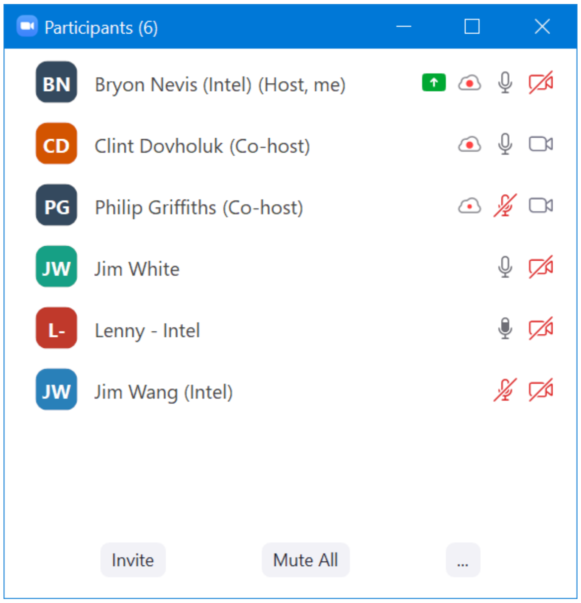
EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

May 11, 2022

Attendees



Participants (6)

BN Bryon Nevis (Intel) (Host, me)

CD Clint Dovholuk (Co-host)

PG Philip Griffiths (Co-host)

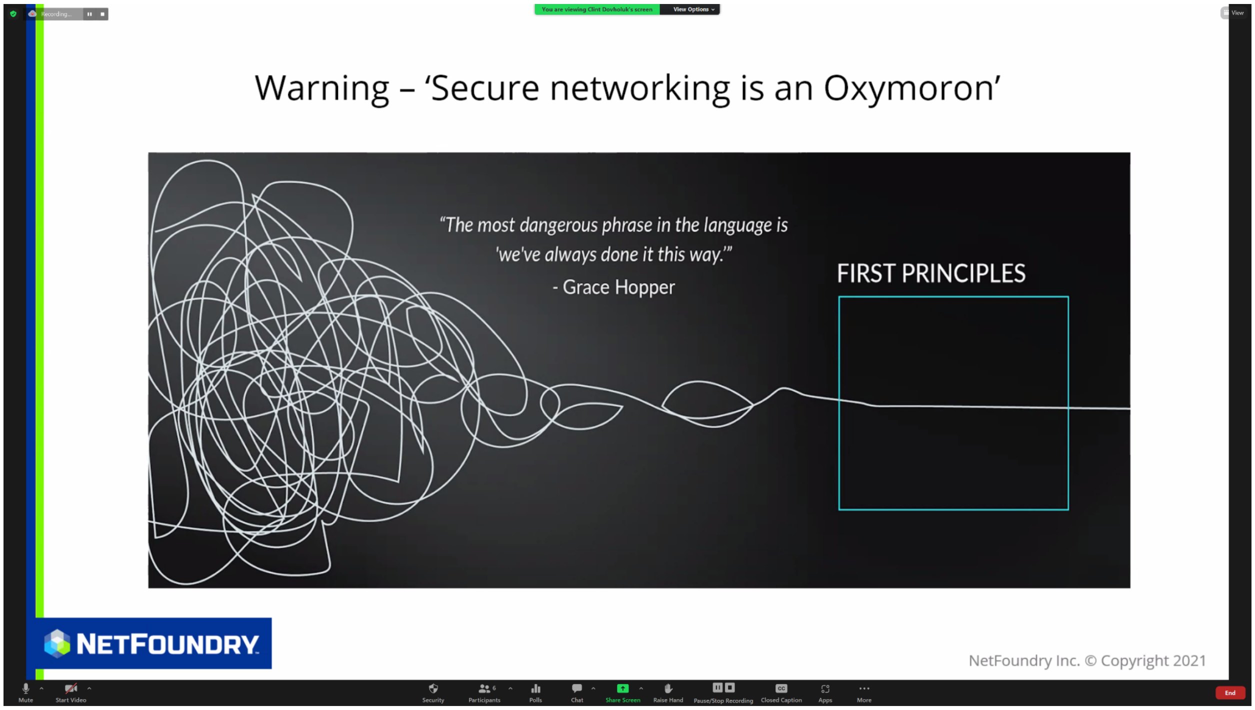
JW Jim White

L- Lenny - Intel

JW Jim Wang (Intel)

Agenda

- Clint Dovholuk @ NetFoundry presenting OpenZiti as a possible solution to EdgeX microservice security.



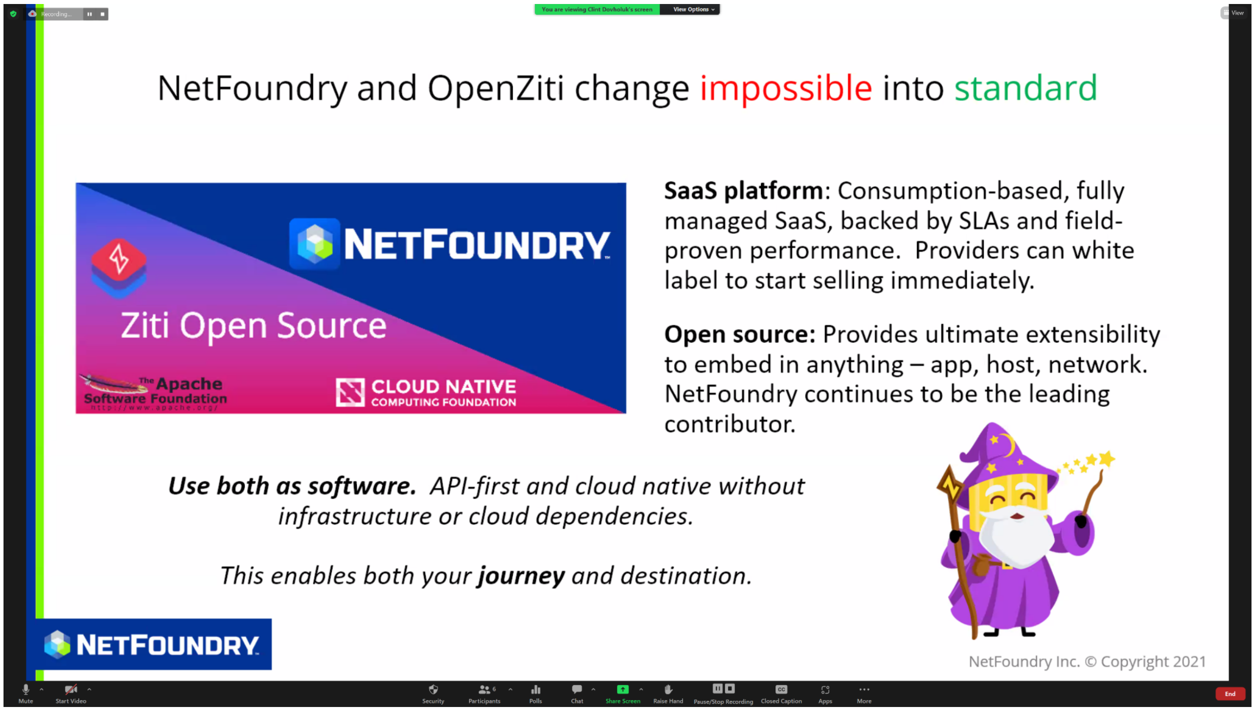
Warning – 'Secure networking is an Oxymoron'

"The most dangerous phrase in the language is 'we've always done it this way.'"
- Grace Hopper

FIRST PRINCIPLES

NETFOUNDRY

NetFoundry Inc. © Copyright 2021



NetFoundry and OpenZiti change impossible into standard

SaaS platform: Consumption-based, fully managed SaaS, backed by SLAs and field-proven performance. Providers can white label to start selling immediately.

