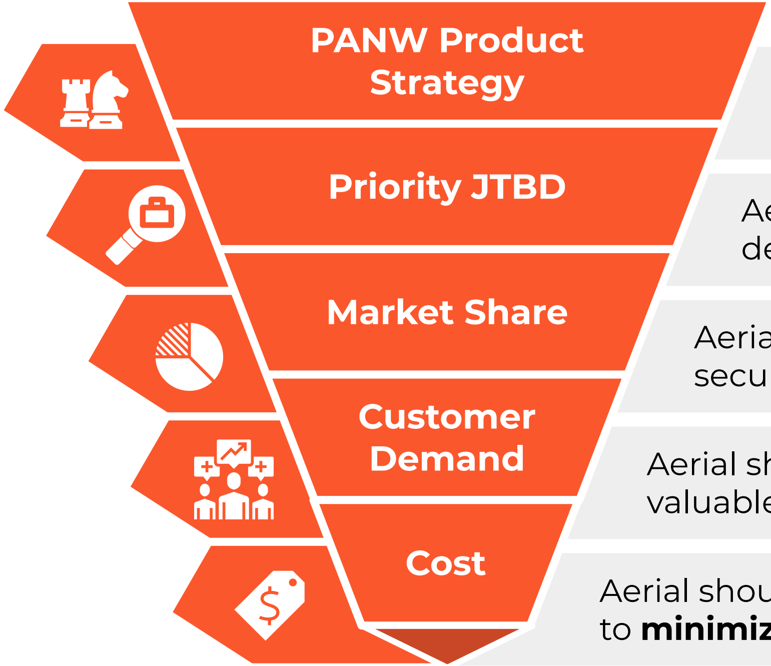
BIGFIX

Sources: Team Analysis, PANW and Customer Interviews, Competitor Benchmarking

Technical Feasibility

The Aerial MVP requires PANW to prioritize API integrations

Proposed Prioritization Funnel for API Integrations



Aerial should **support PANW's position** in the market to and **complement its existing product** portfolio

Aerial should **prioritize the JTBD** identified for the MVP to deliver on its **value proposition**

Aerial should focus on integrating products **widely used** in the security ecosystem to **generate broad appeal**

Aerial should prioritize integrations specifically requested by and valuable to **PANW customers** to drive **rapid adoption**

Aerial should prioritize the **least expensive and complex integrations** to **minimize development costs**

Sources: Team Analysis, Competitor Benchmarking (e.g. Axonius), Grand VIew Research (UEM), MarketsandMarkets (EMM, ITAM/ITSM), Mordor Intelligence (EDR, Threat Intelligence), BusinessWire (Cloud), Fortune BUsiness Insights (IAM, Networking), Datamation (Data Security), Statista (Cloud, Networking), Global Market Insights (NAC), Allied Market Research (PAM), Datanyze (CMBD)

Proposed CAASM API Integration (1/7)

🟧 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
1E Tachyon	UEM, MDM/EMM
Absolute	EDR/EPP, MDM/EMM
Adaptive Shield	Cloud Security, Cloud
ADP	HR, IAM
Airlock Digital	EDR/EPP; Data Security
Alcide	Cloud Security, Cloud
Alert Logic	EDR/EPP
Alibaba Cloud	Cloud Infra, Cloud
Amazon Web Services	Cloud Infra, Cloud
Aqua Security	Containers, Cloud
Arista Extensible OS	Networking
Armis	IoT, Network Security
Aruba	Networking
Aruba AirWave	Networking
Aruba Central	Networking
Aruba ClearPass	NAC, Network Security
Atera	ITAM/ITSM, RMM
Aternity	ITAM/ITSM, Config Mgmt.
Atlassian Jira Assets	ITAM/ITSM
Atlassian Jira Service Dsk	ITAM/ITSM
Atlassian Jira Software	DevOps
Automox	Config Mgmt.
Auvik	Networking
Awake Security	Networking
Axonius Users	ITAM/ITSM
Azure Defender for IoT	OT/IoT, Network Security
Azure DevOps	DevOps
BambooHR	HR, IAM
baramundi	UEM, MDM/EMM
Barracuda CloudGen)	IAM
BeyondTrust Passwords	PAM, IAM
BeyondTrust Privileged	PAM, IAM
BeyondTrust Bomgar	IT Agent, Config Mgmt.
BigID	Data Security
Bitdefender GravityZone	EDR/EPP
bitFit	ITAM/ITSM
BitSight Security Ratings	Cyber Intelligence
BlackBerry UEM	EDR/EPP, MDM, UEM
BlueCat Enterprise DNS	Networking
BMC Atrium ADDM	CMDB, ITAM/ITSM
BMC Atrium CMDB	CMDB, ITAM/ITSM
BMC TrueSight	Config Mgmt., DevOps
Box Platform	Data Security
CA Service Management	ITAM/ITSM, CMDB
CA Spectrum	Networking
Censys	IoT, Network Security
Centrify Identity Services	IAM
Ceridian Dayforce	HR
Check Point Infinity	EDR/EPP, Fwall, NetSec
Checkmarx SAST	AppSec, DevOps
Chef	Config Mgmt.
Cherwell IT Service Mgmt	ITAM/ITSM
Cisco	Networking
Cisco AMP	EDR/EPP
Cisco DNA Center	Networking
Cisco Firepower Mgmt	Networking
Cisco ISE	IAM

Sources: Competitor Benchmarking (e.g. Axonius)

Proposed CAASM API Integration (2/7)

