VECTRA®

SECURITY THAT THINKS.®

Cloud Infrastructure from an Attackers Perspective

Kat Traxler | Principal Security Researcher – Public Cloud
ktraxler@vectra.ai

November 2023

About Me

kattraxler.github.io. // @NightmareJs

- Researching the tactics, techniques and procedures of threat actors in the cloud
- Passionate about communicating the unique risks of the cloud
- In my past lives I've worked in:
  - Cloud Security Engineering
  - Application Security Penetration Testing
  - Secure Code Review
  - Cloud Security Architecture
  - App Development
  - Security Training and Course Development

What Makes the Cloud Uniquely Challenging?

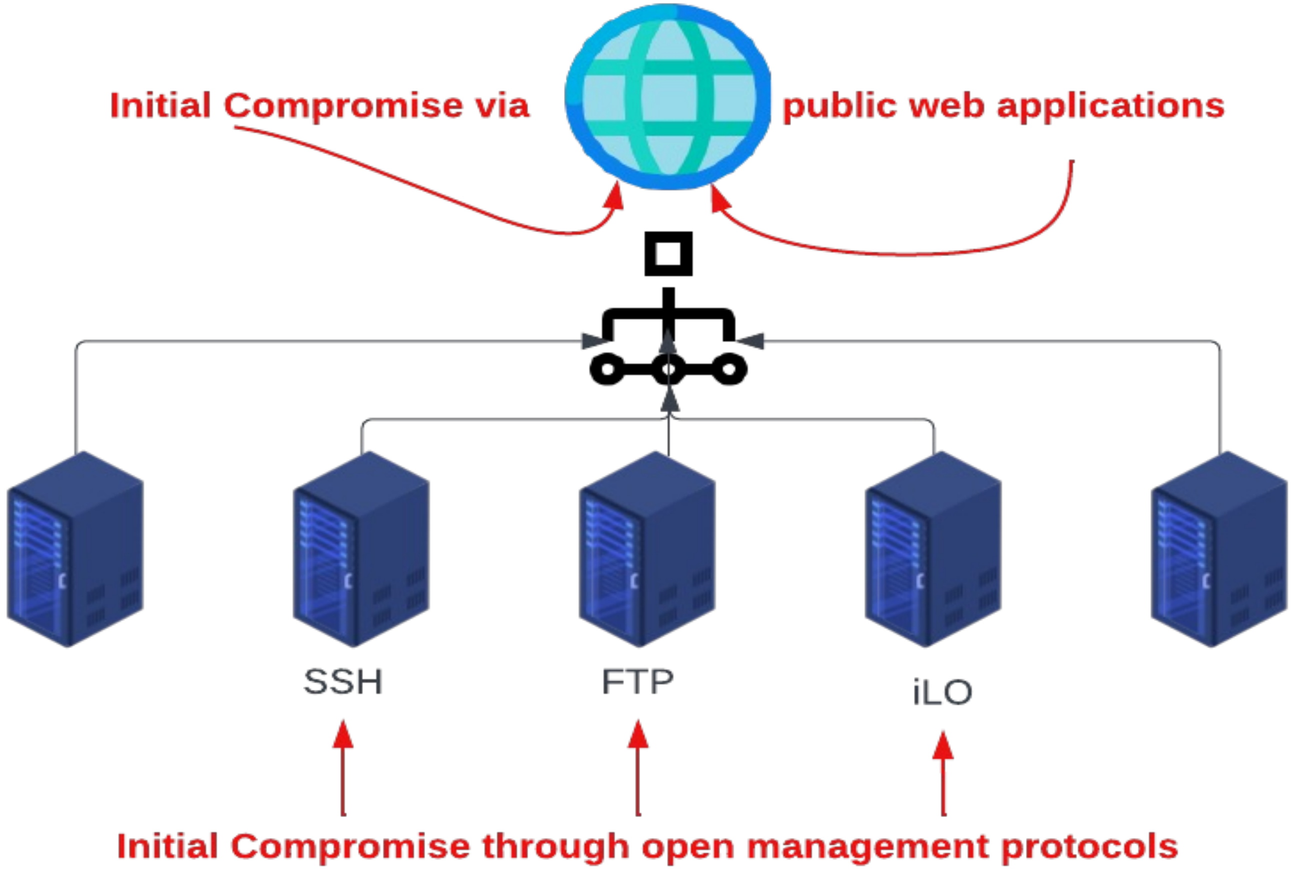
In the cloud, the playing field is scrambled?

