The bridge to possible

Data Security and Compliance in Cloud Native and On-prem Applications

Peter Bosch, Distinguished Engineer

Cisco Webex App

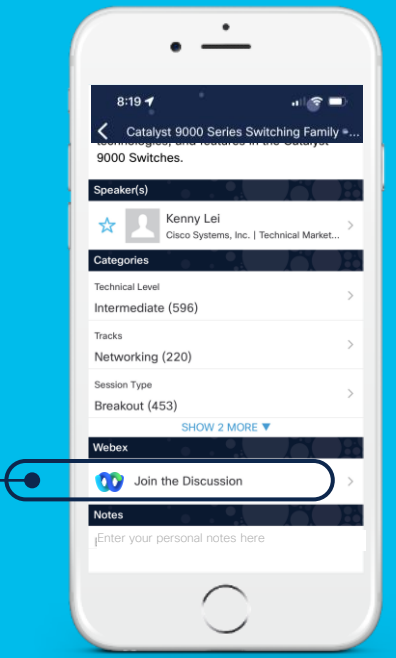
Questions?

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 until February 24, 2023.



Apps are being used to solve your customer's problems

Increasingly, software assets for apps come from everywhere, run anywhere, and are being accessed from anyplace

Yet you are responsible for their scale, performance, security, and trust

How do you keep those apps secure?

Contact Us Login

Panoptica
Cloud-Native Application Security, Simplified

Get Started Features Resources Pricing Get Panoptica Free

Simplified Cloud-Native Application Security for DevSecOps, Platform, and DevOps teams

Panoptica makes it easy to secure your containers, APIs, and serverless functions, and manage software bills of materials.

Try a Point and Click Demo

Find, track and classify data;
Secure it and make your business compliant

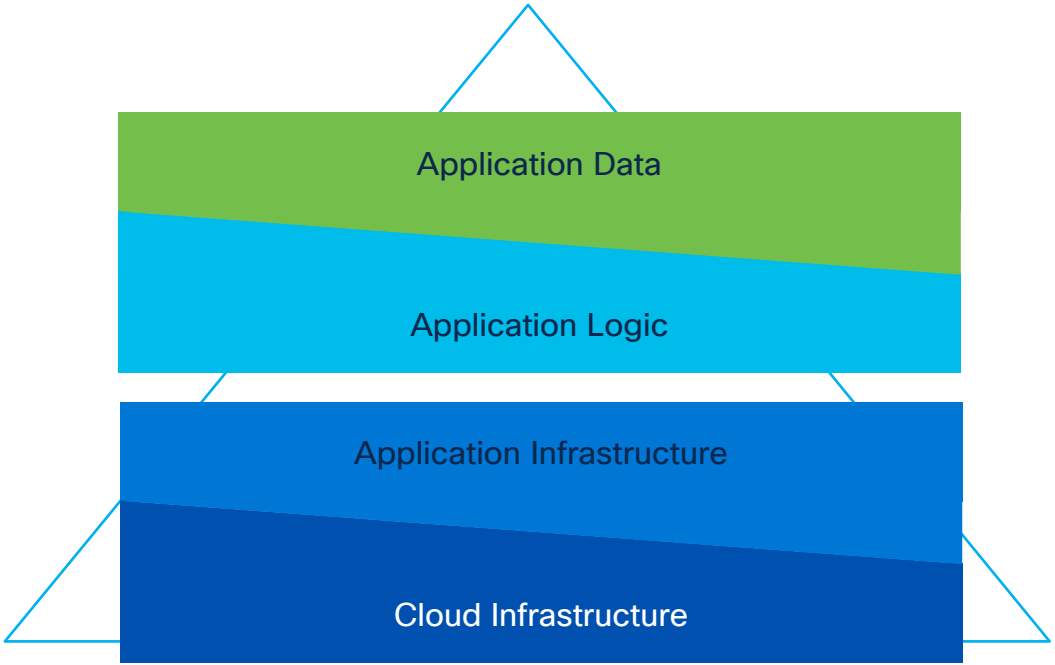
Application security at its core

Protect the processor Make sure nobody steals it

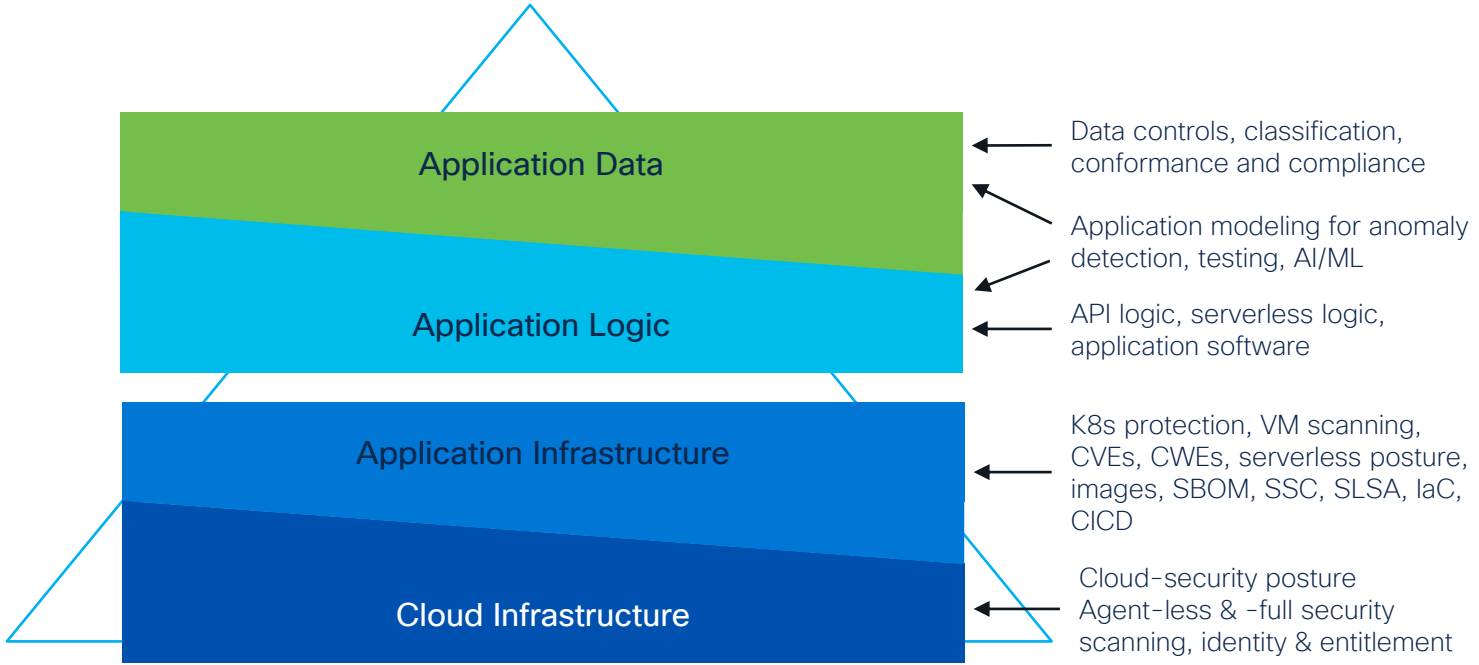
Protect the application Make sure nobody denies its use

