Enforcing a Strong Zero Trust Ransomware Defense

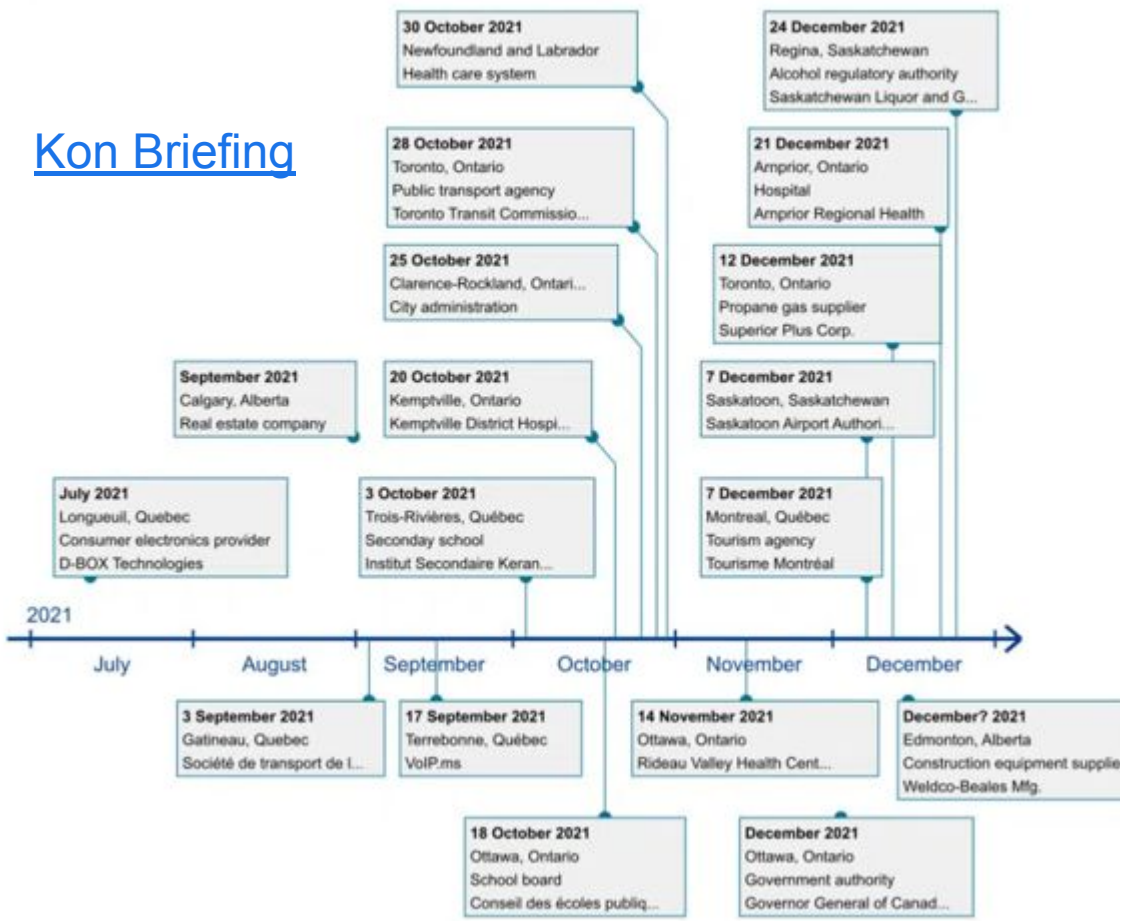
Dev Sharma
Senior Manager, Network and Security BU

Feb 24, 2023

PERIMETER

Major cyberattacks were recorded in Canada in the second half of 2021

Cyber attacks Canada, 2nd half 2021

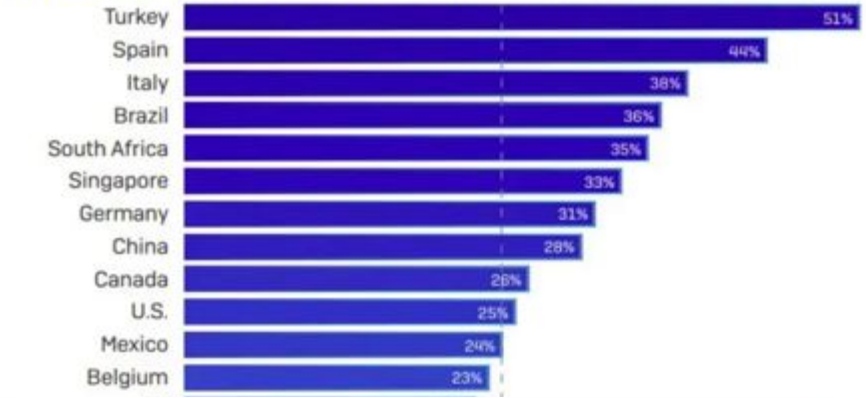


Kon Briefing

Canada was the fourth-hardest hit country by cyberattacks in December 2021

Spend is over $10B$

26% of Canadian companies managed to stop ransomware attacks prior to data encryption



Number of victim organizations with data published on leak sites by country							
United States	151	Belgium	4	Chile	1	Pakistan	1
Canada	39	Sweden	4	Colombia	1	Peru	1
Germany	26	South Africa	3	Croatia	1	Poland	1
United Kingdom	17	Spain	3	Greece	1	Portugal	1
France	16	Japan	2	Hong Kong	1	Saudi Arabia	1
India	11	Mexico	2	Jamaica	1	Singapore	1
Australia	7	New Zealand	2	Kenya	1	Sri Lanka	1
Brazil	5	South Korea	2	Luxembourg	1	Taiwan	1
Israel	5	Switzerland	2	Malaysia	1	Thailand	1
Italy	5	Austria	1	Norway	1	United Arab Emirates	1

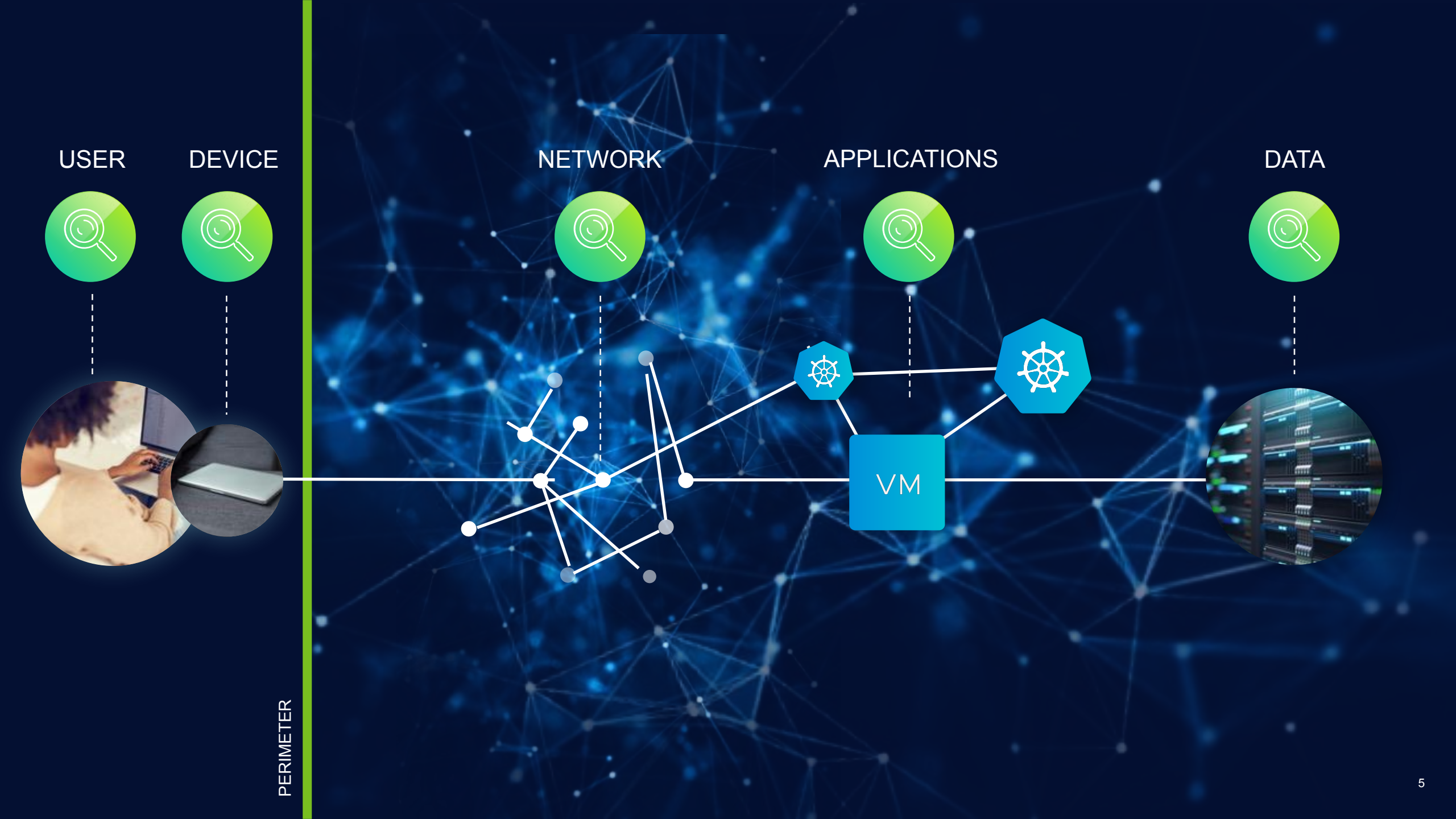
Figure 3: Numbers of victim organizations with data published on leak sites by country, Jan. 2020 – Jan. 2021

