F5 & HashiCorp

SMOKE THE COMPETITION

CONTRATULATIONS

LEADERBOARD

Name	Partner	Total Points
Dave Unger	InterVision	400
Justin Stevens	Bridge Data	400
Colby Canutt	Optiv	400

Checkpoint 1 - Review

Question: How much money do you earn for demoing a PIO registered AWAF, NGINX or Shape meeting as a "Starter"?

Answer: $600 => $for demo + $250 Starter Bonus (Achieved on 5th - 9th opportunity

Question: When a Client Authenticates through Vault, what is given back to the client?

Answer: Token

$250 - Host Customer Workshop

1. OWASP Top w/AWAF, Zero Trust w/Shape, Encrypted Threats w/SSLO, Mod Apps w/NGINX
2. F5 provides Hands-on Lab and Content
3. Invite your customers (min 8 customers)

$200 - Host Customer Meeting with F5

1. Target attendees to follow-up meetings
2. Register an opportunity
3. Invite your F5 friends

$200 – Demo Solution

1. Can be during initial meeting or follow-up meeting
2. Run live or recorded demo

$500 – AppSec Discovery Scans

1. $250 – NGINX Discover Engine resulting in High or Med opportunity
2. $250 – Shape PDT resulting in High or Med opportunity

Call To Action

SE All Stars

Partner SE Incentive

FY21

The SE All Stars incentive rewards Partner SE's for enablement achievement and demonstration of skills!

What does this mean for Partner SEs?

- Earn $200 per meeting shadowed
- Earn $200 for each partner led demo (including virtual)
- Earn $250 for hosting a customer-facing workshop (including virtual)
- Earn points for each skill confirmed into a qualified account to achieve higher program status and bonus kicker payouts!

Points Bonus

- Earn 1 point per Skill (shadow, demo, customer workshop) demonstrated and confirmed into a qualified account
- Points accumulate to drive Partner SEs higher on the list of SE MVPs that F5 account teams can reference, as follows:
  - 1-4 points = Rookie Status
  - 5-9 points = Starter Status
  - 10+ points + All Star Status
- F5 will also track and publish the product focus of deals partner SEs perform these skills into to further designate their specialty(ies)
- Partner SE's earn bonus kickers for achieving these Program Status as follows:
  - Reach Starter status and receive a $200 "Starter bonus"
  - Reach All-Star status and receive a $400 "F5 All Star bonus"
  - Reach All-Star status and be the highest point earner to become the SE MVP and win a gift valued at $1000 (In case of tie, $1000 will be split equally between recipients)

How do Partner SEs take advantage of this opportunity?

- Partner registers new SSLo, Adv WAF, NGINX, F5CS or Shape opportunity
- Once deal registration is approved, Partner sets-up customer meeting (inclusive of local F5 sales team)
- Partner SE attends meeting to "Shadow" F5 Field SE and provides recap of meeting to F5 Channel SE for approval
- Partner can also opt to lead the customer demo and/or host a Customer-Facing Workshop on SSLo, Adv WAF, NGINX, F5CS or Shape (min. 8 attendees) to earn more
- Each skill confirmed earns points towards higher program achievement and bonus kickers
- Program funds are limited, so act fast to earn!

Click here for details

OWASP Top 10

2003 OWASP Top 10

1. Unvalidated parameters
2. Broken access control
3. Broken account and session management
4. Cross-site scripting (XSS)
5. Buffer overflows
6. Command injection flaws
7. Error handling problems
8. Insecure use of cryptography
9. Remote administration flaws
10. Web and application server misconfiguration

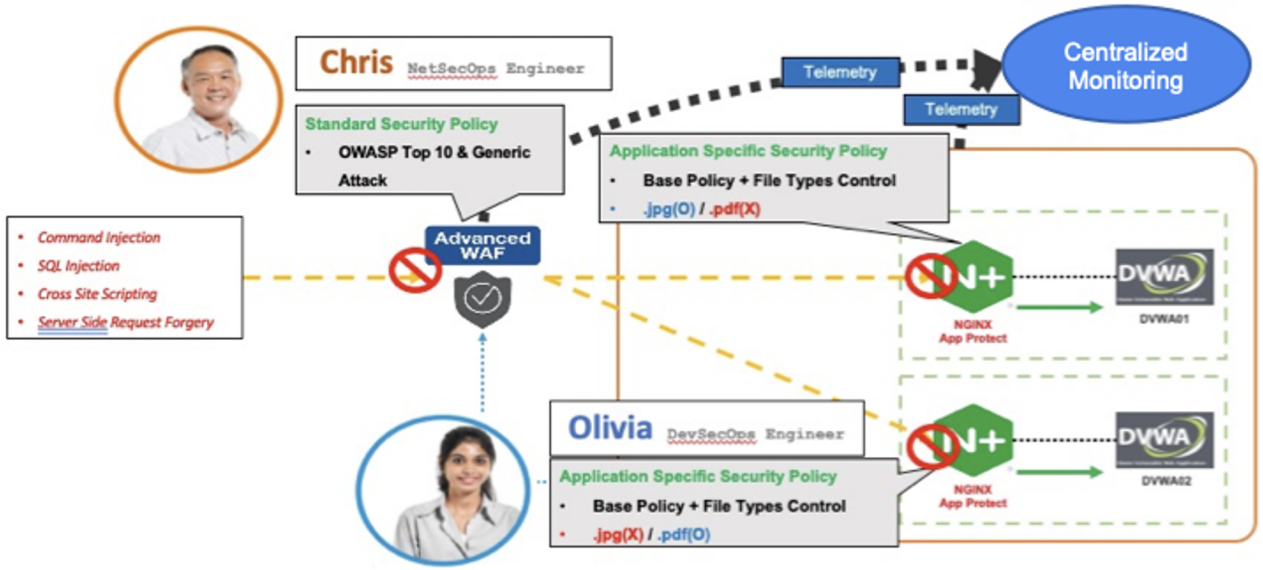
2017 OWASP Top 10

1. Injection
2. Broken authentication
3. Sensitive data exposure
4. XML external entities (XXE)
5. Broken access control
6. Security misconfiguration
7. Cross-site scripting (XSS)
8. Insecure deserialisation
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring

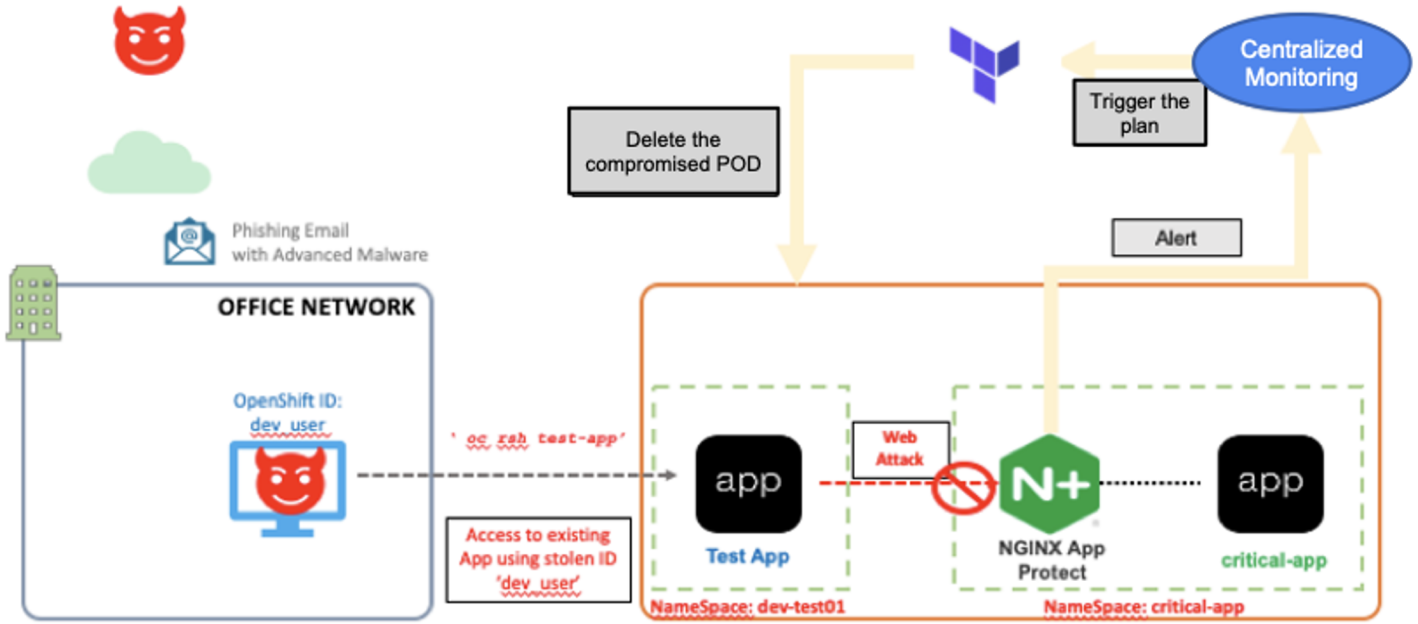
2019 API OWASP Top 10

1. Broken Object Level Authorization
2. Broken authentication
3. Excessive Data Exposure
4. Lack of Resources & Rate Limiting
5. Broken Function Level Authorization
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Assets Management
10. Insufficient logging and monitoring