Protect data Make sure nobody copies, leaks or encrypts it

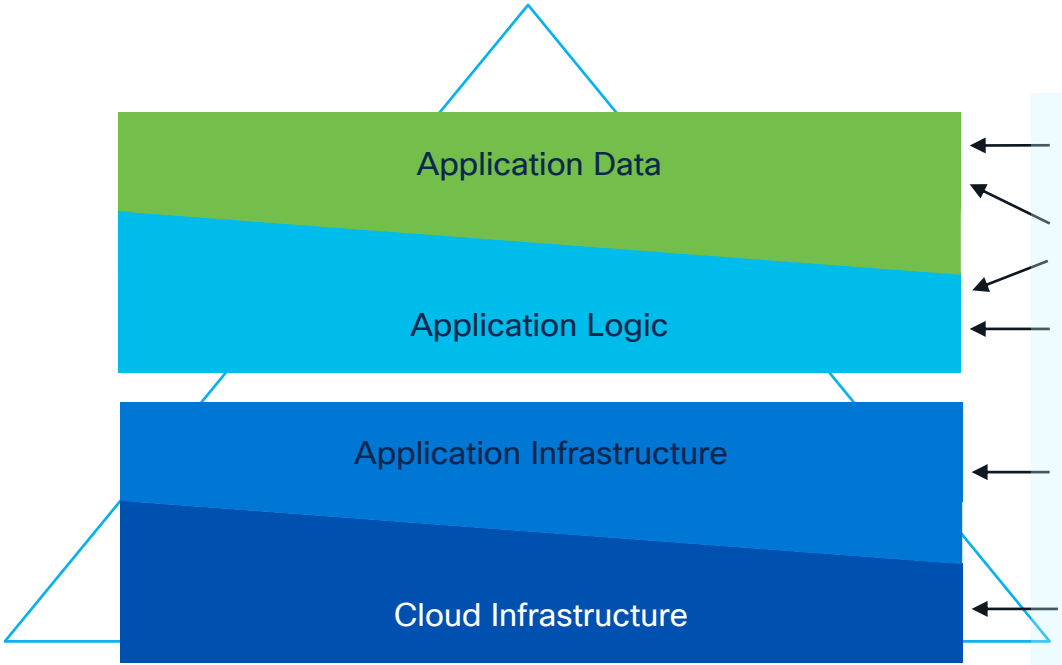
Pyramid of necessities for application security