The average cost of a data breach is over $4 million

The average time to identify a breach in Canada is 168 days

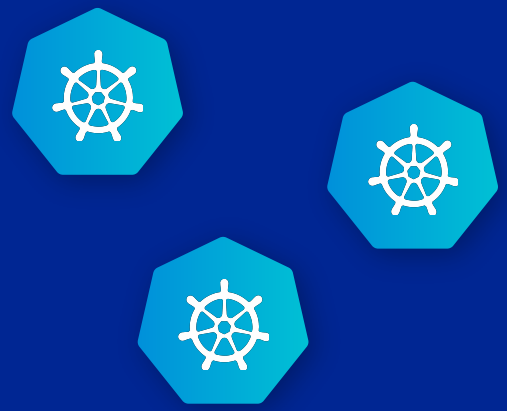
Average spend on security is 11.1% of an organization's IT budget

Lateral Security Is the New Battleground


USER
DEVICE
NETWORK
APPLICATIONS
DATA
VM
PERIMETER

1

Protect the inner workings of an application.

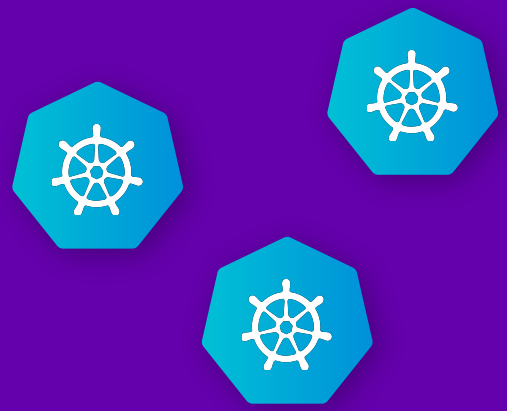


Private Cloud

Web App Database

VM VM VM

Hypervisor



Public Cloud

Web App Database

VM VM VM

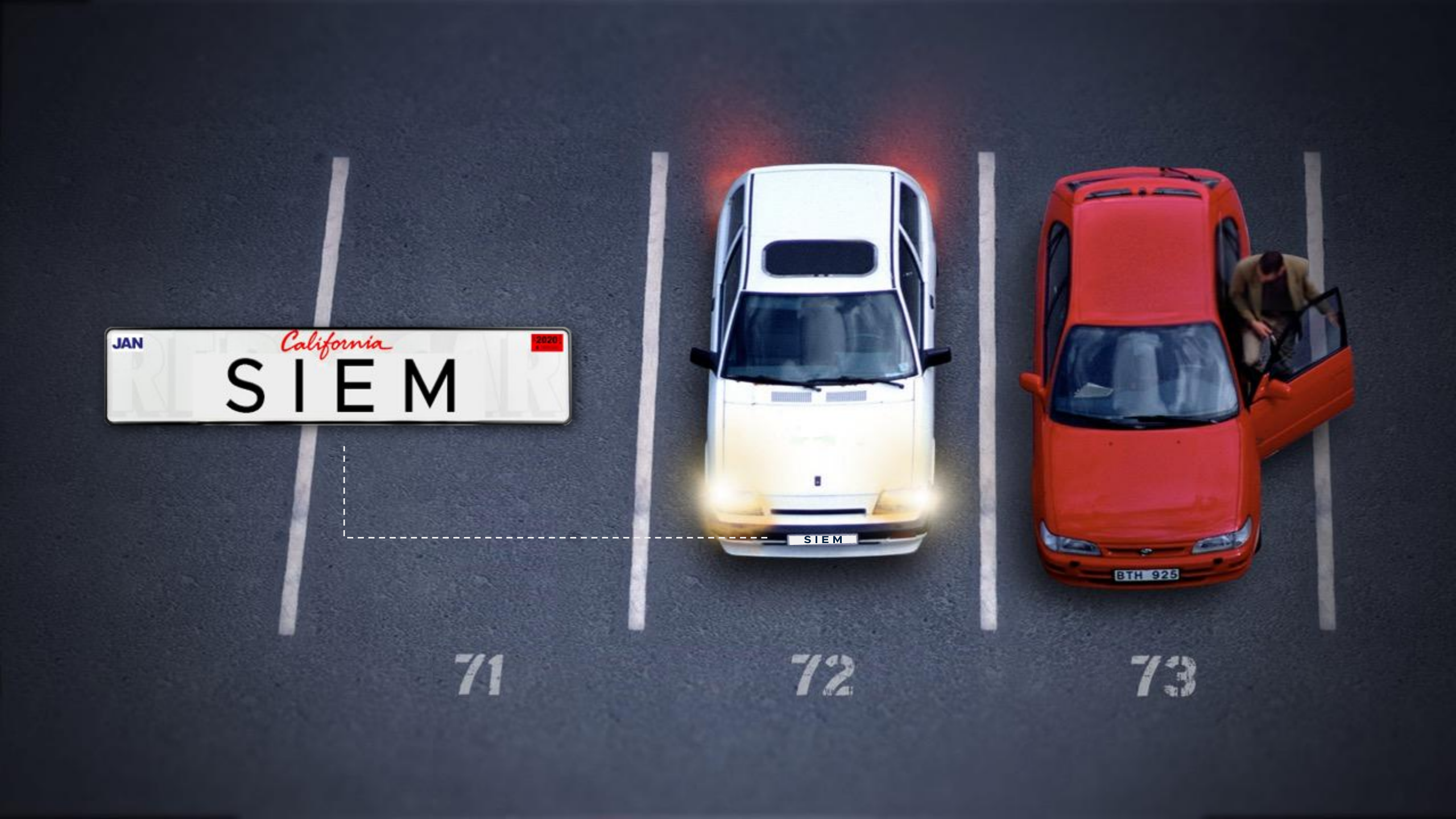
Hypervisor

Modern Apps

Traditional Apps

2

You can’t stop what you can’t see.