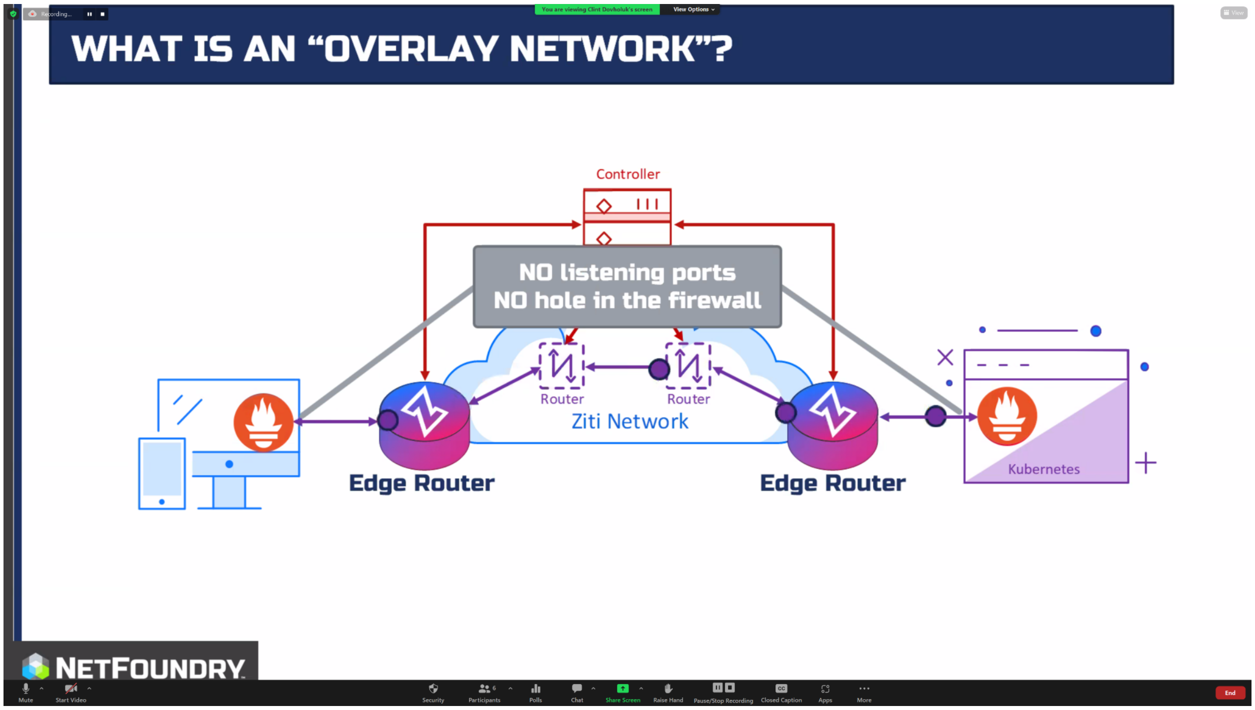
Open source: Provides ultimate extensibility to embed in anything – app, host, network. NetFoundry continues to be the leading contributor.

Use both as software. *API-first and cloud native without infrastructure or cloud dependencies.*

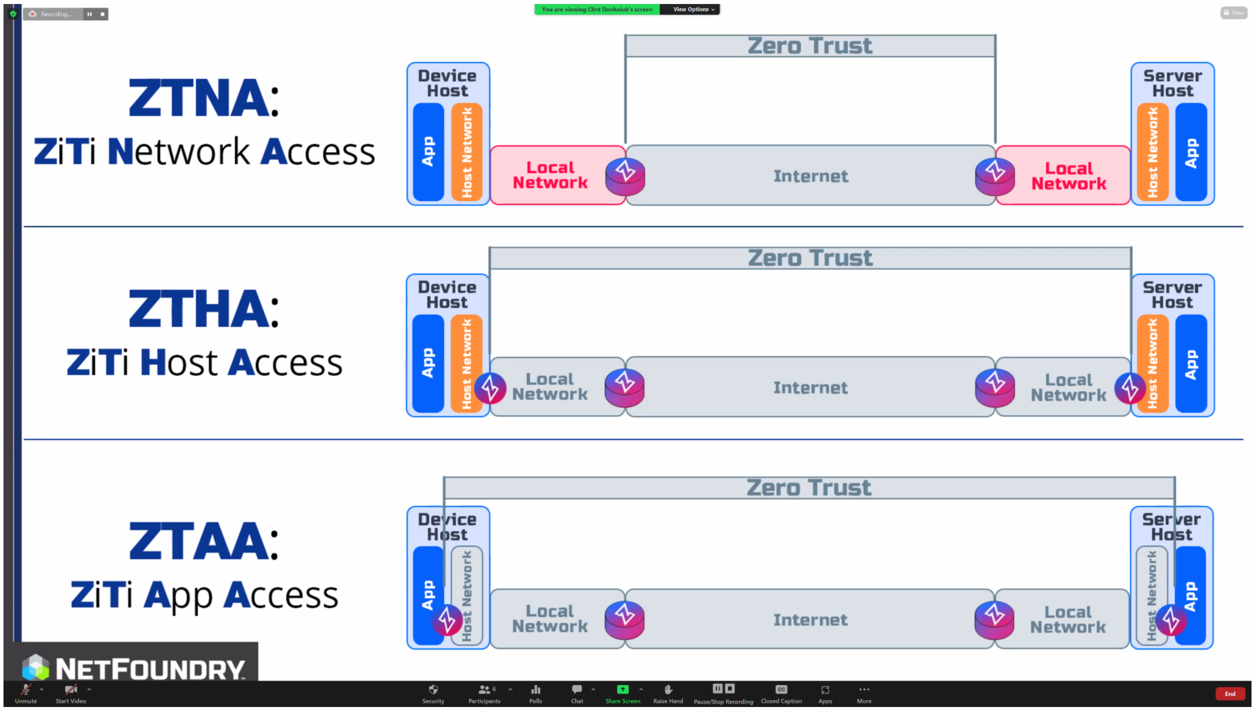
*This enables both your **journey** and destination.*

NETFOUNDRY

NetFoundry Inc. © Copyright 2021



WHAT IS AN "OVERLAY NETWORK"?

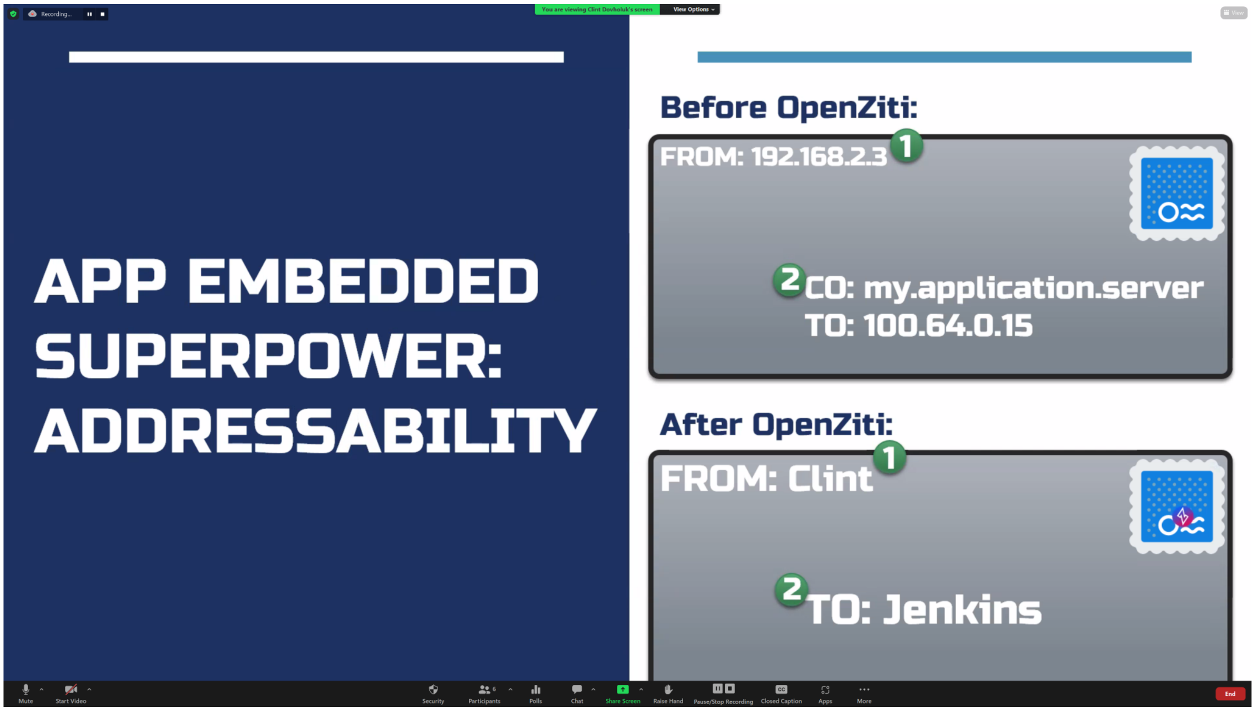


ZTNA: ZiTi Network Access

ZTHA: ZiTi Host Access

ZTAA: ZiTi App Access

“THE BEAST”
VS
“MAD MAX”



APP EMBEDDED SUPERPOWER: ADDRESSABILITY

Before OpenZiti:

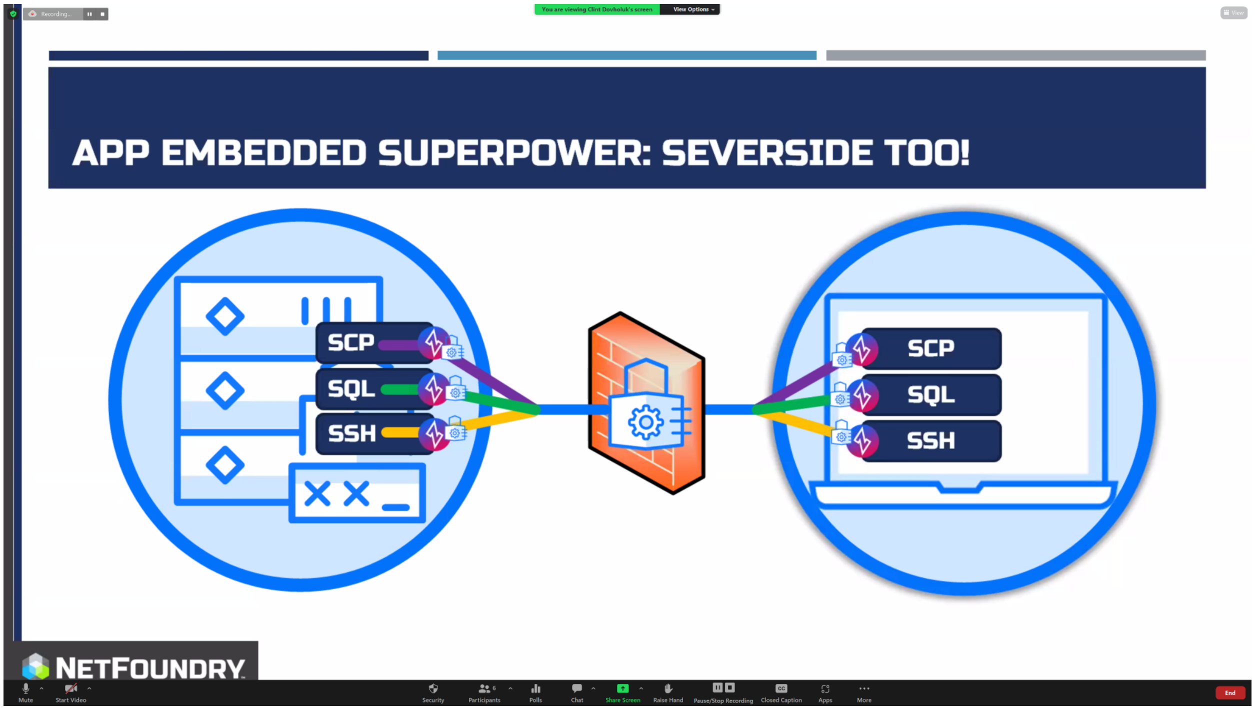
1 FROM: 192.168.2.3

2 CO: my.application.server
TO: 100.64.0.15

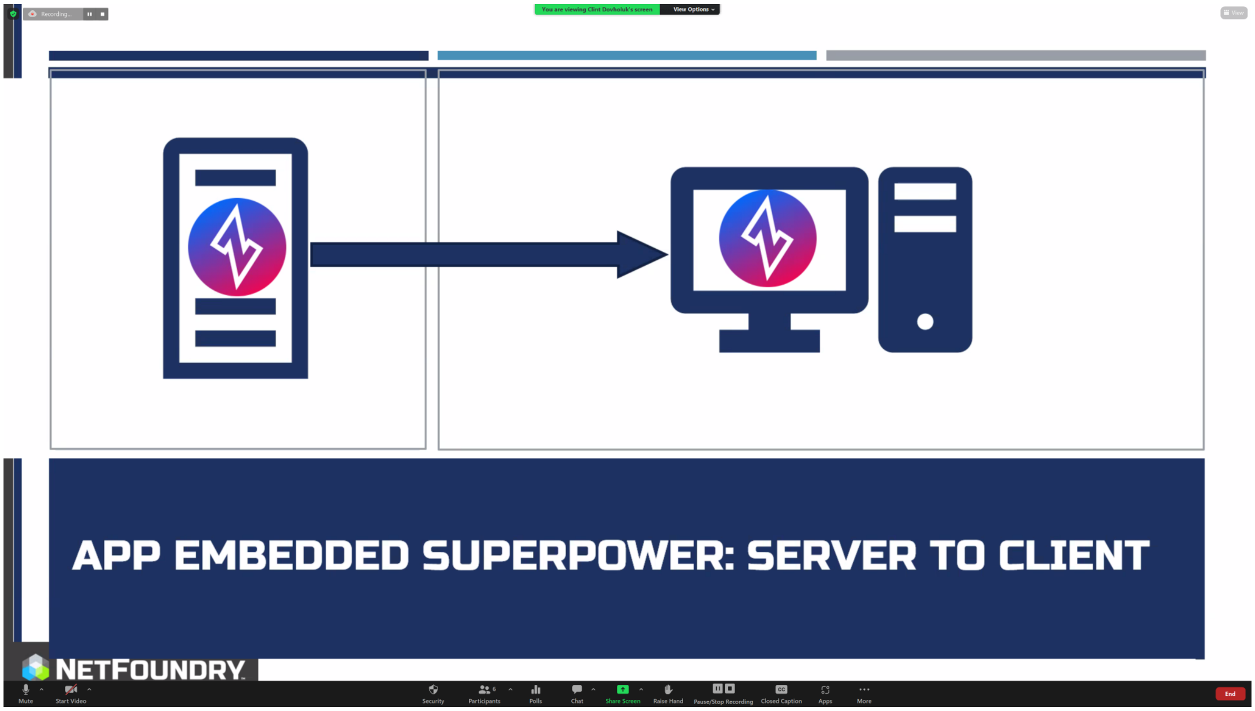
After OpenZiti:

1 FROM: Clint

2 TO: Jenkins



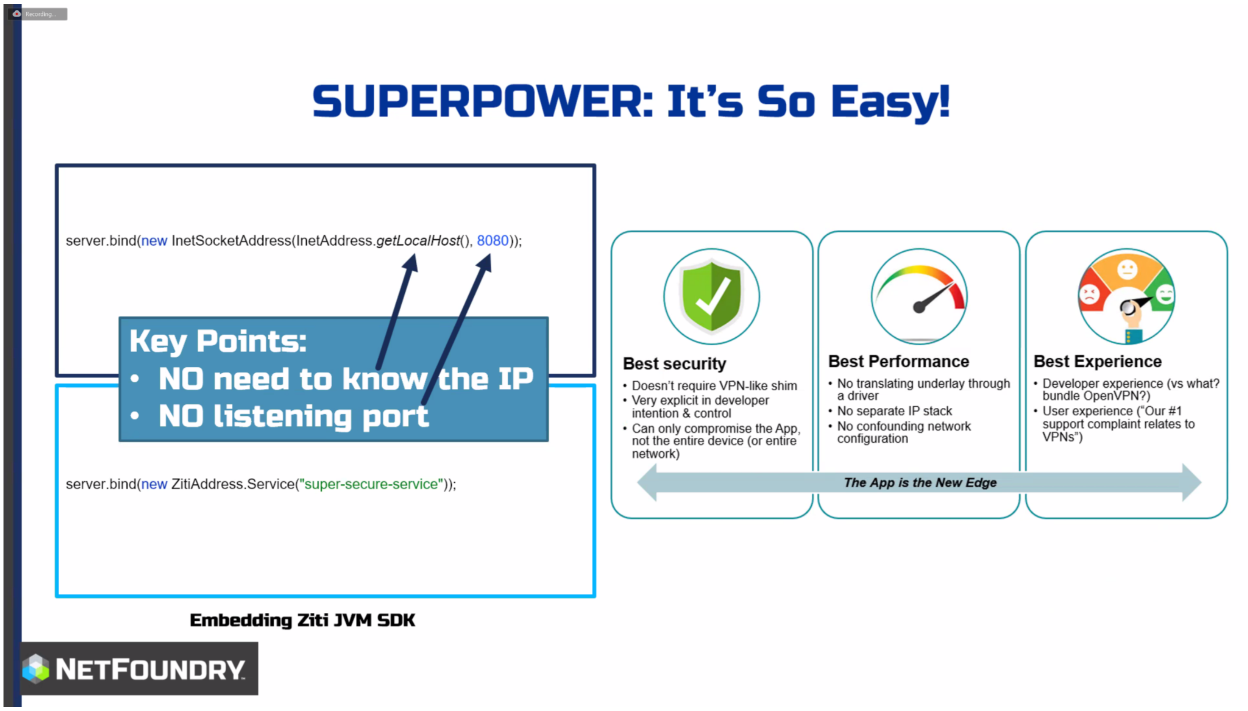
APP EMBEDDED SUPERPOWER: SEVERSIDE TOO!



