
cisco Live!
ALL IN

The bridge to possible

Serverless isn't Secureless

How to Secure Serverless Functions

Ran Ilany, ET&I
@ranilany
PSOETI-2100

Cisco Webex App

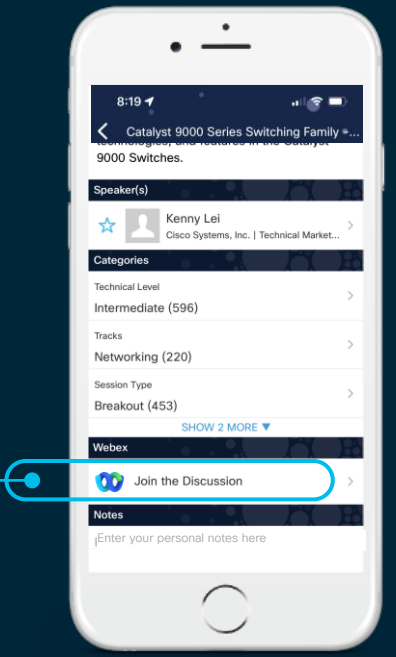
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#PSOETI-2100

A-bit-about-me

Ran Ilany

Director Eng. ET&I at Cisco

Co-Founder, CEO Portshift (Cisco acquired)

Head Security I/S, Check Point

Founder, CEO, BladeFusion (ISS/IBM)

VP R&D, MainControl (IBM)

Cloud Native Security Platforms

Containers, k8, Serverless, API, Service Mesh

Head of Cisco ET&I Israel

We are hiring!

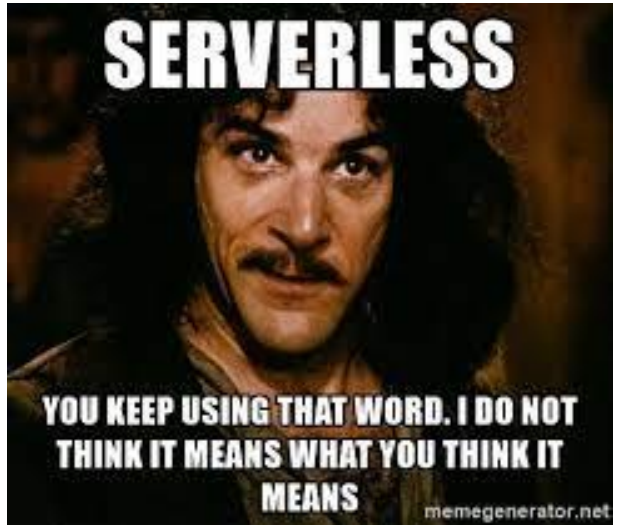
Agenda

- What is Serverless
- The Attack Surface
- Security Model: Shared Responsibility
- Standards on Serverless Security
- Cisco’s solution: Panoptica
- Demo
- Conclusion

What Are Serverless Applications?

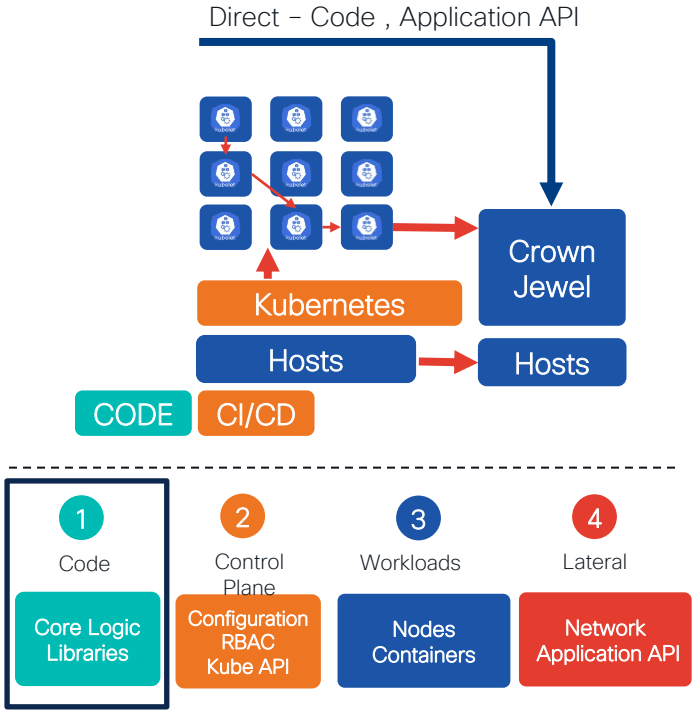
- A cloud-native development model that allows developers to build and run applications without having to manage servers
  - There are still servers in serverless but they are abstracted away from app development