JAN
California
2020
SIEM
SIEM
BTH 925
71
72
73

Modern Apps

Web App Database

VM VM VM

Hypervisor

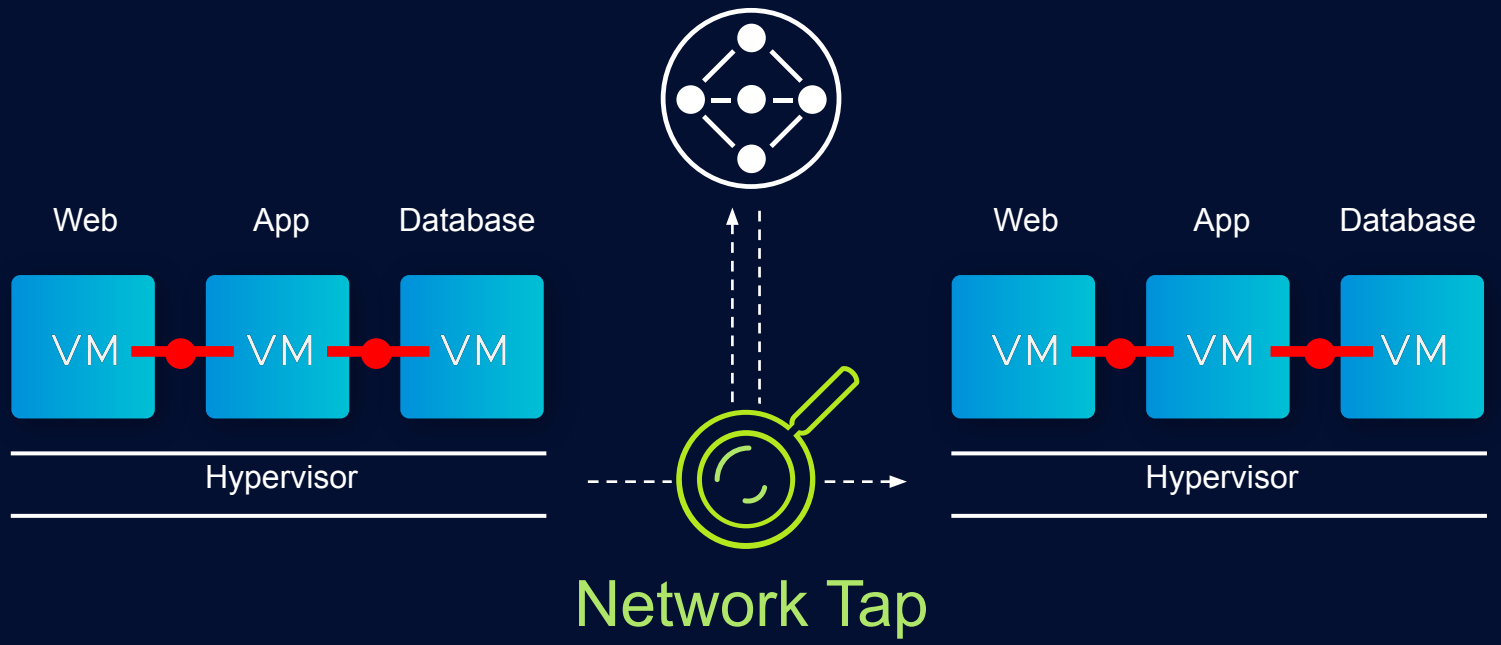
Web App Database

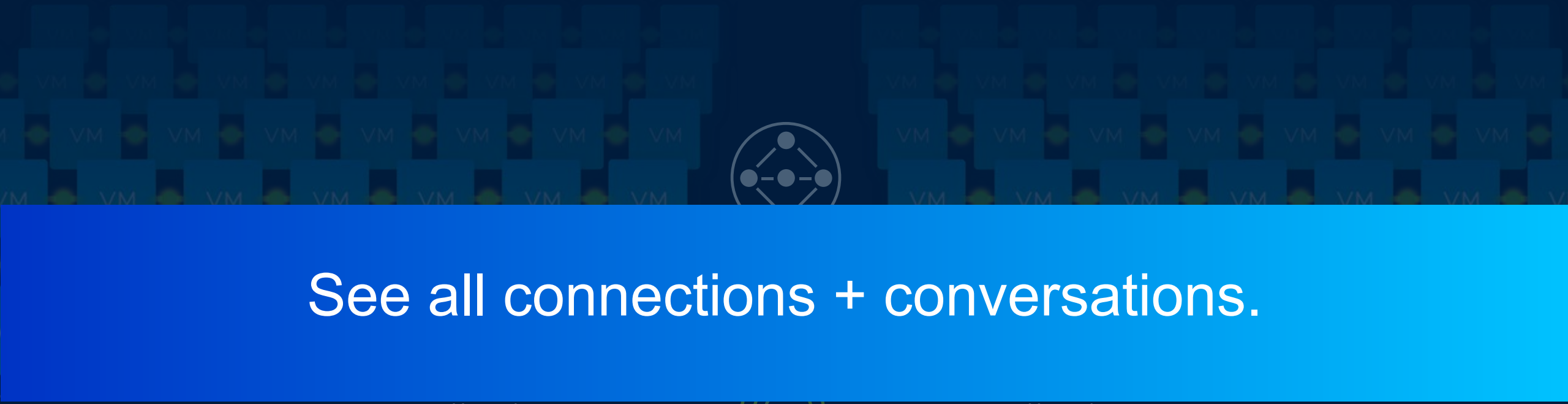
VM VM VM

Hypervisor

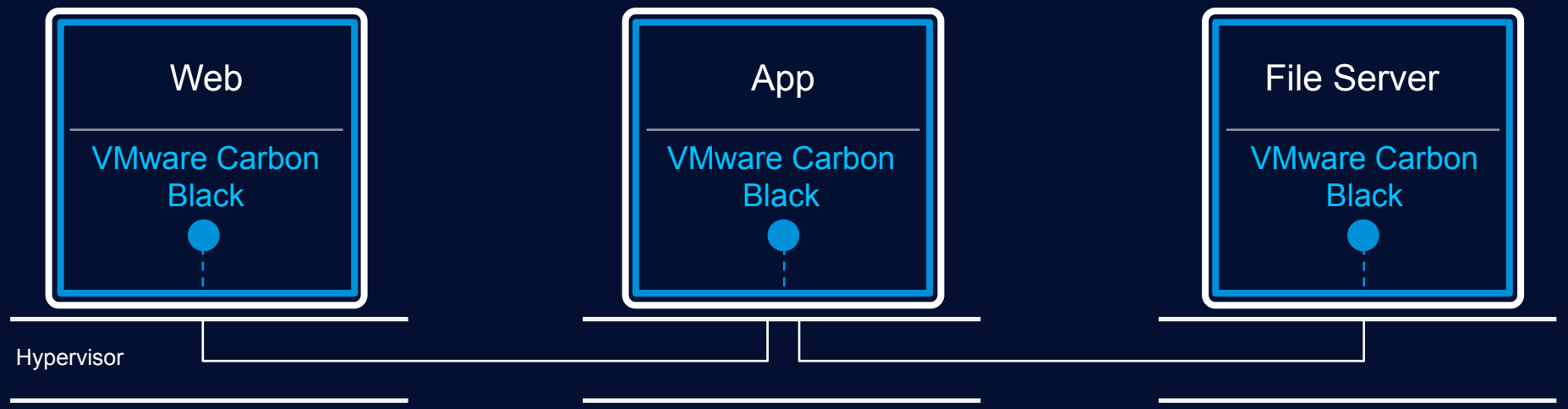
Traditional Apps

No Network Changes


Web
App
Database
VM
VM
VM
Hypervisor
Web
App
Database
VM
VM
VM
Hypervisor
Network Tap

