The Road to Zero-Trust:

Past, Present, and Future

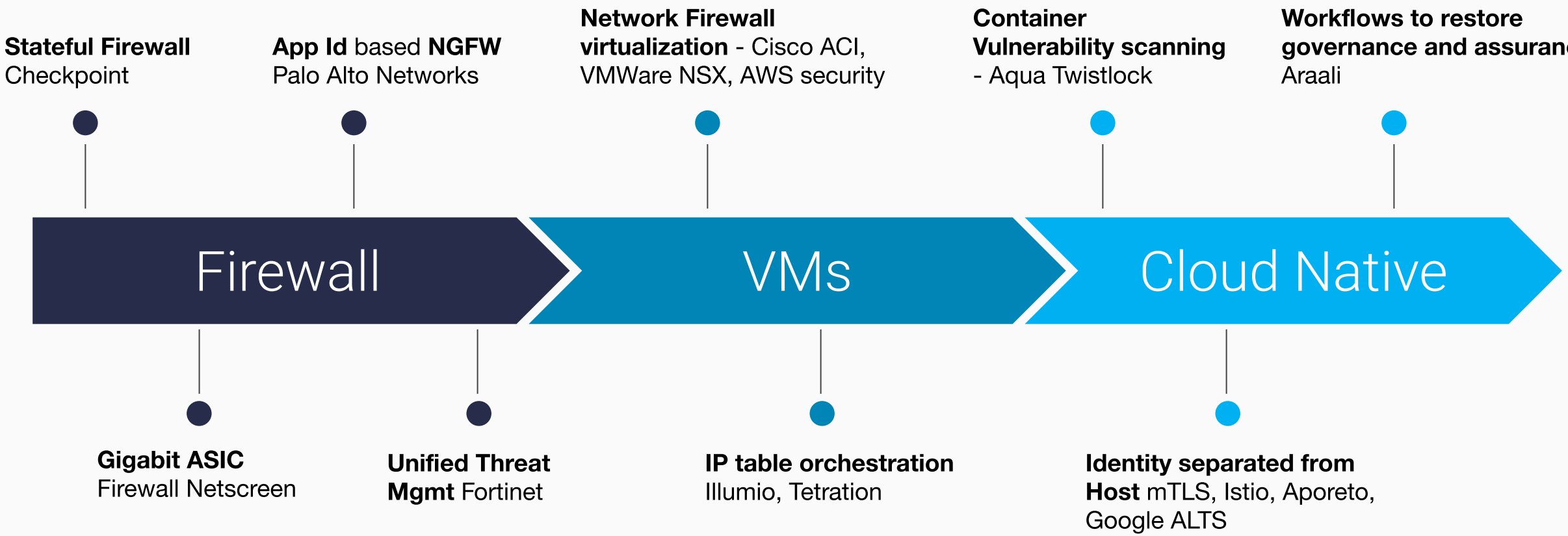
About the Speaker

Abhishek Singh

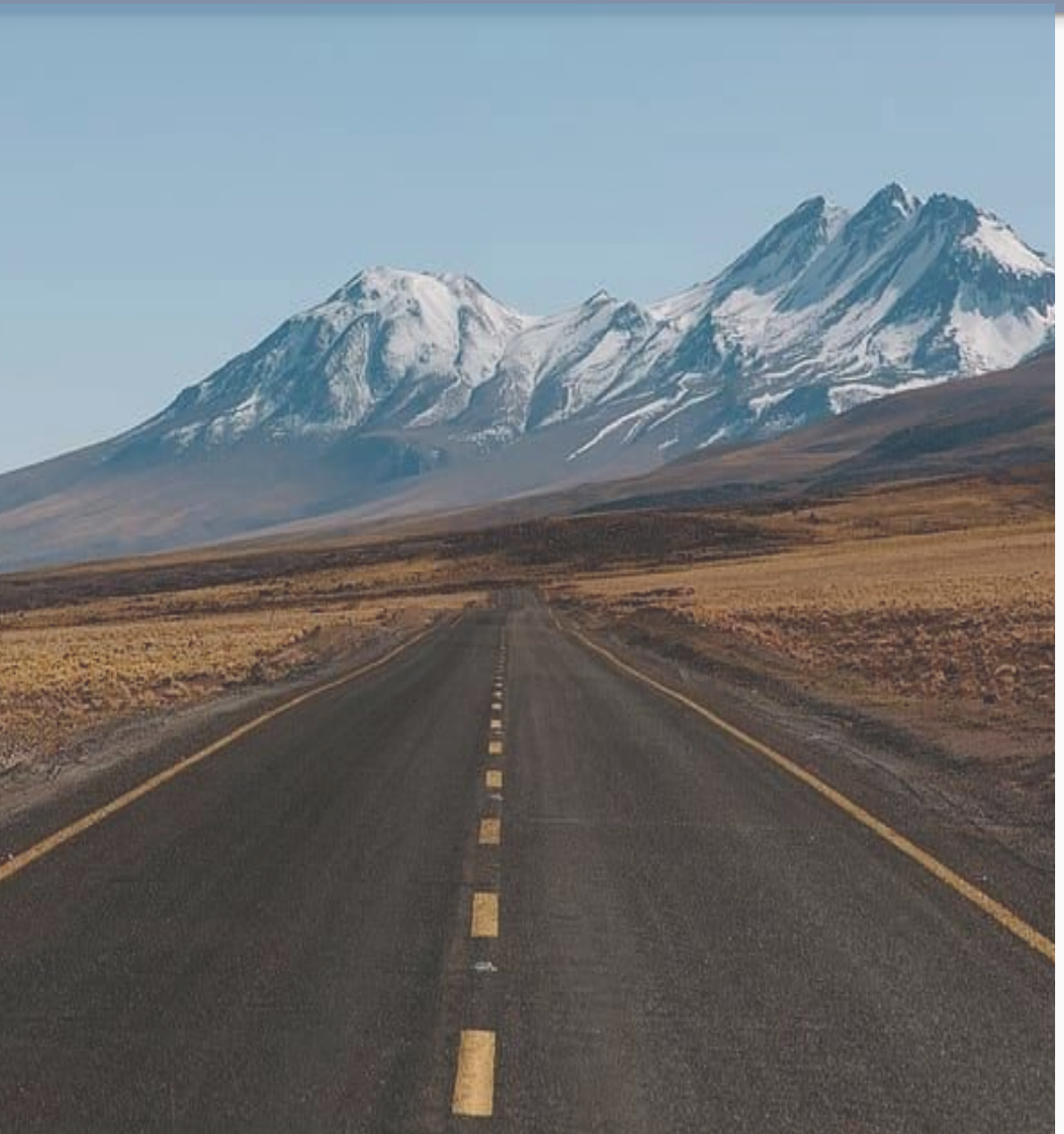
CEO of Araali Networks

- Co-Founder/VP Eng at Tetration Analytics
- Engineering leadership at Aruba, Cisco, & Ericsson
- M.S. John Hopkins University
- B.Tech. Indian Institute of Technology, Kanpur

Security Over The Years



Overview



- Why zero-trust?
- Evolution and adoption of zero-trust
- Current relevance of zero-trust
- How zero-trust prevents cyber-harm
  - Action Replay of Equifax Breach/Remote Code Execution
  - Action Replay of CapitalOne Breach/SSRF Attack

Why Bother?

Unauthorized Access to Data/Resources

- Data is the new oil
- Financial data, HR data, Sales/Competitive, IP, Customer data

Don't care?

- Compliance and privacy laws do
- Breach notification requirements (60 days of detection)

Why bother detecting then?

- Because someone else will
- Respond > Detect > Automated Prevention (Holy Grail)