APP EMBEDDED SUPERPOWER: SERVER TO CLIENT

APP EMBEDDED SUPERPOWER: END TO END ENCRYPTION

ChaChaPoly1305 (libsodium) - no current algorithm flexibility



SUPERPOWER: It's So Easy!

```
server.bind(new InetSocketAddress(InetAddress.getLocalHost(), 8080));
```

Key Points:

- NO need to know the IP
- NO listening port

```
server.bind(new ZitiAddress.Service("super-secure-service"));
```

Embedding Ziti JVM SDK

Best security

- Doesn't require VPN-like shim
- Very explicit in developer intention & control
- Can only compromise the App, not the entire device (or entire network)

Best Performance

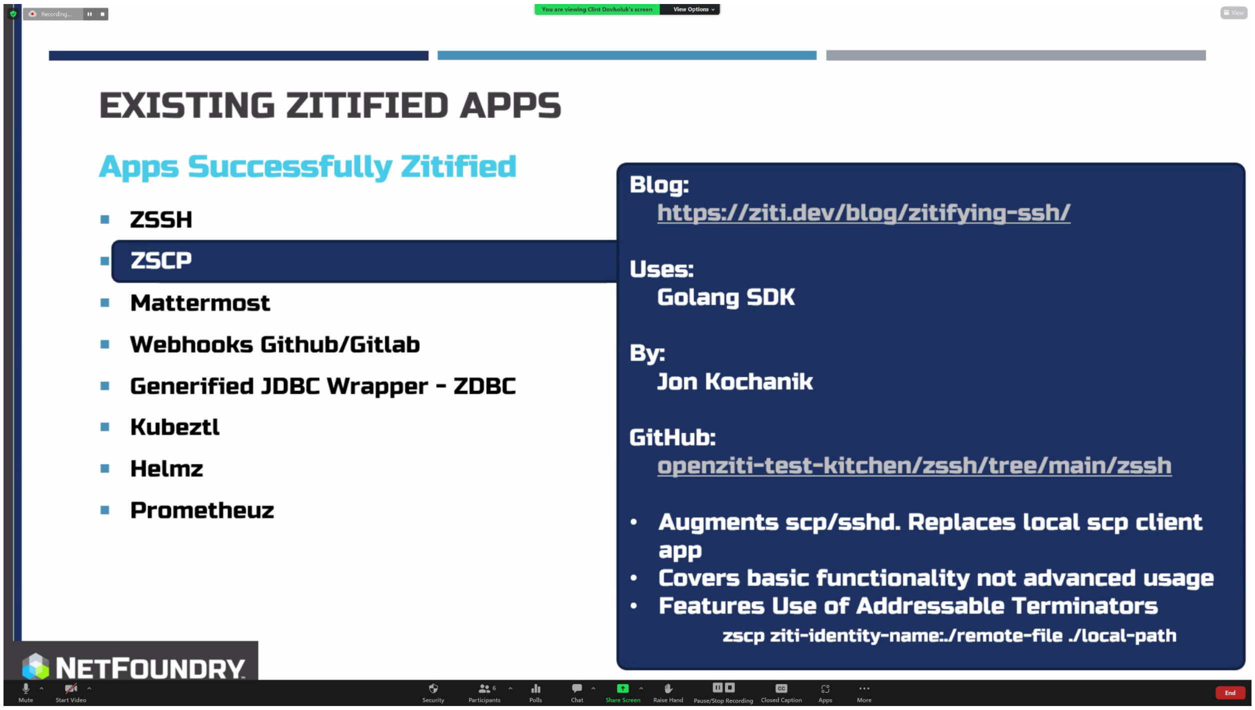
- No translating underlay through a driver
- No separate IP stack
- No confounding network configuration

Best Experience

- Developer experience (vs what? bundle OpenVPN?)
- User experience ("Our #1 support complaint relates to VPNs")

The App is the New Edge

NETFOUNDRY



EXISTING ZITIFIED APPS

Apps Successfully Zitified

- ZSSH
- ZSCP
- Mattermost
- Webhooks Github/Gitlab
- Generified JDBC Wrapper - ZDBC
- Kubeztl
- Helmz
- Prometheuz

Blog:
https://ziti.dev/blog/zitifying-ssh/

Uses:
Golang SDK

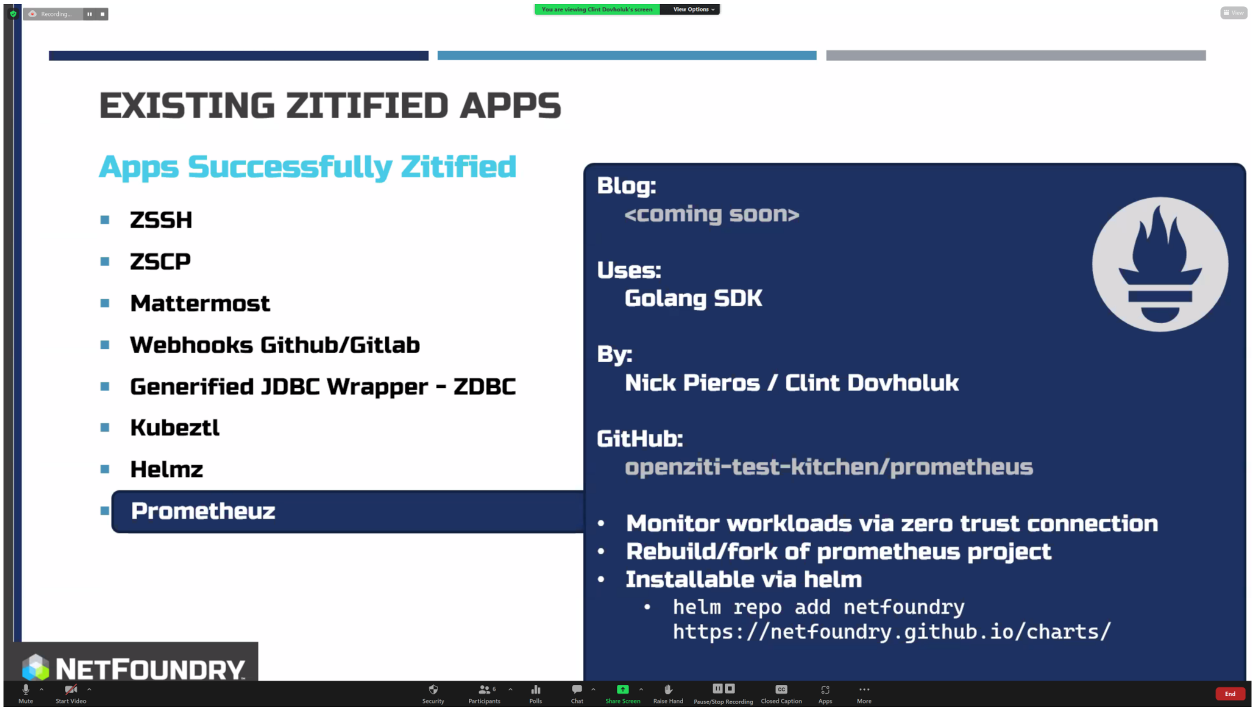
By:
Jon Kochanik

GitHub:
openziti-test-kitchen/zssh/tree/main/zssh

- Augments scp/sshd. Replaces local scp client app
- Covers basic functionality not advanced usage
- Features Use of Addressable Terminators

```
zscp ziti-identity-name:./remote-file ./local-path
```

NETFOUNDRY



EXISTING ZITIFIED APPS

Apps Successfully Zitified

- ZSSH
- ZSCP
- Mattermost
- Webhooks Github/Gitlab
- Generified JDBC Wrapper - ZDBC
- Kubeztl
- Helmz
- Prometheuz