- Shared Responsibility Model
- Lack of Physical Control
- Multiple (and new) Attack Vectors
- Multi-Tenancy

Agenda

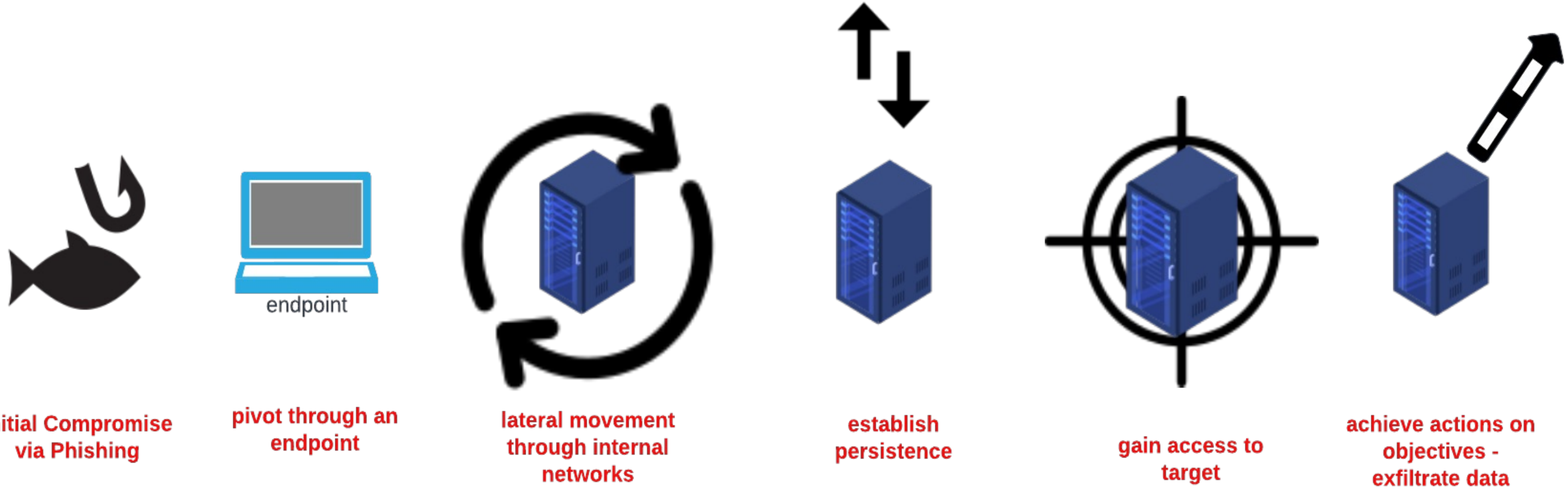
- Traditional Tech Stack
  - Threat Model, Attack Progression, Defender Visibility
- Cloud Control-Plane Architecture
  - Threat Model, Attack Progression, Defender Visibility
- Cloud-Native Attacks
  - Exfiltration over the backbone
- Detection Strategies for Cloud-Native Attacks

Traditional Tech Stack - **Threat Model**



External access is well guarded - Creating a thick, outer shell defended by network and web application firewalls