Pyramid of necessities for application security

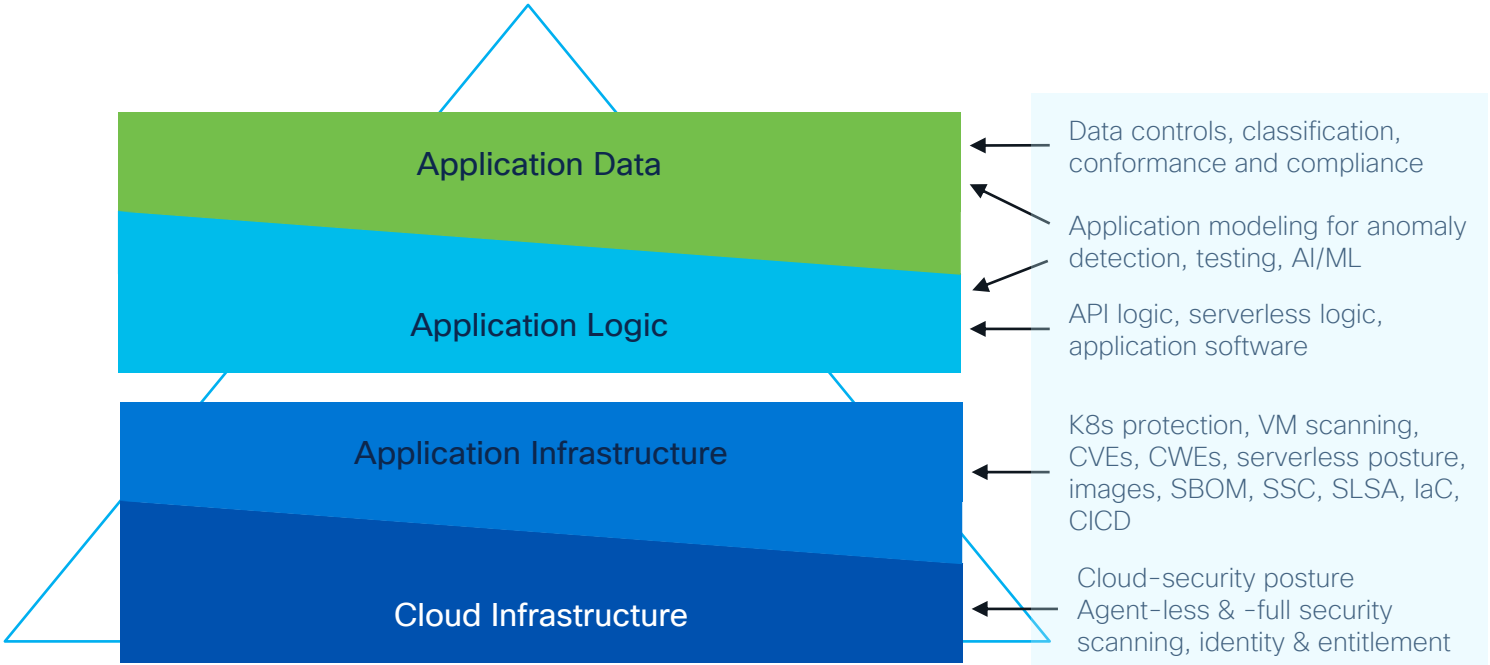


Pyramid of necessities for application security



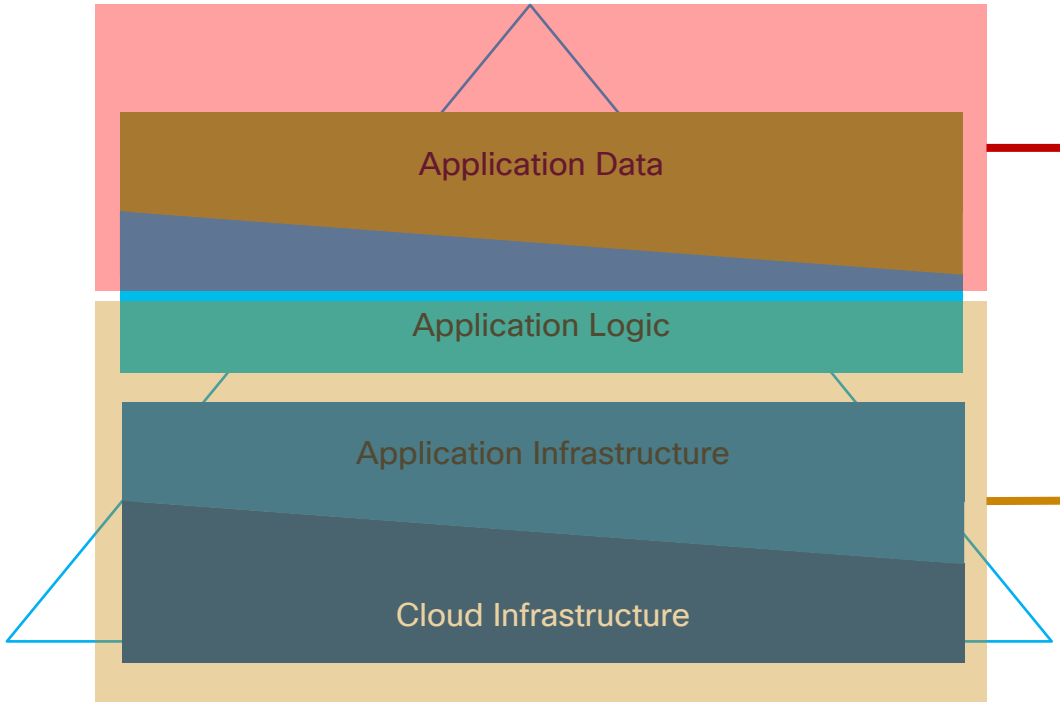
A snap-on-truck lot of tooling!

Pyramid of necessities for application security

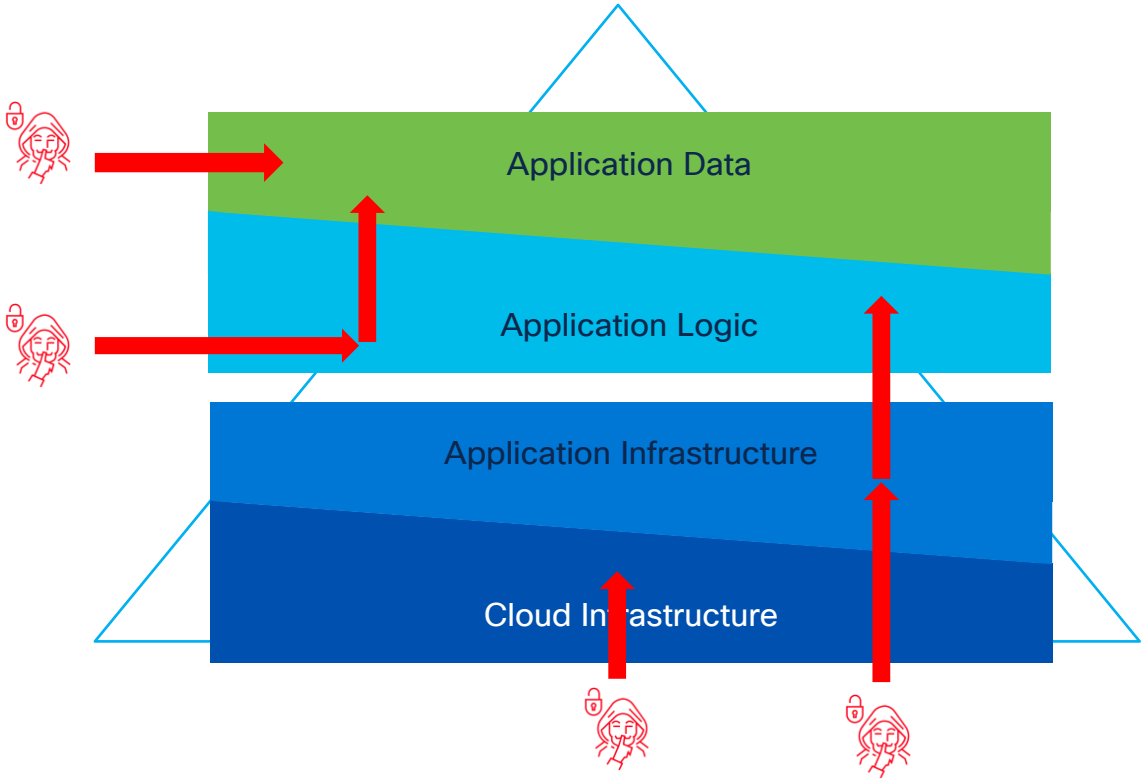


Tooling is important – but showing where assets are at risk even more so!