Layered Security Policy for Modern Apps



Protecting Critical Apps with automated response




HashiCorp

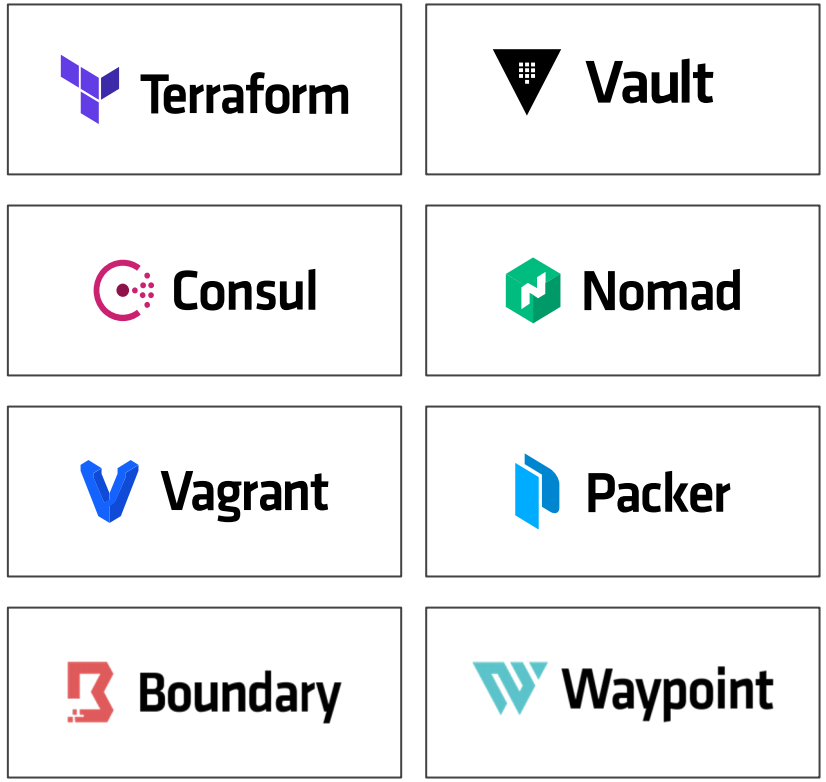
About HashiCorp

Leading Cloud Infrastructure Automation

Our software stack enables the provisioning, securing, connecting and running of apps and the infrastructure to support them.

We unlock the cloud operating model for every business and enable their digital transformation strategies to succeed.

Founded	Employees	Funding
2012	1400+	349M
Founders Armon Dadgar Mitchell Hashimoto		$5.1B Valuation



Evolving application workload delivery

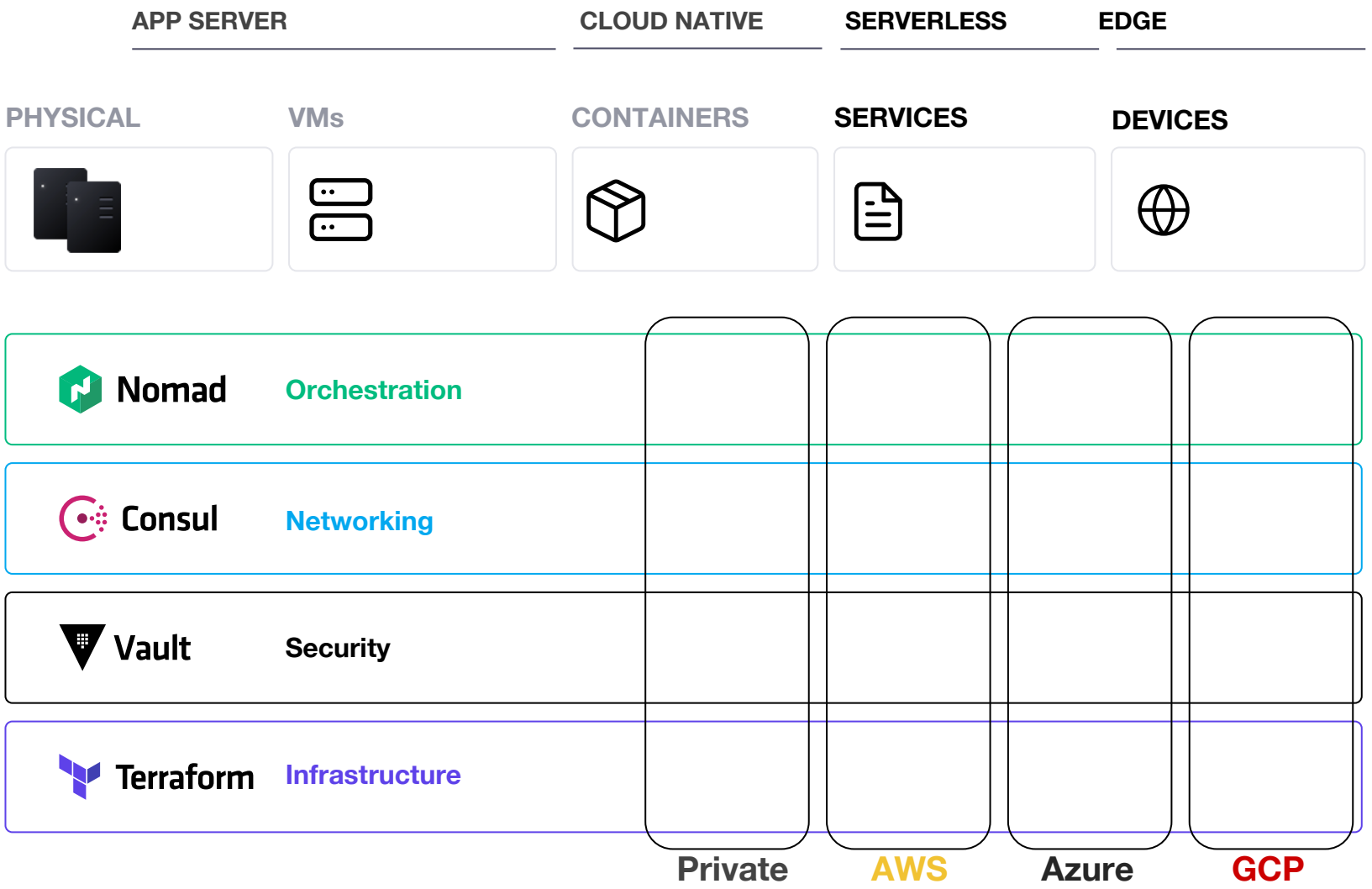
Challenge

How to deliver applications to the cloud with consistency?

Net-New Applications require **Speed to Market** to succeed.

Solution

Establish central shared service platforms with a single control plane, and consistent workflows.



