



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?***



Panoptica

Cloud-Native Application Security, Simplified

Contact Us

Login

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





**You keep your data on the Internet!**

**Lose it and your business is in trouble**

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

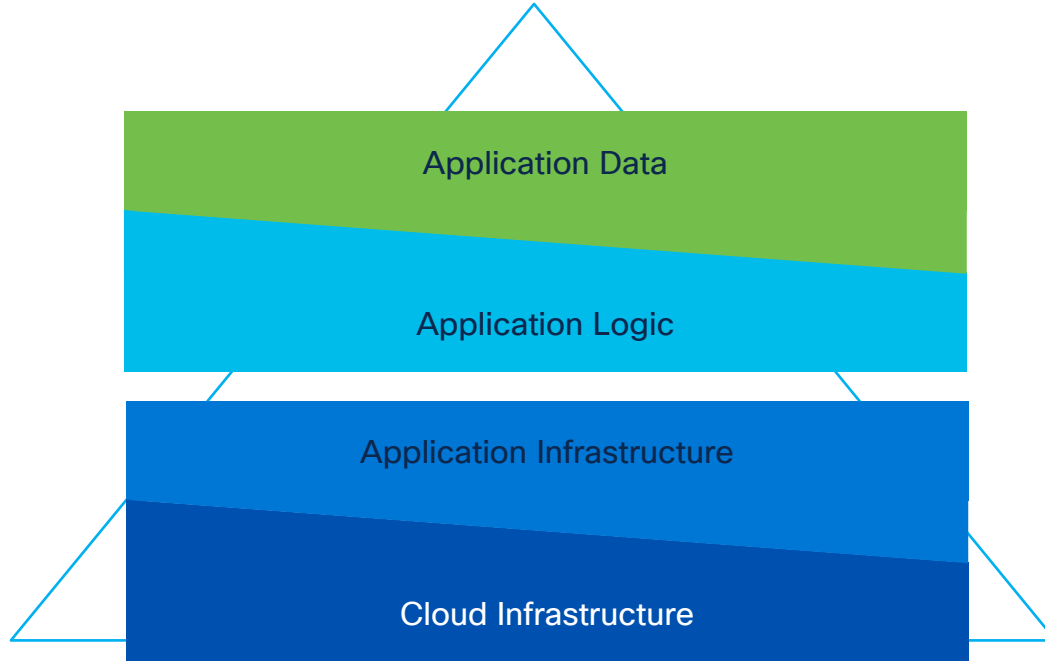
# Application security at its core

**Protect the processor** Make sure nobody steals it

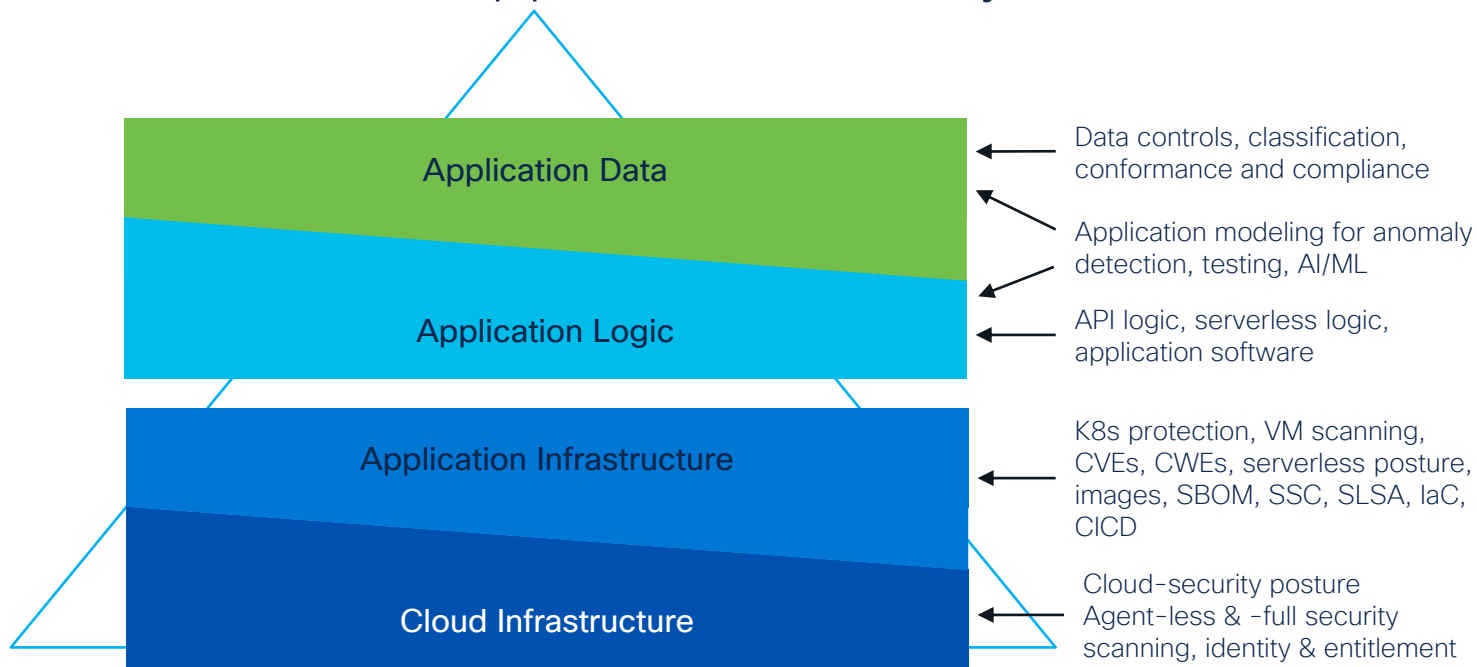
**Protect the application** Make sure nobody denies its use