Traditional Tech Stack - **Attack Progression**



Initial Compromise via Phishing

pivot through an endpoint

lateral movement through internal networks

establish persistence

gain access to target

achieve actions on objectives - exfiltrate data

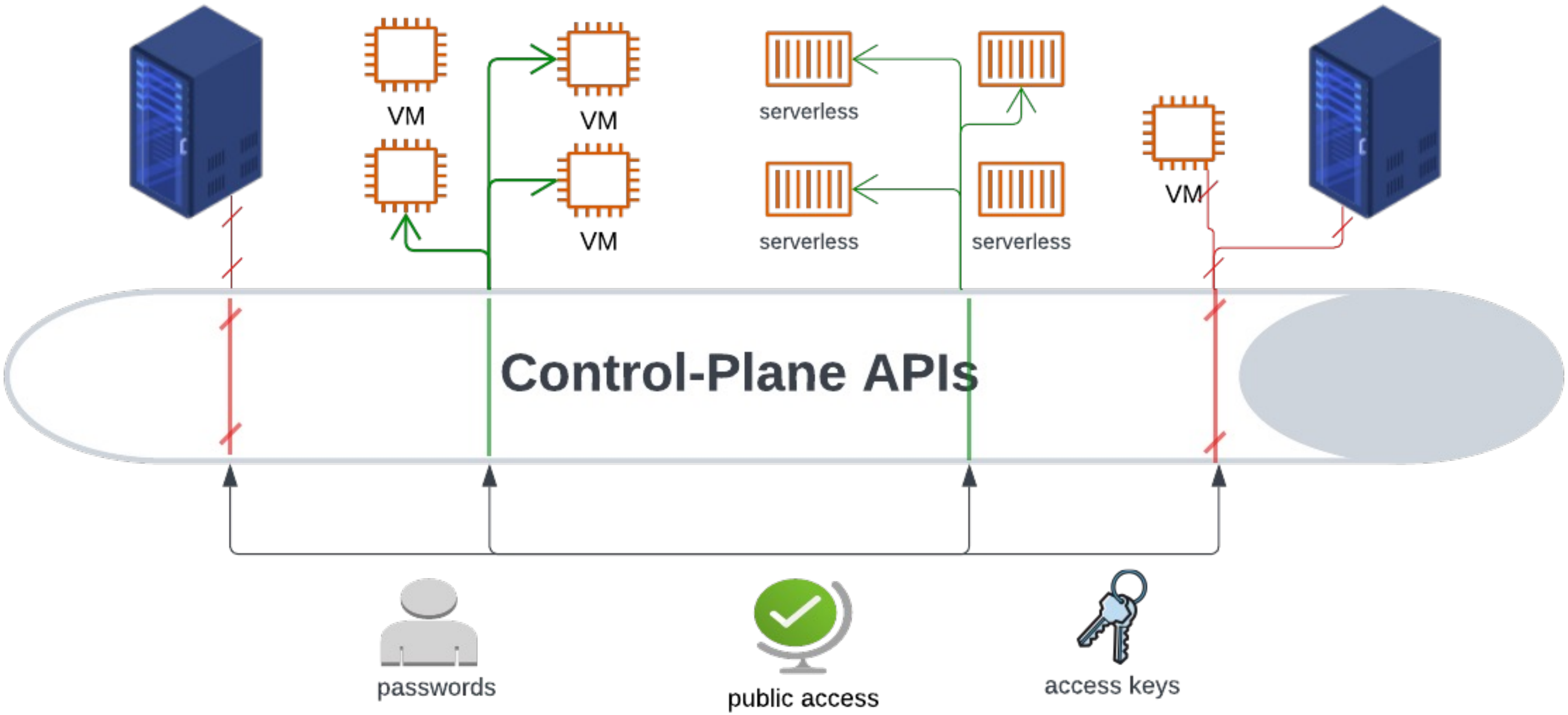
Attacker techniques are dictated by the characteristics of the tech stack