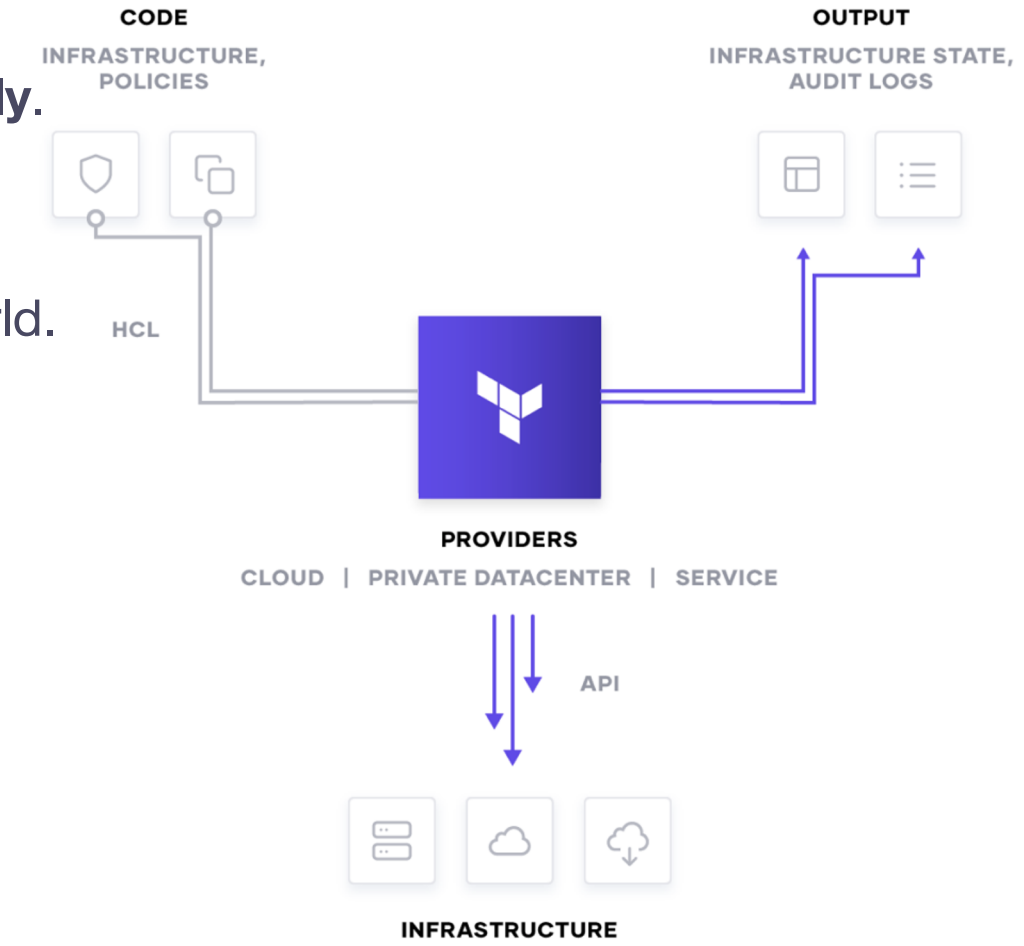
Terraform

Provides an **Infrastructure as Code** approach enabling **DevOps** to deploy Cloud Infrastructure **Efficiently** and **Safely**.

Revolutionary approach within the **DevOps World**.

Simple, Declarative **Syntax** that works in a **Multi-Cloud** world.

Embraced by a **Massive Open Source Community**.