🟧 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
Cisco Meraki	Networking
Cisco Prime	Networking
Cisco Security Manager	Networking
Cisco Stealthwatch	Networking
Cisco UCS Manager	Networking
Cisco Umbrella	Networking
Cisco Unified Comms	IoT, Network Security
Cisco Webex	Remote Conferencing
Citrix ADC	Networking, DevOps
Citrix Director	ITAM/SM, Cloud, DevOps
Citrix Endpoint Mgmt	UEM, MDM/EMM
Claroty	OT, Network Security
CloudHealth	Cloud Infra, Cloud
Cloudfit CFS	Cloud Infra, Cloud
Cloudflare DNS	Networking
CloudPassage Halo	Cloud Infra, Cloud
CoalfireOne	Risk Mgmt.
Code42	DLP, Data Security
Cofense PhishMe	Security Awareness, GRC

Integration	Category
Commvault	Data Security
Contrast Security	AppSec, DevOps
CrowdStrike Falcon	EDR/EPP
CSCDomainManager	Networking
CSV	CMDB, ITAM/ITSM
CyberArk Endpoint Mngr	PAM, IAM
CyberArk Privileged	PAM, IAM
Cybereason Deep Detect	EDR/EPP
CyCognito Platform	Cyber Intelligence
CylancePROTECT	EDR/EPP
Cynet 360	EDR/EPP
Darktrace	Cyber Intelligence, EDR
Datadog	Cloud Mgmt., Cloud
Datto RMM	EDR/EPP, Config Mgmt.
Dell EMC Avamar	DLP, Data Security
Dell iDRAC	RMM, ITAM/ITSM
Dell OpenManage	Infra, NetSec, ITAM/ITSM
Devo	SIEM
Device42	CMDB, ITAM/ITSM

Integration	Category
DigiCert CertCentral	Cert Mgmt., NetSec
DigiCert PKI Platform	Cert Mgmt., NetSec
Digital Shadows	Cyber Intelligence
DivvyCloud	Cloud Mgmt., Cloud
DNS Made Easy	Networking
Dragos Platform	OT, Network Security
Dropbox	Cloud Mgmt., Cloud
Druva Cloud Platform	DLP, Data Security
Duo Beyond	IAM
Dynatrace	Cloud Mgmt., Cloud
Eclypsium	Firmware Sec., NetSec
edgescan	VA Tool
EfficientIP SOLIDserver	Networking
Elasticsearch	CMDB, ITAM/ITSM
Endgame	EDR/EPP
ESET Endpoint Security	EDR/EPP
ExtraHop Reveal(x)	NDR, Network Security
Extreme Networks Cntrl	NAC, Network Security
Extreme Networks WiNG	Networking

Sources: Competitor Benchmarking (e.g. Axonius)

Proposed CAASM API Integration (3/7)

🟧 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
F-Secure Policy Manager	UEM, MDM/EMM
F-Secure Protection	UEM, MDM/EMM
F5 BIG-IP iControl	Networking
F5 BIG-IQ Mgmt	Infra, NetSec, ITAM/SM
FireEye Security	EDR/EPP
FireMon Security Mngr	NetSec
Flexera IT Asset Mgmt	ITAM/ITSM
FlexNet Manager Suite	License Mgmt.
Forcepoint Web Security	IAM, Config Mgmt.
Forcepoint Web Security	IAM, Config Mgmt.
Foreman	Config Mgmt.
ForeScout CounterACT	NAC, Network Security
FortiEDR (enSilo)	EDR/EPP
Fortify Software Security	AppSec, DevOps
FortiClient EMS	EDR/EPP
Fortinet FortiGate	Firewall, NetSec
FreeIPA	IAM
Freshservice	ITAM/ITSM
Frontline VM	VA Tool

Integration	Category
Gigamon GigaVUE-FM	Networking
Gigamon ThreatINSIGHT	MDR, Cyber Intelligence
GitHub	Version Control, DevOps
GitLab	DevOps
Google Cloud Platform	Infra, Cloud, ITAM/ITSM,
Google Workspace	MDM/EMM, IAM
Guardicore	Cloud Security, Cloud
HashiCorp Consul	Networking
Have I Been Pwned	VA Tool
Heimdal Security	Data Security, EDR/PP
HP Integrated Lights-Out	Config Mgmt.
HP Network Node Mngr	Networking
HPE Intelligent	Networking
HPE OneView	ITAM/ITSM
HP Web Jetadmin	Infra, NetSec ITAM/ITSM
HyperSQL	CMDB, ITAM/ITSM
HYPR Passwordless	IAM
IBM BigFix	IT Agent, Config Mgmt.
IBM BigFix Inventory	IT Agent, Config Mgmt.

Integration	Category
IBM Cloud	Cloud Infra, Cloud
IBM Guardium	Data Security
IBM Hardware Mgmt	Infra, Cluster, Containers
IBM MaaS360	CMDB, ITAM/SM, MDM
IBM QRadar	SIEM
IBM Tivoli	Config Mgmt.
iboss cloud	Networking, Cloud Sec
Icinga	Networking
IGEL Universal	MDM/EMM
Illumio Adaptive Security	Networking
Illusive Networks	Deception. Cyber Intel
Imperva DAM	IT Agent, Config Mgmt.
Indegy Industrial	OT, Network Security
Infinipoint	ITAM/SM, Config Mgmt.
Infoblox DDI	Networking
Infoblox NetMRI	Networking
Intrigue	Cyber Intelligence
IP Fabric	Networking
iTop	CMDB, ITAM/ITSM

Sources: Competitor Benchmarking (e.g. Axonius)

paloalto NETWORKS

Proposed CAASM API Integration (4/7)