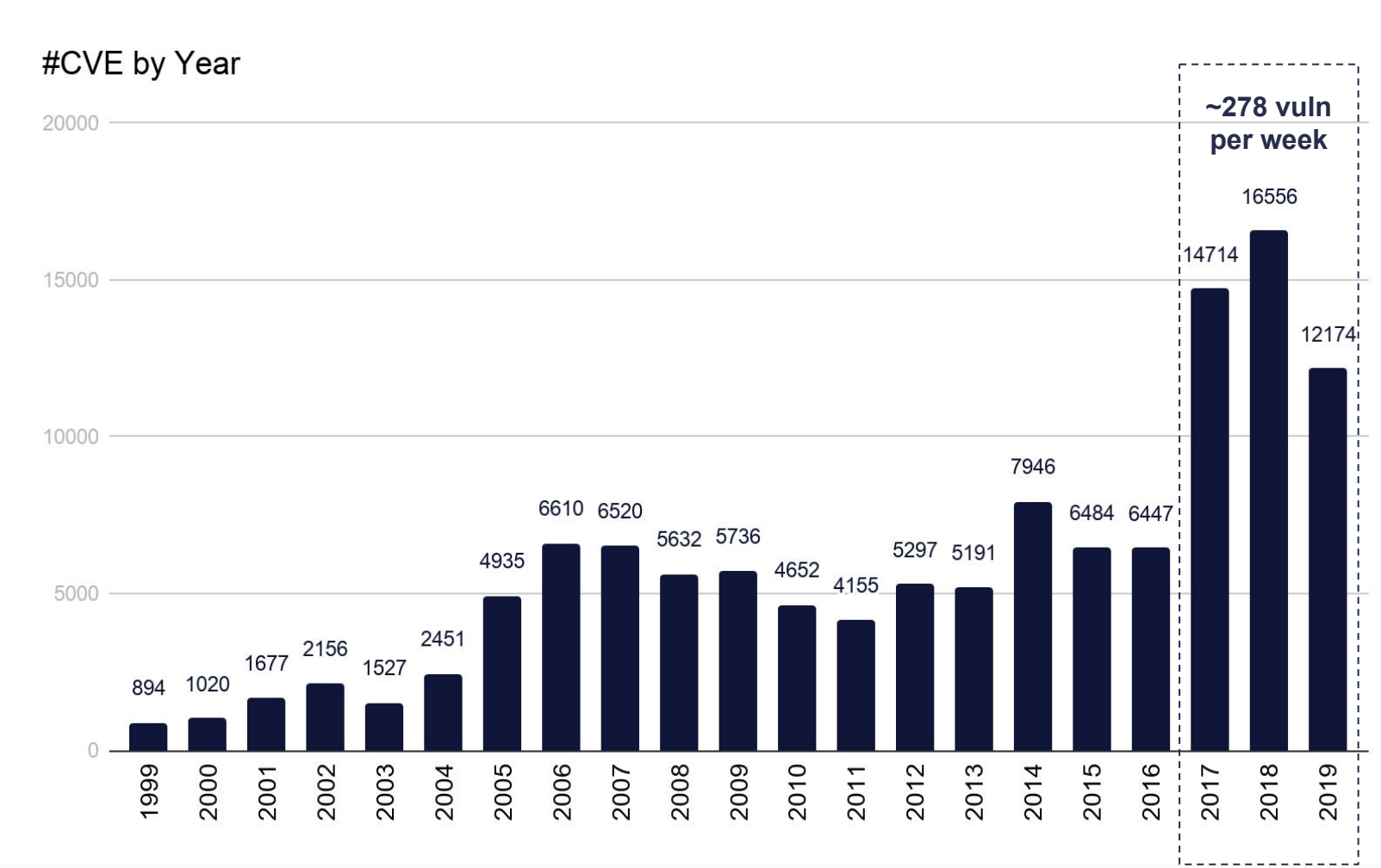
Attack Vectors

- Intrusion Attempts and Insider Threats
  - Hacktivists < Insiders < Organized Crime < State Actors

Weaknesses

- Applications: vulnerability
- Credentials: theft, brute force attacks
- Injection: Tricking, Trojans, and Phishing
- Missing Controls, insecure defaults
- Misconfigurations and human errors

Applications Are Vulnerable



Current Models

- Manually review each CVE from NVD feed (+ mailing lists + release notes, etc.) - triage, tag
- Monitor patches/new versions/ re-analysis
- Issue security advisories

Not practical for high velocity teams where CVEs become a Whac-A-Mole game

Source: https://www.cvedetails.com/browse-by-date.php

Passwords and Credentials Are A Problem

FINANCE

Equifax used the word 'admin' for the login and password of a database

PUBLISHED THU, SEP 14 2017•2:47 PM EDT | UPDATED THU, SEP 14 2017•4:59 PM EDT

Thomas Franck
@TOMWFRANCK

SHARE

Application Security , Big Data Security Analytics , Breach Notification

Microsoft Error Exposed 250 Million Elasticsearch Records

Five Customer Service Databases Were Left Internet-Accessible for Three Weeks

Jeremy Kirk (jeremy_kirk) · January 23, 2020

July 7, 2020

Exposed dating service databases leak sensitive info on romance-seekers

Bradley Barth

Follow @bbb1216bbb

Collectively, the two websites exposed data related to 102 million accounts, including email addresses, mobile device information and search preferences, WizCase said in a blog post. "Every server was easily accessible via the internet and not password protected," the report stated.

SECURITY

Facebook Breach Results In 267 Million Phone Records, User IDs Left Out In Open

By Ramish Zafar

Dec 20, 2019

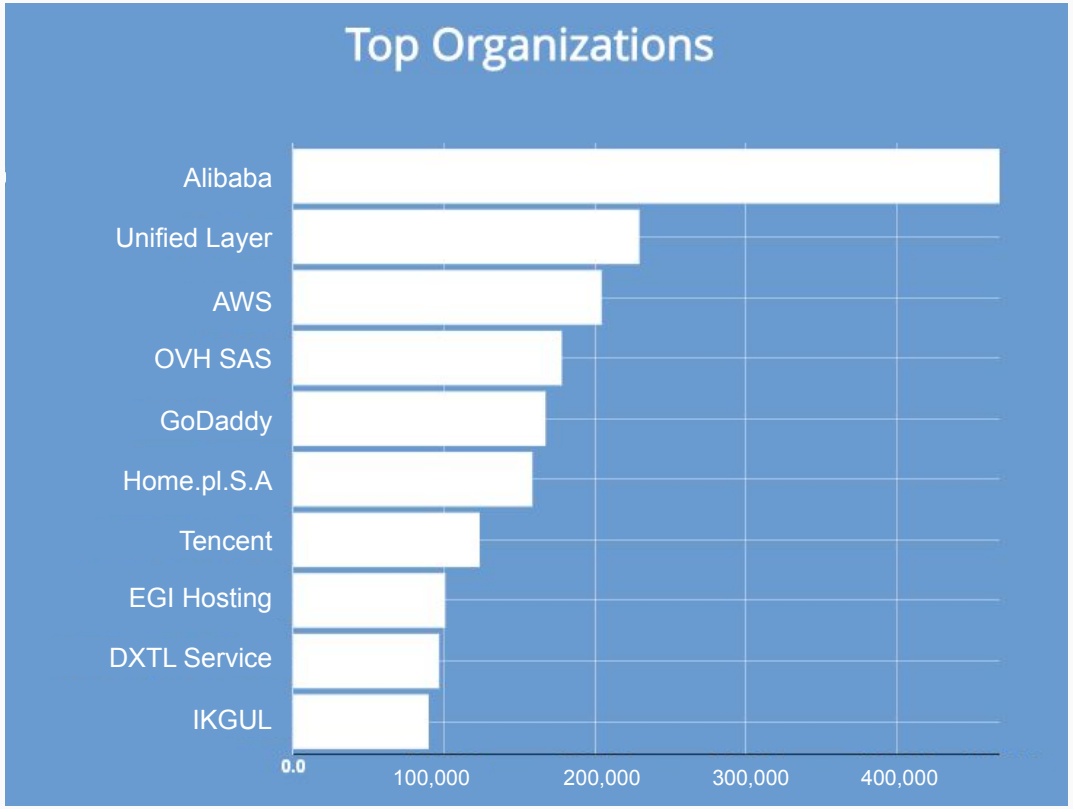
SHARE TWEET SUBMIT

Facebook Records of 267 Million Accounts Found On An Elasticsearch Server By Researcher In Latest Discovery Of Data Scraping

Missing Controls/Insecure Cloud Defaults

Over 4.9M instances of MySQL - open for public

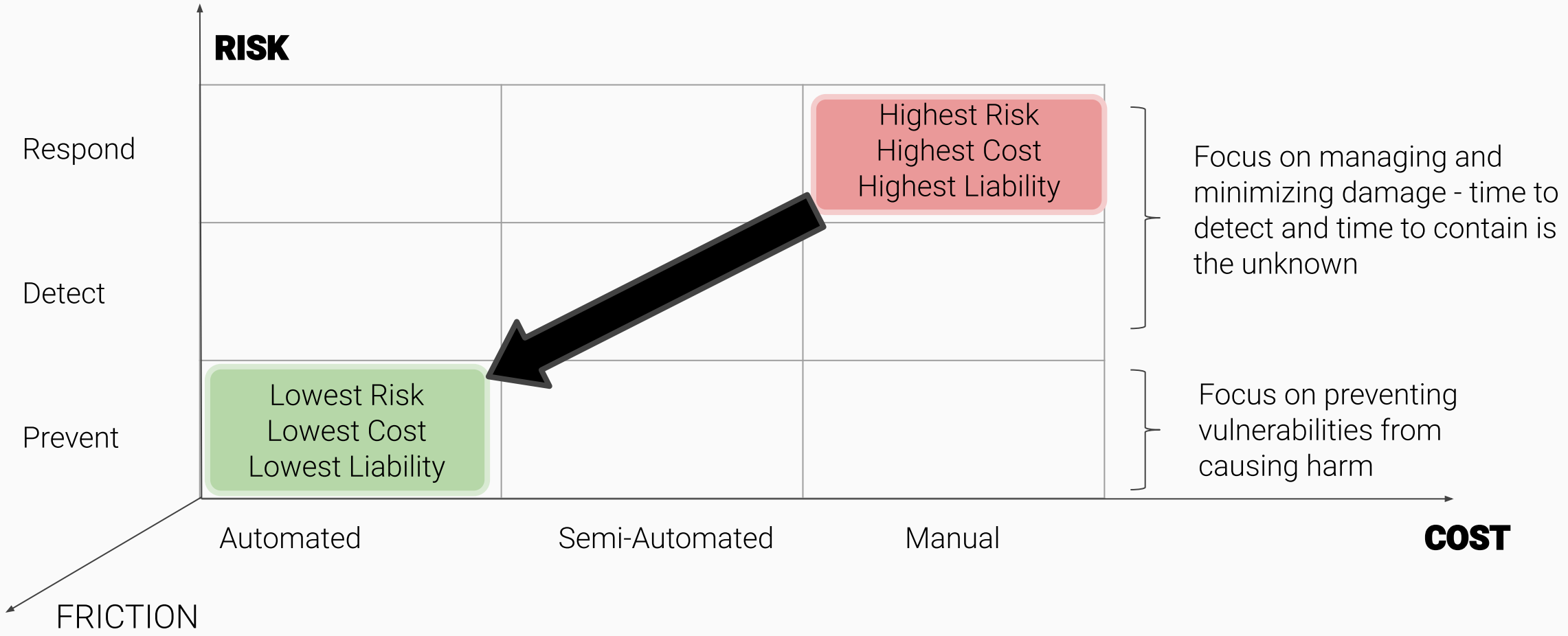
Across Cloud Providers



Source: Shodan.io | Search mysql | Updated - June 28, 2020
Unified Layer - Web Hosting Service https://www.unifiedlayers.com/
DXTL Service - DXTL Tseung Kwan O Service
IKGUL - Internet Keeper Global http://www.ik.com/