Blog:
<coming soon>

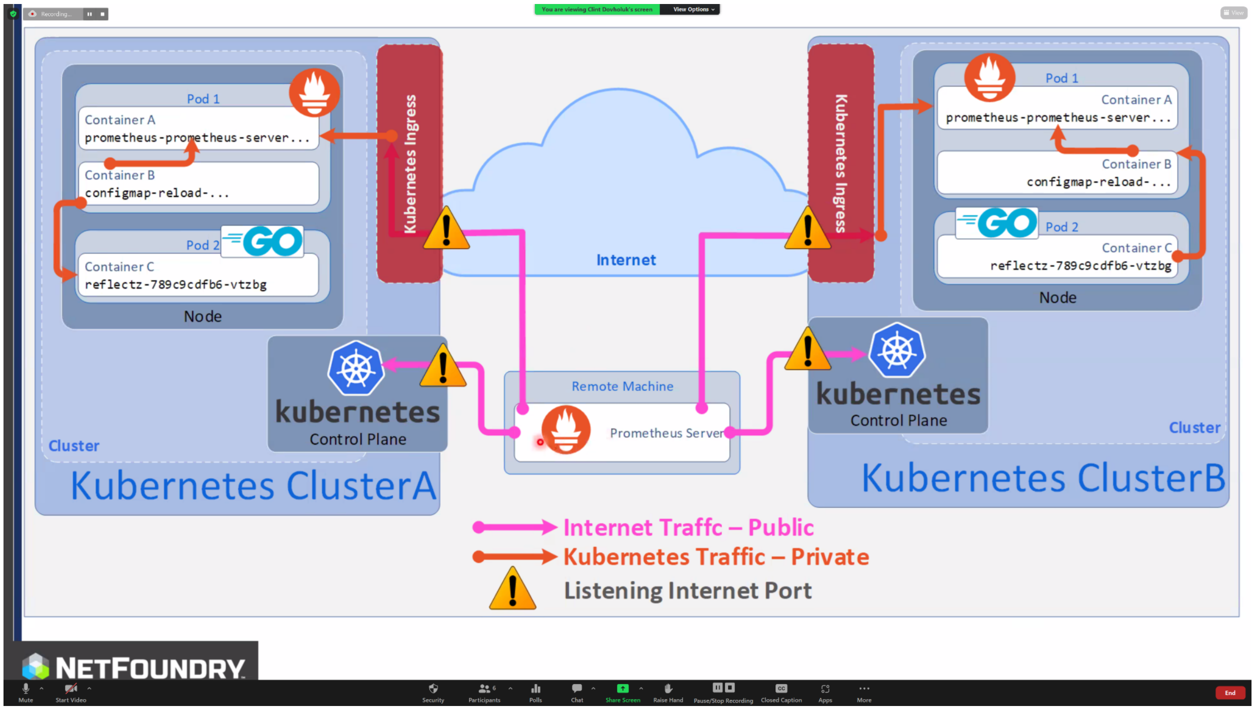
Uses:
Golang SDK

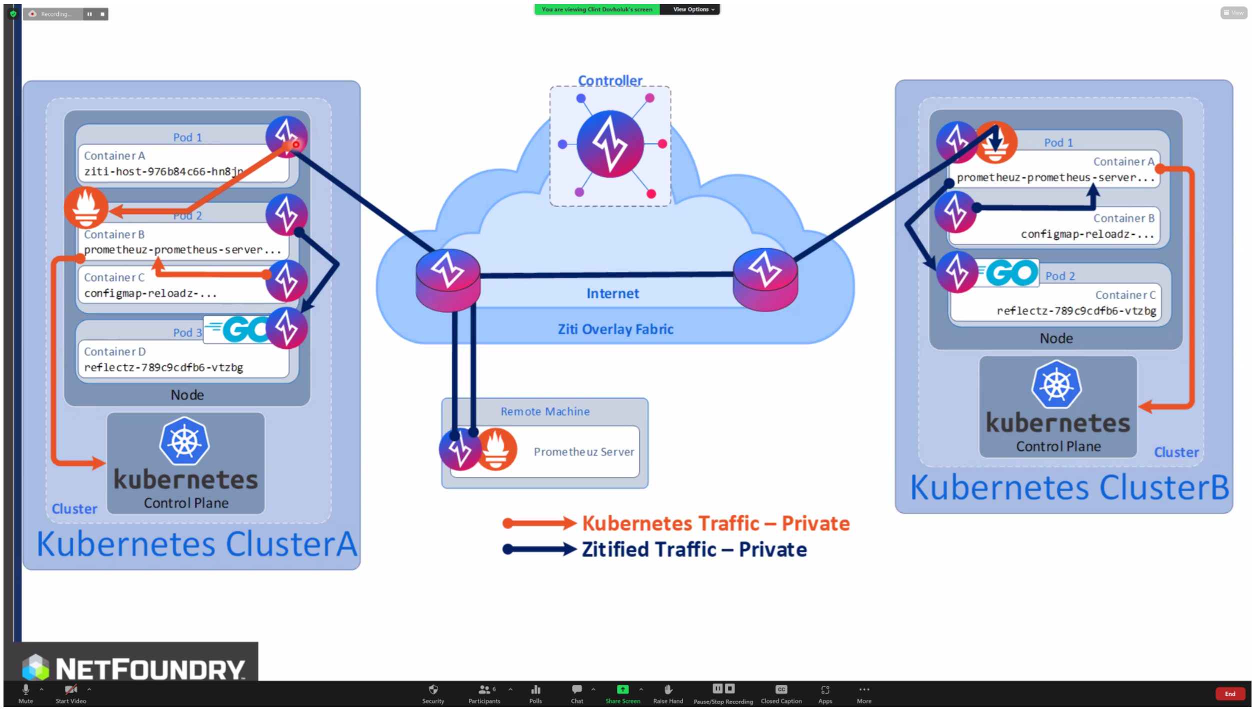
By:
Nick Pieros / Clint Dovholuk

GitHub:
openziti-test-kitchen/prometheus

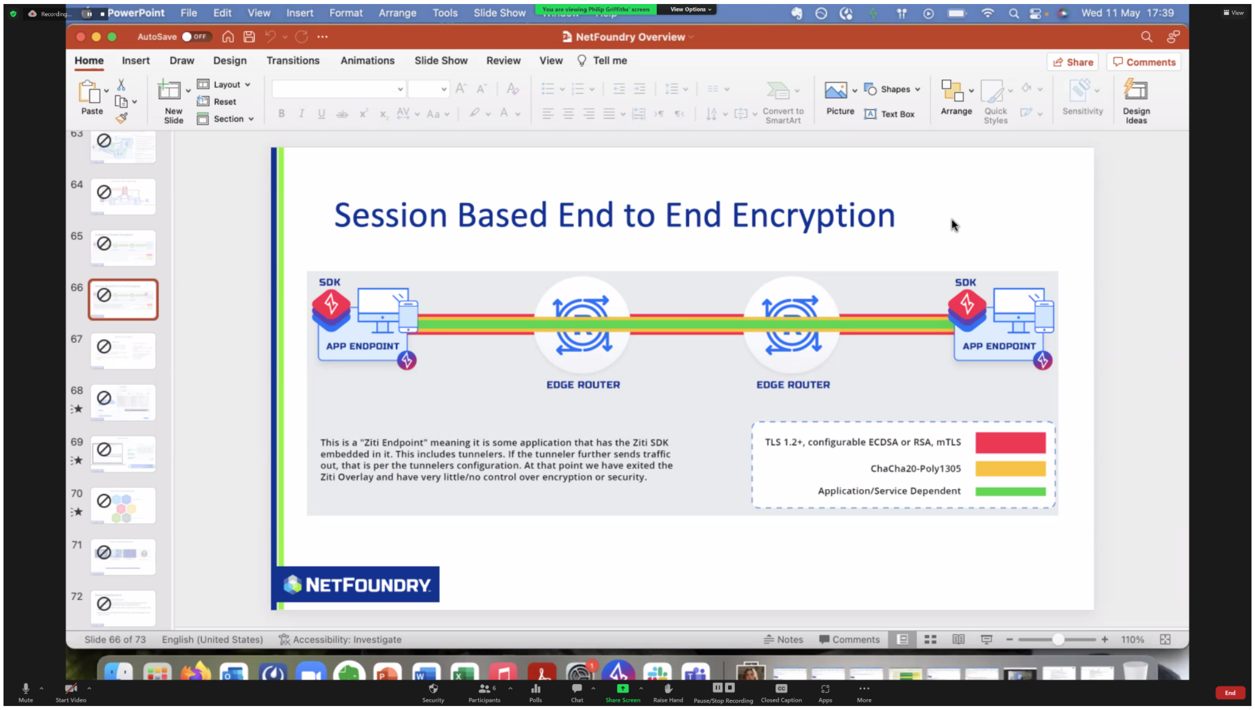
- Monitor workloads via zero trust connection
- Rebuild/fork of prometheus project
- Installable via helm
  - helm repo add netfoundry https://netfoundry.github.io/charts/