**Protect data** Make sure nobody copies, leaks or encrypts it

# Pyramid of necessities for application security

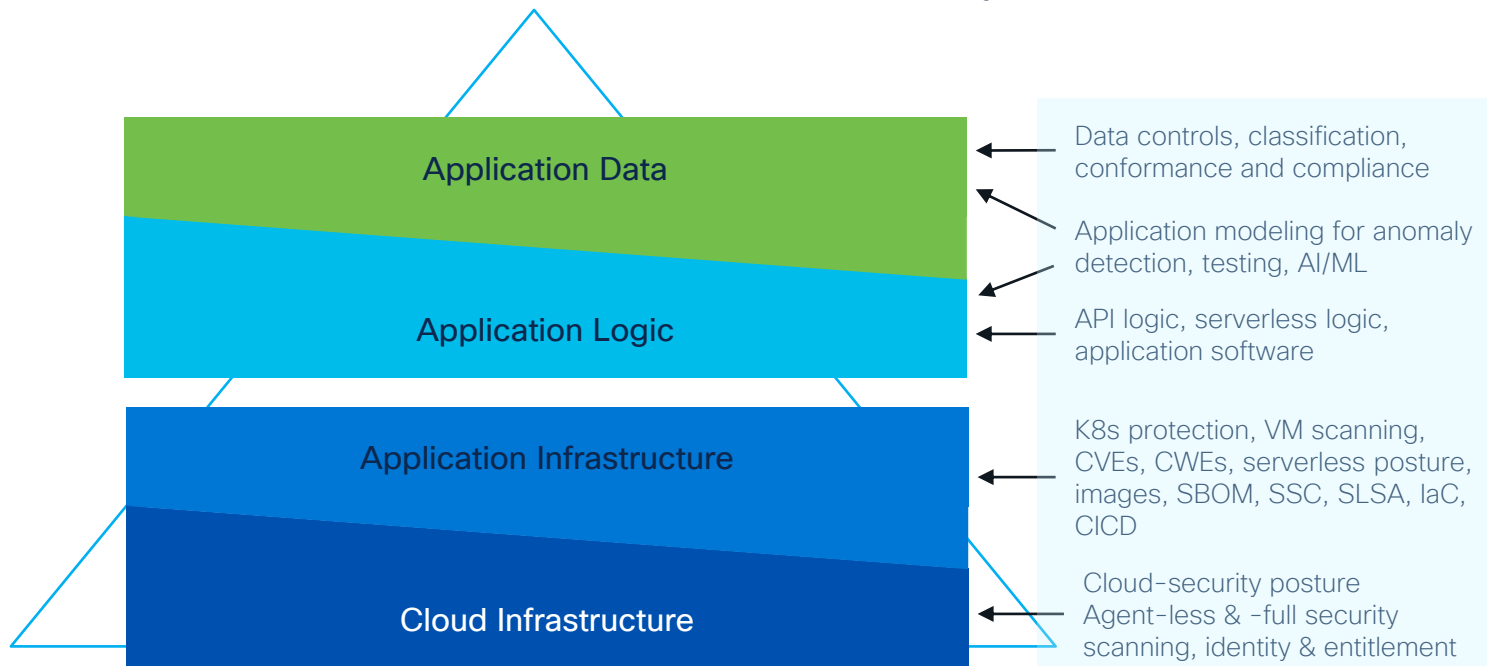


# Pyramid of necessities for application security



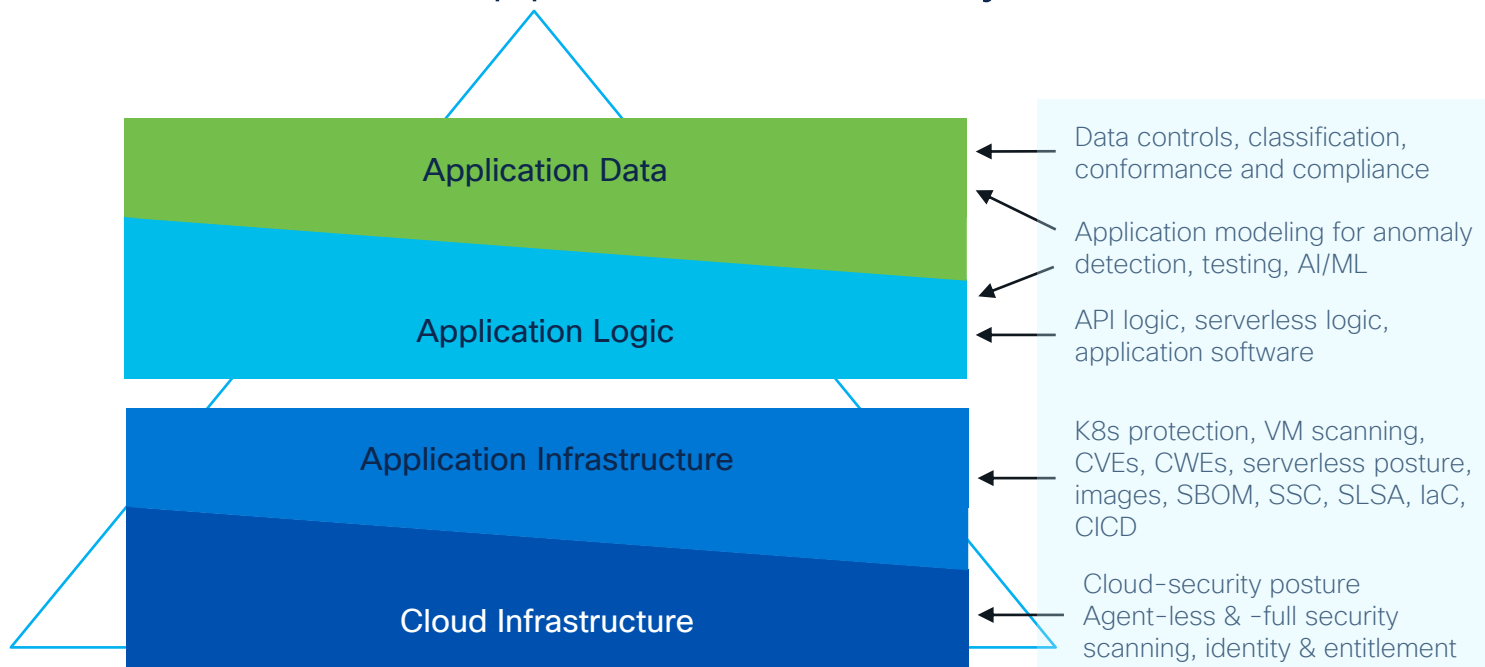


# Pyramid of necessities for application security



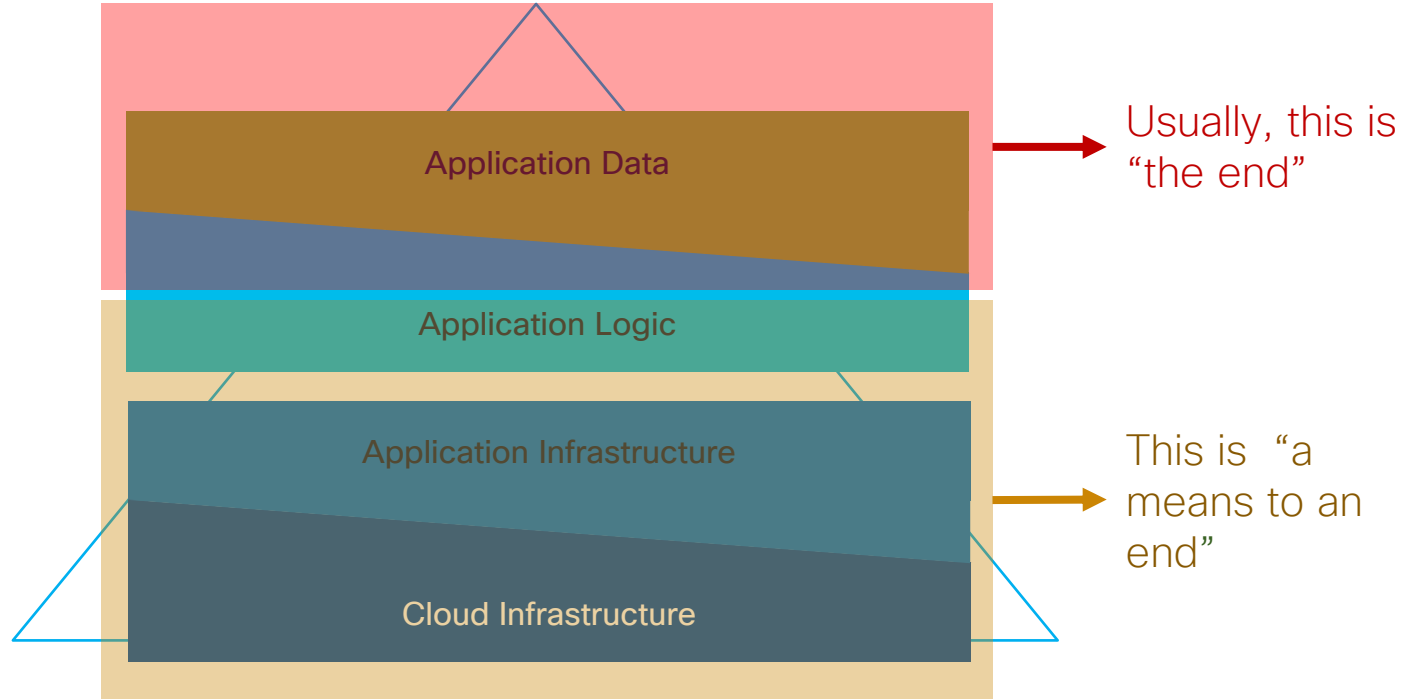
↑  
A snap-on-truck  
lot of tooling!