🟧 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
Ivanti Endpoint Security	EDR/EPP
🟧 Ivanti Security Controls	UEM, MDM/EMM
🟧 Ivanti Service Manager	ITAM/ITSM
🟧 Ivanti Unified Endpoint	UEM
🟧 Jamf Pro	MDM/EMM
🟧 Jamf Protect	EDR/EPP
JSON	CMDB, ITAM/ITSM
JumpCloud	IAM, Directory
🟧 Juniper Junos	Networking
🟧 Juniper Junos Networks	Networking
🟧 Kaseya VSA	IT Agent, Config Mgmt.
Kaspersky Security	EDR/EPP
Kenna Security Platform	VA Tool
Keycloak	IAM
KnowBe4	Security Awareness, GRC
Kolide Fleet	EDR/EPP
Kolide K2	EDR/EPP
Kubernetes	Containers, Cloud
L0phtCrack 7	Password Mgmt., IAM

Integration	Category
Lacework	Cloud Security, Cloud
🟧 Lansweeper	CMDB, ITAM/SM
LastPass	Password Mgmt., IAM
LibreNMS	Networking
LimaCharlie	DevOps
Linux SSH	ITAM/ITSM
LogMeIn Central	MDM/EMM, UEM
LogicMonitor	Infra, NetSec, ITAM/ITSM
LogRhythm	SIEM
Lookout Mobile	EDR/EPP
Malwarebytes Endpoint	EDR/EPP
ManageEngine	EDR/EPP, MDM/EMM
Masscan	VA Tool
🟧 McAfee ePO	EDR/EPP
McAfee MVision Cloud	Cloud Security
Medigate	Networking
Men&Mice DNS Mgmt	Networking
Micro Focus GroupWise	Collaboration
Micro Focus Servers	Config Mgmt.

Integration	Category
Micro Focus SiteScope	Infra, NetSec, ITAM/ITSM,
🟧 Microsoft Active Drctry	IAM, Directory
🟧 Microsoft Azure	Cloud Infra, Cloud
Microsoft Azure AD	IAM, Directory
Microsoft BAM	DLP, Data Security
Microsoft Cloud Security	Cloud Security, Cloud
Microsoft Defender ATP	EDR/EPP
Microsoft Hyper-V	Virtualization, ITAM/ITSM
Microsoft KMS	ITAM/ITSM
Microsoft Lync	Collaboration
Microsoft SCCM	Config Mgmt.
Minerva Labs Endpoint	EDR/EPP
Mist	Infra, Cloud Security
🟧 MobileIron EMM	MDM/EMM
MongoDB	DevOps
Mosyle	MDM/EMM
Nagios XI	Networking
Nasuni	Storage Mgmt.
Nectus	Networking, Infra, ITAM

Sources: Competitor Benchmarking (e.g. Axonius)

Proposed CAASM API Integration (5/7)

🟧 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
NetApp	Storage Mgmt.
NetBox	Networking
NetBrain	Networking
NetIQ Advanced	IAM
Netskope	Networking
Nexthink	ITAM/ITSM
Nmap Security Scanner	VA Tool
Nozomi Guardian	OT/IoT, Network Security
Nutanix AHV	Virtualization, ITAM/ITSM
ObserveIT	UEBA, Network Security
Observium	Networking
Okta	IAM
OmniVista 2500 NMS	Networking
OneLogin	IAM
OpenStack	Cloud Infra, Cloud
openDCIM	Networking
OpenVAS	VA Tool
OpsRamp	ITAM/ITSM
OPSWAT MetaAccess	NAC, Network Security

Integration	Category
Oracle Cloud	Cloud Infra, Cloud
Oracle VM	Virtualization, ITAM/ITSM
Orca Cloud	Cloud Security, Cloud
Ovirt	Virtualization, ITAM/ITSM
PacketFence	NAC, Network Security
Panorays	Cyber Intelligence
PaperCut	IoT, Network Security
PDQ Inventory	ITAM/ITSM
phpIPAM	Networking
PingOne Directory	IAM, Directory
Pivotal Cloud Foundry	Cloud Mgmt., Cloud
PKWARE	DLP, Data Security
Preempt	IAM
PrivX	PAM, IAM
Promisec Endpoint	EDR/EPP
Proofpoint	Email Security
Proofpoint's ObserveIT	UEBA, Network Security
Proxmox VE	Virtualization, ITAM/ITSM
Pulse Connect Secure	Networking

Integration	Category
Puppet	Config Mgmt.
Pure Storage Pure1	Storage Mgmt.
Qualys Cloud Platform	VA Tool
Quest KACE	Networking
Rancher	Containers, Cloud
Randori	Cyber Intelligence
Rapid7 InsightIDR	SIEM
Rapid7 InsightVM	VA Tool
Rapid7 Nexpose	VA Tool
Red Canary	EDR/EPP
Red Hat Ansible Tower	ITAM/ITSM
Red Hat Satellite	Config Mgmt.
RedSeal	Networking
Remediant SecureONE	IAM
RescueAssist (GoToAssist)	IT Agent, ITAM/ITSM
RiskIQ Digital Footprint	ASM., Cyber Intel
RiskSense	VA Tool
Riverbed SCC	Ntwng, AppSec, DevOps
RSA Archer	Risk Mgmt., GRC

Sources: Competitor Benchmarking (e.g. Axonius)

Proposed CAASM API Integration (6/7)