Cloud Architecture, Threat Model and Attacker Techniques

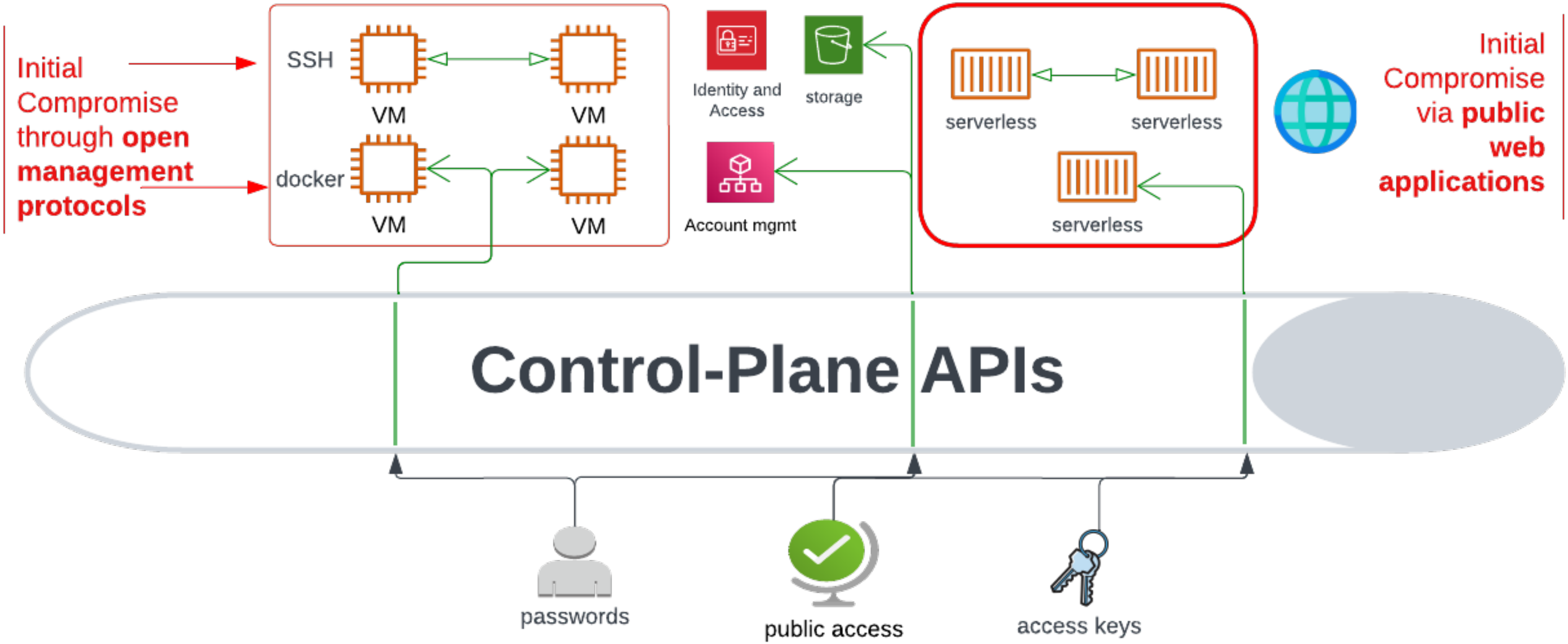
How do attackers work within the layers of abstraction in the cloud