Value from an attacker standpoint …

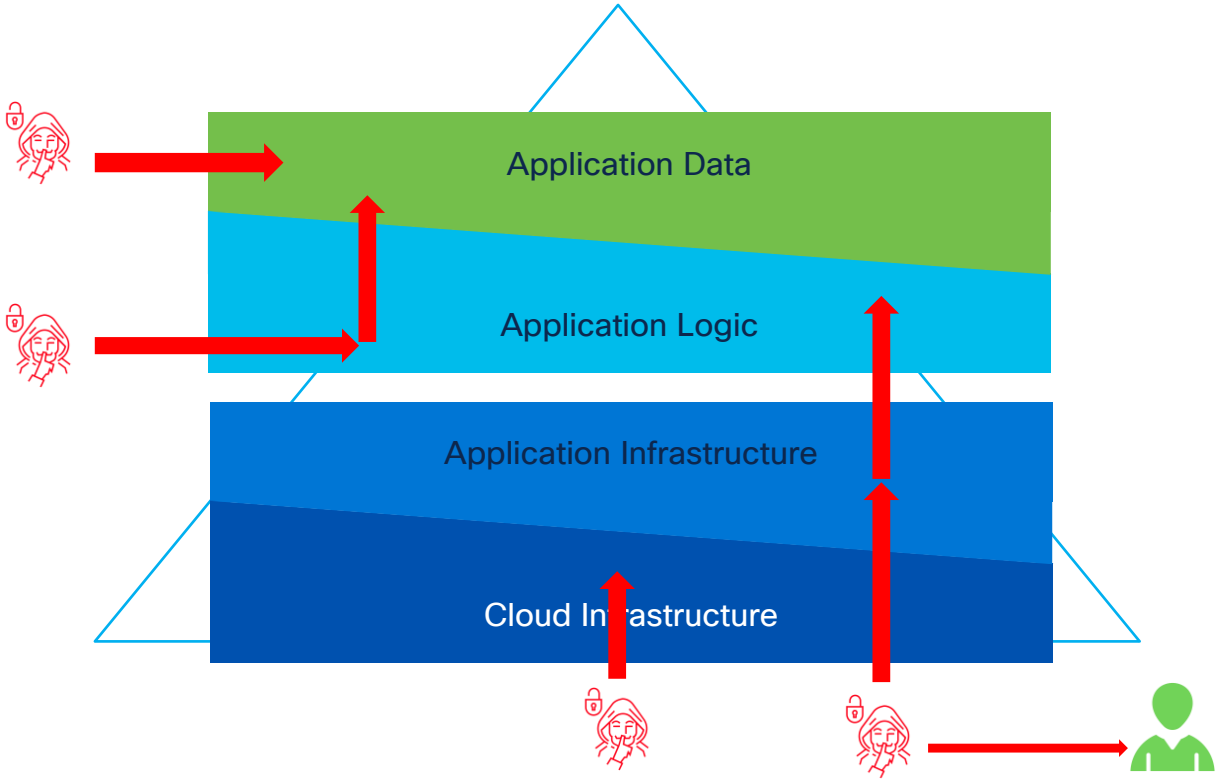


Pyramid of necessities for application security



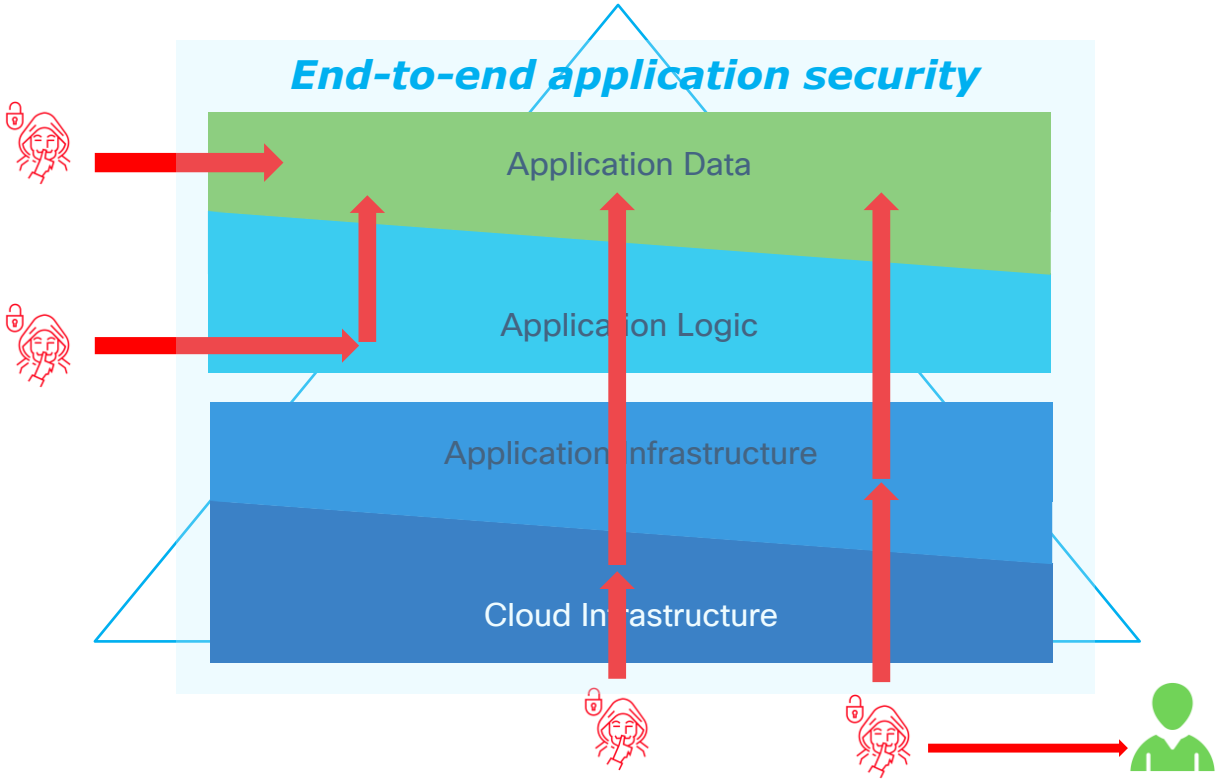
What methods do hackers have to get to critical assets?