🟥 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
Rumble Discovery	Networking
Sage People	HR, IAM
Sal	MDM/EMM
SaltStack Open Source	SOAR, Config. Mgmt.
SaltStack Enterprise	SOAR, Config Mgmt.
Schneider EcoStruxure IT	DCIM, Data Security
ScopNET	NAC, Network Security
Secdo Endpoint	EDR/EPP
SecureW2 JoinNow	NAC, Network Security
Secureworks Red Cloak	EDR/EPP
Secureworks Taegis XDR	Cyber Intelligence
Sensu	Cloud Mgmt., Cloud
SentinelOne	EDR/EPP
SentinelOne Ranger	EDR/EPP
ServiceNow	CMDB, ITAM/ITSM
SevOne Data Platform	Networking
Shodan	IoT, Network Security
Signal Sciences	AppSec, DevOps
Skybox Firewall	Fiwall, Network Security

Integration	Category
Slack	Collaboration
Smokescreen	Deception
Snipe-IT	ITAM/ITSM
Snow Software Asset Mgt	ITAM/ITSM
SolarWinds Network	ITAM/ITSM
SolarWinds Service Desk	CMDB, ITAM/ITSM
SonicWall	Fwall, Network Security
Sophos Central	EDR/EPP
Sophos Cloud Optix	Cloud Security, Cloud
Sophos Endpoint	EDR/EPP
SOTI MobiControl	MDM/EMM
Spacewalk	Config Mgmt.
Specops Inventory	IT Agent, Config Mgmt.
Spiceworks	Networking
Splunk	SIEM
SQLite	CMDB, ITAM/ITSM
SQL Server	CMDB,ITAM/ITSM
Sumo Logic	Cloud Mgmt., Cloud
Symantec CWP	Config Mgmt., EDR/EPP

Integration	Category
Symantec CCS	VA Tool
Symantec DCS	Data Security
Symantec DLP	DLP, Data Security
Symantec EDR	EDR/EPP
Symantec Encryption	Encryption, Data Security
Symantec Altiris	ITAM/ITSM, Config Mgmt.
Symantec Endpoint	EDR/EPP
SysAid	ITAM/ITSM, Ticketing
Tanium Asset	ITAM/ITSM, Config Mgmt.
Tanium Discover	ITAM/ITSM, Config Mgmt.
Tanium Interact	ITAM/ITSM, Config Mgmt.
Tanium System Status	ITAM/ITSM, Config Mgmt.
TCPWave (IPAM)	Networking
Tenable Nessus	VA Tool
Tenable Nessus CSV File	VA Tool
Tenable.io	VA Tool
Tenable.sc	VA Tool
Threat Stack	Cloud Security, Cloud
Thycotic Secret Server	PAM, IAM

Sources: Competitor Benchmarking (e.g. Axonius)

Proposed CAASM API Integration (7/7)

🟥 Priority, based on interviews & competitor analysis

TO BE REFINED/PRIORITIZED BASED ON PANW CUSTOMER NEEDS

Integration	Category
Torii	SaaS Mgmt, Cloud Infra
🟥 Trend Micro Apex One	EDR/EPP
🟥 Trend Micro Cloud Apps	Cloud Security, Cloud
🟥 Trend Micro Deep Sec	Config Mgmt., EDR/EPP
Tripwire Enterprise	EDR/EPP
TrueFort	AppSec, DevOps
Tufin SecureTrack	Firewall
Twistlock	Containers, Cloud
Ubiquiti Networks UniFi	Networking
UKG Pro	HCM, IAM
Universal SSH Key Mngr	ITAM/ITSM
UpGuard CyberRisk	Cyber Intelligence
Uptycs	UEM, MDM/EMM
Vectra AI	Networking
Venafi	NetSec, Data Security
🟥 VMware Carbon Black	EDR/EPP
VMWare ESXi	Virtualization, ITAM/ITS
VMware Horizon	Virtualization, ITAM/ITSM
VMware vCloud Director	Cloud Mgmt., Cloud

Integration	Category
VMware vROps	Cloud Infra, Cloud
🟥 VMware Workspace ONE	MDM/EMM, UEM
Wazuh	EDR/EPP
Wasp AssetCloud	ITAM/ITSM
Webroot Endpoint	EDR/EPP
🟥 Web Server Information	ITAM/ITSM
🟥 Windows DHCP Server	Networking
🟥 Windows WMI	ITAM/ITSM
🟥 Windows SFC	Cloud Infra, Cloud
🟥 Windows SUS	Config Mgmt.
Wiz	Cloud Security
Workday	ERP
Zabbix	Cloud Mgmt., Cloud
Zerto	DLP, Data Security
Zoom	Remote Conferencing
Zscaler Web Security	Secure Web Gateways, Network Security

Sources: Competitor Benchmarking (e.g. Axonius)

Next Steps

Concretize **product roadmap** with PANW team

Build support for **incident response**

Continue building **API integrations** with existing PANW products

Release **alpha version** and iterate

Why now?

Market Trends

1. Work from home and movement to Cloud = more assets

2. EDR → XDR
   ITSM → EASM
   Products are becoming integrated.

Build Exposure

3. Bring in customers with needs not addressed by existing products.

4. Defend against other market entrants by creating a "sticky product"

Why now?