Cloud Control-Plane **Architecture**

Value Proposition of the Cloud



Cloud Architecture - **Threat Model**

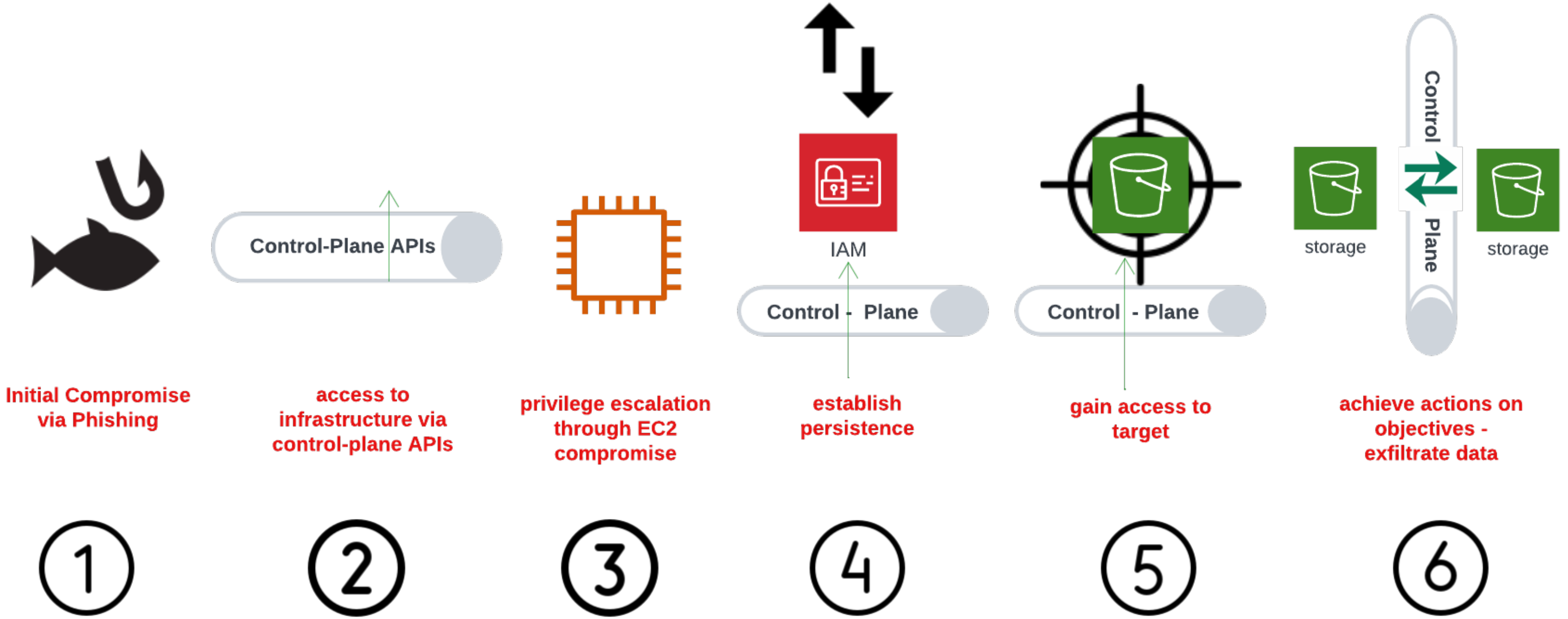


Initial Compromise through **open management protocols**

Initial Compromise via **public web applications**

Initial Compromise through **cloud control-plane**

Cloud Architecture – **Attack Progression**