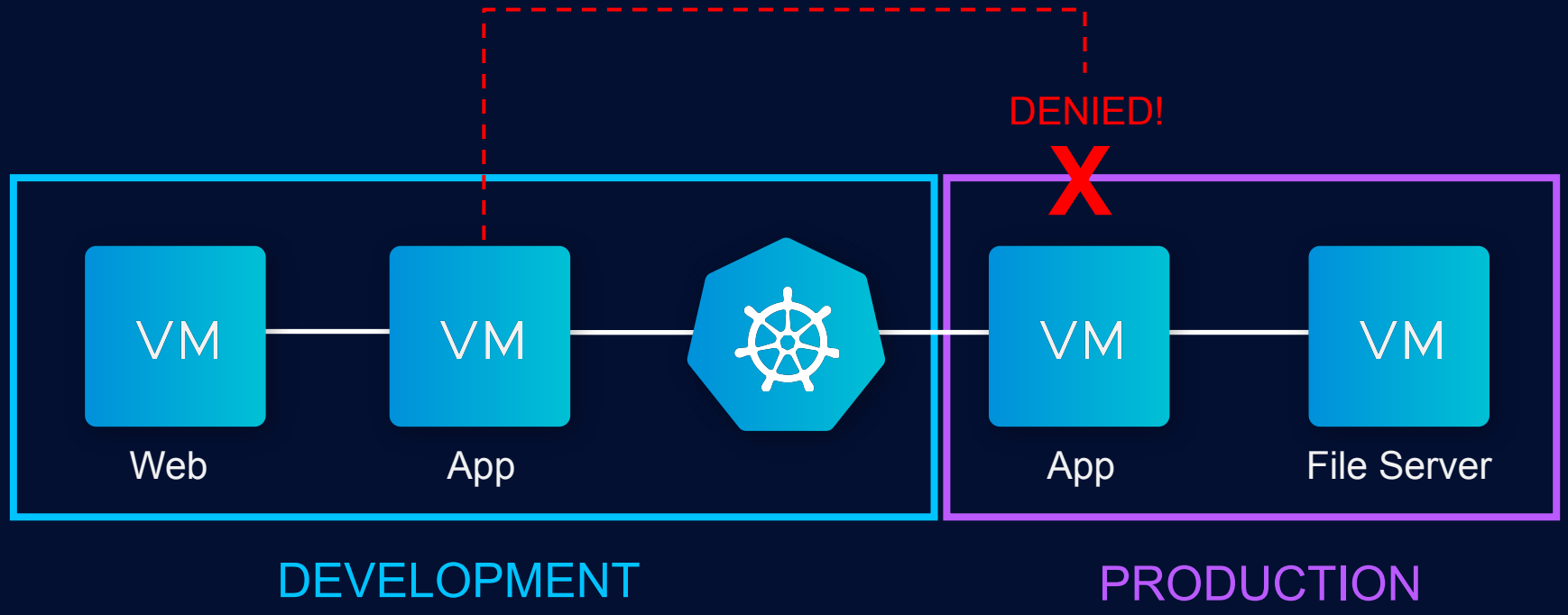


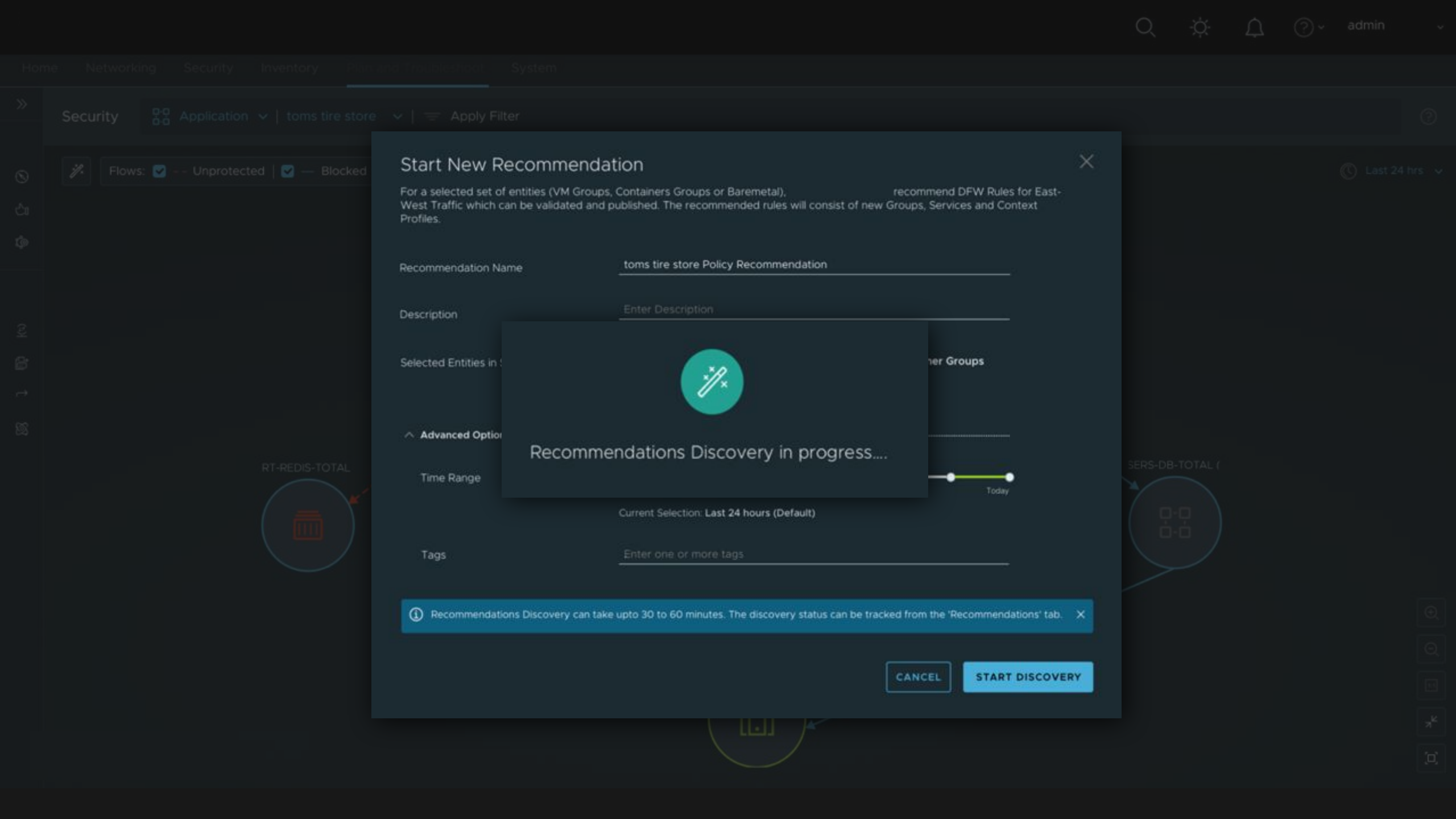
See all connections + conversations.