Market Trends

1 Work from home and movement to Cloud = more assets

2 EDR → XDR ITSM → EASM Products are becoming integrated.

Build Exposure

3 Bring in customers with needs not addressed by existing products.

4 Defend against other market entrants by creating a "sticky product"

Proactive Competitive Strategy

1. **Create the best product first**
2. **Leverage resources and sales team to dominate the market**

AERIAL

Team
Class Context
Motivation
Problem
User Story
Solution
What is CAASM?
User Workflows
MVP Video
User Prototype Experience

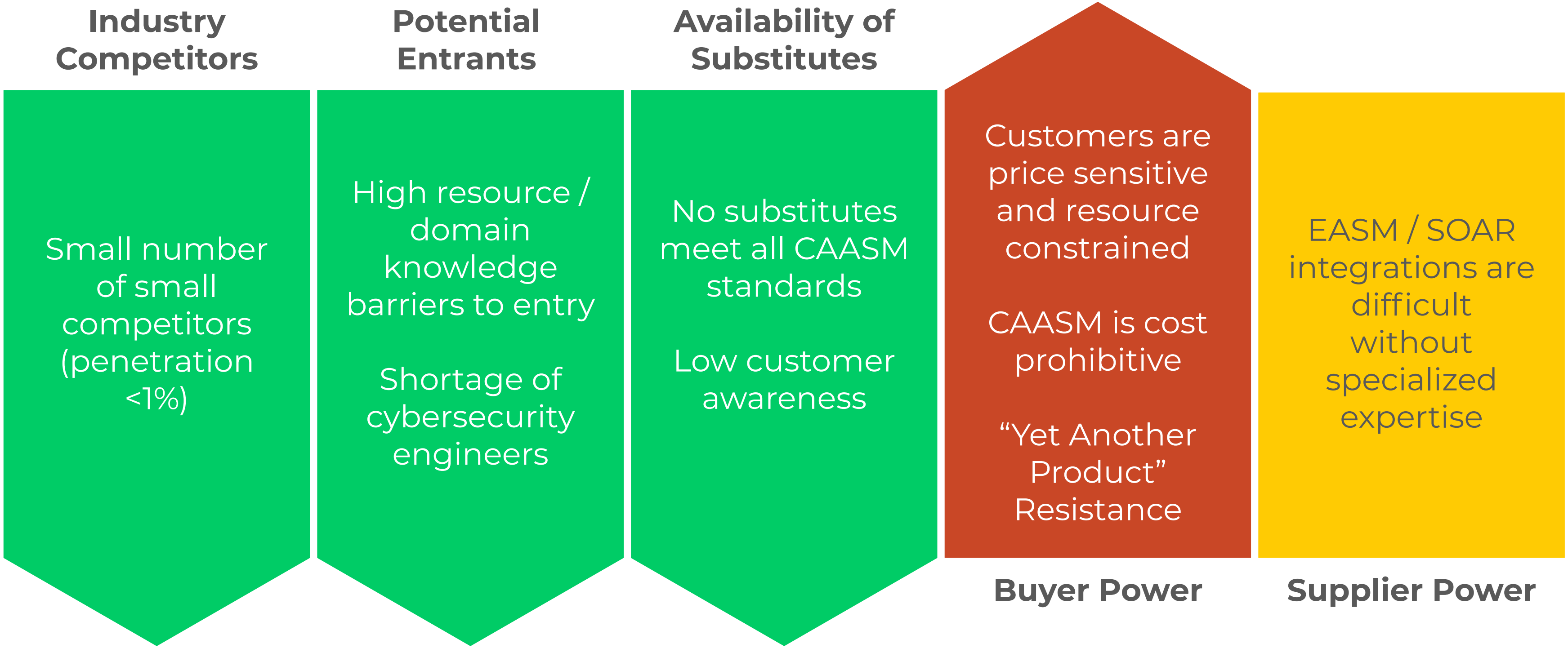
Value Proposition
Pricing
Cost to Build
Margins
Business Processes
Technical Roadmap
Tech Trends
Technical Feasibility
Ecosystem
Integrations Prioritization

Thank you! Questions?

Appendix

Competitive analysis suggests the market is attractive

Porter's Five Forces



Industry Competitors

Small number of small competitors (penetration <1%)

Potential Entrants

High resource / domain knowledge barriers to entry

Shortage of cybersecurity engineers

Availability of Substitutes

No substitutes meet all CAASM standards

Low customer awareness

Buyer Power

Customers are price sensitive and resource constrained

CAASM is cost prohibitive

"Yet Another Product" Resistance

Supplier Power

EASM / SOAR integrations are difficult without specialized expertise

Sources: Gartner Hype Cycle for Security Operations, 2021

Most of Project Aerial’s Competitors are Startups (2/2)

AXONIUS

- Large start-up (~500 employees) worth ~$1.2 billion
- Product meets 22/50 CAASM standards
- Leader in the CAASM space with the most customers

JupiterOne

- Moderately-sized new start-up (~150 employees)
- Product meets 16/50 CAASM standards
- Offer CAASM free-of-charge for small entities (<1000 assets)

brinqa

- Moderately-sized start-up (~100 employees)
- Product meets 19/50 CAASM standards
- Offer different variations with scalable pricing model

panaseer

- Moderately-sized new start-up (~200 employees)
- Product meets 16/50 CAASM standards
- Leader in CCM but slowly moving into CAASM space