NETFOUNDRY





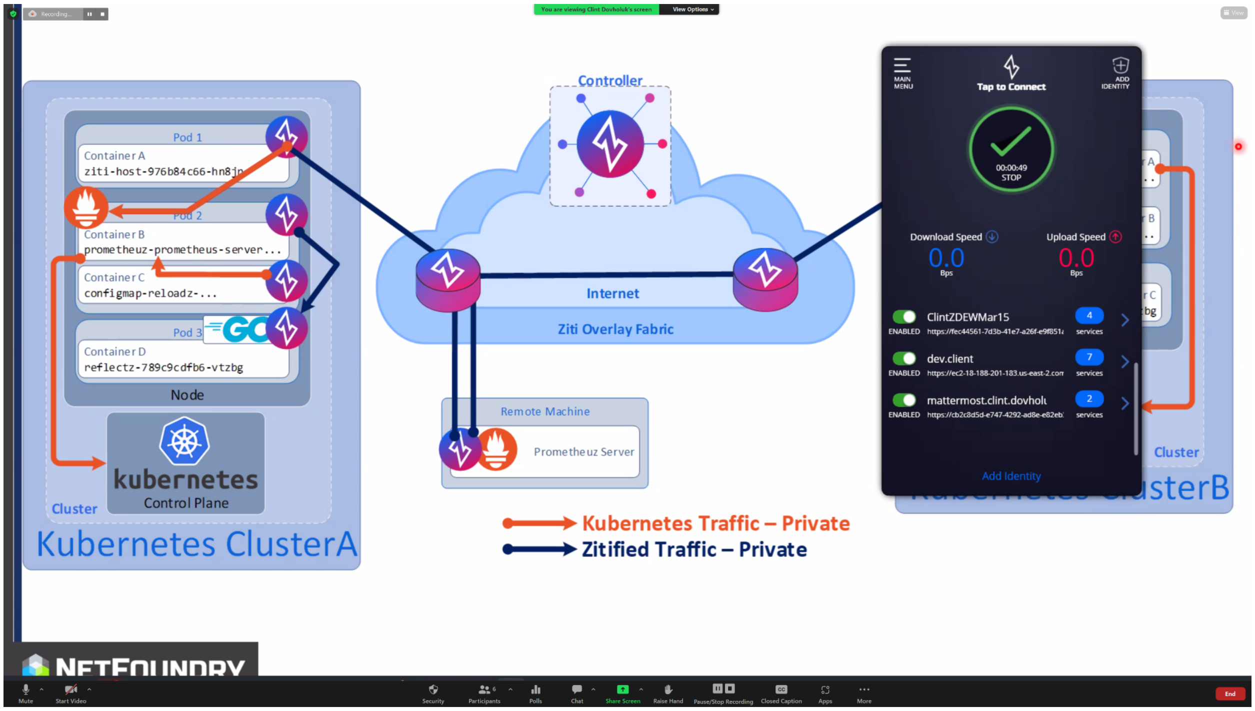
Has a C SDK (est 1MB overhead)
Has a GO SDK



Session Based End to End Encryption

This is a "Ziti Endpoint" meaning it is some application that has the Ziti SDK embedded in it. This includes tunnelers. If the tunneler further sends traffic out, that is per the tunnelers configuration. At that point we have exited the Ziti Overlay and have very little/no control over encryption or security.

TLS 1.2+, configurable ECDSA or RSA, mTLS	🟥
ChaCha20-Poly1305	🟨
Application/Service Dependent	🟩

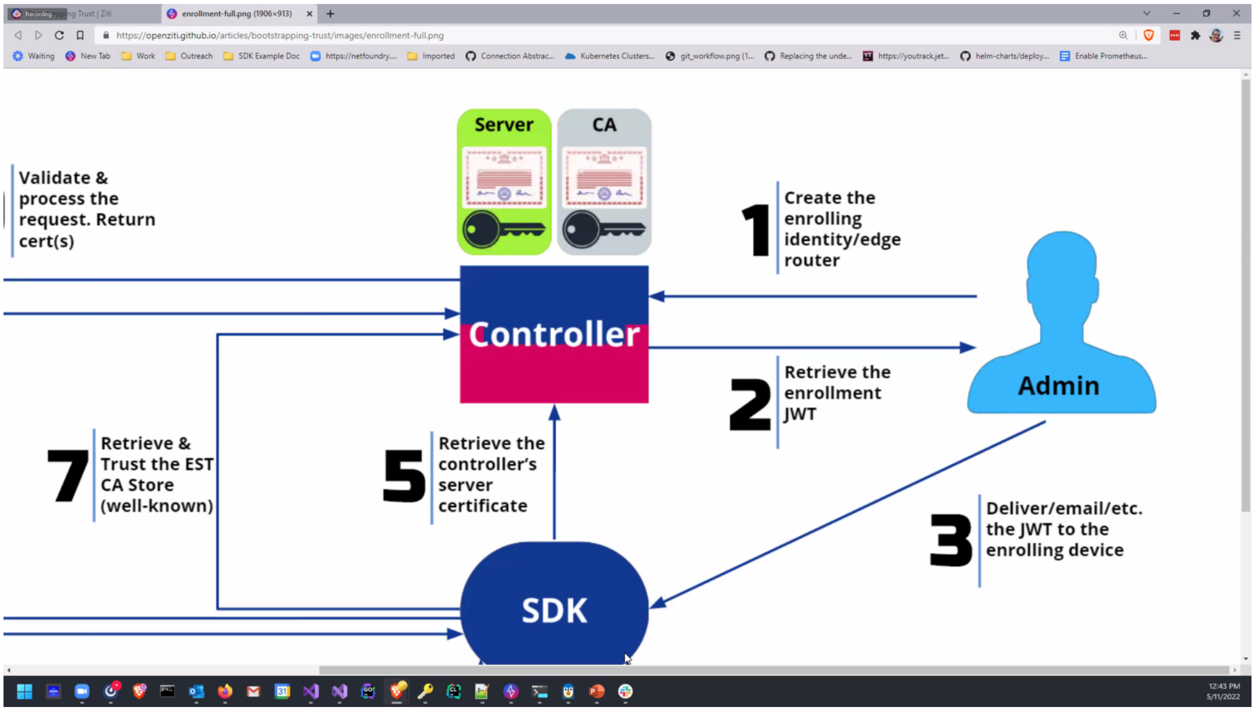


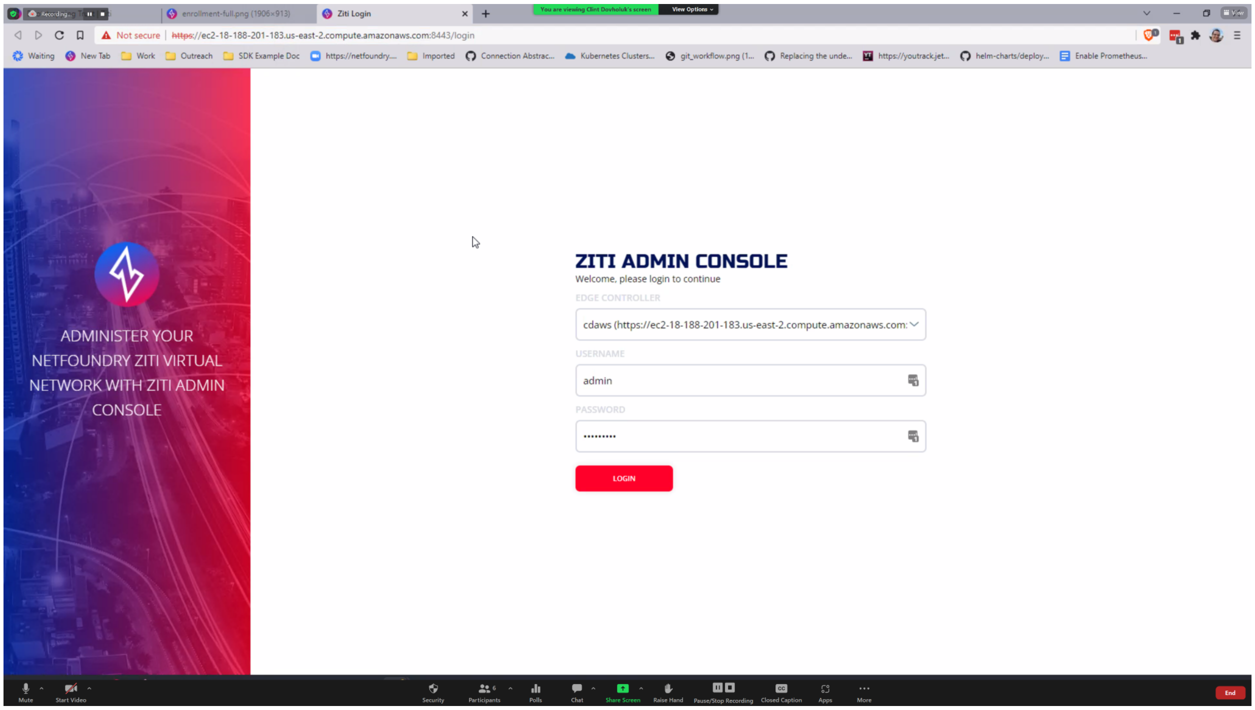
Has flexible policies that can check for antivirus present, mac addresses, etc.