# Pyramid of necessities for application security

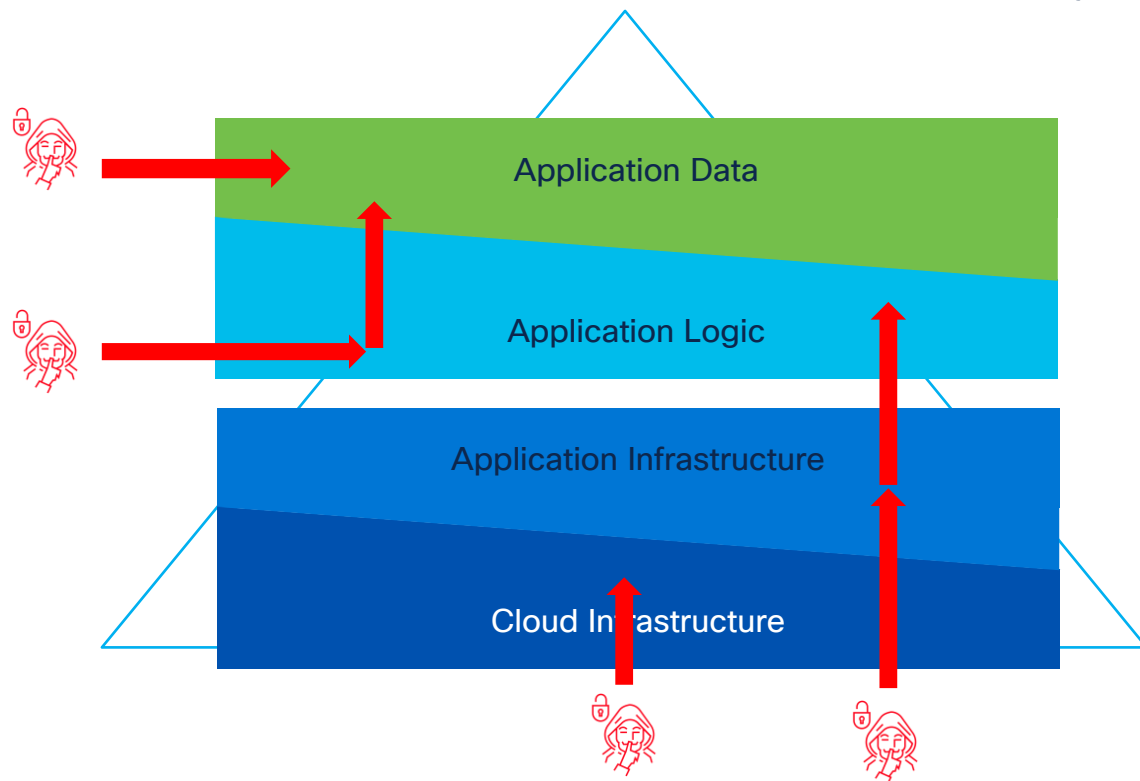


Tooling is important – but showing where assets are at risk even more so!