- Motivations:
  - Eliminate infrastructure complexities
  - Cost saving: pay-per-use billing model
  - Yes, better security



Serverless Application: The Attacker Perspective

- Serverless Apps are more secure by default
  - No access to the host/OS or the filesystem
  - No persistency (ephemeral execution)
  - Classical/known attacks are not applicable
- The only attack vector is the App Libraries/logic
  - Flaws in the application code or dependencies
- Traditional security tools(WAF, FW etc) can't protect serverless functions



Serverless: Where Things Can Go Wrong?

- Application code
  - Vulnerable library code
  - Vulnerable logic
    e.g. SQL Injection, Crypto mining (e.g. April 22 CATO Labs)
- Cloud serverless configuration
  - Permissions: Least-Privileged
  - Secrets/Access credentials
  - Authentication and Authorization

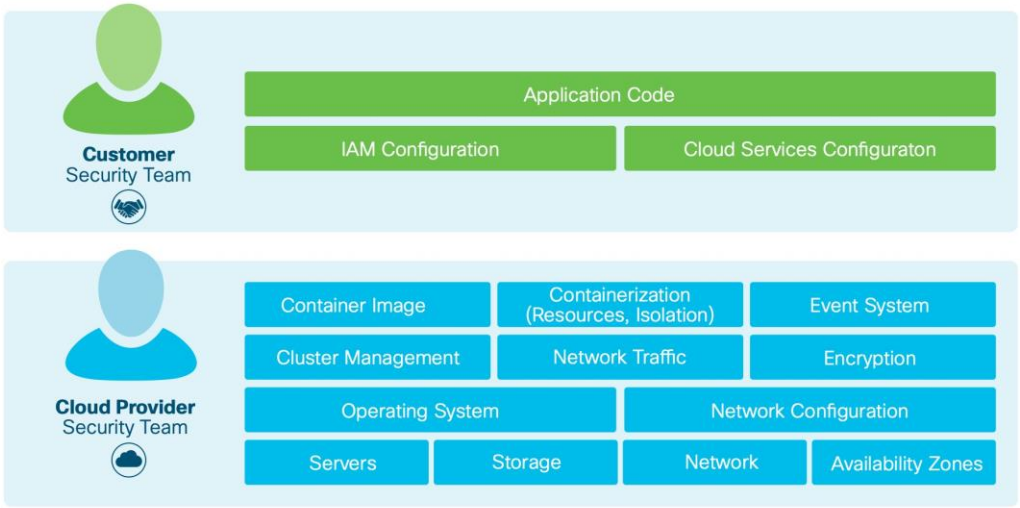
Serverless: It’s A Shared Responsibility

The Shared Responsibility Model

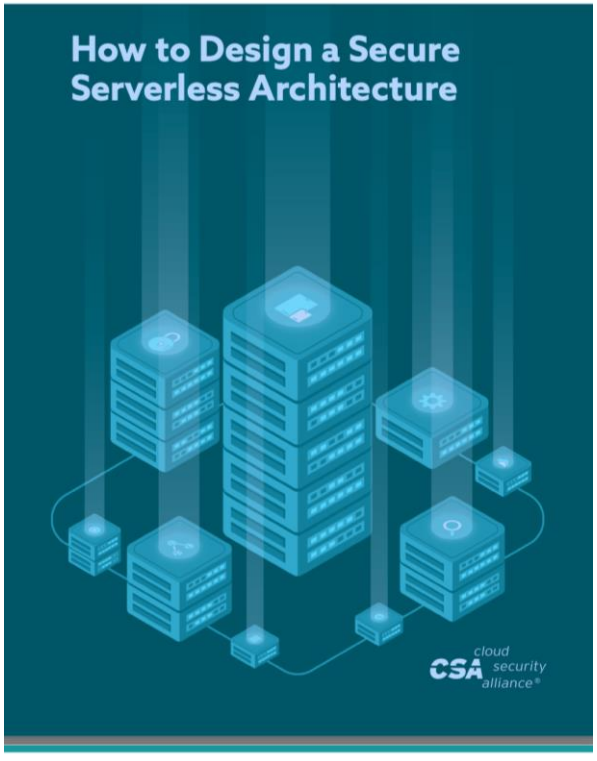
Security in the Cloud is a shared responsibility model