Where You Want to Be

Where most companies and solutions are focused
Promised land



Source: Managing Risk and Information Security; Malcolm Harkins


OH SUSANNA SALOON
BEWARE!
POKER PLAYING &
LOOSE WOMEN
ARE PERMITTED
OH SUSANNA
VINTAGE PHOTO PARLOR
2019
GOLDEN, CO

THE PAST

From the Beginning of Time

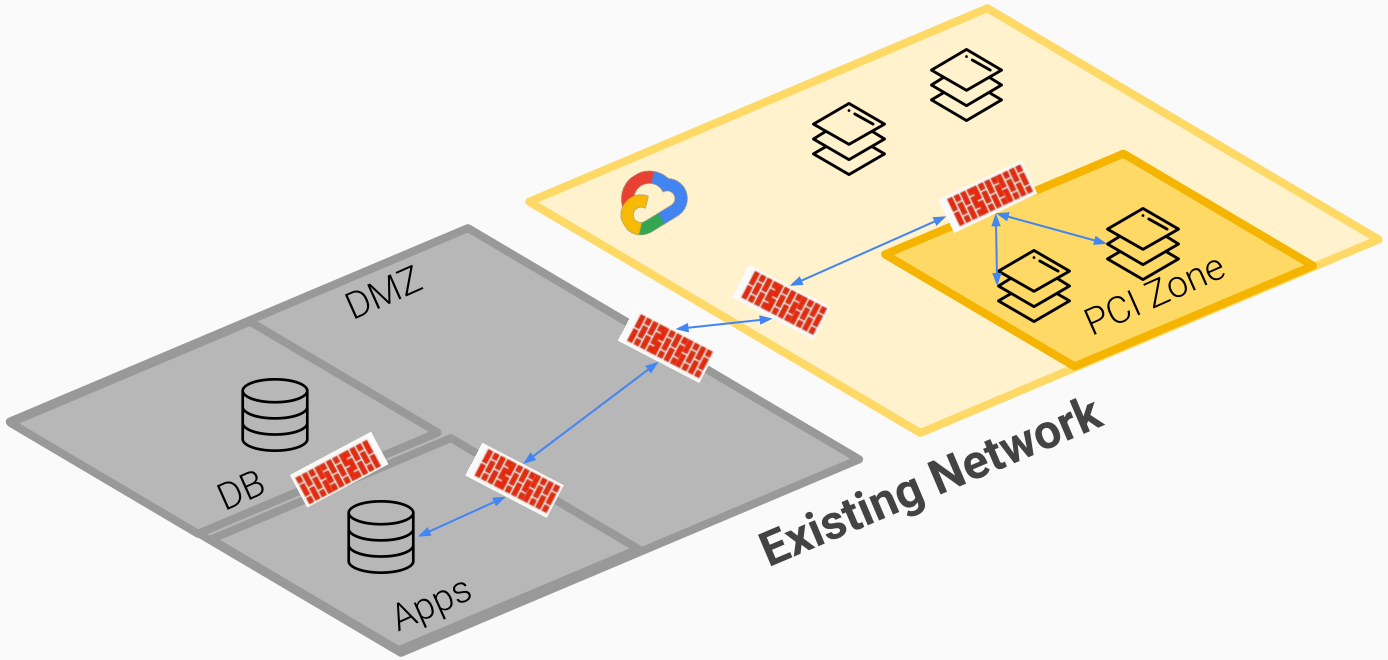
- **Wild Wild West (ARPANET/1969)**
  - Democracy, freedom, expression
  - Privacy trumps accountability
  - University culture
  - TCP/IP (1983)
  - WWW (1990)
- **Hackers are born, and celebrated too**
  - (Robert) Morris worm (1988)
    - rsh/rexec, finger, sendmail
    - weak passwords
  - First felony conviction in US, 1986 Computer Fraud and Abuse Act
  - CERT/CC @ CMU is born

- **Network Filtering**
- **War against intrusion**
  - IDS (2000)
  - IPS (2005)
- **Deny vs Allow Policies**
  - Signature matching
  - Application Id
- **Firewall**
  - Stateful Firewall (Checkpoint)
  - NGFW (2013 - PANW, Fortinet)

Perimeter World

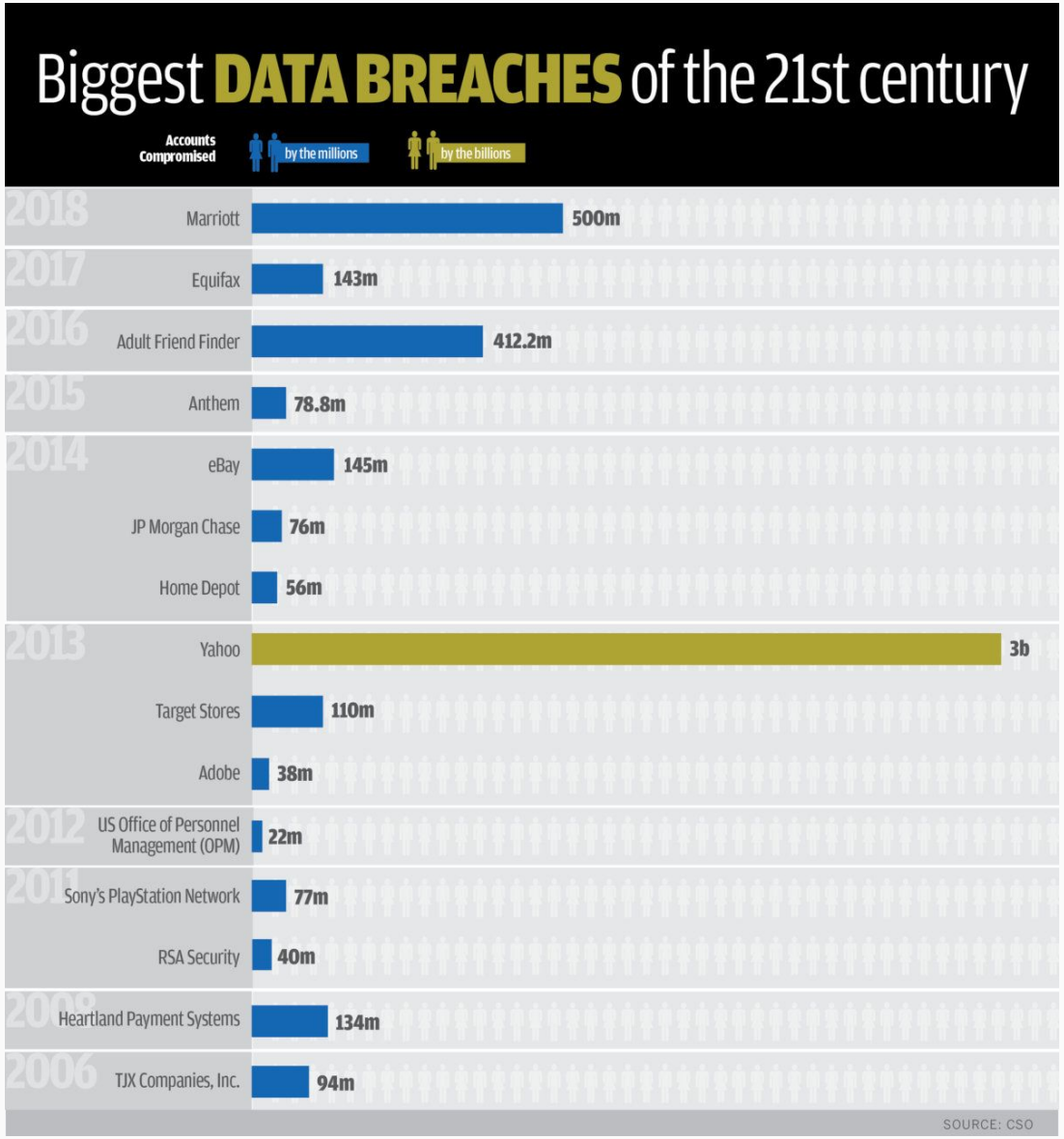
- DMZ itself represented a perimeter mindset
  - Free inside lateral movement
- Security was primarily protecting access to network
- **Intranet, Network Shares, VPN**