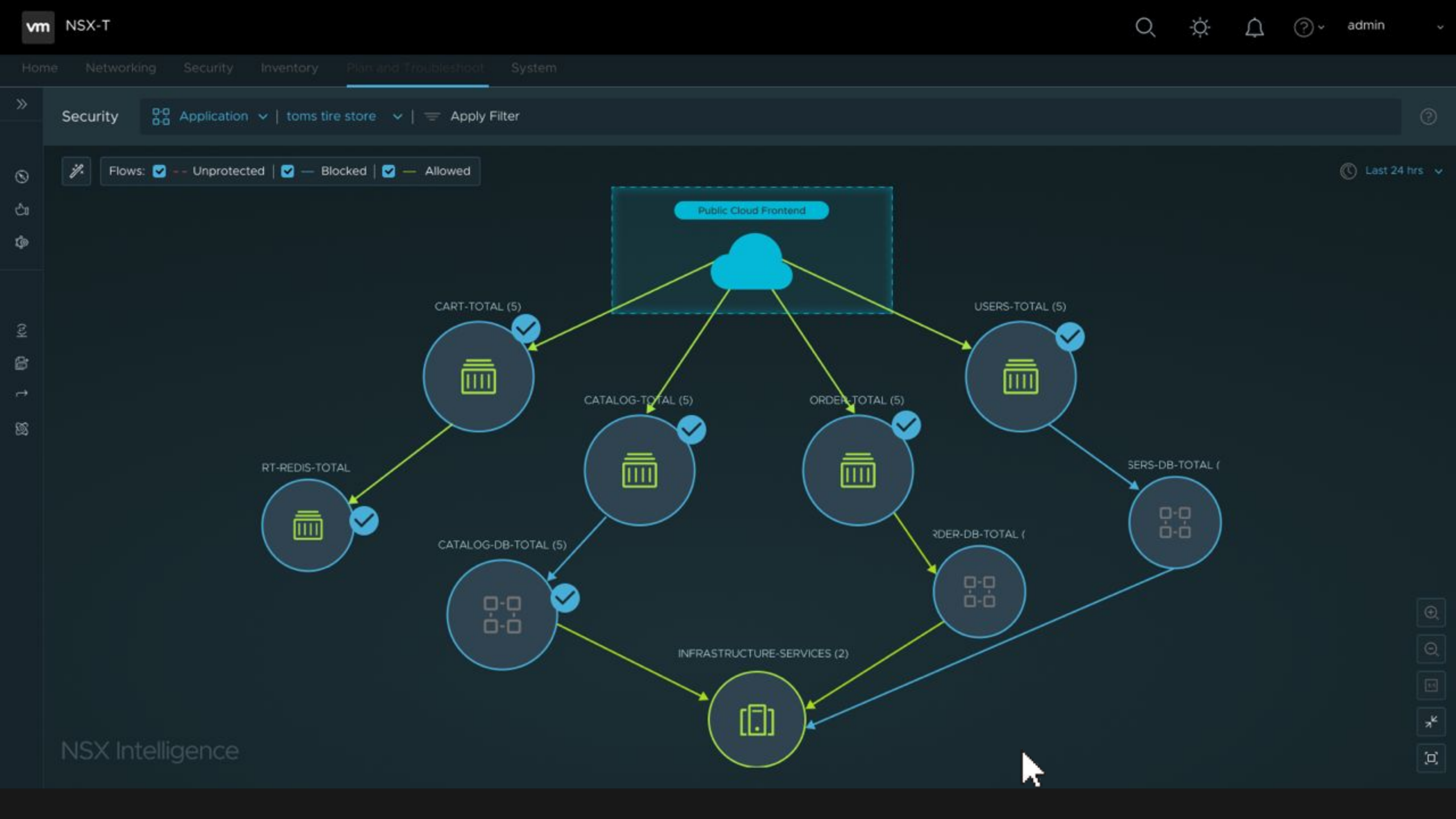


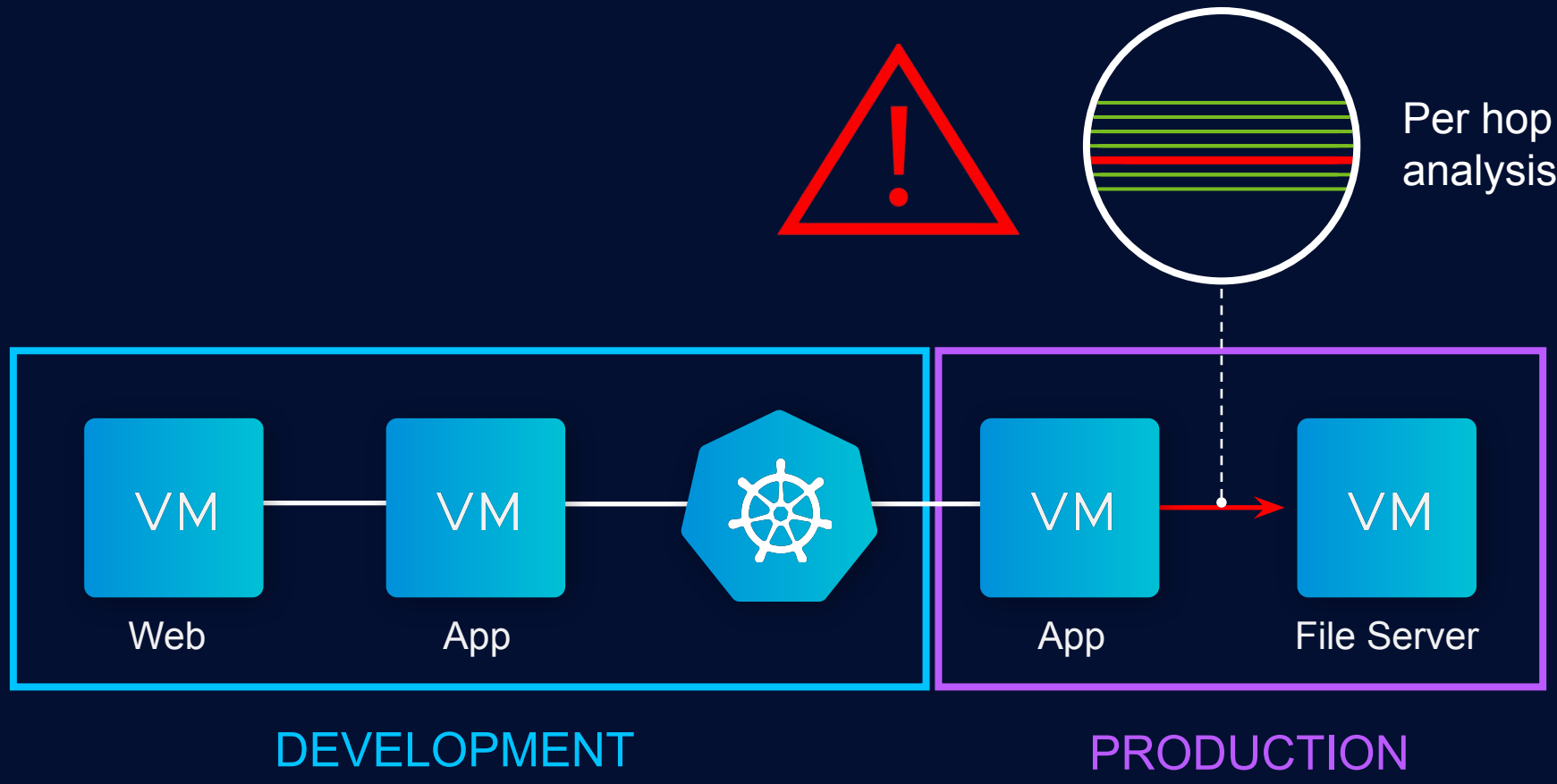
NGAV / MDR / Threat Intelligence / Audit & Remediation / EDR for Workloads

Vulnerability Management / Workload Inventory & Lifecycle Management


DENIED!
VM
VM
VM
VM
Web
App
App
File Server
DEVELOPMENT
PRODUCTION


admin
Home
Networking
Security
Inventory
System
Security
Application
toms tire store
Apply Filter
Flows:
Unprotected
Blocked
Last 24 hrs
Start New Recommendation
For a selected set of entities (VM Groups, Containers Groups or Baremetal), recommend DFW Rules for East-West Traffic which can be validated and published. The recommended rules will consist of new Groups, Services and Context Profiles.
Recommendation Name
toms tire store Policy Recommendation
Description
Enter Description
Selected Entities in
Groups
Advanced Optio
Time Range
Today
Current Selection: Last 24 hours (Default)
Tags
Enter one or more tags
Recommendations Discovery in progress....
Recommendations Discovery can take upto 30 to 60 minutes. The discovery status can be tracked from the 'Recommendations' tab.
CANCEL
START DISCOVERY
RT-REDIS-TOTAL
SERS-DB-TOTAL (


NSX-T
admin
Home
Networking
Security
Inventory
Plan and Troubleshoot
System
Security
Application
toms tire store
Apply Filter
Flows:
Unprotected
Blocked
Allowed
Last 24 hrs
Public Cloud Frontend
CART-TOTAL (5)
USERS-TOTAL (5)
CATALOG-TOTAL (5)
ORDER-TOTAL (5)
RT-REDIS-TOTAL
SERS-DB-TOTAL (
CATALOG-DB-TOTAL (5)
RDER-DB-TOTAL (
INFRASTRUCTURE-SERVICES (2)
NSX Intelligence


Per hop traffic analysis
VM
VM
VM
VM
Web
App
App
File Server
DEVELOPMENT
PRODUCTION

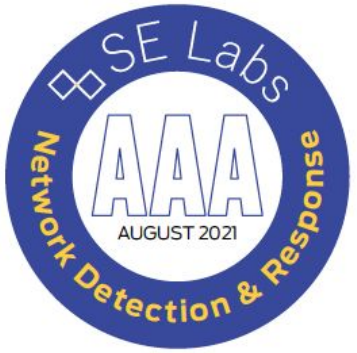
SE Labs

SE Labs Breach Response Detection Test

VMware NSX Network Detection and Response

August 2021

RATINGS



Total Rating	100%
Detection Accuracy	100%
Legitimate Accuracy	100%

LEGITIMATE ACCURACY

False Positives	0%

THREAT RESPONSE DETAILS

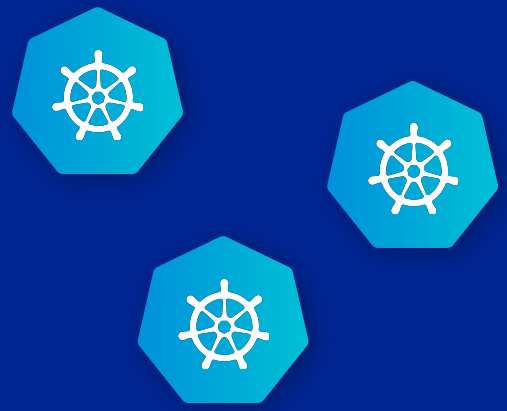
Threat	Target	Score	Overall Score
FIN7 & Carbanak		100%	100%
OilRig		100%	
APT3		100%	
APT29		100%	

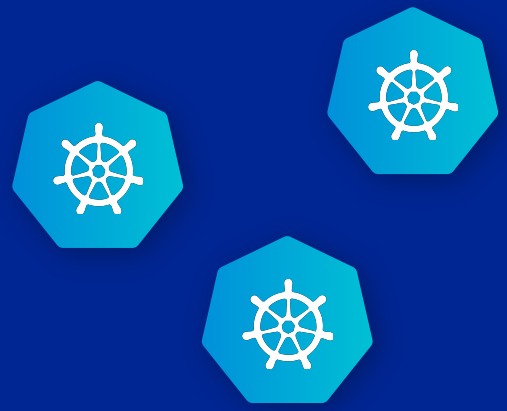
This is a summary of the full test report available selabs.uk/vmware.