Pyramid of necessities for application security



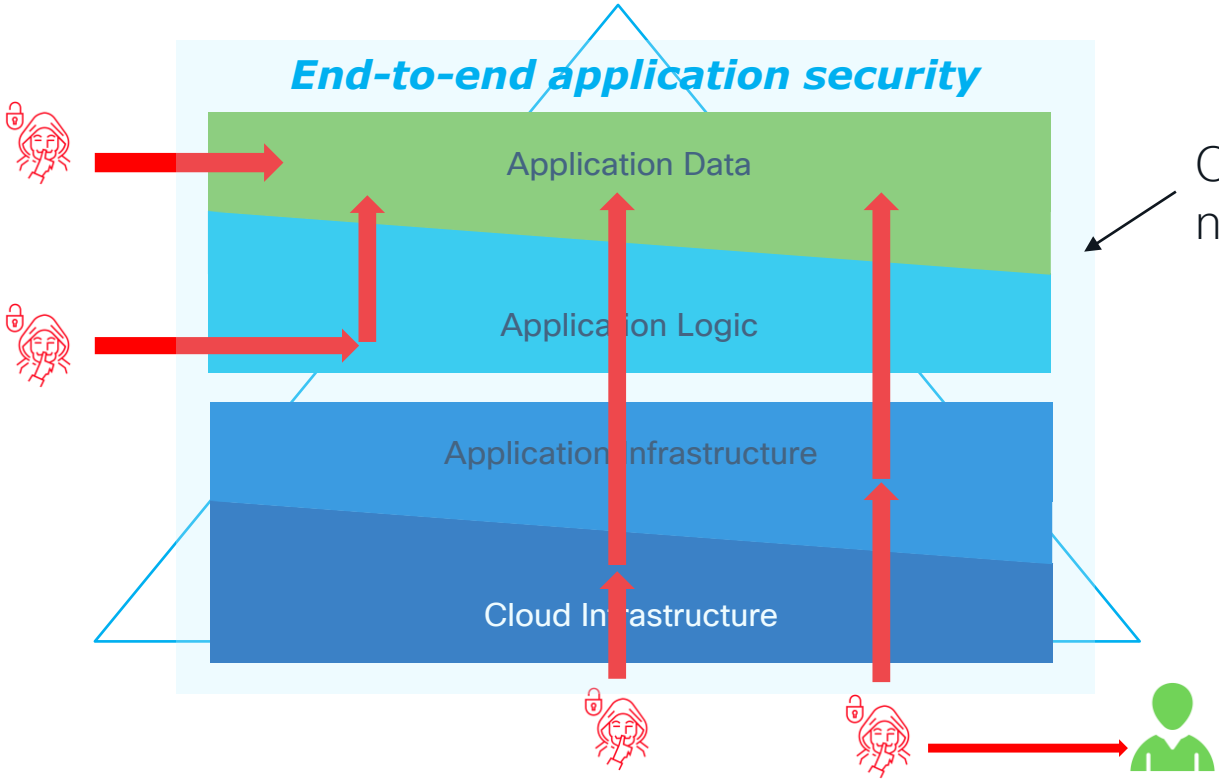
What methods do hackers have to get to critical assets?

Pyramid of necessities for application security



What methods do hackers have to get to critical assets?

Pyramid of necessities for application security



What methods do hackers have to get to critical assets?

Definitions of attacks and position

attack vector

An attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.

attack surface

An attack surface is the set of entry points for unauthorized access into any system. It includes all vulnerabilities and endpoints that can be exploited to carry out a security attack.

attack path

An attack path is a visualization of the chain of events that occurs when attack vectors are exploited.

attack flow

Attack flow is a data model with supporting tooling and examples for describing sequences of adversary behaviors.

Enterprises need to know the potential attack flows through their apps! Knowing attacks paths enables protecting against them!

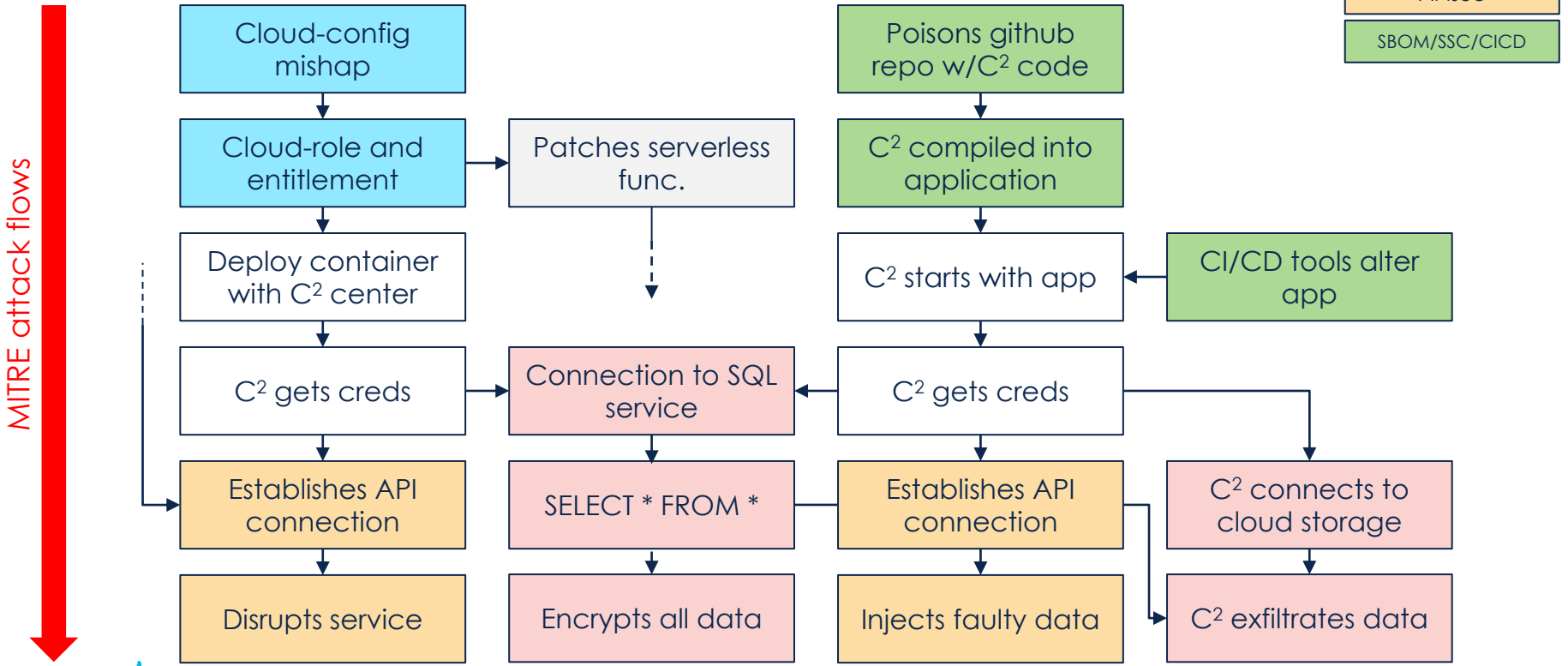
Attack flow analysis today …

Focuses primarily on cloud security (client credentials, poor application config, poor API tokens for resources)

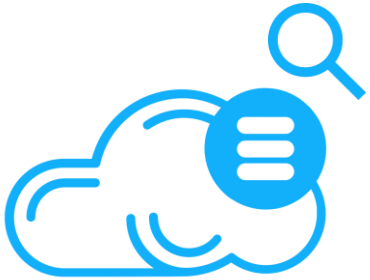
Attack flow analysis (often) does not include workload-, CI/CD-, API-, serverless-, and SBOM/SSC based attack vectors