# Value from an attacker standpoint ...

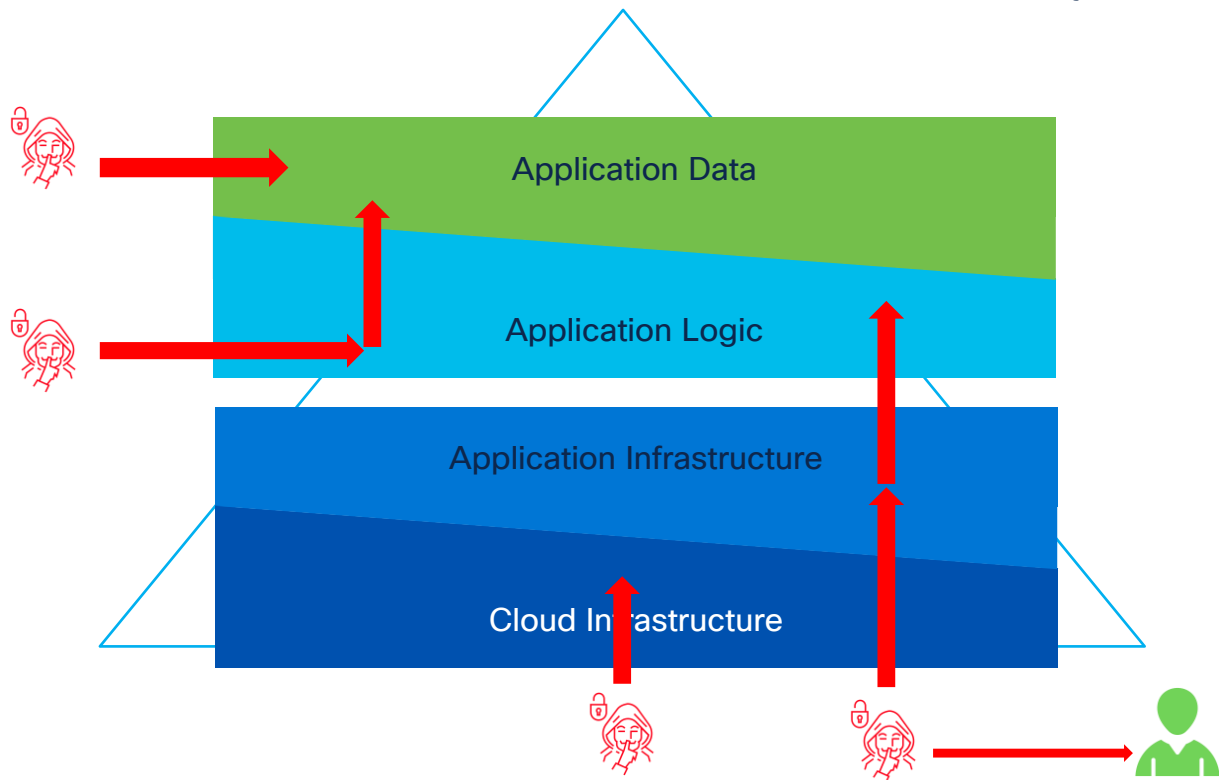


# Pyramid of necessities for application security



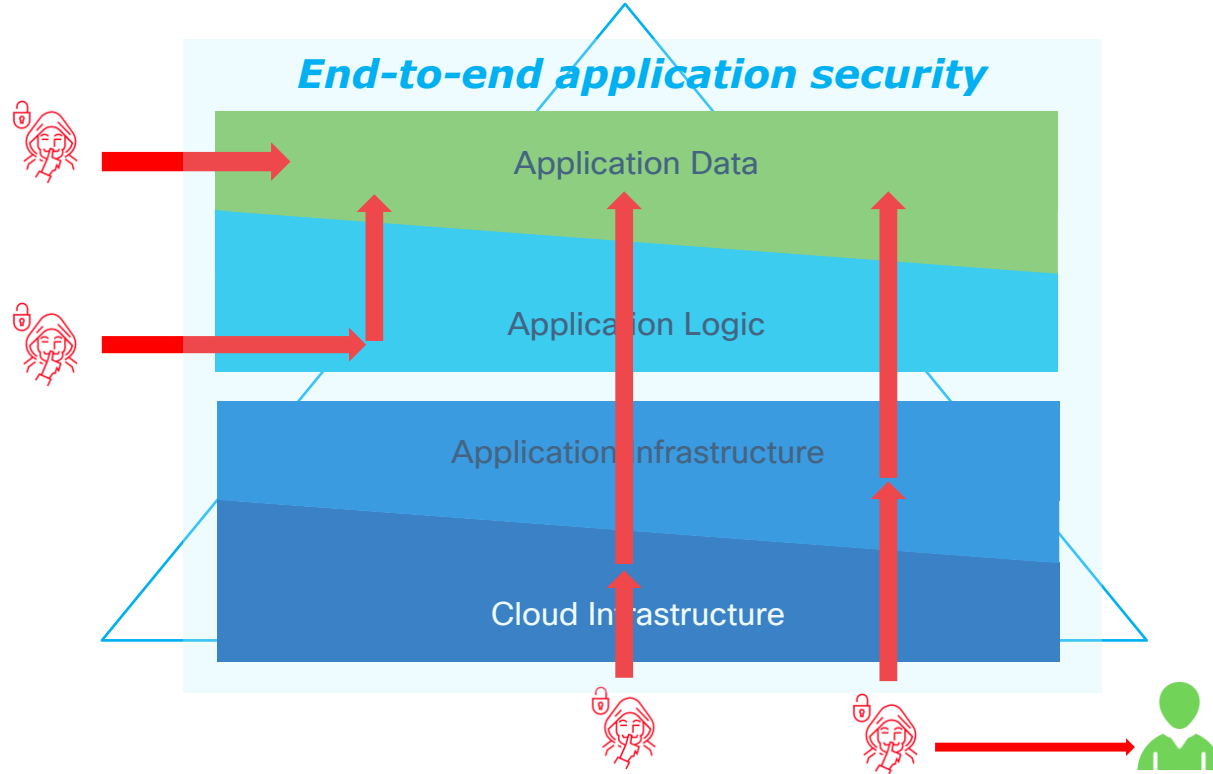