Enrollment process:

- Can bring your own CA
- Can integrate with SPIFFE
- Controller is the root of trust that bootstraps a full PKI
- Quickstart creates a PKI

  - Create an identity which is a JWT
  - JWT is distributed out of band
  - JWT is one time use
  - Create private key on the client. Connects to well-known endpoint to trust the server. Uses JWT to authorize CSR and returns certificate. Identities are X.509 based.
  - With SPIFFE in play can use 3rd party CA feature, can make Ziti automatically trust the SPIFFE cert.
  -
-


Recording...ng Trust | Ziti
enrollment-full.png (1906×913)
https://openziti.github.io/articles/bootstrapping-trust/images/enrollment-full.png
Waiting
New Tab
Work
Outreach
SDK Example Doc
https://netfoundry....
Imported
Connection Abstrac...
Kubernetes Clusters...
git_workflow.png (1...
Replacing the unde...
https://youtrack.jet...
helm-charts/deploy...
Enable Prometheus...
Server
CA
Validate & process the request. Return cert(s)
1 Create the enrolling identity/edge router
Controller
2 Retrieve the enrollment JWT
Admin
7 Retrieve & Trust the EST CA Store (well-known)
5 Retrieve the controller's server certificate
3 Deliver/email/etc. the JWT to the enrolling device
SDK
12:43 PM
5/11/2022



https://ec2-18-188-201-183.us-east-2.compute.amazonaws.com:8443/login

ADMINISTER YOUR NETFOUNDRY ZITI VIRTUAL NETWORK WITH ZITI ADMIN CONSOLE

ZITI ADMIN CONSOLE

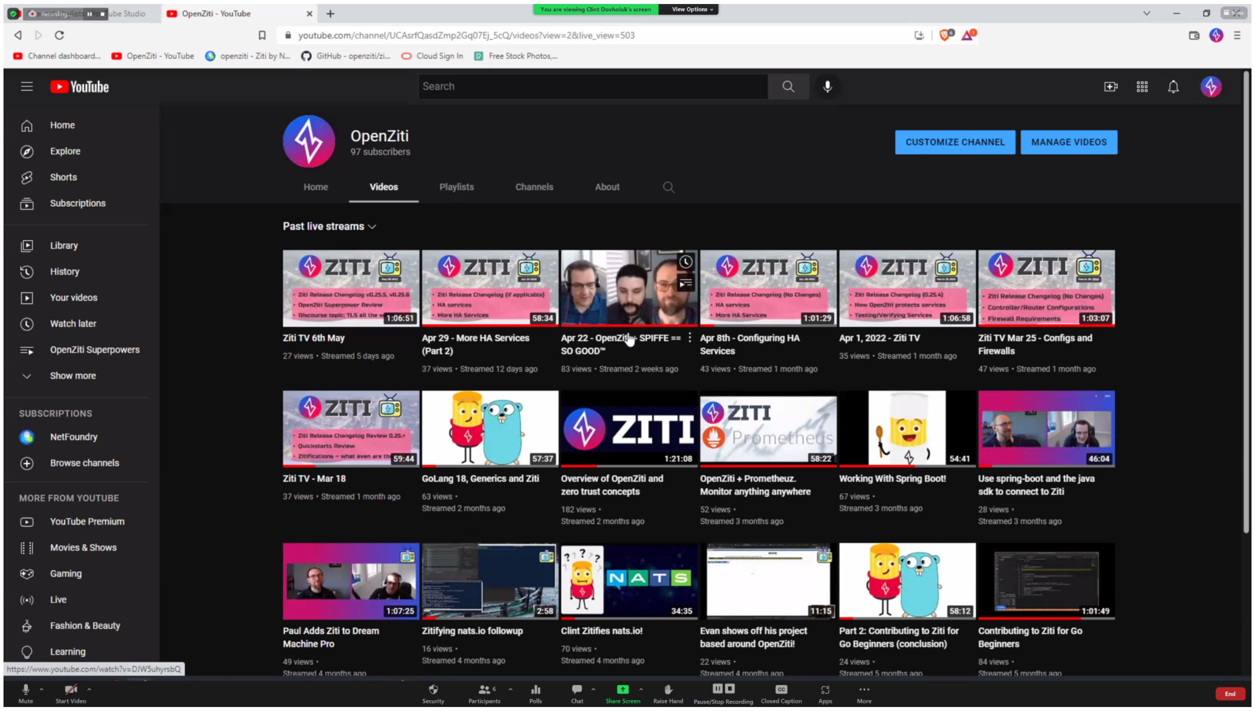
Welcome, please login to continue

EDGE CONTROLLER: cdaws (https://ec2-18-188-201-183.us-east-2.compute.amazonaws.com:

USERNAME: admin

PASSWORD: ••••••••••

LOGIN



youtube.com/channel/UCAsrfQasdZmp2Gq07Ej_5cQ/videos?view=2&live_view=503

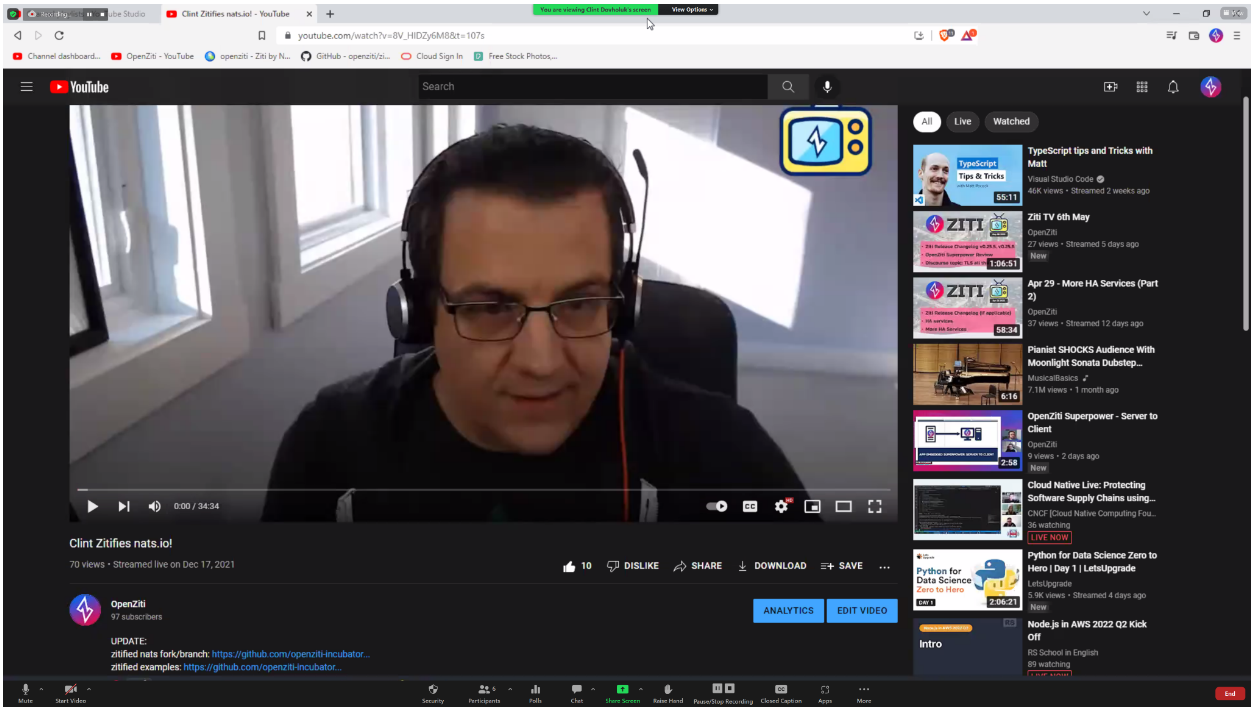
OpenZiti
97 subscribers

Past live streams

- Ziti TV 6th May — 27 views • Streamed 5 days ago — 1:06:51
- Apr 29 - More HA Services (Part 2) — 37 views • Streamed 12 days ago — 58:34
- Apr 22 - OpenZiti - SPIFFE == SO GOOD™ — 83 views • Streamed 2 weeks ago
- Apr 8th - Configuring HA Services — 43 views • Streamed 1 month ago — 1:01:29
- Apr 1, 2022 - Ziti TV — 35 views • Streamed 1 month ago — 1:06:58
- Ziti TV Mar 25 - Configs and Firewalls — 47 views • Streamed 1 month ago — 1:03:07
- Ziti TV - Mar 18 — 37 views • Streamed 1 month ago — 59:44
- GoLang 18, Generics and Ziti — 63 views • Streamed 2 months ago — 57:37
- Overview of OpenZiti and zero trust concepts — 182 views • Streamed 2 months ago — 1:21:08
- OpenZiti + Prometheuz. Monitor anything anywhere — 52 views • Streamed 3 months ago — 58:22
- Working With Spring Boot! — 67 views • Streamed 3 months ago — 54:41
- Use spring-boot and the java sdk to connect to Ziti — 28 views • Streamed 3 months ago — 46:04
- Paul Adds Ziti to Dream Machine Pro — 49 views • Streamed 4 months ago — 1:07:25
- Zitifying nats.io followup — 16 views • Streamed 4 months ago — 2:58
- Clint Zitifies nats.io! — 70 views • Streamed 4 months ago — 34:35
- Evan shows off his project based around OpenZiti! — 22 views • Streamed 4 months ago — 11:15
- Part 2: Contributing to Ziti for Go Beginners (conclusion) — 24 views • Streamed 5 months ago — 58:12
- Contributing to Ziti for Go Beginners — 84 views • Streamed 5 months ago — 1:01:49

- Benefits of Ziti used with spire
    - Privacy of the ziti network overlay
    - Lacks of ports
    - Portability (outbound internet)
- Edge routers are the nodes that have the open ports. These are mTLS authenticated.