Defense in Depth - Network Based Segmentation

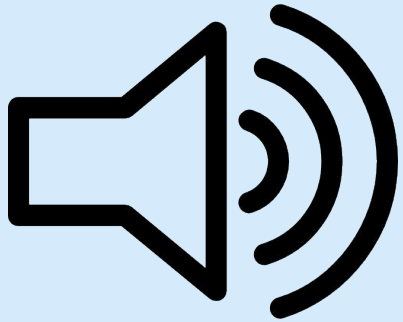


- Privileged network segments
- Data tier tucked away
- Firewall guards crossovers

Increased Spending...But Breaches Galore

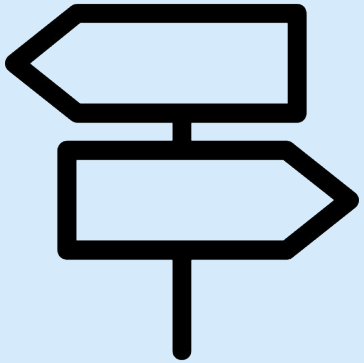


Problems Remained Unsolved



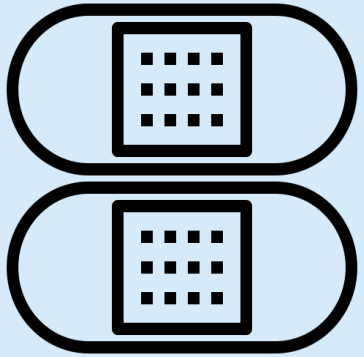
Chasing buzzwords

- CARTA [1)]
- Zero-Trust
- SDP [2)]



Chasing Technology

- Network Processor
- Big Data
- ML
- FPGA [3)]
- Containers



Band-Aid Approach

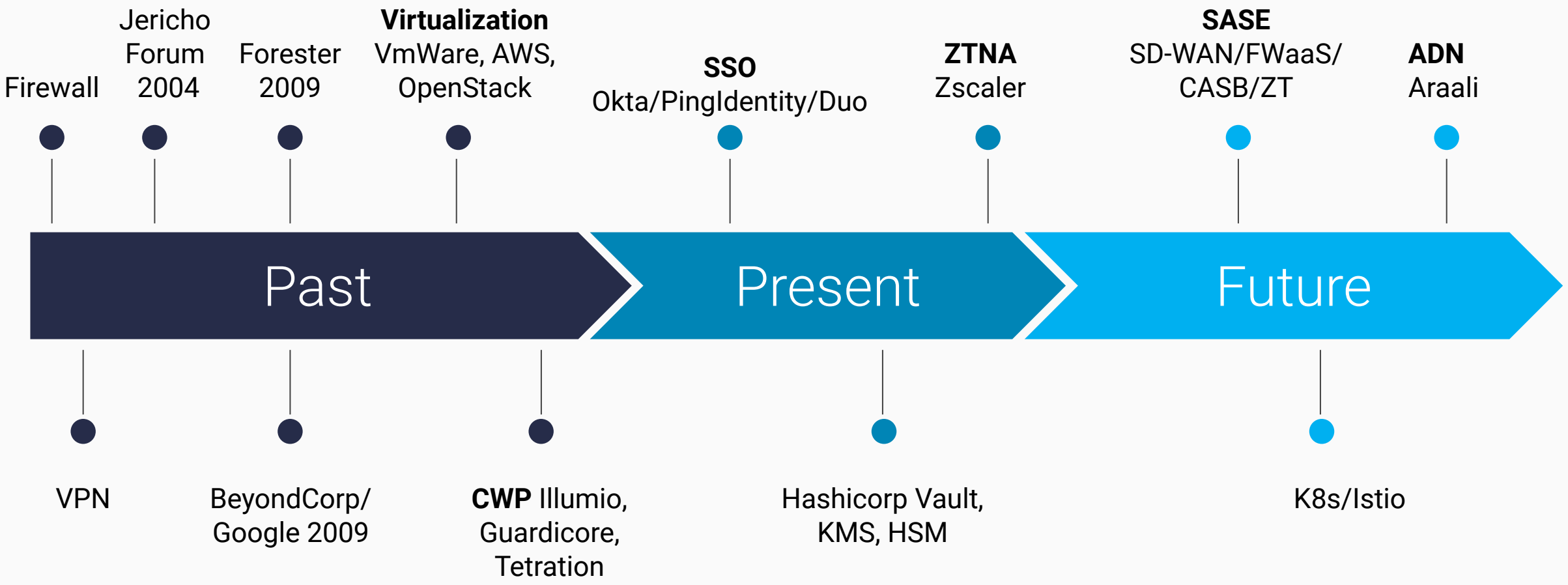
- vs. First Principle approach
- vs. reimagining Architecture

1) CARTA - Continuous Adaptive Risk and Trust Assessment
2) SDP - Software Defined Perimeter
3) FPGA - Field Programmable Gate Arrays

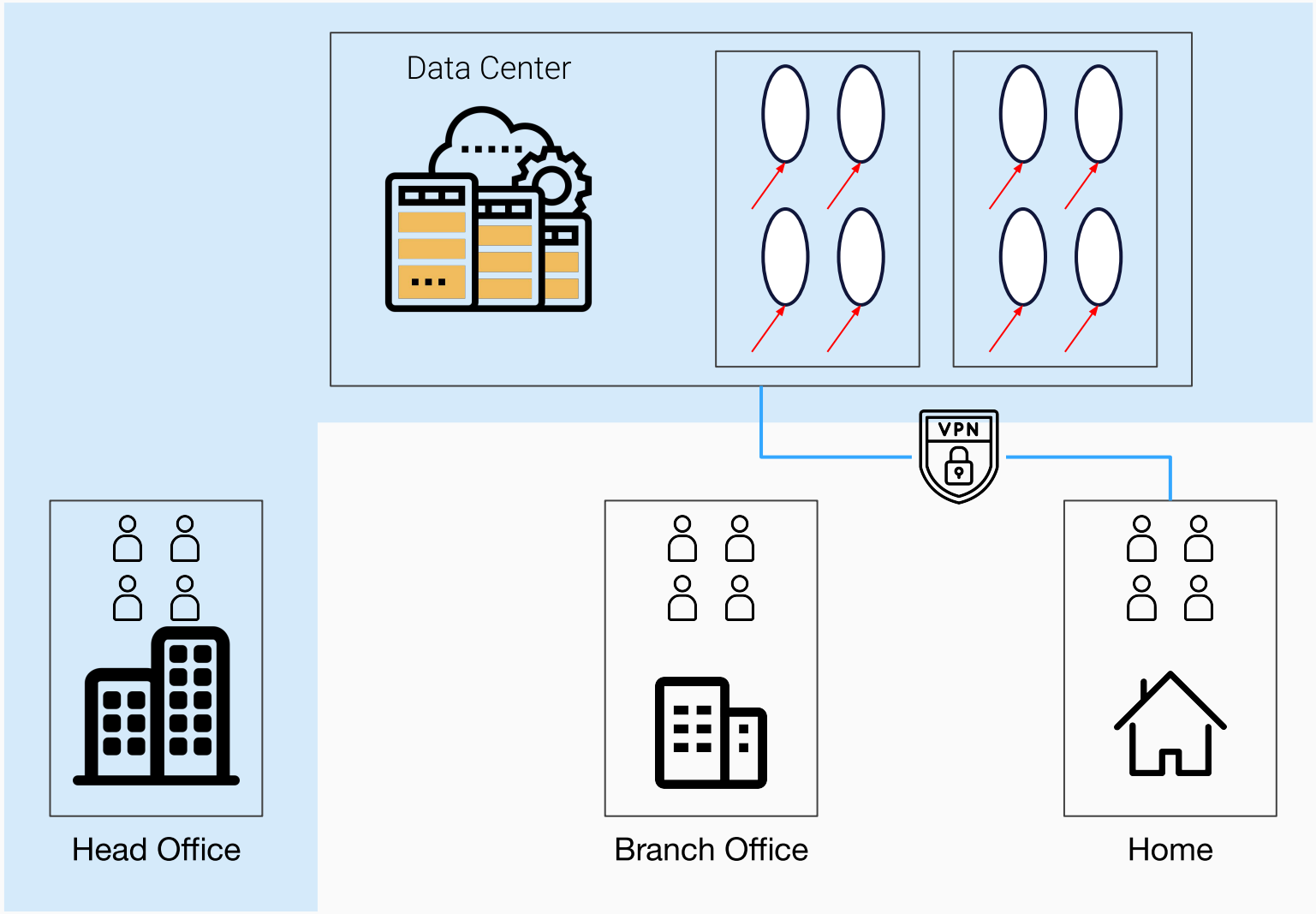
Zero Trust: A Foundational Fix

- **Always Verify vs “Trust, but Verify”**
  - Continuous verification
  - Verify what?
- **Privileges**
  - AuthN - first establish identity
  - AuthZ - then verify privileges
- **Grain of Identity matter**
  - Access to Car, Bus, Ship? Or person?
  - Smallest possible grain -> 0
- **Least Privilege**
  - On a “need to know” basis
  - Minimum possible privilege -> 0

Zero-Trust Timeline



2009: Driven by User and Endpoint Mobility



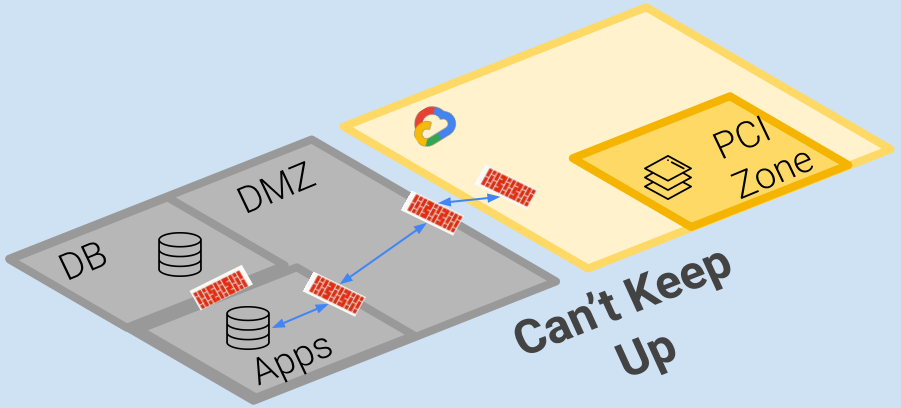
The Perimeter extended from Data center to Head Office.