- Users
- Cloud Providers

Serverless leaves the App code and configurations to the user



Serverless Security Guidelines



CLOUD NATIVE COMPUTING FOUNDATION

CNCF WG-Serverless Whitepaper

Abstract

This paper describes a new model of cloud native computing enabled by emerging "serverless" architectures and their supporting platforms. It defines what server-less computing is, highlights use cases and successful examples of serverless computing, and shows how serverless computing differs from (and interrelates with) other cloud application development models such as Infra-structure-as-a- Service (IaaS), Platform-as-a-Service (PaaS), and container orchestration or Containers-as-a-Service (CaaS).

This paper, published by the CNCF Serverless Working Group, includes a logical description of the mechanics of a generic serverless platform with an associat-ed programming model and message format, but it does not prescribe a standard. It introduces several industry serverless platforms and their capabili-ties, but it does not recommend a particular implementation.

The CNCF Serverless Working Group is a forum for the CNCF community to explore the intersection of cloud native and serverless technology. The working group focuses on defining common terminology, scope of serverless as it relates to cloud native technology. This includes identifying common use cases and patterns with existing serverless implementations and analyzing the role of serverless relative to container orchestration. Their work will summarize potential next steps for the community and/or CNCF, outlining areas for possible harmonization, candidate projects and interoperability work.

To get involved in CNCF's work to advance serverless computing, join the CNCF Serverless Working Group or the community project CloudEvents, a draft specification for a common, vendor-neutral format for event data that is aimed to be proposed to the CNCF TOC as an official project later this year.

WG Chair/TOC Sponsor: Ken Owens (Mastercard)

WG Members (alphabetical by last name):
Sarah Allen (Google), Ben Browning (Red Hat), Lee Calcote (SolarWinds), Amir Chaudhry (Docker), Doug Davis (IBM), Louis Fourie (Huawei), Antonio Gulli (Goo-gle), Yaron Haviv (iguazio), Daniel Krook (IBM), Orit Nissan-Messing (iguazio), Chris Munns (AWS), Ken Owens (Mastercard), Mark Peek (VMWare), Cathy Zhang (Huawei), Chris A.

Additional Contributors (alphabetical by last name):

ABOUT CNCF

The Cloud Native Computing Foundation (CNCF) hosts critical projects of cloud native software stacks, including Kubernetes® and Prometheus™. CNCF provides a neutral home for collaboration, bringing together the industry's top developers, end users and vendors, including the world's largest public cloud providers.

Cloud native computing uses an open source software stack to orchestrate containerized services on any public, private or hybrid cloud. CNCF is part of The Linux Foundation, a nonprofit organization. For more

Panoptica:
Cisco's Secure Application Cloud

Panoptica
Cisco's Secure Application Cloud

- A SaaS solution providing cloud native security
- Seamless deployment with cloud accounts
- Serverless functions security risks:
  - Vulnerable code (SBOM)
  - Code integrity degradation
  - Exposed Secrets
  - Overly permissive permissions
  - Public exposure
  - Data Exphiltration options

Demo

Avoiding the “Garbage in garbage out” effect
- Thousands of functions
- Multi cloud accounts
- Abuse of user credentials
- Clones of credentials

Guidelines
- Code should never leave its original site
- Scheduled and auto event driven analysis
- Enforcement
- Multi accounts (Root account, Terraform provider)

Conclusion

- Serverless applications has a different security posture
- It requires dedicated security tools that addresses their ephemeral nature
- Cisco's Panoptica is a cloud native serverless security solution that addresses these security needs

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you


cisco Live!
ALL IN