Initial Compromise via Phishing

access to infrastructure via control-plane APIs

privilege escalation through EC2 compromise

establish persistence

gain access to target

achieve actions on objectives - exfiltrate data

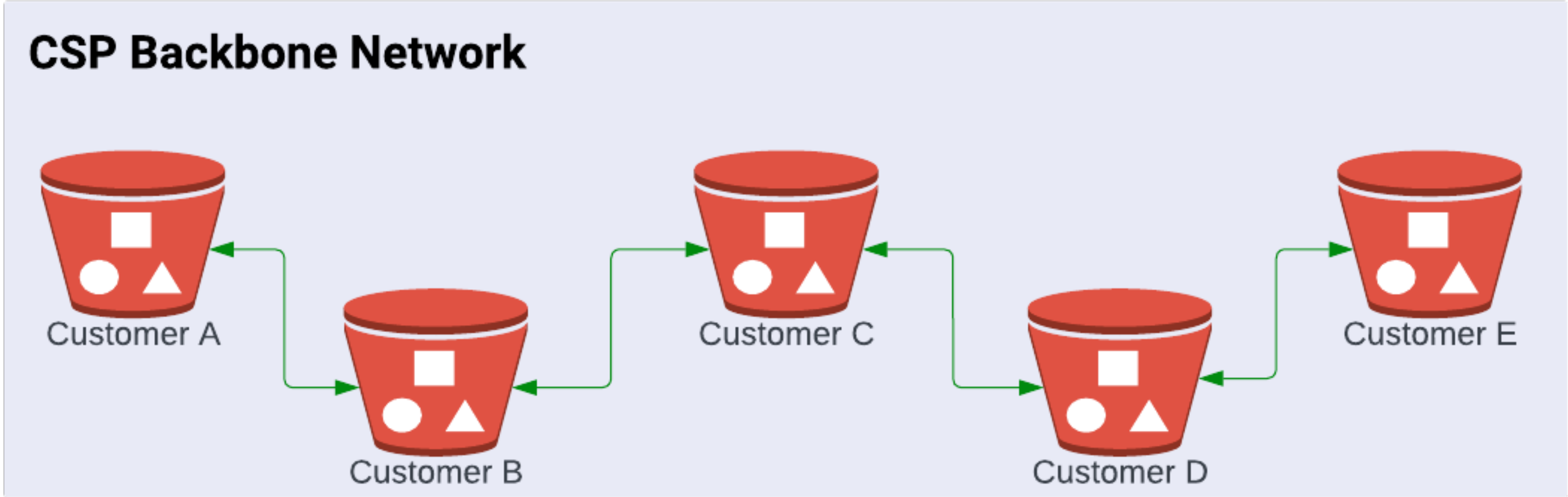
Cloud-Native Attack Techniques

Data exfiltration leveraging cloud architecture

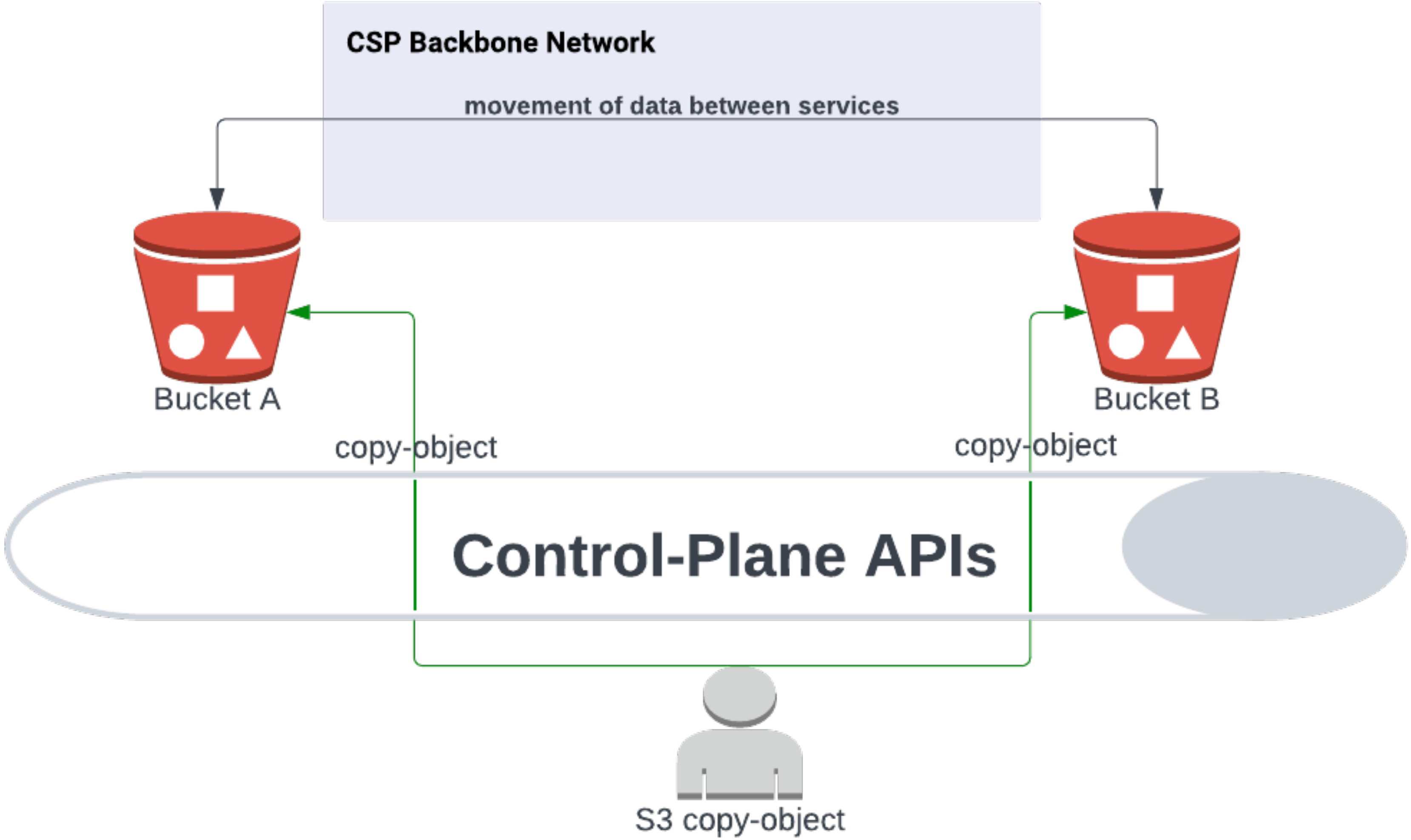