What methods do hackers have to get to critical assets?

# Pyramid of necessities for application security



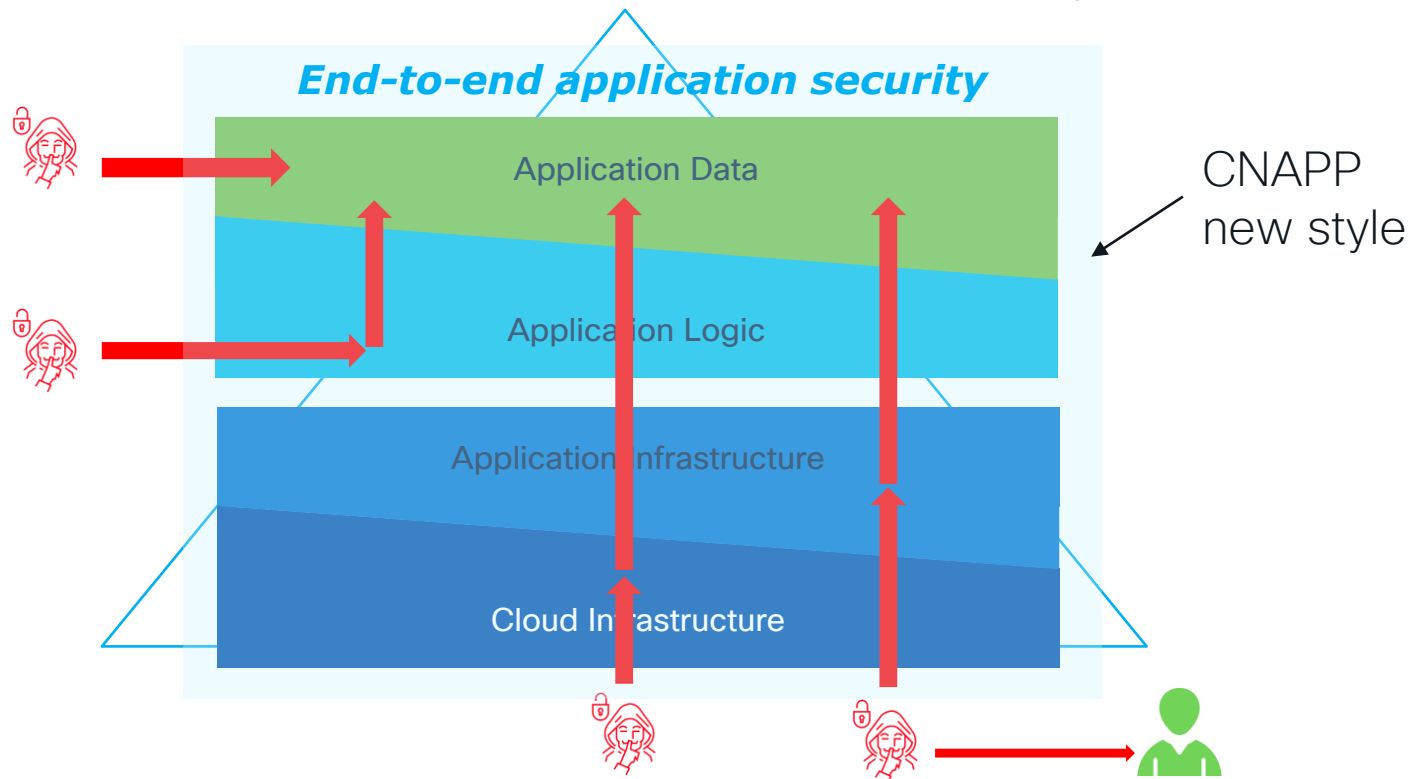
What methods do hackers have to get to critical assets?