Attack flow analyses (often) do not visualize per asset protected (CPU, application and data)

Attack vectors, surfaces and paths



Four phases for attack paths and applications



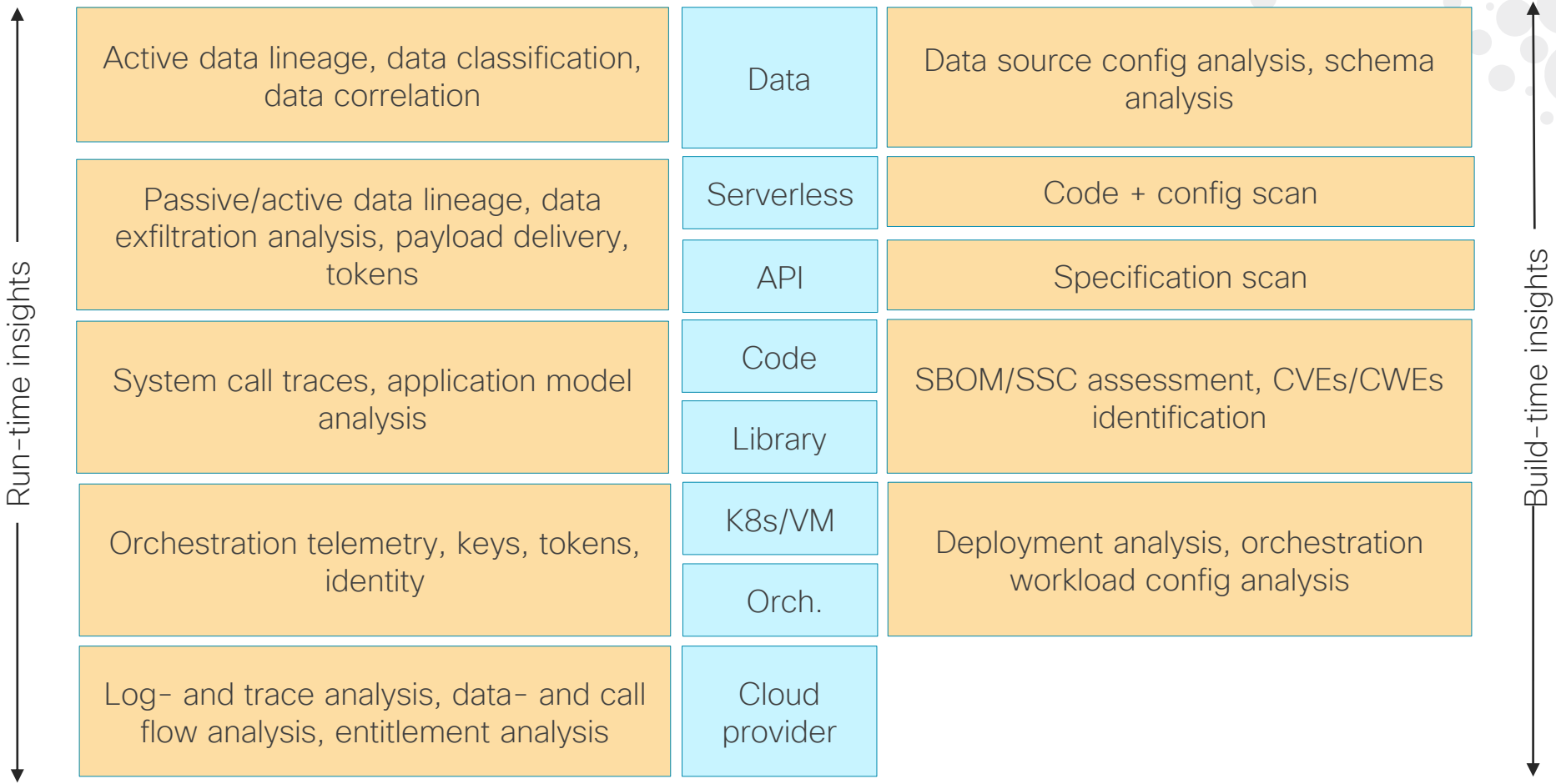
Find and analyze data

Find and analyze the app topology

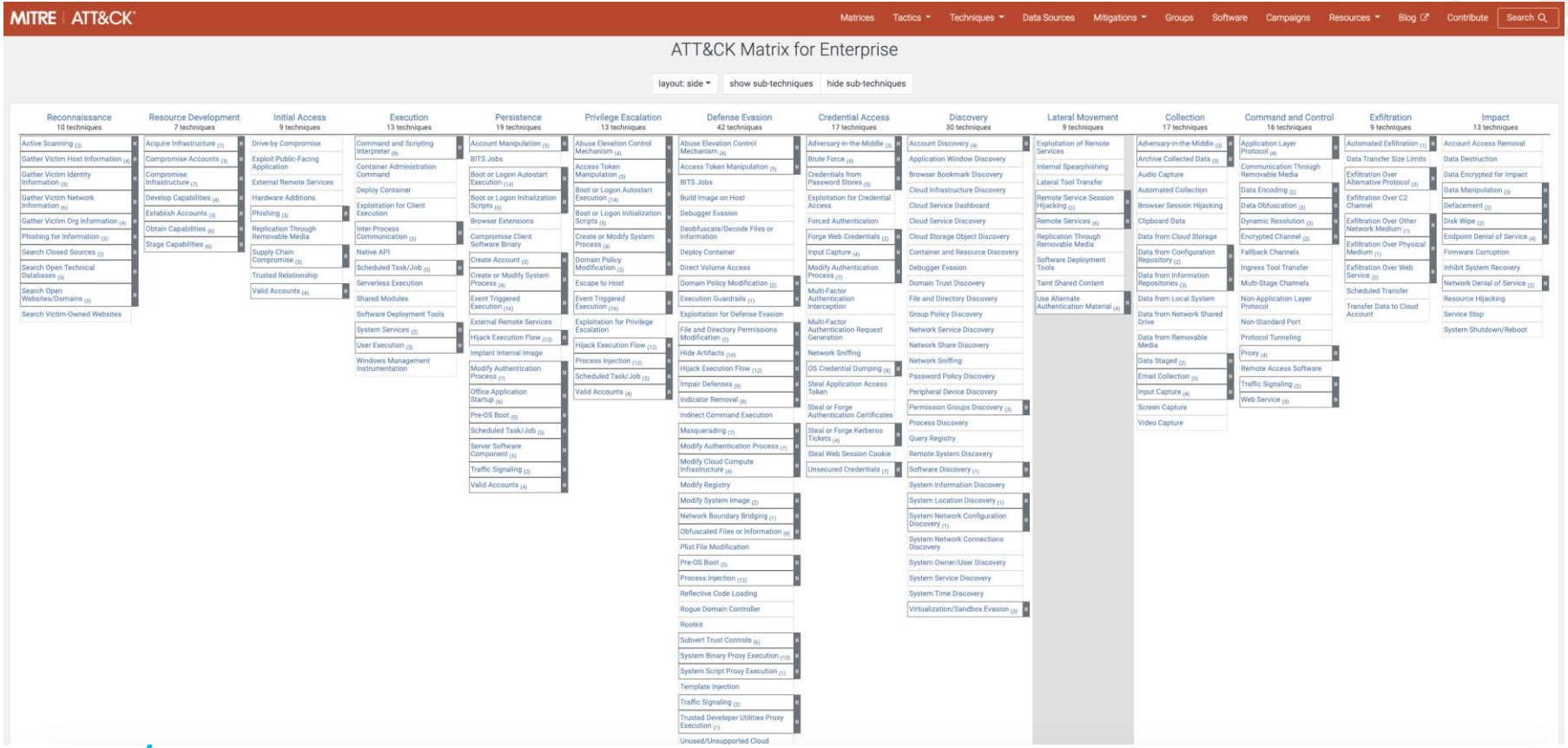
Find potential attack vectors and flows

Remediate the application

Data and application topology



Attack vectors, paths and flows



Attack vectors, paths and flows

MITRE ATT&CK

OWASP, OWASP API, OWASP Serverless, OWASP CICD, etc…