SEVCO SECURITY

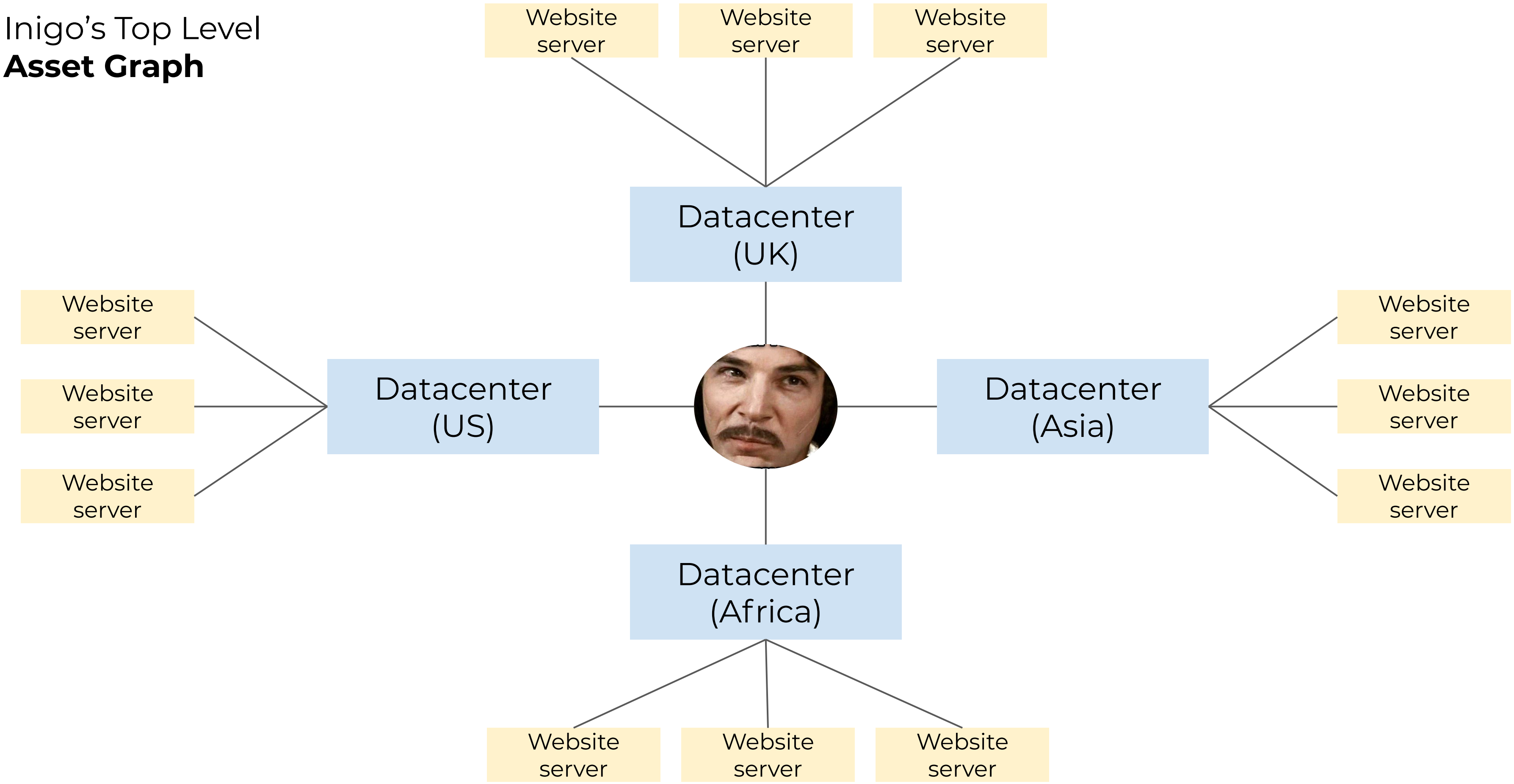
- Small and new start-up (~50 employees)
- Product meets 21/50 CAASM standards
- Offer a wide array of features for asset discovery and management

AIRTRACK

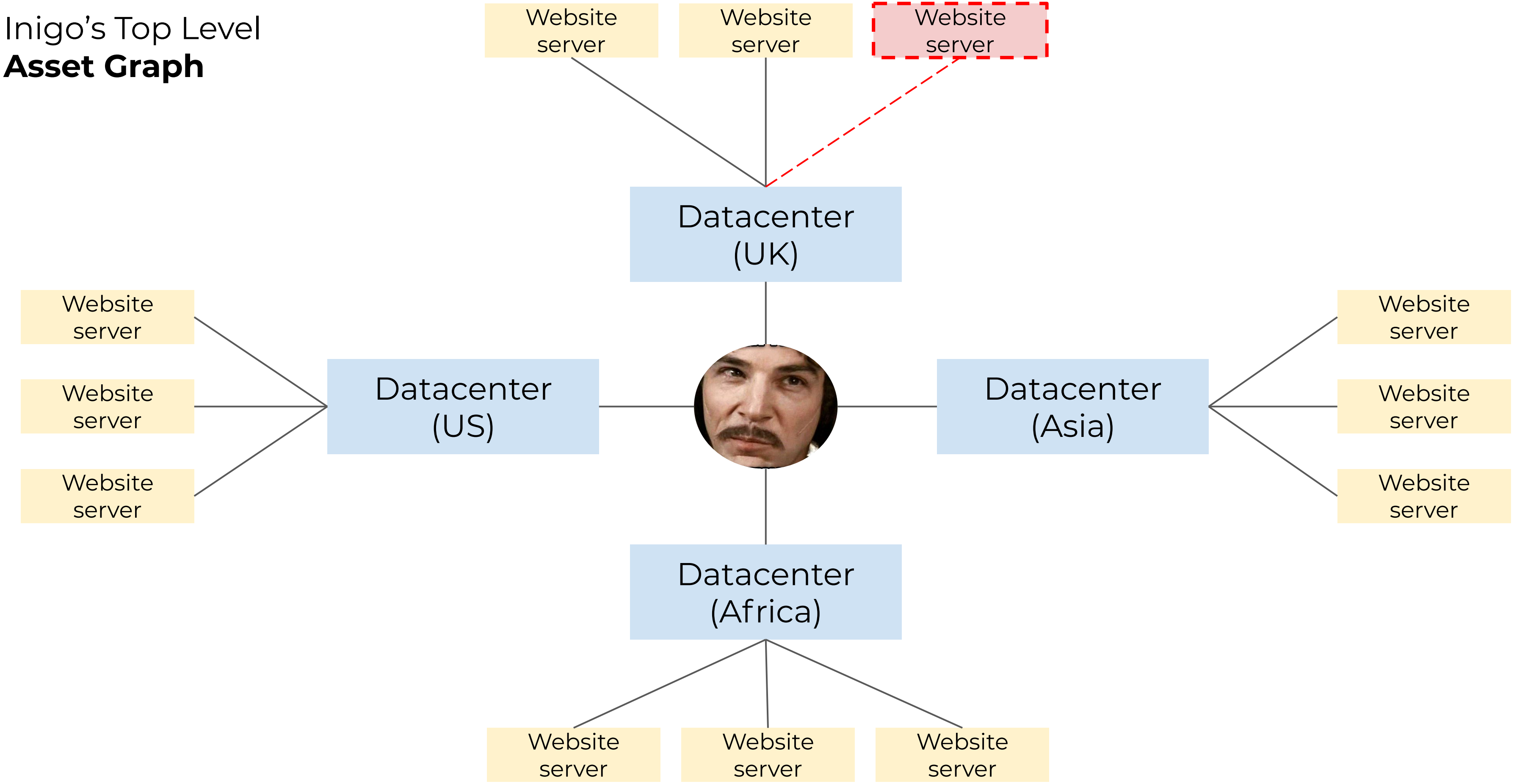
- Small and unfunded start-up (~15 employees)
- Product meets most CAASM standards among competitors (34/50)
- Cheap and subscription-based product