Rest of users VPN in. Once in, you had full privilege

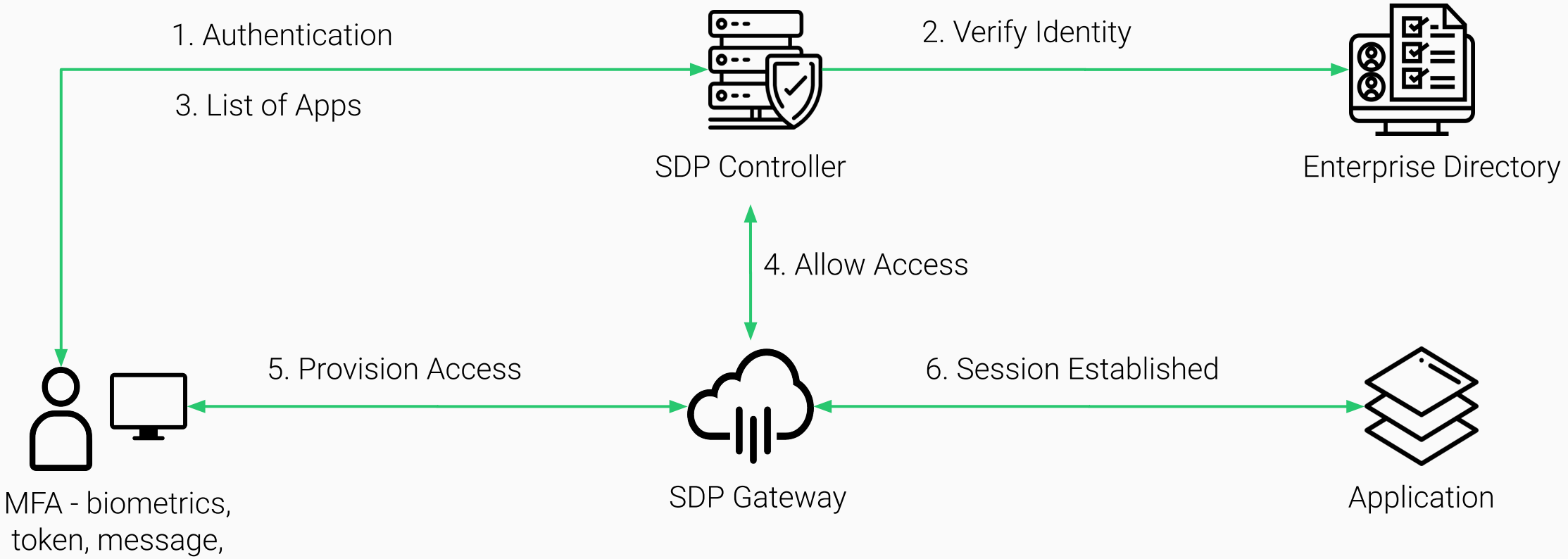
2020: Driven by Cloud and Cloud-native

- **DevOps**
  - Push on Green
  - Constant churn
- **Cloud**
  - Infrastructure as code
  - Ephemeral resources
  - Dynamic scaling
  - Insecure defaults

- **Cloud Native/K8s**
  - Pooled resources
  - POD directly visible
  - Orchestrated
    - Lost placement control

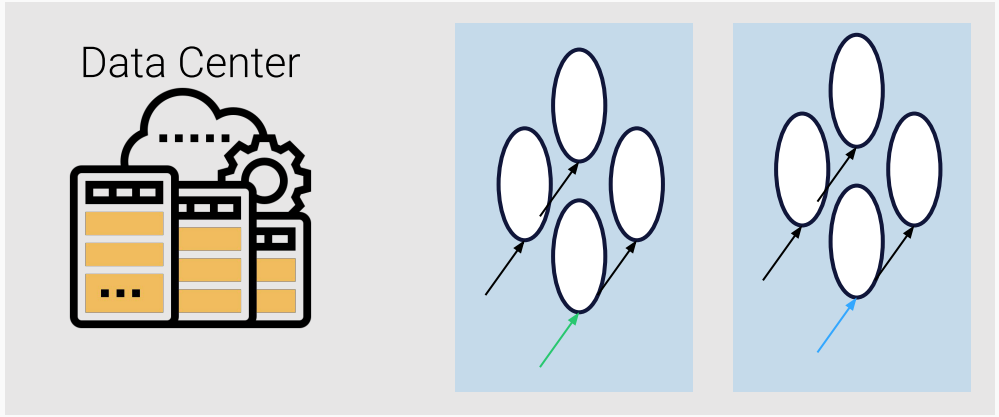


User Access: BeyondCorp/SDP/ZTNA



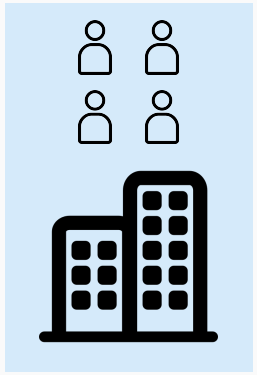
Source: Gartner (April 2019), ID 386774

“Need to know” User Access

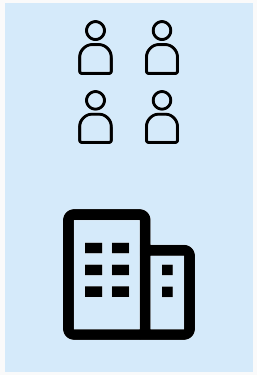


okta BeyondCorp

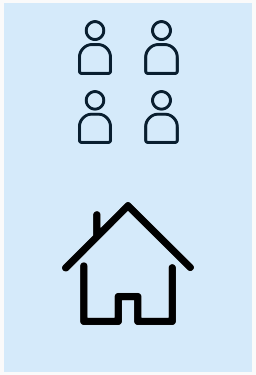
Beyond Corp/Okta enabled org. to verify identify and provide access and privileges to the right corp user