Detection scores represent the product's behaviour when encountering network-specific threat techniques.

SE Labs helps advance the effectiveness of computer security through innovative, detailed and intelligence-led testing, run with integrity. We support businesses that are researching, buying and deploying security solutions. We are able to test a wide range of products and services using cutting edge testing methodologies that lead the security testing industry. SE Labs focusses on achieving detailed results, integrity in the testing process, useful threat intelligence and test innovation.

Modern Apps





Web App Database

VM VM VM

Hypervisor

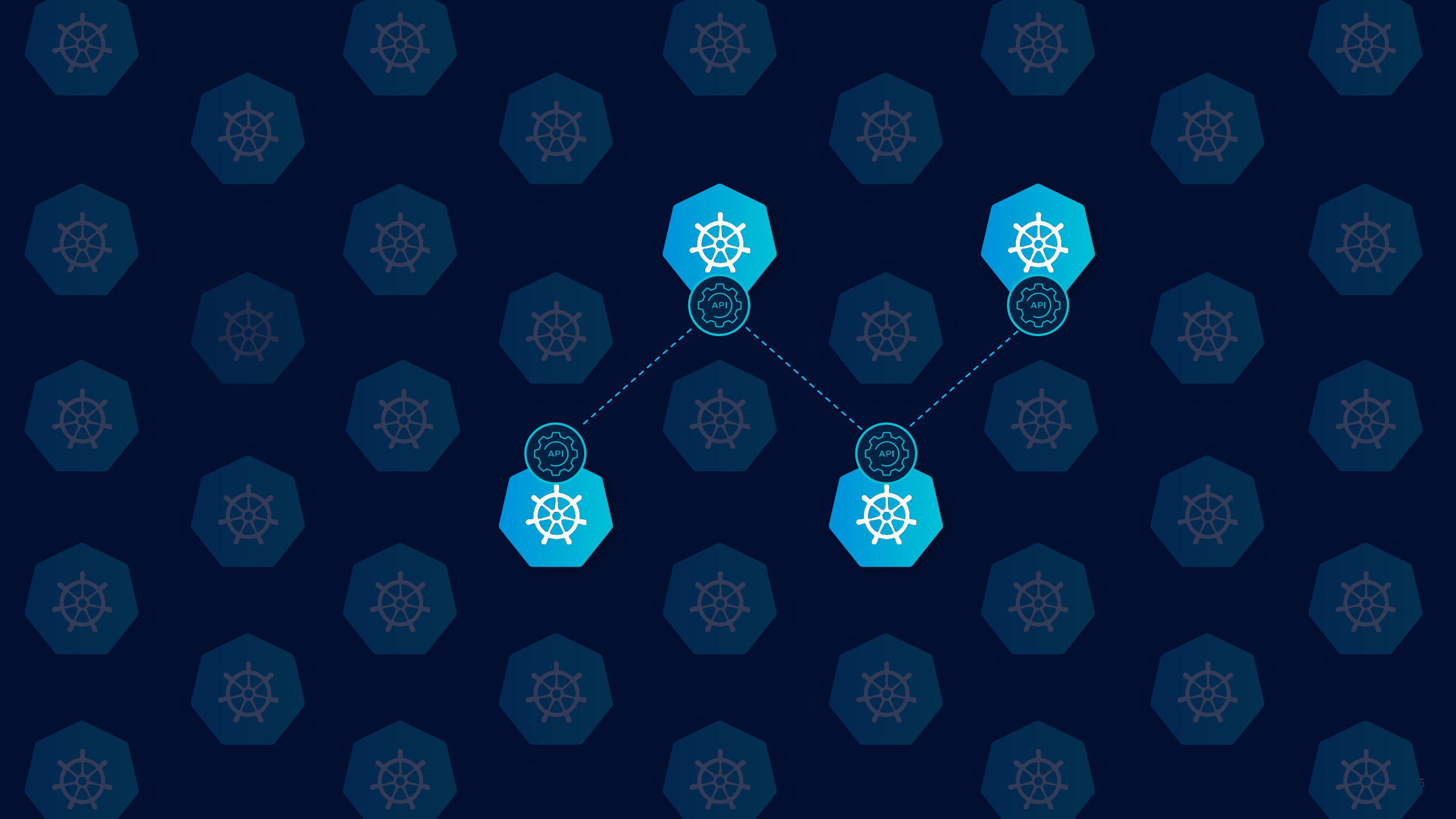
Web App Database

VM VM VM

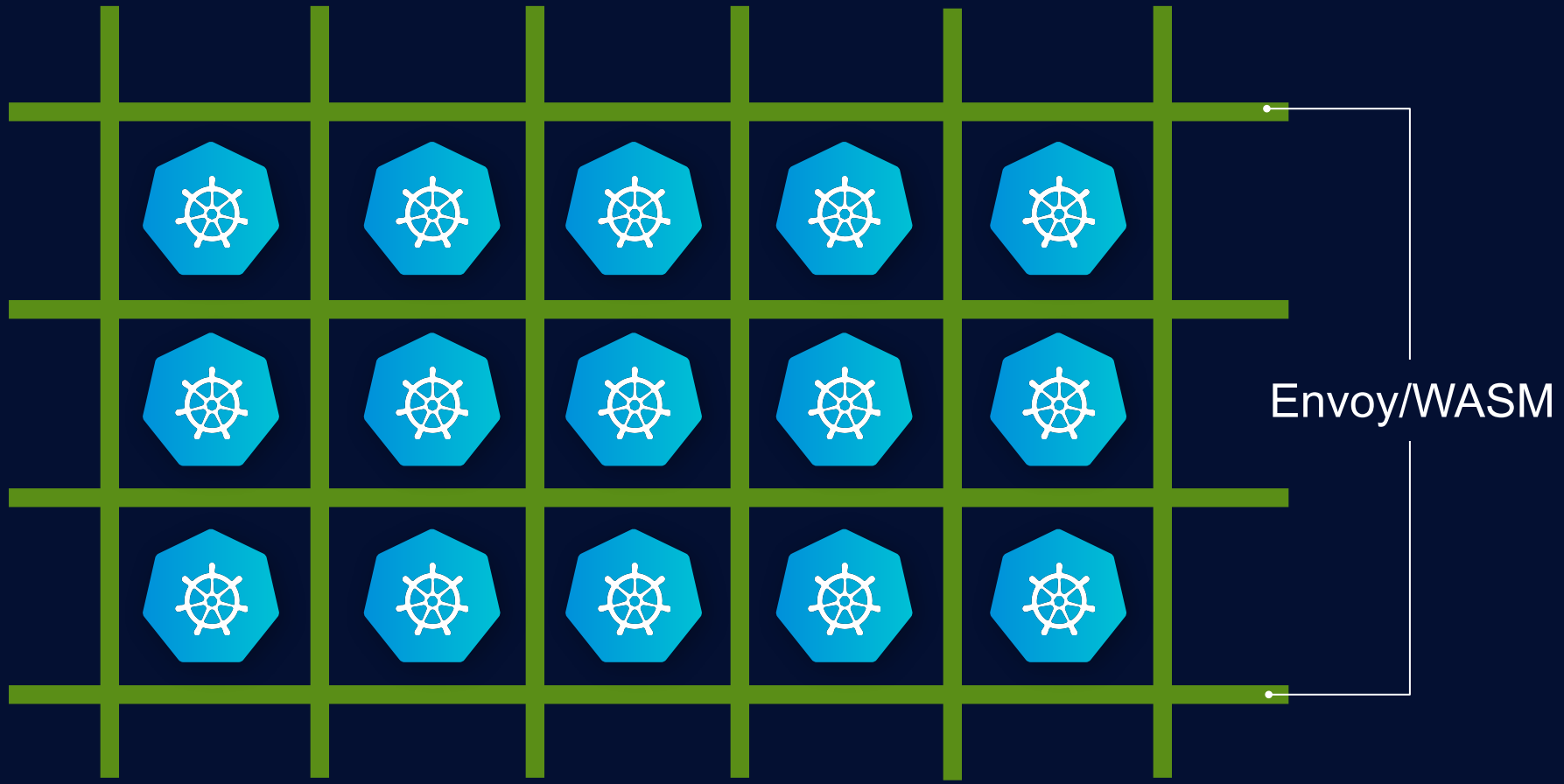
Hypervisor

Traditional Apps

The API Is the New Endpoint

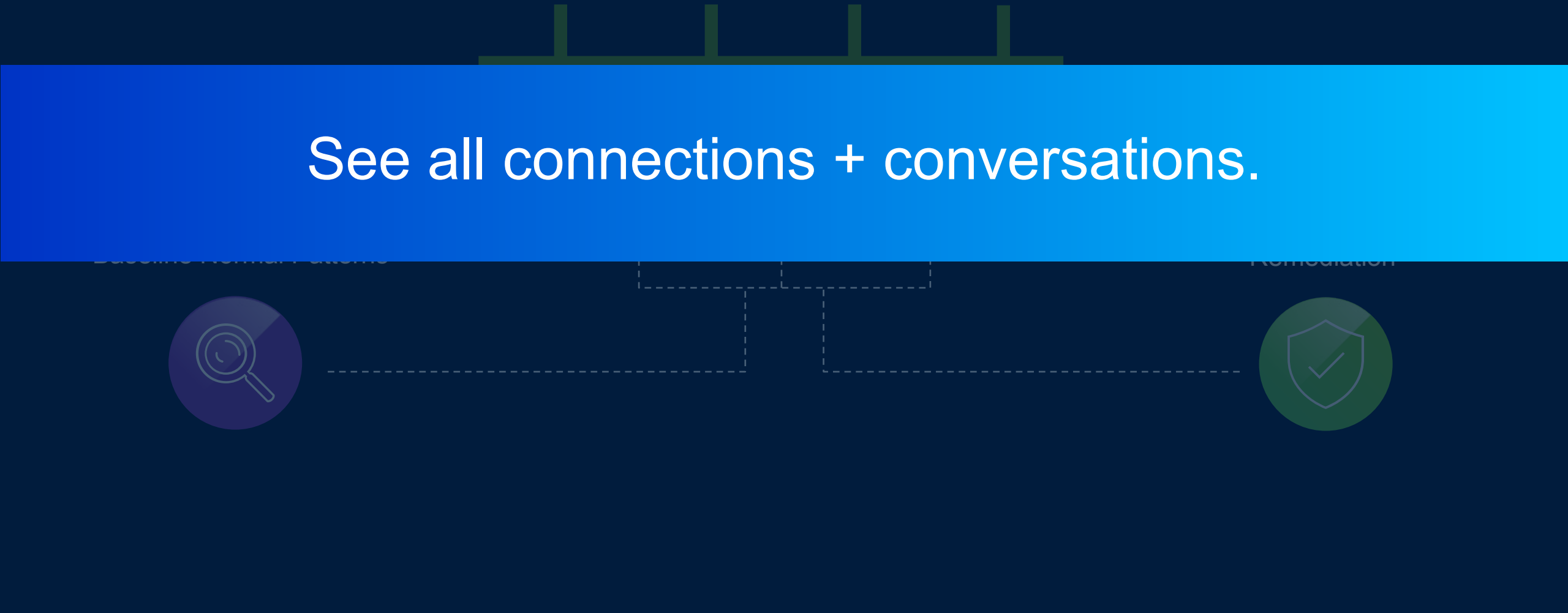

API
API
API
API

Built on Open Standards

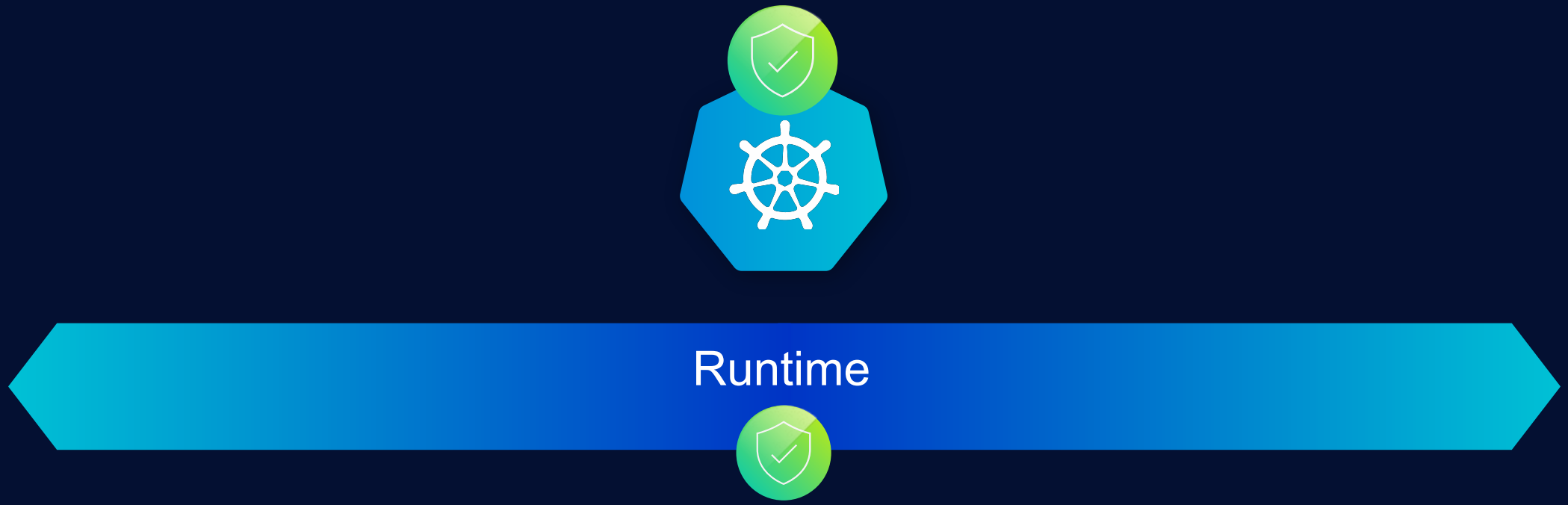


Transparent Insertion

API Visibility and Security



Full Lifecycle Container Security



Workload and Network Visibility, Encryption

Ingress and Egress Management

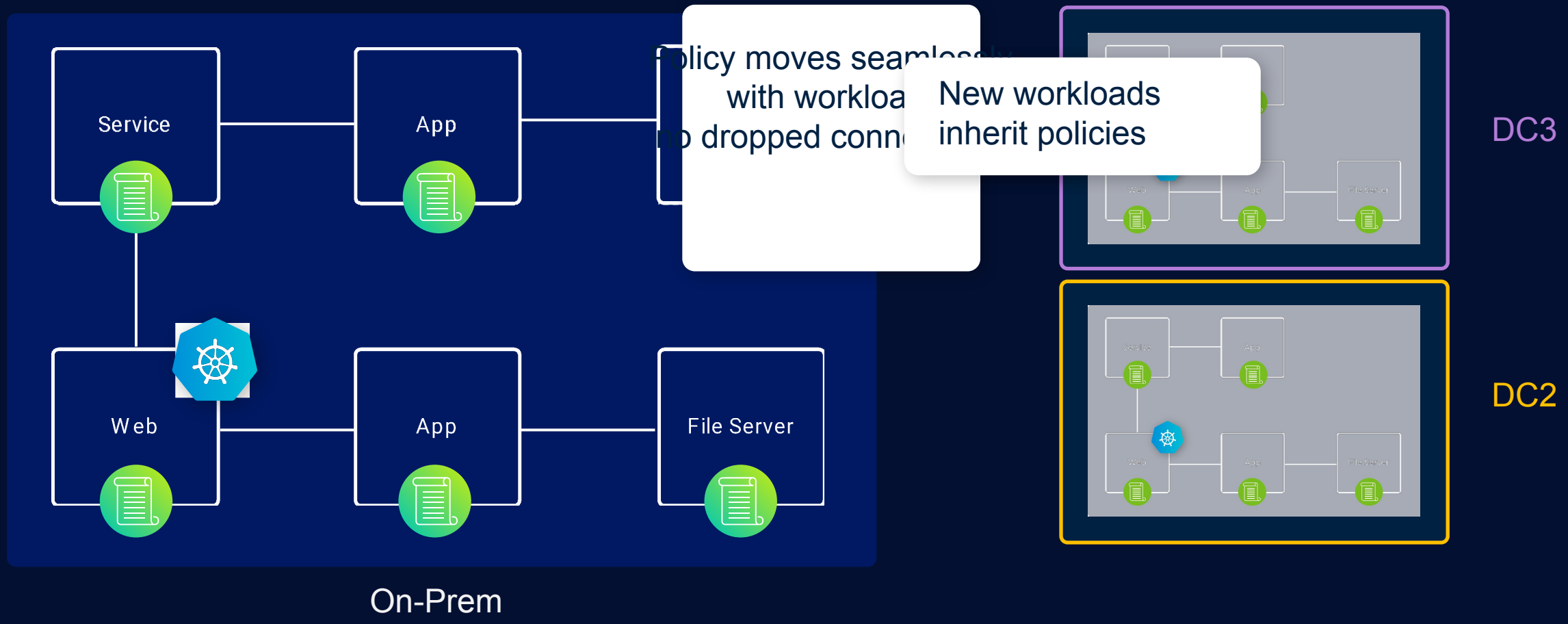
Workload and Network Anomaly Detection