1000 +
Providers

1M+
Weekly D/Ls

30,000+
HUG Members

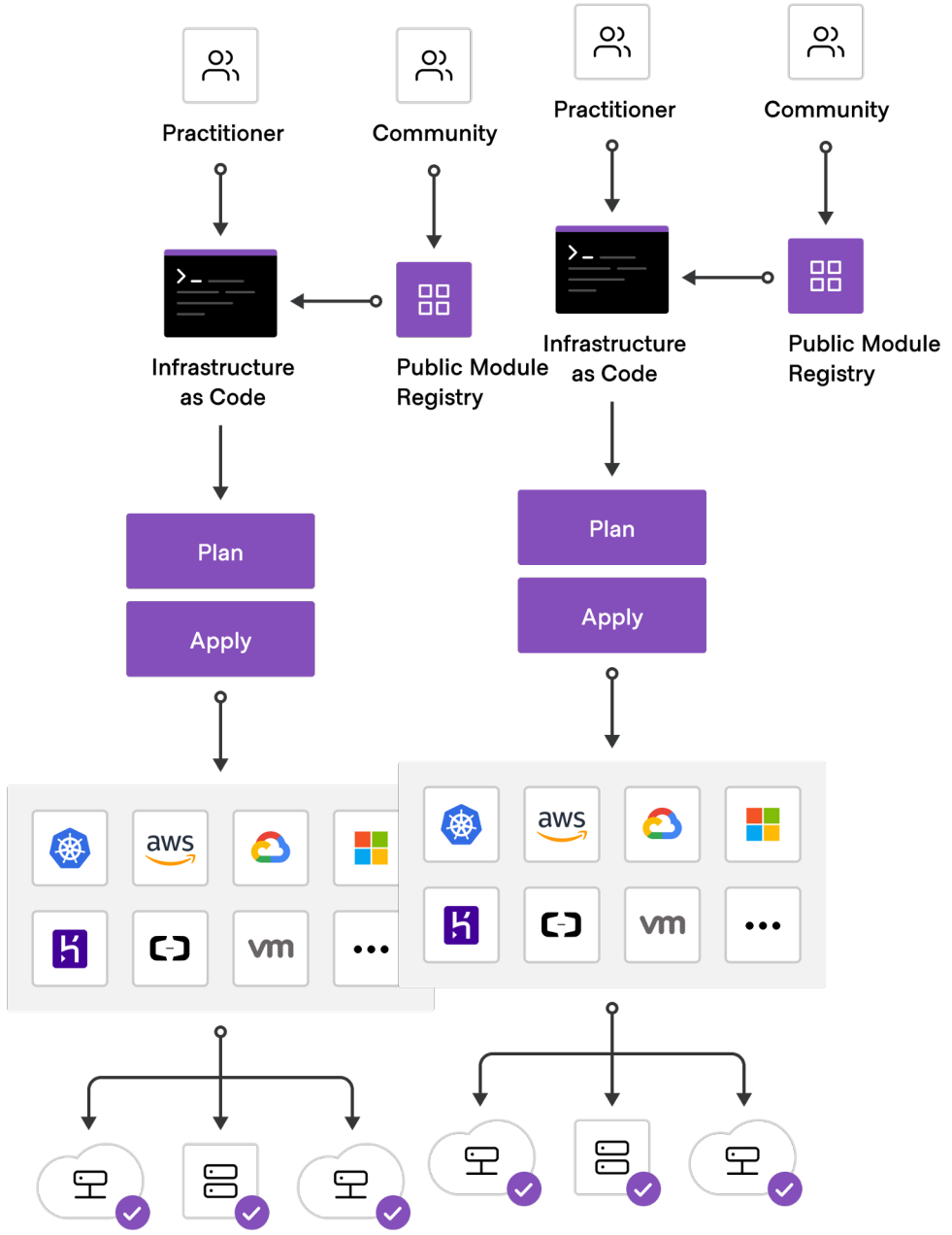
Guiding Principle

Infrastructure as Code

Using version control and automation to reduce human error and failed builds

Terraform infrastructure as code and policy as code to automate everything.

Open source providers allow rapid creation and support for any infrastructure



Vault

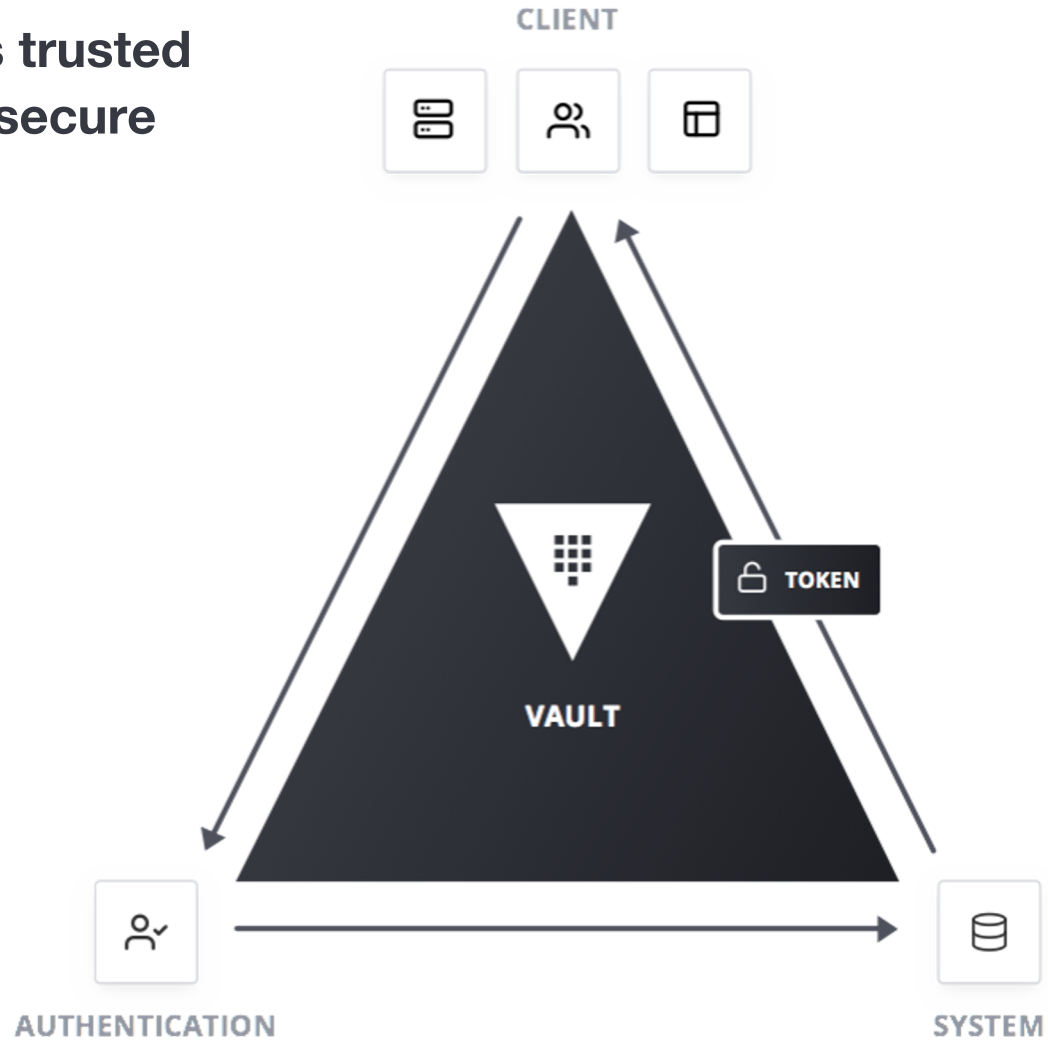
Provides the foundation for cloud security that leverages trusted sources of identity to keep secrets and application data secure in the cloud operating model

- **Secrets management** to centrally store and protect secrets across clouds and applications
- **Data encryption** to keep application data secure across environments and workloads
- **Advanced Data Protection** to secure workloads and data across traditional systems, clouds, and infrastructure.