Head Office



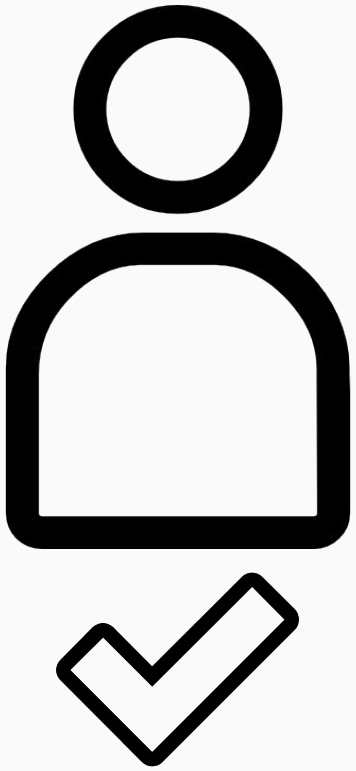
Branch Office

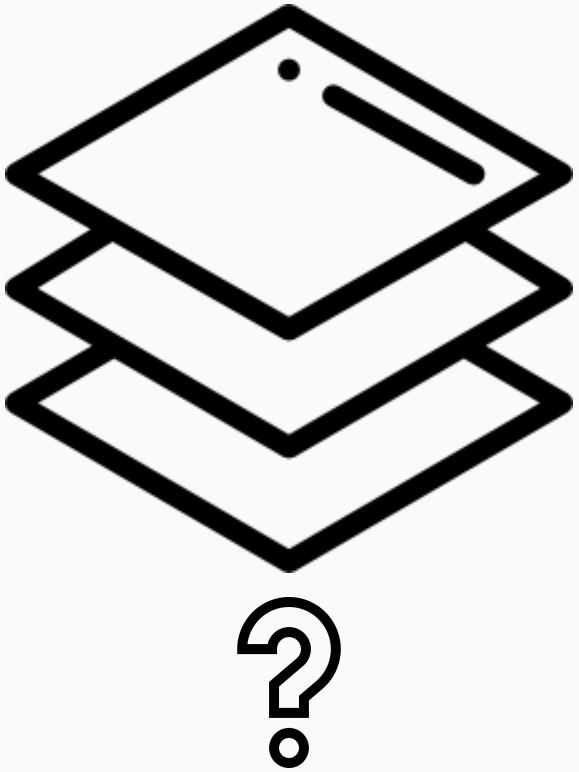


Home

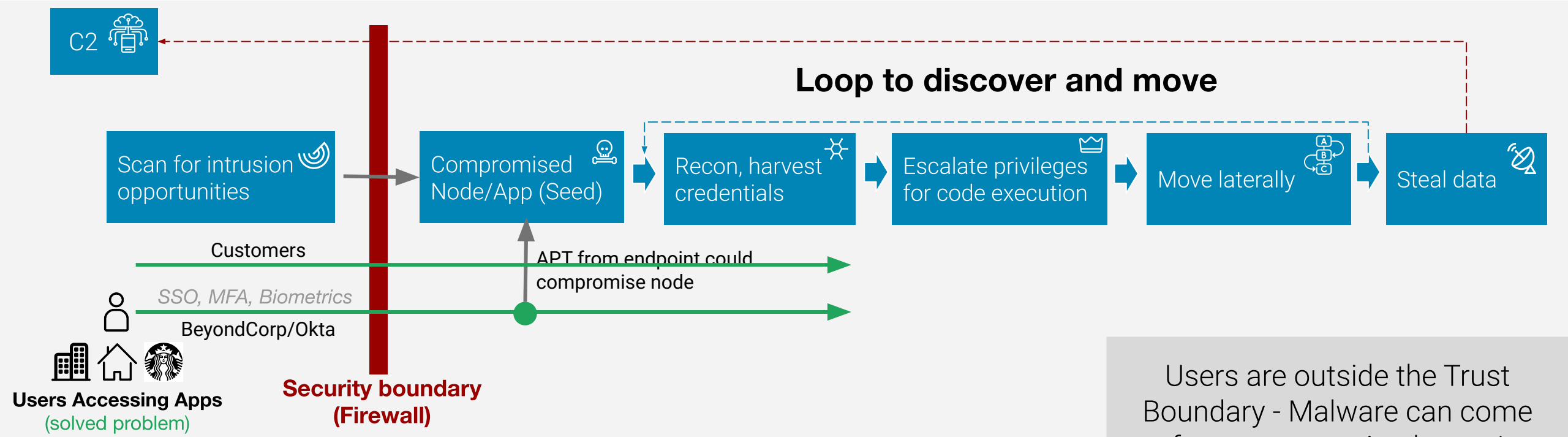
Cafe

Solved for users, but what about apps?





Applications Are Under Constant Siege

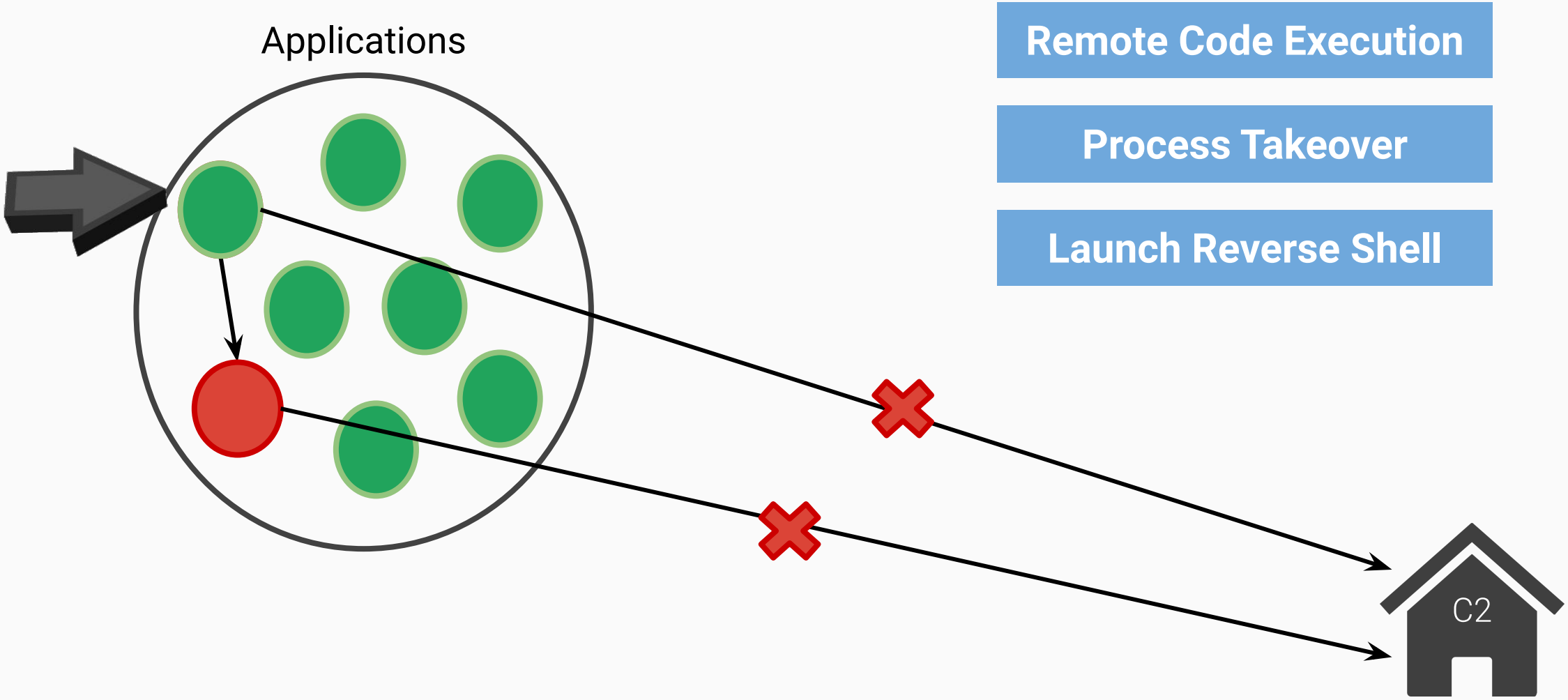


Users are outside the Trust Boundary - Malware can come from compromised users!

Corporate and customer access

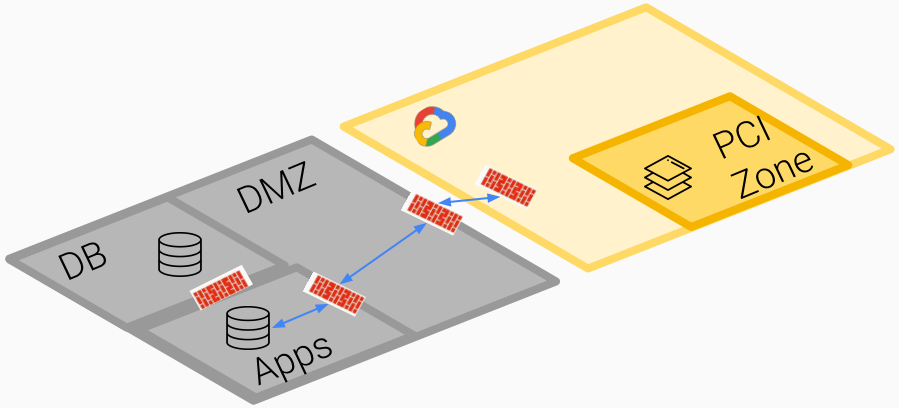
- {Public, Private} Trust has a porous perimeter, and many such entry points
- Creating a least privilege environment is hard but necessary → automate with Araali

And Vulnerable Too



Current Attempts: Network Based

- **Automation** to the rescue: IPTables orchestration
  - IP was ephemeral
    - Tags to the rescue
      - Translation to network controls was problematic
- **Machine Learning**, discover application dependency
  - Context was lacking
- Et tu, **K8s**
  - Pod is an IP address
  - Pod > Container > Process
- **Still segmenting networks!**
  - Networks, Subnets, Pods, IPs have privilege!!




LEFT
EXIT 12
Outdated Solutions
The Promised Land
(Micro Segmentation & Zero-Trust)
The Future of Security