Malicious Activity Detection

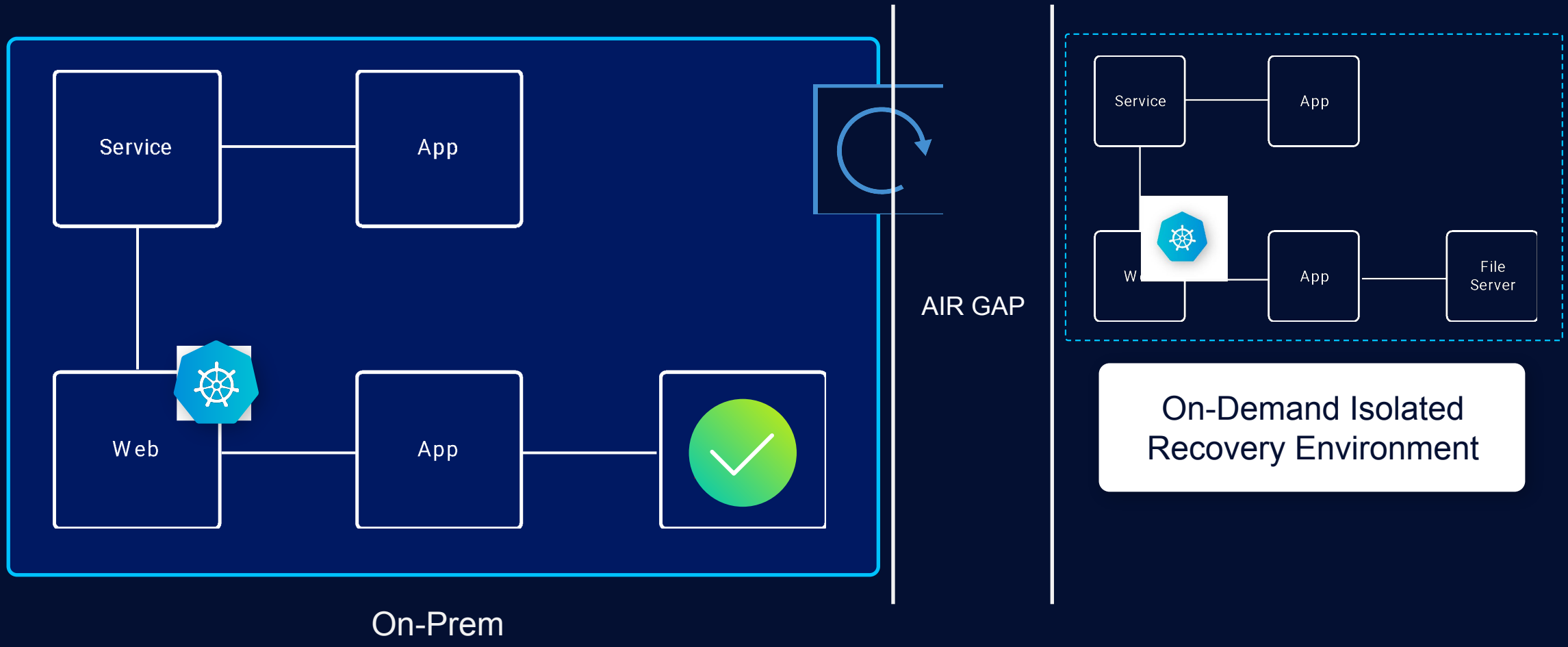
3

The cloud operating model = better security.

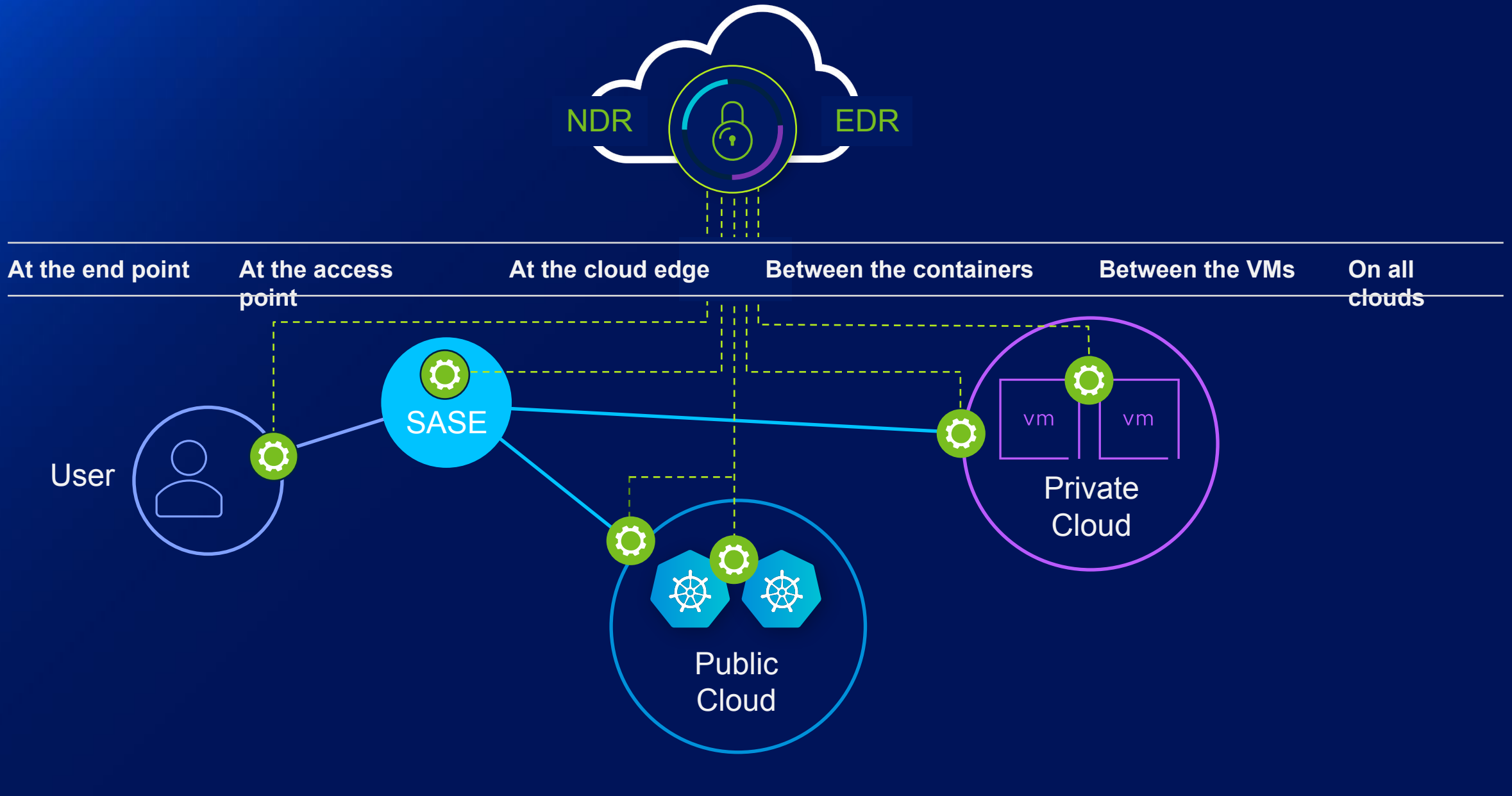

ON PREM
True Cloud Operating Model
Security As Code


Service
App
Web
App
File Server
New workloads
inherit policies
DC3
DC2
On-Prem

Restore Swiftly with VMware Ransomware Recovery



VMware Contexa: Sees More, Stops More



Your Workloads Are More Secure with VMware

Protect the inner workings of modern and traditional apps

You can’t stop what you can’t see

Security needs to fit the cloud operating model

Thank You