Sources: https://www.capterra.co.uk/

Inigo’s Top Level **Asset Graph**



Inigo's Top Level **Asset Graph**



One of his servers in the UK is . . . vulnerable

Website server

What Inigo wants:

- Website **should *not* go down** for the UK
- Services running on that server should be **restarted**
- **Redundant data stores** should be used instead of corrupted ones
- Nearby servers should step in to **handle the load** while the vulnerable one is down

1. Which server (asset) is down?
2. What's running on that server / connected to it?

What is an **Asset?**

Datacenter

Website Server

Serverless Function

IAM Role

Hosted Domain

Endpoint Detection & Response (EDR) → anything that runs a service

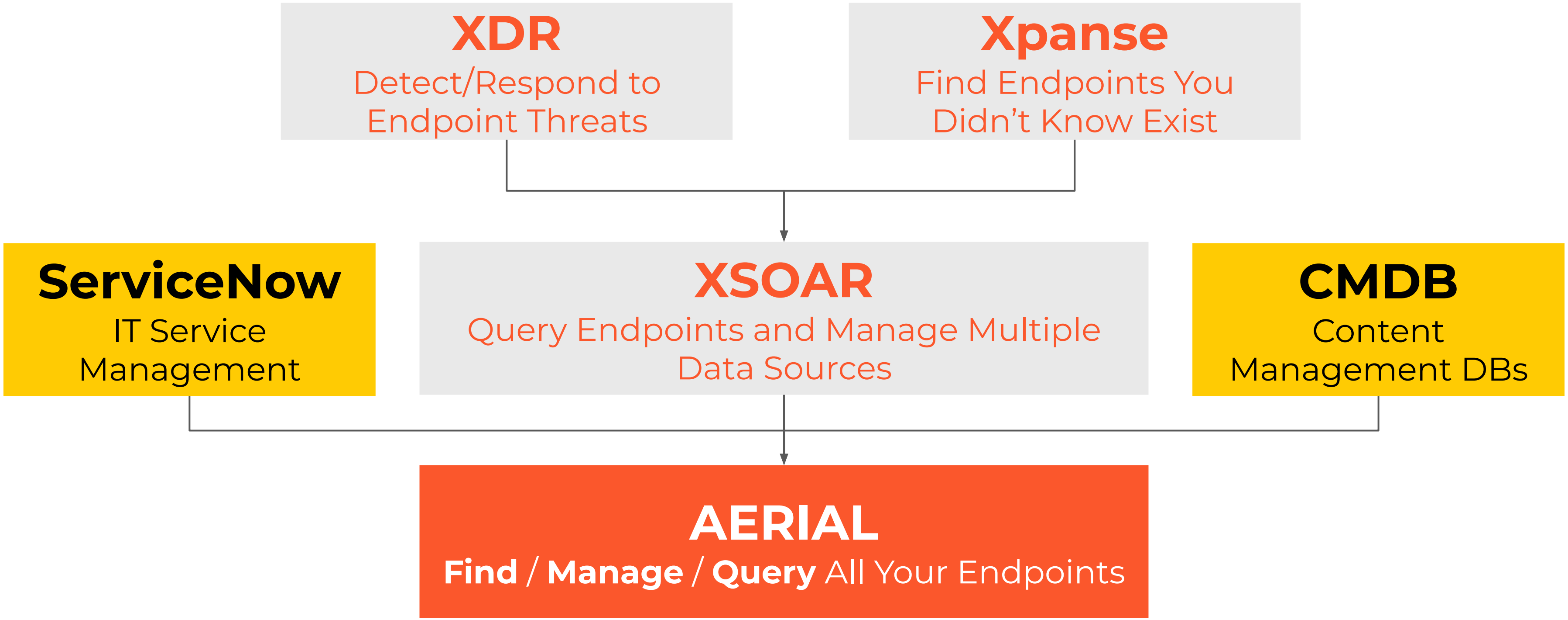
External Attack Surface Management → anything with an external IP address

Configuration Management Database → anything that has been configured/installed

Our simpler definition: **entities that are owned by an organization that have value and could be compromised.**