2T+
Transactions

1M+
Monthly D/Ls

475+
Enterprise Customers

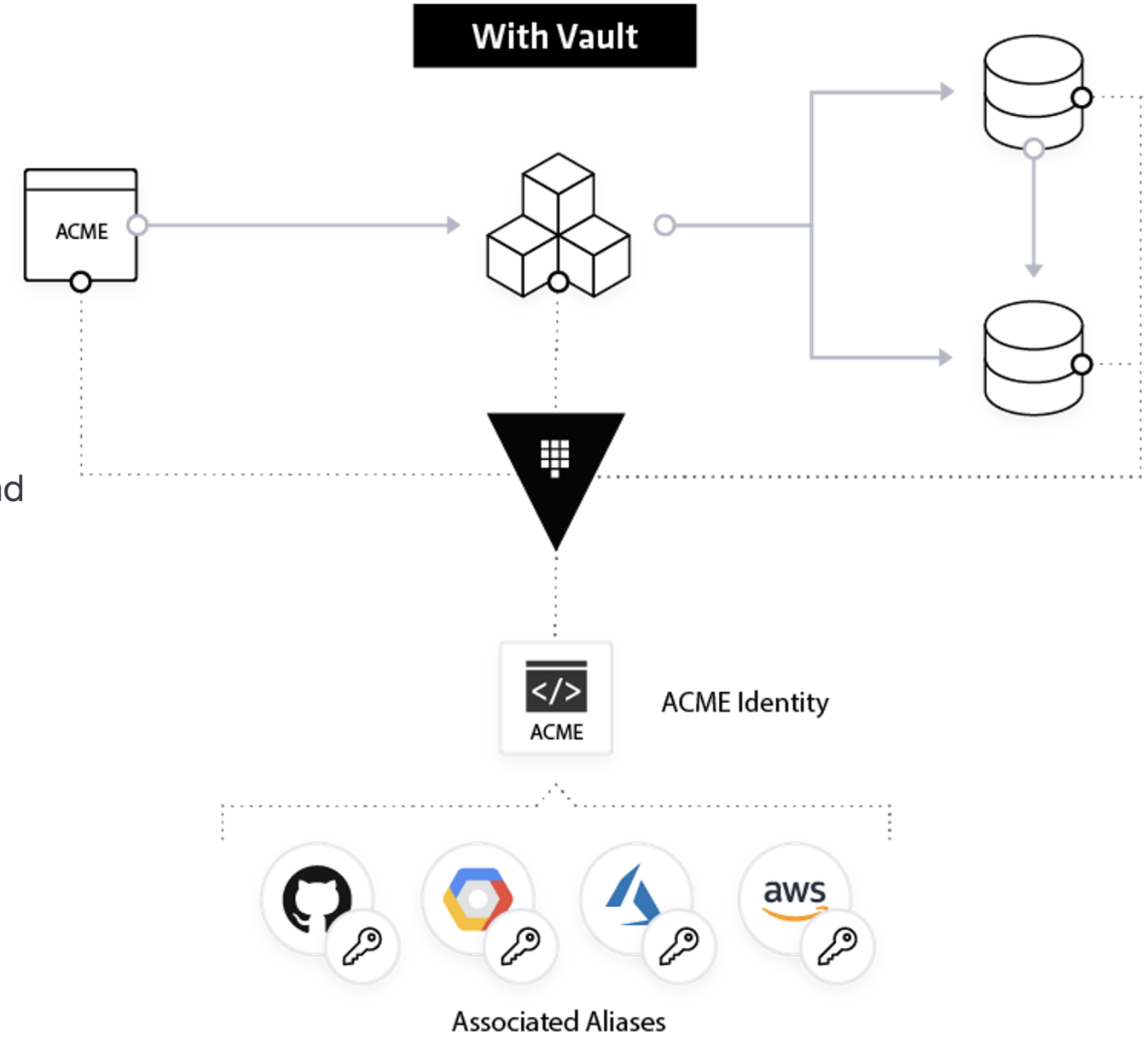


Trusted by:

Guiding Principle:

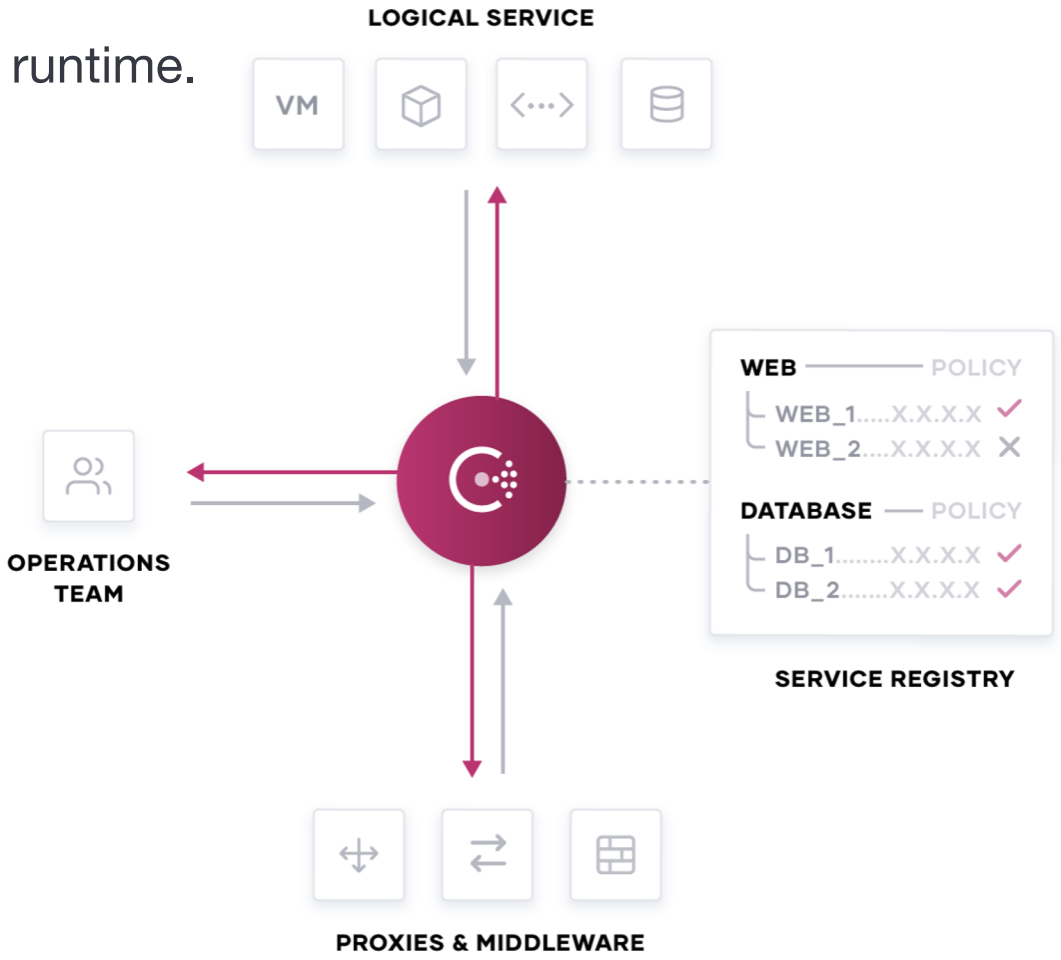
Identity Brokering

- Authenticate and access different clouds, systems, and endpoints using trusted identities
- Leverage multiple identities across different platforms with single policy enforcement
- Integrate trusted identities in the same application workflow to reduce operational overhead



Consul

Discover and securely connect any service on any cloud or runtime.



- Decouple networking from IP addresses to support dynamic networking
- Provide an automated services networking and security based on logical services
- Services can be discovered, connected and secured with service name as identity.
- Captures telemetry data which can be observed via UI or exported to third-party tools