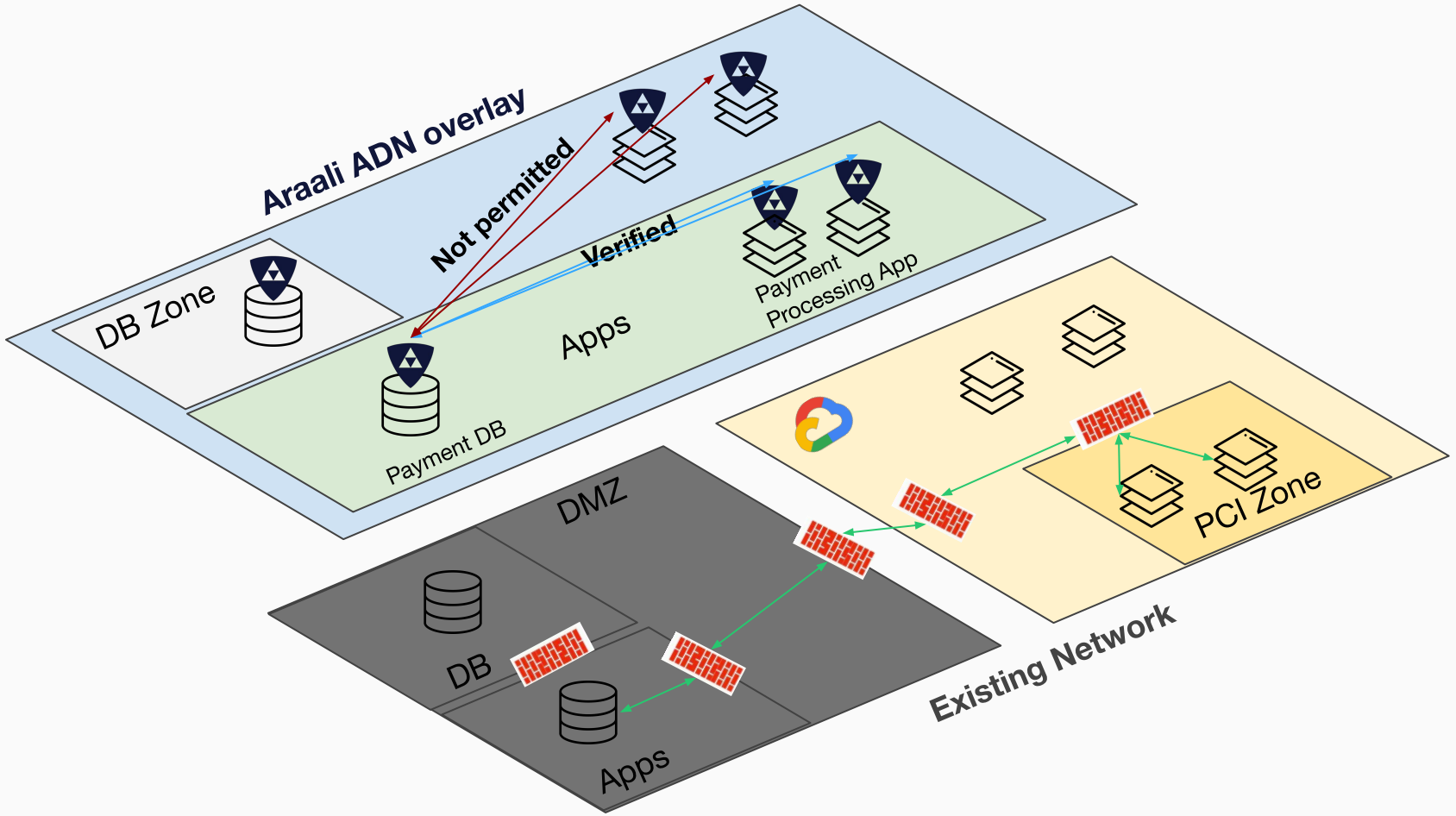
What if we turn the problem upside-down?

Network Driven
Application Security

Application Defined
Networking

Application Defined Networking

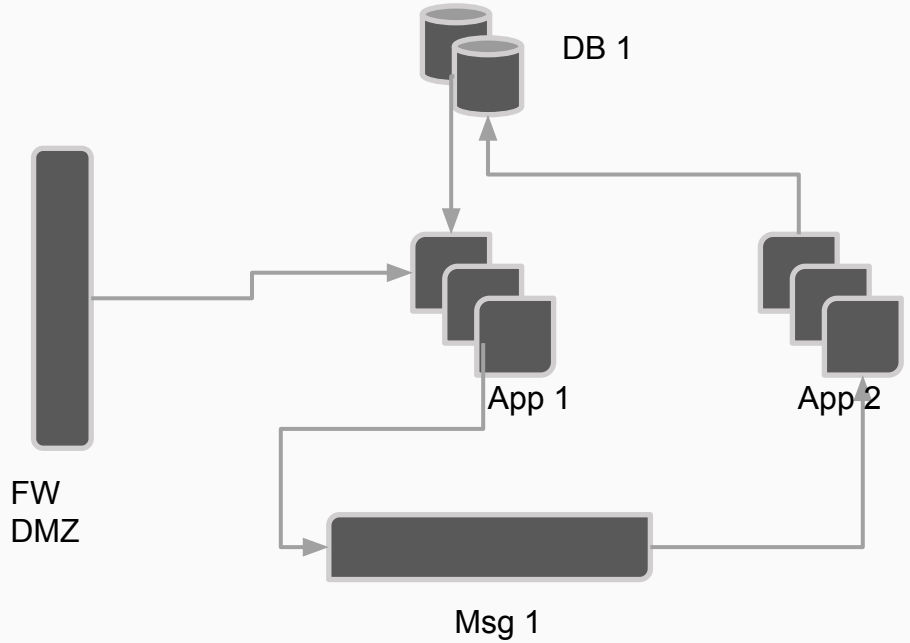
Security Overlay Boundaries: **Processes, App, Zone** - could span networks and infrastructure elements, multiple clouds



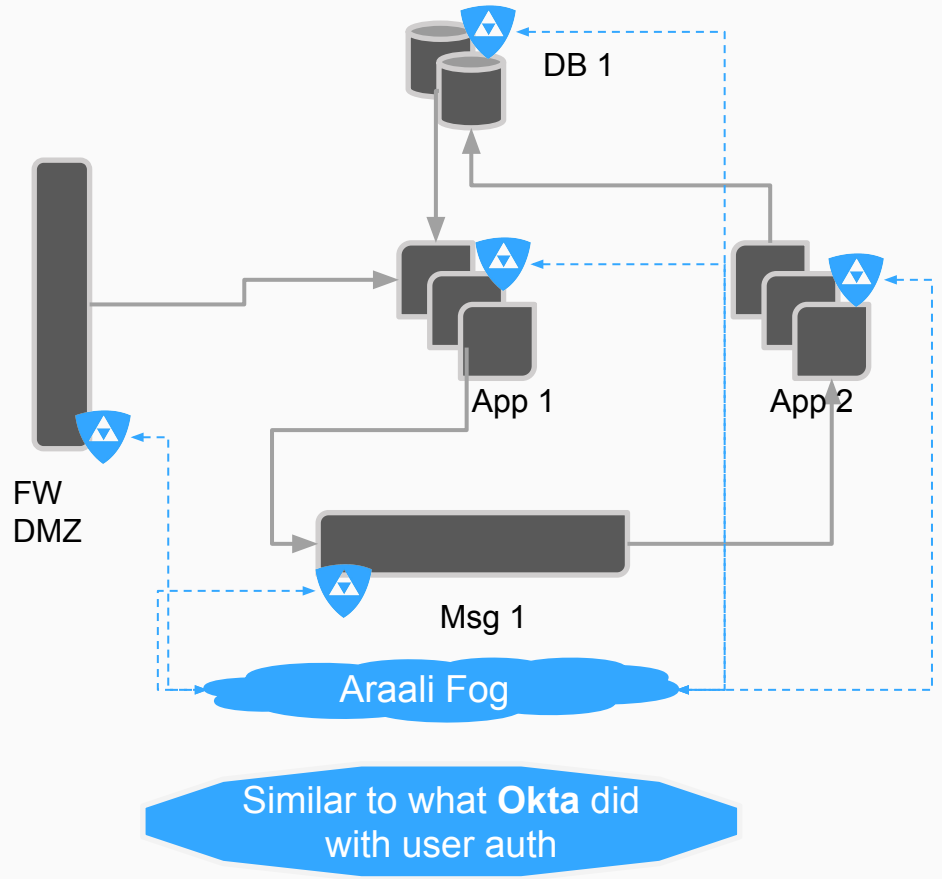
- Automatic self-organizing overlay offers much more flexibility and simplicity
- Privileges on a need to know basis
- Outside threats and malware have no privileges in this trust fabric, thereby no ability to cause damage

2FA for Apps - Say Goodbye to Stolen Credentials

Before: it's free for all, relying on perimeter protection, and passwords/secrets to access DBs and services.

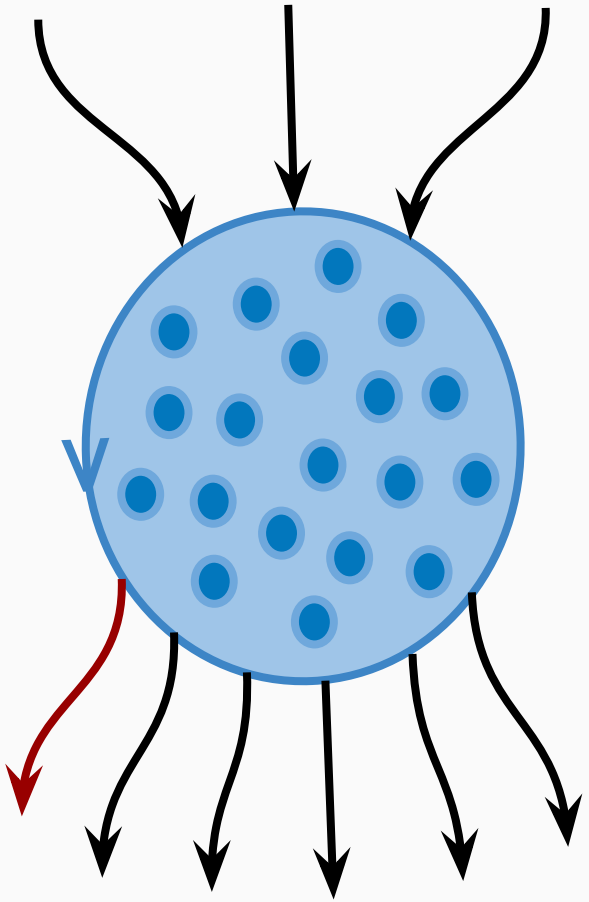


After: Apps are Araalified, enabling authentication of each app with Araali fog (admission into our trusted fabric). Granular control and audit follows