Center for Internet Security findings

Cisco security research

Expanding on traditional attack vectors/paths with attacks flows ***across*** the stack

Panoptica

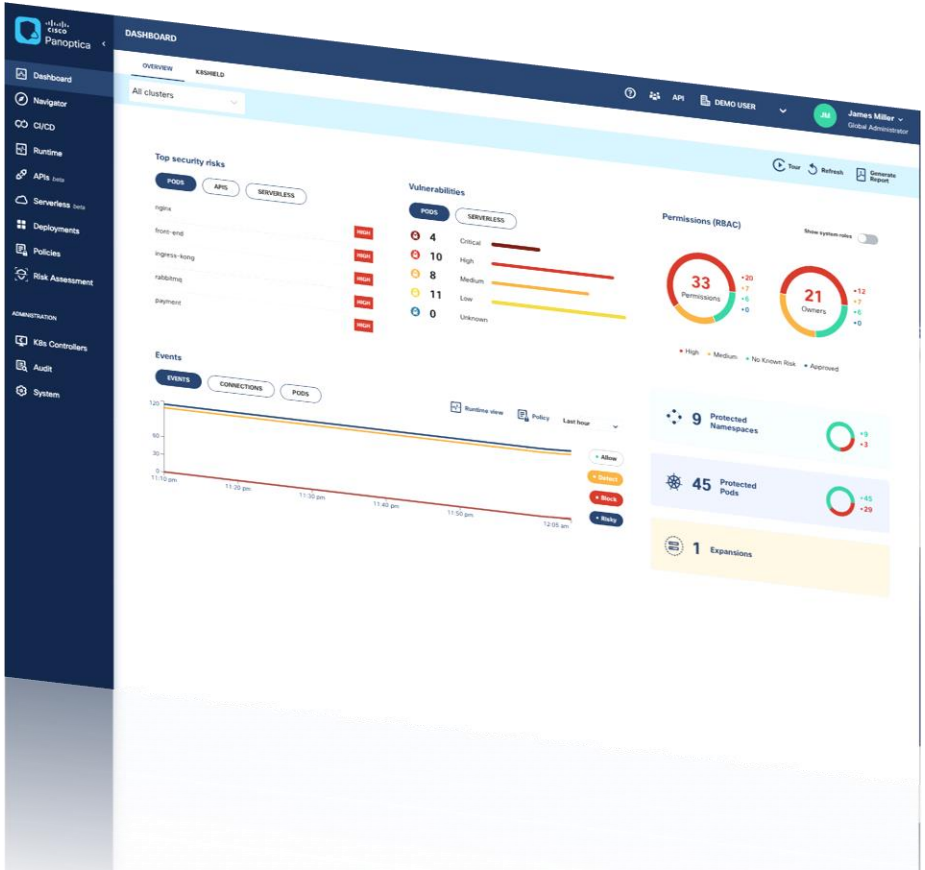
“Cloud-native application protection”

Present all artefacts of the application(s), where they come from and their vulnerabilities

Control container, virtual machines, images, SBOM, supply chain, CI/CD,

Define and enforce security policies and compliance for the enterprise

Manage the risks through a MITRE ATT&CK framework, security policies and compliance rules



cisco Live!