CSP Backbone Network

Backbone networks connect managed services like S3 buckets and enable the cloud control plane

Only identity-layer controls are available to restrict **data movement** between cloud-native storage repositories



Data Exfiltration Over the Backbone



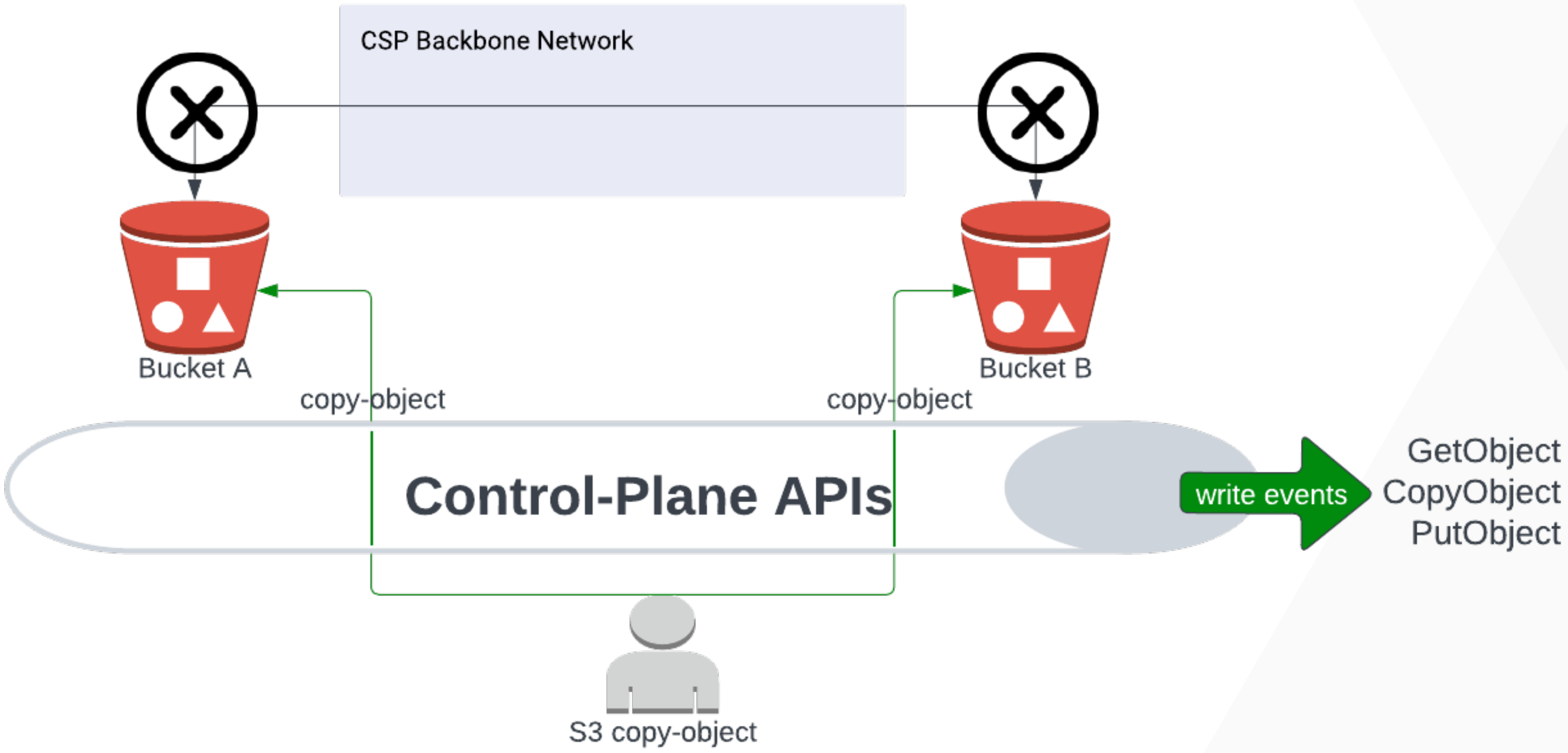
Data movement between managed services occurs over the providers' network