# 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!



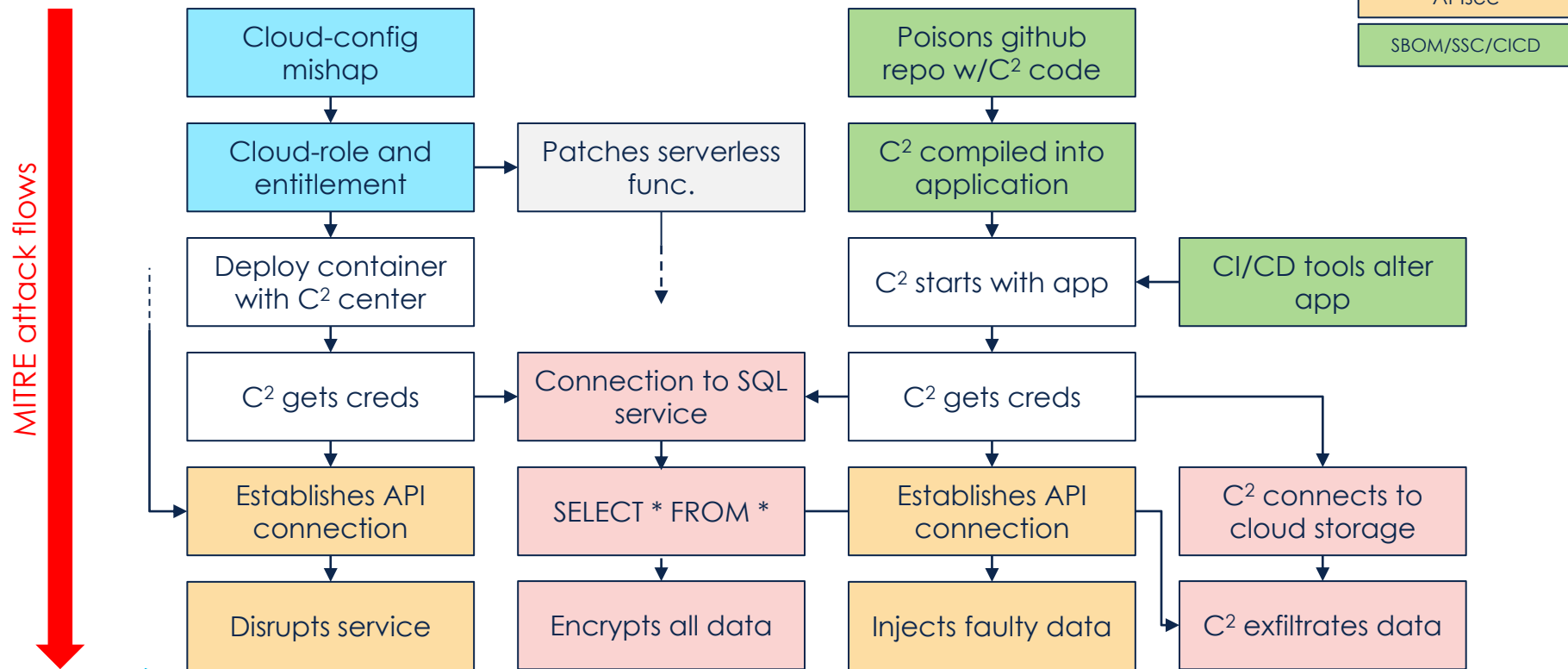
# Attack flow analysis today ...