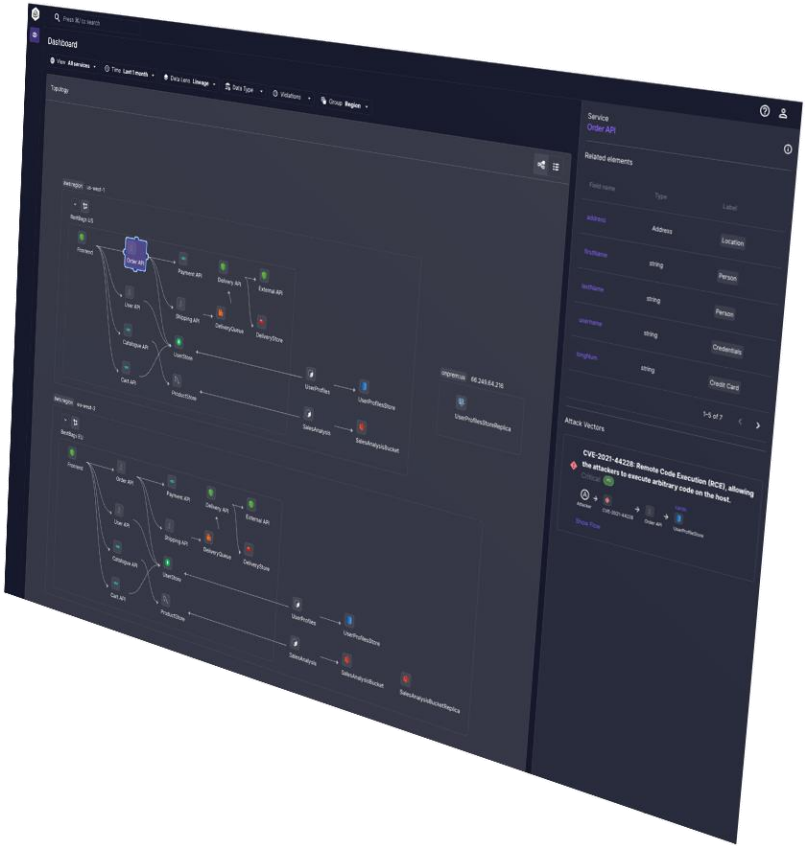
Data security

Real-time data visibility and **security analysis**

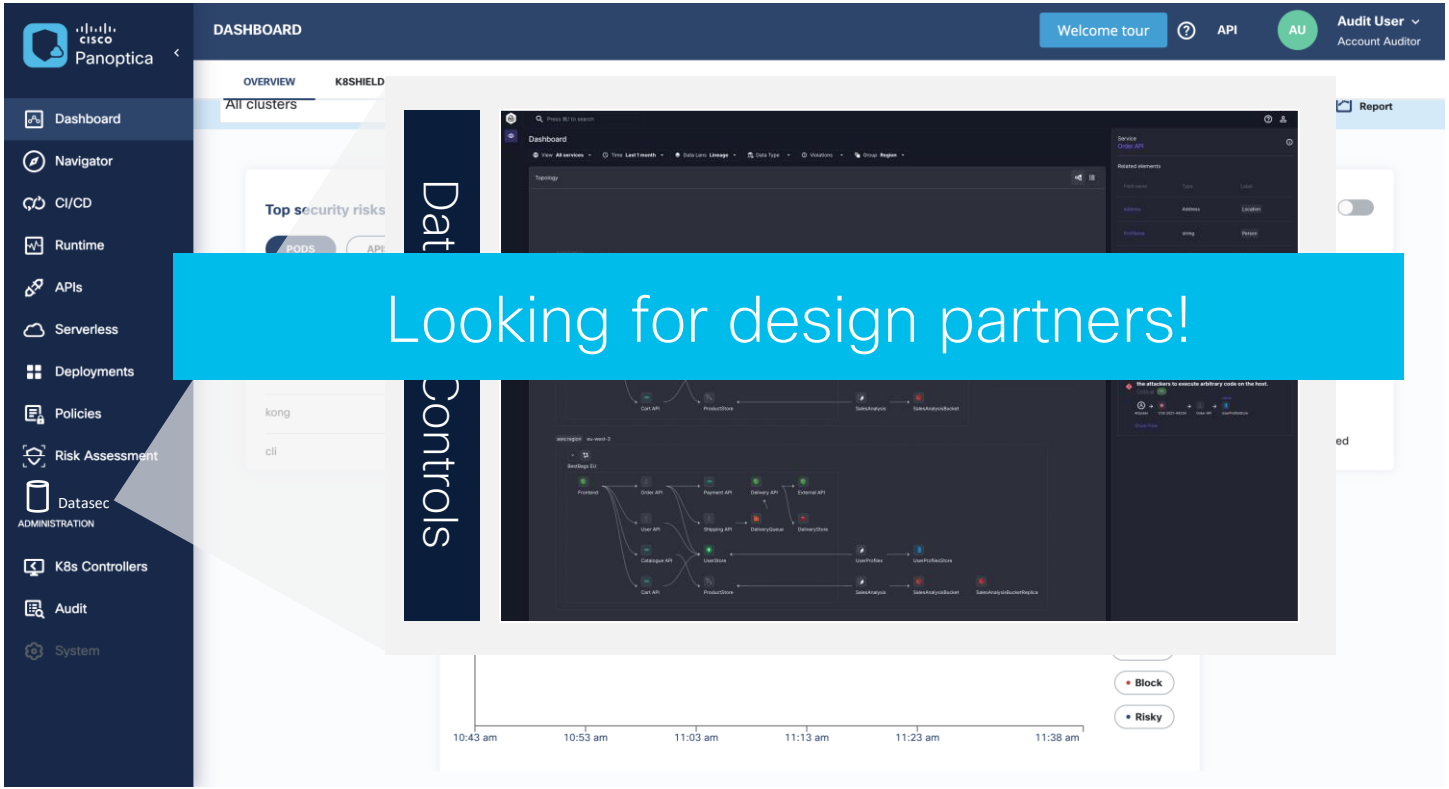
For data understand where:

- It sits, how it is used and how it moves
- Who can touch it legitimately at-rest and where it is vulnerable
- Where it sits in flight?
- Where it is most vulnerable through app/cloud attack vectors
- What it costs when you lose, leak, or have it corrupted
- How to get breaches fixed at-rest and in-flight
- Whether it is compliant with existing regulations, standards, and corporate rules

Understand all **for data at rest**, **and** **data in motion**, for apps running in cloud and on prem.



Datasec, Panoptica and remediation



Data sources and app topology
Find and list all data at-rest, and in-motion. How is the app deployed? Who can do what?

Tagging, labeling and correlation
Associate meaning to data by analyzing schemas and artefacts; cross-correlate between data

Visibility, controls & governance
Expose data: what data is available where and to whom?
Lay down rules how data is controlled and handled by policy

Security and attack flows
What is the attack surface of the application? How can data be stolen, or corrupted through attack flows?

Impact analysis of breaches
What are the costs of a breach of governed data? What needs to be protected first?

Workflows
Step-by-step recovery of leaked, corrupted or mishandled data after an attack. How can data be protected pro-actively

Demo

Try OpenClarity on GitHub

https://github.com/openclarity

Try Panoptica

https://www.panoptica.app/

Become a Cisco Design Partner

www.ciscodesignpartners.com

Check out the Cisco Tech Blogs

https://techblog.cisco.com

Call to action/continue your learning

BRKETI-2511 'Intro to Panoptica’

Panoptica is demonstrated in the Cisco Showcase in the World of Solutions all week

More information on data security can be obtained at Innovation Forum (i.e., whisper suites)

Private meetings are hosted for those customers interested in discussing Panoptica further

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

Visit the Cisco Showcase for related demos.

Book your one-on-one Meet the Engineer meeting.

Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.

Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.


cisco
The bridge to possible
Thank you
cisco Live!


CISCO Live!
ALL IN