Cloud Defenders Visibility

Network Layer Logs ?

Host Layer Logs ?	Host Logs ?	Cloud-Plane Logs ?
✗	✗	✓

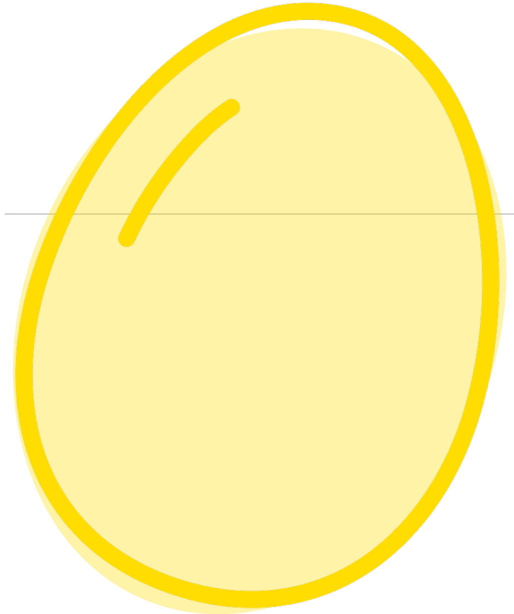
Cloud Control-Plane Logs Tell the Tale



Cloud-Plane Visibility into Attack Techniques

Data Exfiltration From S3 Bucket to S3 Bucket

VPC Flow Logs



IAM Permissions

-
  ```
  "Action": [
  "s3:PutObject",
  "s3:GetObject",
  "s3:CopyObject" ]
  ```

Cloud Trail

- Captured as a Data-Plane Event

-
  ```
  {eventSource":"s3.amazonaws.com","eventName":"CopyObject","awsRegion":"us-east-1","sourceIPAddress":"75.72.14.230","userAgent":"[aws-cli/2.2.43 Python/3.8.8 Darwin/20.5.0 exe/x86_64 prompt/off command/s3.sync]”}
  ```
- Both Src and Dest Buckets Logged

Debrief

- Adversaries leverage cloud-native services just like normal cloud customers
- They leave their footprints across the cloud control plane
- Distinguishing between benign activity and a malicious actor is what we specialize in at Vectra

VECTRA®
SECURITY THAT THINKS.®

VECTRA®

SECURITY THAT THINKS.®

Copyright © 2020 Vectra.AI, Inc.