All the **things that track assets**

🟨 External Products ⬜ PANW Products 🟧 Aerial



XDR
Detect/Respond to Endpoint Threats

Xpanse
Find Endpoints You Didn’t Know Exist

ServiceNow
IT Service Management

XSOAR
Query Endpoints and Manage Multiple Data Sources

CMDB
Content Management DBs

AERIAL
Find / **Manage** / **Query** All Your Endpoints

Sources: Team analysis

Finding Assets

Xpanse

Find Endpoints You Didn't Know Exist

Jobs this does:

- **Finds external assets you didn't know exist**
- Find sites that link to dontbememe.com
- Find IAM roles that have write access
- Find serverless functions that generate memes
- Find users and bots with permissions

ONTARIO
QUÉBEC
Ottawa
MAINE
Boston
New York
MONTANA
NORTH DAKOTA
SOUTH DAKOTA
MINNESOTA
WISCONSIN
MICHIGAN
OREGON
IDAHO
WYOMING
NEBRASKA
IOWA
ILLINOIS
INDIANA
OHIO
NEVADA
UTAH
COLORADO
KANSAS
MISSOURI
San Francisco
CALIFORNIA
Las Vegas
Los Angeles
San Diego
ARIZONA
NEW MEXICO
OKLAHOMA
ARKANSAS
MISSISSIPPI
ALABAMA
TEXAS
LOUISIANA
Houston
SOUTH CAROLINA
FLORIDA
Gulf of California
Gulf of Mexico
Mexico

This is a map of **Florin**. Yes, Florin.

Managing Assets

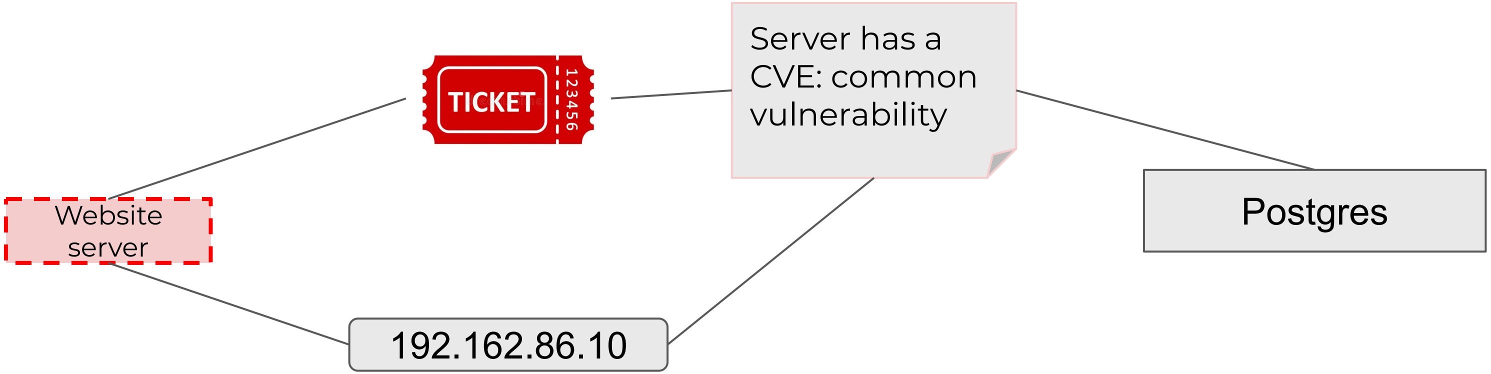
XDR
Detect/Respond to Endpoint Threats

ServiceNow
IT Service Management

CMDB
Content Management DBs

Jobs this does:

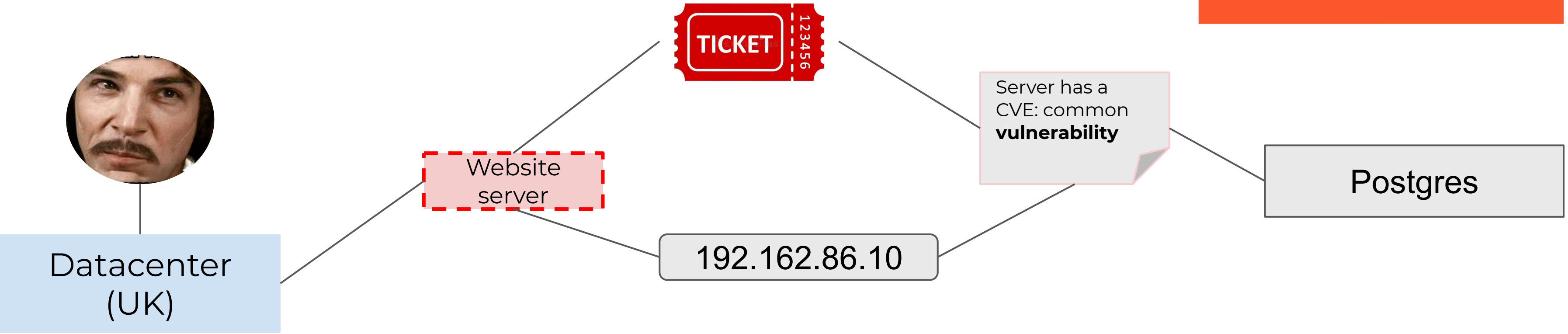
- **Connect external IP to running services**
- Find open **tickets** (incidents)
- Find asset **history** (past incidents)
- Find out how **compliant** the asset is



Server has a CVE: common vulnerability

Querying Assets

AERIAL



192.162.86.10

Website server	**IP: 192.162.86.10, Running postgres 11.7, found 1 CVE, 42 dependencies, UK**
Website server	IP: 192.162.86.11, Running mongodb v3, found 0 CVE, 96 dependencies, UK
Hosted Domain	IP: 192.162.86.12, Running postgres 11.9, found 0 CVE, 42 dependencies, UK