1M+

Monthly D/Ls

50k+

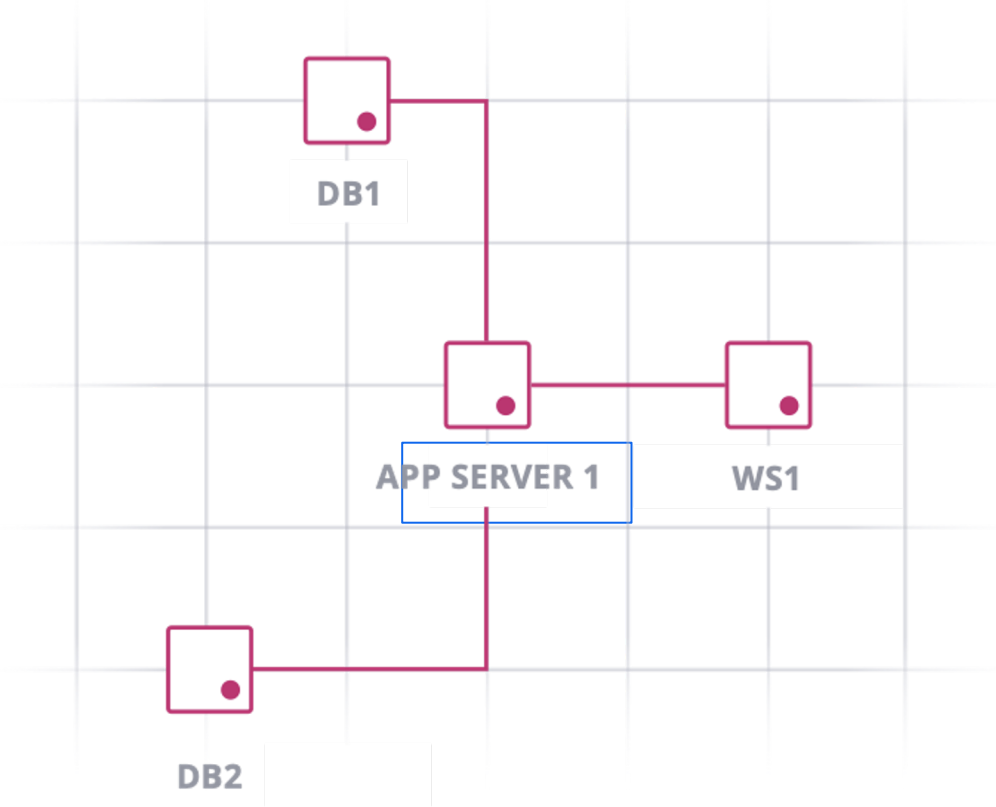
Used at scale with 50k+ agents

Trusted by: Mercedes-Benz

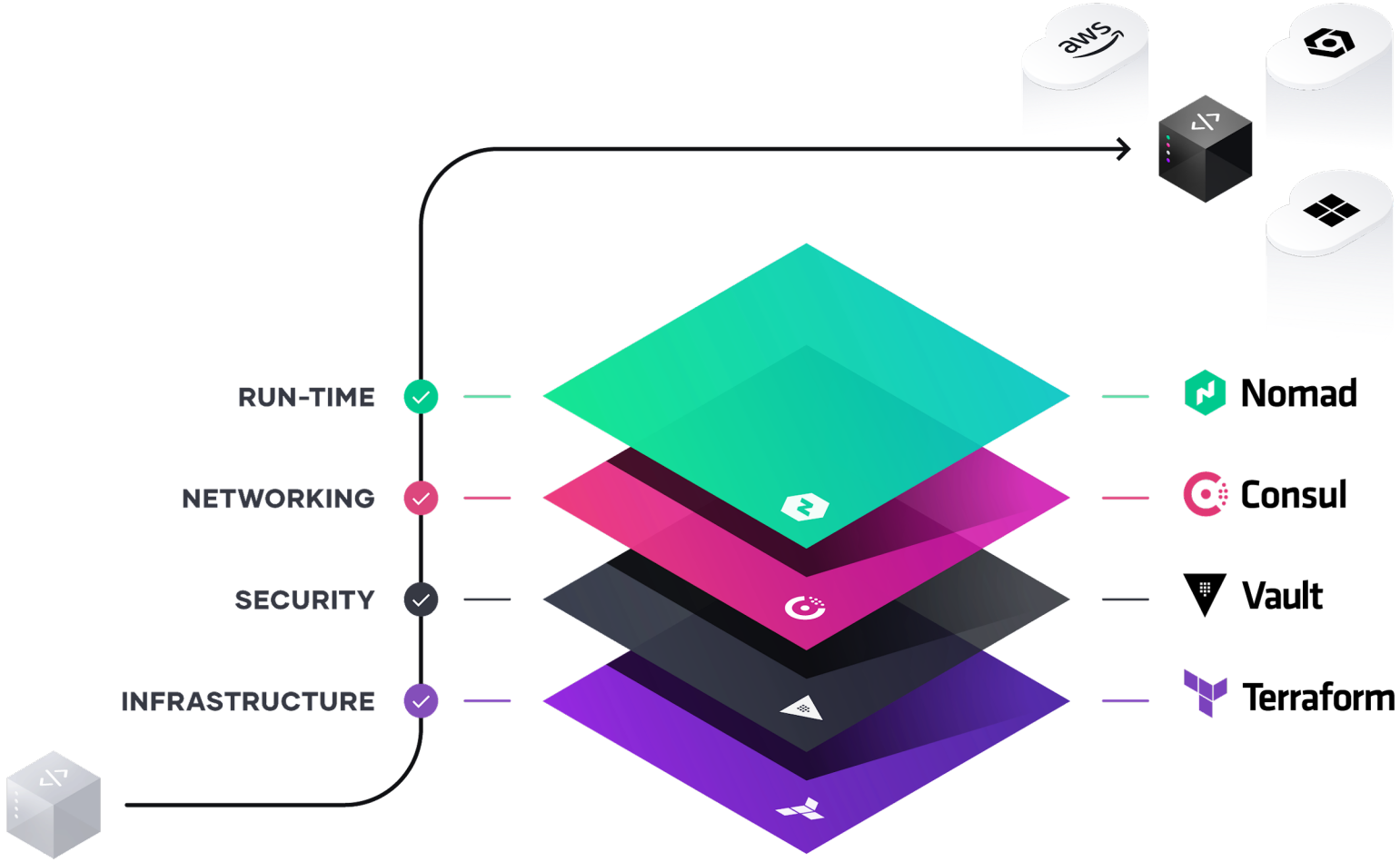
Guiding Principle

Shared Registry

- Allow networking operations to decouple from IP addresses
- Automated networking and security based on logical services
- Services can be discovered, connected and secured with service name as identity.



Delivering app workloads to multi-cloud environments with a single control plane at every layer



F5 & HashiCorp

SMOKE THE COMPETITION

SMOKE THE COMPETITION CHECKPOINTS

- ❑ 8/12 - Mitigate OWASP Top 10
- ❑ 9/02 - NGINX KIC
- ❑ 9/23 - Bots & App Fraud
- ❑ 10/14 - Putting it all together

Complete the challenge

F5 AND HASHICORP TECH FAIRS

- ❑ **Bay Area**
- ❑ **Sacramento**
- ❑ **Portland**

TOPGOLF

Join the fun

How to SMOKE THE COMPETITION

Activity/Task	Points Earned
Attend Checkpoint Calls	200 / Call
Complete a Task (Two per checkpoint)	100 / Task
Register PIO Opportunity by 10/18	500 / Opportunity
Close PIO Opportunity by 10/18	1,000 / Opportunity