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

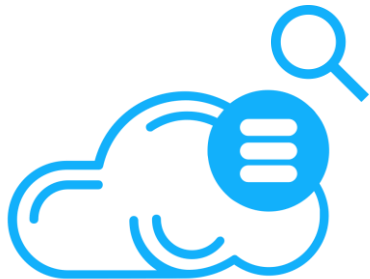
Attack flow analysis (often) does not include workload-, CI/CD-, API-, serverless-, and SBOM/SSC based attack vectors

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

Run-time insights

Active data lineage, data classification, data correlation	Data	Data source config analysis, schema analysis
Passive/active data lineage, data exfiltration analysis, payload delivery, tokens	Serverless	Code + config scan
System call traces, application model analysis	API	Specification scan
	Code	SBOM/SSC assessment, CVEs/CWEs identification
Orchestration telemetry, keys, tokens, identity	Library	
	K8s/VM	Deployment analysis, orchestration workload config analysis
	Orch.	
Log- and trace analysis, data- and call flow analysis, entitlement analysis	Cloud provider	

Build-time insights

# Attack vectors, paths and flows

## ATT&CK Matrix for Enterprise

layout: side show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (2)	Drive-by Compromise	Command and Scripting Interpreter (6)	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (2)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (3)	Exploit Public Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (2)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (2)	Browser Bookmark Discovery	Automated Collection	Audio Capture	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact	Data Manipulation (3)
Gather Victim Network Information (3)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (3)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Defacement (2)
Gather Victim Org Information (4)	Establish Accounts (3)	Phishing (3)	Inter-Process Communication (2)	Compromise Client Software Binary	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (3)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Phishing for Information (3)	Obtain Capabilities (4)	Replication Through Removable Media	Native API	Create Account (3)	Create or Modify System Process (4)	Deallocate/Decode Files or Information	Forge Web Credentials (2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Stage Capabilities (4)	Supply Chain Compromise (3)	Scheduled Task/Job (3)	Create or Modify System Process (4)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Scheduled Transfer	Resource Hijacking
Search Open Technical Databases (2)	Trusted Relationship	Serverless Execution	Shared Modules	Event Triggered Execution (14)	Escape to Host	Direct Volume Access	Modify Authentication Process (3)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Web Service (2)	Service Stop
Search Open Websites/Domains (2)	Valid Accounts (4)	Software Deployment Tools	Windows Management Instrumentation	External Remote Services	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Ingress Tool Transfer	Transfer Data to Cloud Account	System Shutdown/Reboot
Search Victim-Owned Websites		System Services (2)		Hijack Execution Flow (12)	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Multi-Stage Channels		
		User Execution (3)		Scheduled Task/Job (3)	Scheduled Task/Job (3)	Exploitation for Defense Evasion	Network Sniffing	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		
		Windows Management Instrumentation		Valid Accounts (4)	Valid Accounts (4)	File and Directory Permissions Modification (2)	OS Credential Dumping (3)	Network Share Discovery		Data from Removable Media	Protocol Tunneling		
						Hide Artifacts (1)	Steal Application Access Token	Network Sniffing		Data Staged (2)	Proxy (4)		
						Hijack Execution Flow (12)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (3)	Remote Access Software		
						Process Injection (12)	Unsecured Credentials (7)	Peripheral Device Discovery		Input Capture (4)	Traffic Signaling (2)		
						Scheduled Task/Job (3)		Permission Groups Discovery (3)		Screen Capture	Web Service (3)		
						Indirect Command Execution		Process Discovery		Video Capture			
						Masquerading (7)		Query Registry					
						Modify Authentication Process (3)		Remote System Discovery					
						Modify Cloud Compute Infrastructure (4)		Software Discovery (1)					
						Modify Registry		System Information Discovery					
						Modify System Image (2)		System Location Discovery (3)					
						Network Boundary Bridging (1)		System Network Configuration Discovery (1)					
						Obfuscated Files or Information (5)		System Network Connections Discovery					
						Plat File Modification		System Owner/User Discovery					
						Pre-OS Boot (3)		System Service Discovery					
						Process Injection (22)		System Time Discovery					
						Reflective Code Loading		Virtualization/Sandbox Evasion (3)					
						Rogue Domain Controller							
						Rootkit							
						Subvert Trust Controls (4)							
						System Binary Proxy Execution (12)							
						System Script Proxy Execution (1)							
						Template Injection							
						Traffic Signaling (2)							
						Trusted Developer Utilities Proxy Execution (1)							
						Unused/Unsupported Cloud							

# Attack vectors, paths and flows

MITRE ATT&CK

OWASP, OWASP API, OWASP Serverless, OWASP CI/CD, etc...