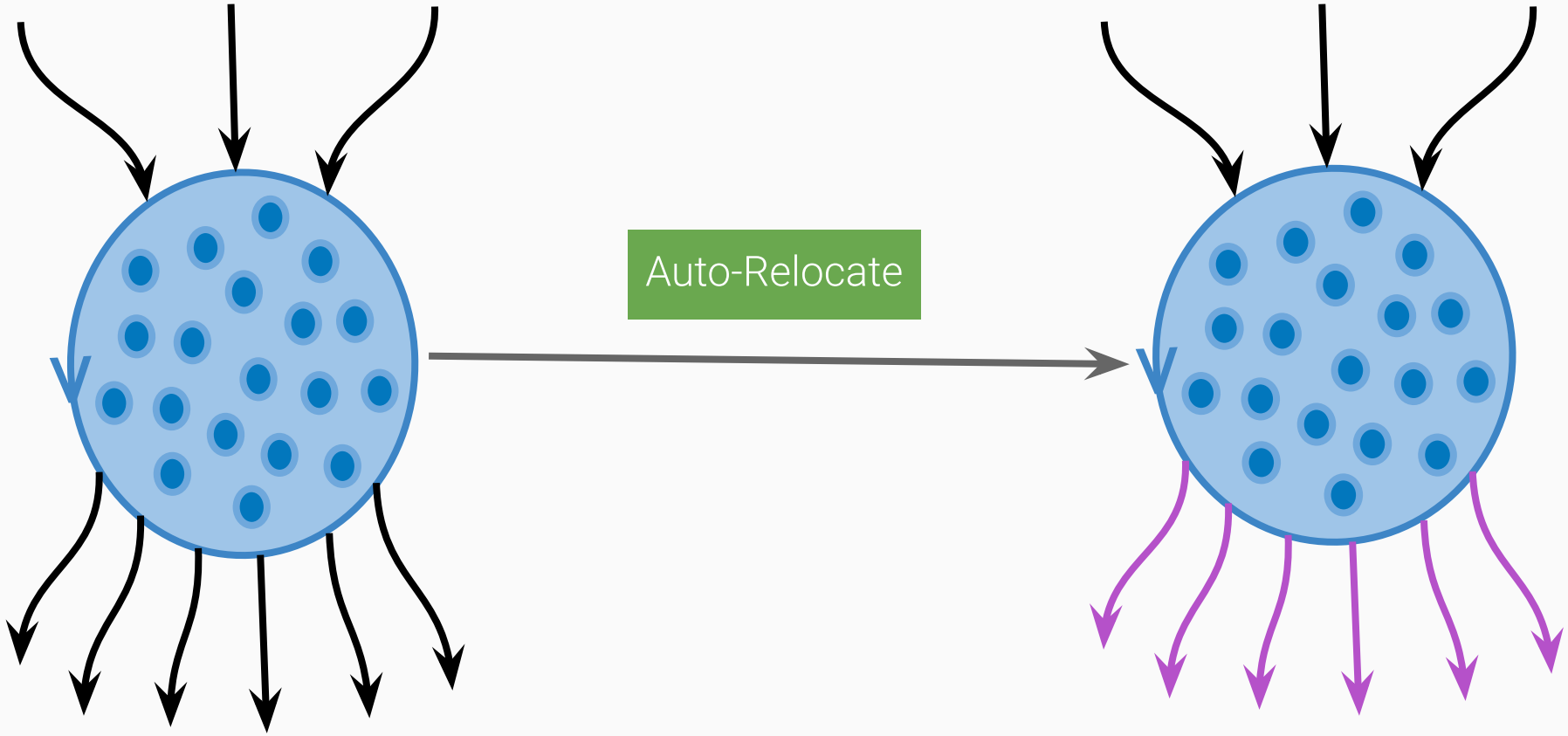


Policy Discovery with Continuous Integration

Continuous Integration Alert:
New policies needed



Policies are Portable and Permanent



Security at the speed of Devops

Single Click

- fortify-vm: single VM
- fortify-image: all VMs
- fortify-k8s: whole cluster

Zero Touch

- No tagging necessary
- No handwriting of policies

Zero Time

- Deterministic
- Self-organizing
- Portable

Choose Your Value

- Visibility - Inventory your exposure
- Alert - guard-rails, mitigation on you
- Block - mitigation is on us

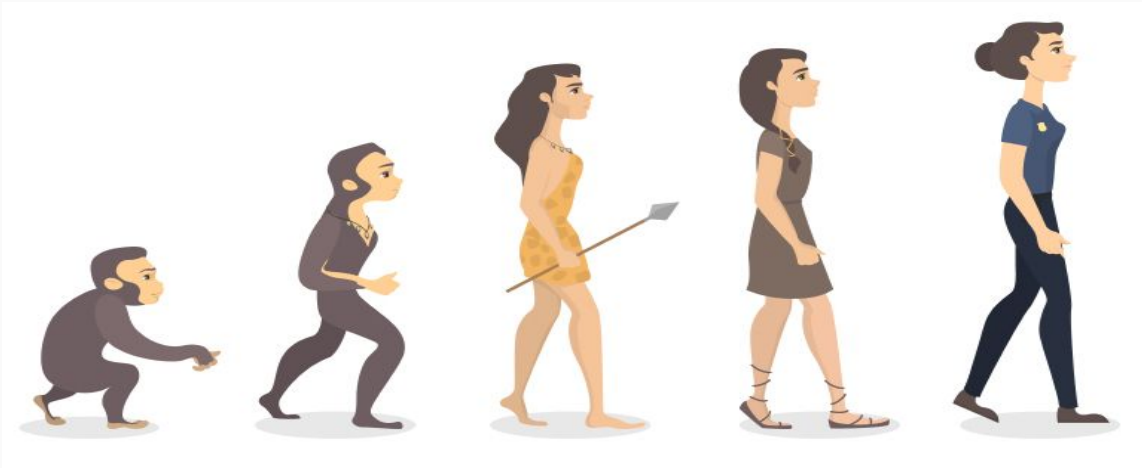
Choose Your Grain

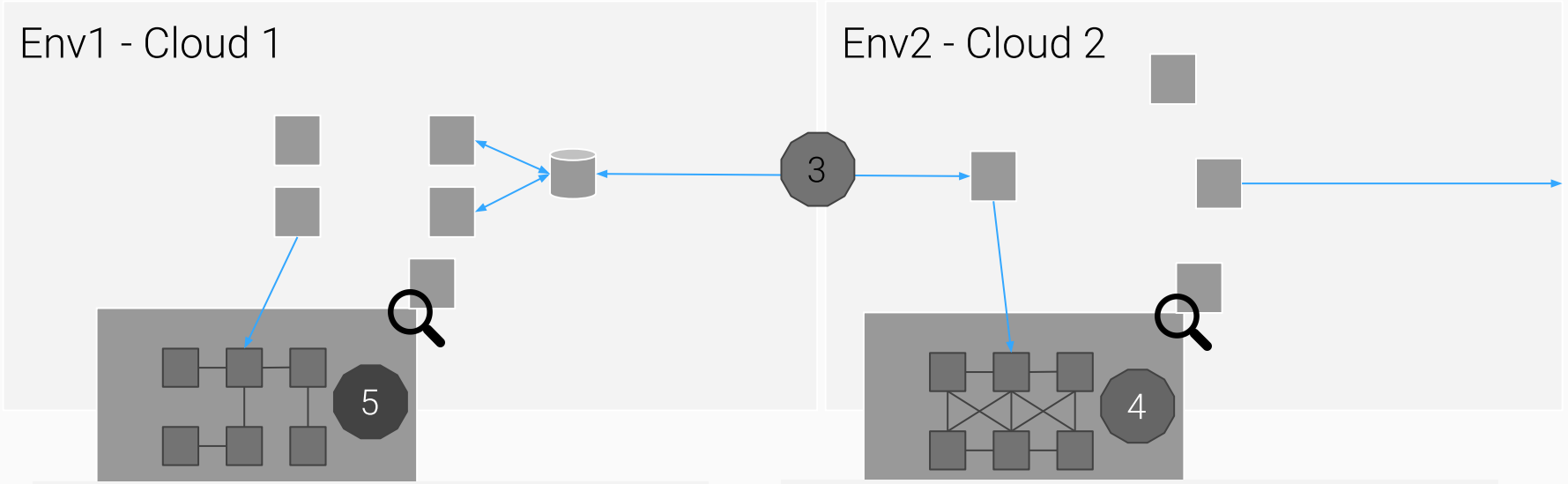
- External Services
- Segment at zone, app boundary
- Verify at process boundary

Zero Trust Journey

Zero Trust Journey

1. Inventory your exposure (sec)
2. Baseline Alerts (sec)
3. Enforce Zone Boundaries
4. Enforce App Boundaries
5. Enforce Process Privileges





Microservices can only talk if they are whitelisted

Microservices in an app can only talk to each other, no one except front end can talk to them

Developer and Security Relationship

Zero-Trust: Not Just for Feds Anymore!

- **Democratized for the cloud generation!**
- Since late 2018, National Institute of Standards and Technology (NIST) and NCCoE cybersecurity researchers have had the opportunity to work closely with the Federal Chief Information Officer (CIO) Council, federal agencies, and industry to address the challenges and opportunities for implementing zero trust architectures across U.S. government networks

Zero Trust Architecture (2nd Draft)
Date Published: February 2020
Comments Due: March 13, 2020 (public comment period is CLOSED)
Email Questions to: zerotrust-arch@nist.gov

- **Targeted for enterprise security architects!**

Araali Networks

Application Defined Networking

Deterministic | Least Privilege | Automated