Zitifying Nats


youtube.com/watch?v=8V_HIDZy6M8&t=107s
YouTube
Search
All
Live
Watched
TypeScript tips and Tricks with Matt
Ziti TV 6th May
Apr 29 - More HA Services (Part 2)
Pianist SHOCKS Audience With Moonlight Sonata Dubstep...
OpenZiti Superpower - Server to Client
Cloud Native Live: Protecting Software Supply Chains using...
Python for Data Science Zero to Hero | Day 1 | LetsUpgrade
Node.js in AWS 2022 Q2 Kick Off
0:00 / 34:34
10
DISLIKE
SHARE
DOWNLOAD
SAVE
ANALYTICS
EDIT VIDEO
Mute
Start Video
Security
Participants
Polls
Chat
Share Screen
Raise Hand
Pause/Stop Recording
Closed Caption
Apps
More
End

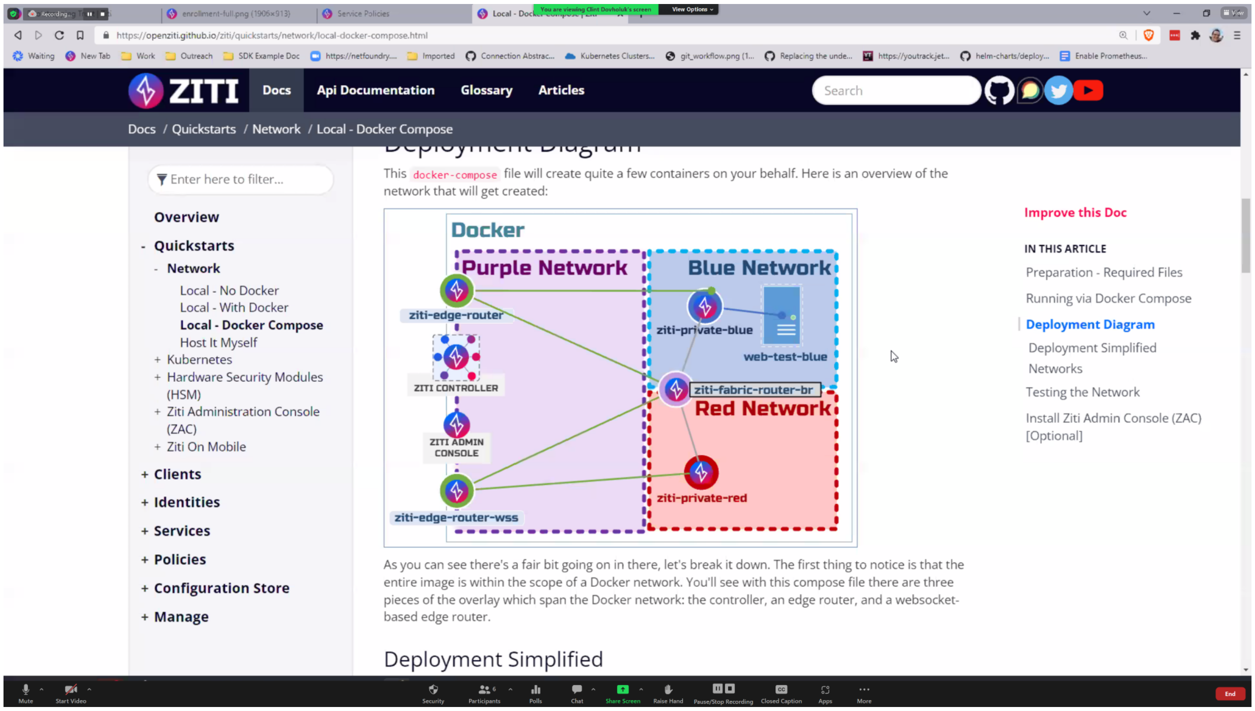
Clint Zitifies nats.io!

70 views • Streamed live on Dec 17, 2021

OpenZiti
97 subscribers

UPDATE:
zitified nats fork/branch: https://github.com/openziti-incubator...
zitified examples: https://github.com/openziti-incubator...

All communication go through the Edge Router. Clients connect to the edge routers that talk the fastest. The Edge router gets you to the Ziti network fabric. Can have a fabric of one edge router if needed.

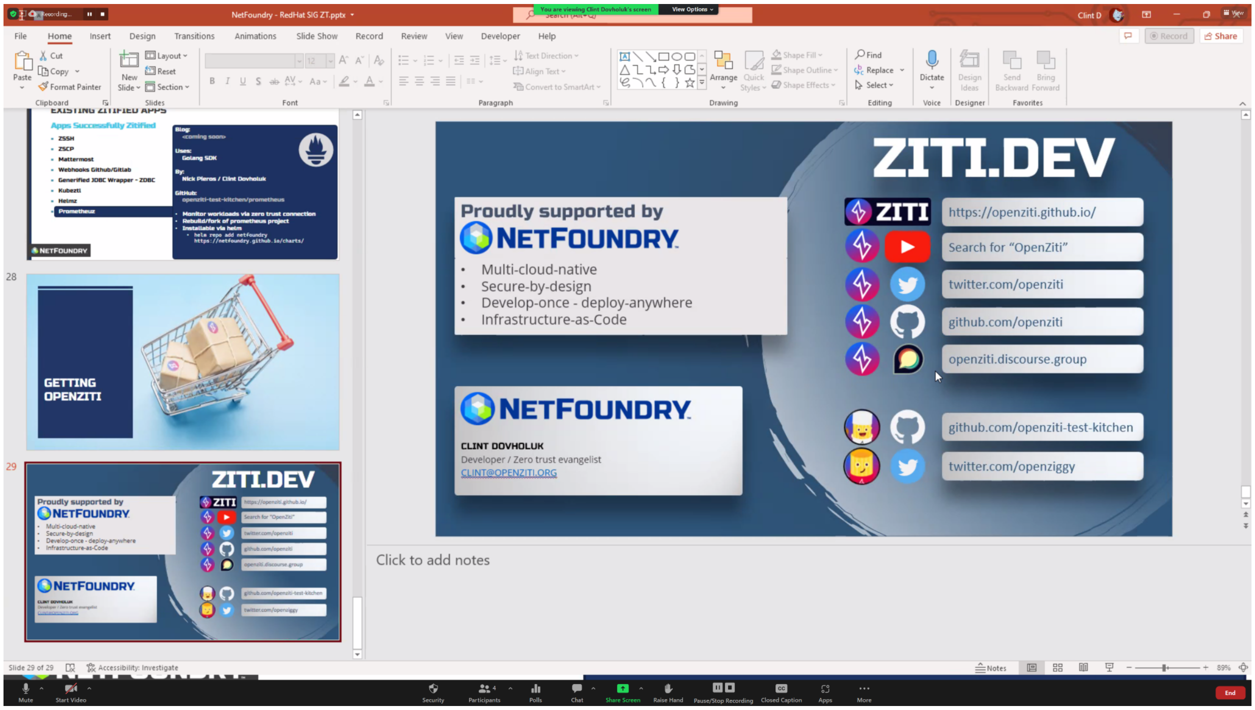


Deployment Diagram

This `docker-compose` file will create quite a few containers on your behalf. Here is an overview of the network that will get created:

As you can see there's a fair bit going on in there, let's break it down. The first thing to notice is that the entire image is within the scope of a Docker network. You'll see with this compose file there are three pieces of the overlay which span the Docker network: the controller, an edge router, and a websocket-based edge router.

Deployment Simplified



EXISTING ZITIFIED APPS

Apps Successfully Zitified

- ZSSH
- ZSCP
- Mattermost
- Webhooks Github/Gitlab
- Generified JDBC Wrapper - ZDBC
- Kubeztl
- Helmz
- Prometheuz

Blog:
<coming soon>

Uses:
Golang SDK

By:
Nick Pieros / Clint Dovholuk

GitHub:
openziti-test-kitchen/prometheus

- Monitor workloads via zero trust connection
- Rebuild/fork of prometheus project
- Installable via helm
  - helm repo add netfoundry https://netfoundry.github.io/charts/

NETFOUNDRY

28

GETTING OPENZITI

29

ZITI.DEV

Proudly supported by NETFOUNDRY

- Multi-cloud-native
- Secure-by-design
- Develop-once - deploy-anywhere
- Infrastructure-as-Code

ZITI https://openziti.github.io/

Search for "OpenZiti"

twitter.com/openziti

github.com/openziti

openziti.discourse.group

github.com/openziti-test-kitchen

twitter.com/openziggy

NETFOUNDRY

CLINT DOVHOLUK
Developer / Zero trust evangelist
CLINT@OPENZITI.ORG

Click to add notes

Have had a conversation about Nats.io potentially adopting openziti.

Standing Agenda

- Review Security Board
- Securing Consul Board (skip)
- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
  - Last checked: Tue Nov 16 05:36:01 UTC 2021
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
- Review action items from previous week

Action Items

- 7/14/21: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.