Center for Internet Security findings

Cisco security research

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

# Panoptica

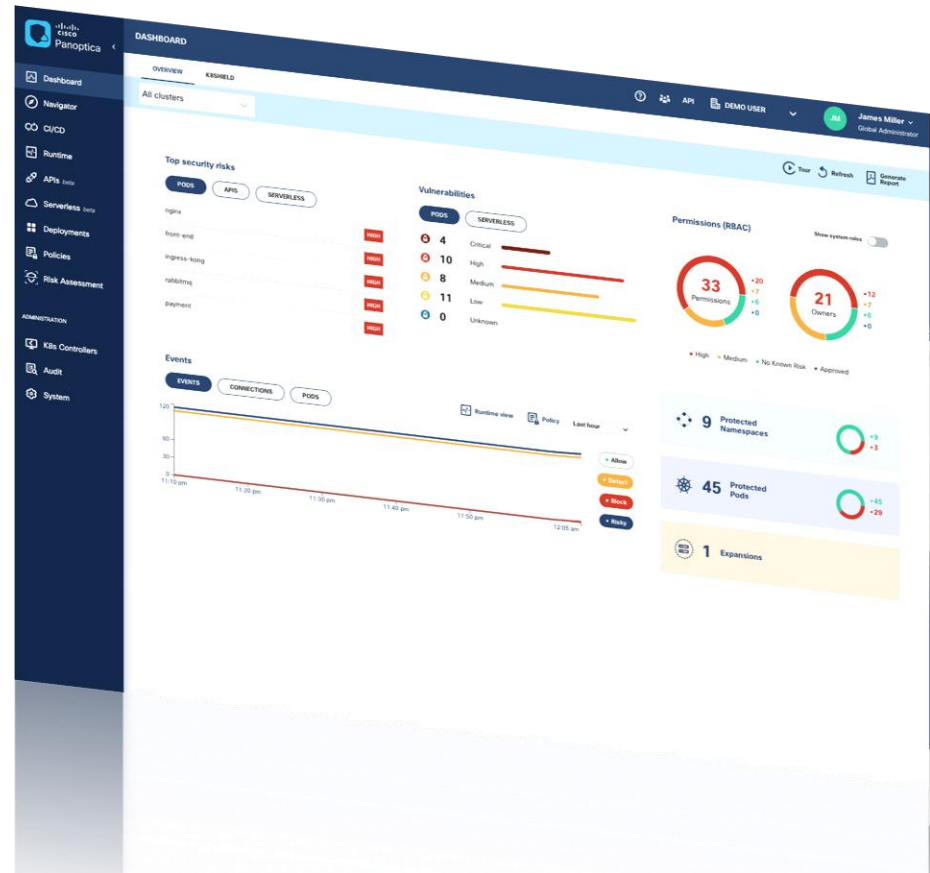
*“Cloud-native application protection”*

**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



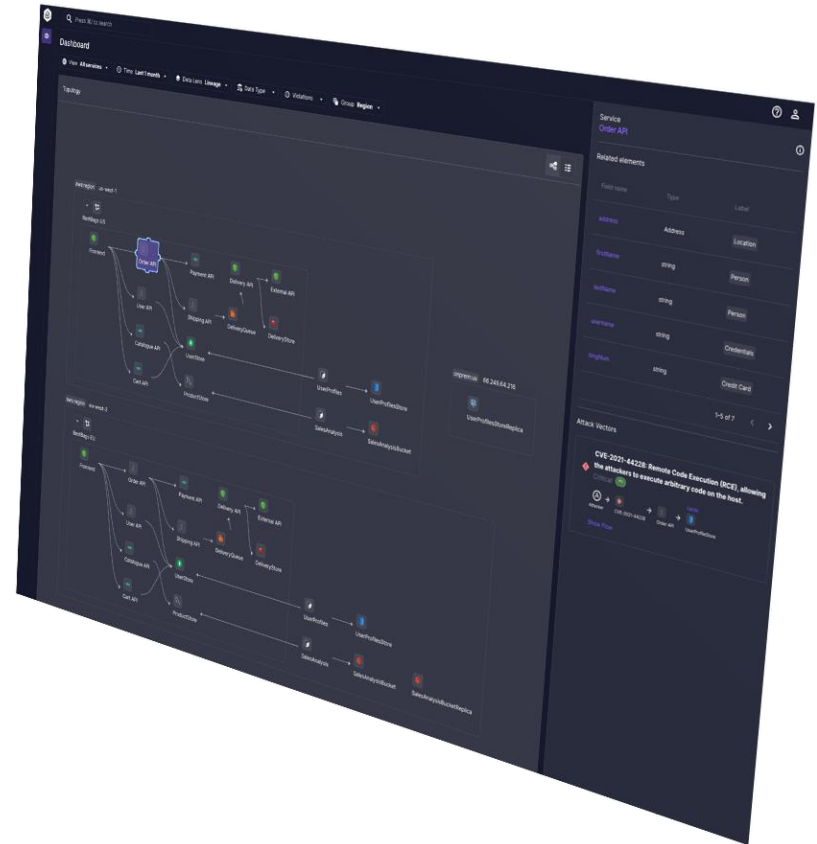
# Data security

## 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

The screenshot displays the Cisco Panoptica dashboard interface. The top navigation bar includes the Cisco Panoptica logo, a 'DASHBOARD' title, and user information for 'Audit User' (Account Auditor). The left sidebar lists various navigation options: Dashboard, Navigator, CI/CD, Runtime, APIs, Serverless, Deployments, Policies, Risk Assessment, Datasec, and an ADMINISTRATION section containing K8s Controllers, Audit, and System. The main content area is divided into sections: 'OVERVIEW' with 'All clusters' and 'Top security risks' (showing 'PODS' and 'API'), 'K8SHIELD', and a 'Datasec Controls' section. A large blue banner with the text 'Looking for design partners!' is overlaid on the dashboard. Below the banner, a timeline shows a sequence of events from 10:43 am to 11:38 am, with buttons for '+ Block' and '+ Risky' at the bottom right.

## 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](http://www.ciscodesignpartners.com)

Check out the Cisco Tech Blogs

<https://techblog.cisco.com>

 Twitter: @CiscoEmerge

 LinkedIn: Emerging Tech & Incubation

 Web: [eti.cisco.com](http://eti.cisco.com)

**CISCO** *Live!*

# 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](https://ciscolive.com/on-demand).



The bridge to possible

# Thank you



CISCO *Live!*

ALL IN