

Unified Zero Trust for Modern Warfighters

Dustin Boyd
Technical Account Executive

Phillip Kramp
Solutions Architect

Where are we?

State of Mission Systems



State of Security



Where do we want to be?

Modern Applications in Contested Environments



Hurdles

Supply Chain Concerns



Complexity of Security



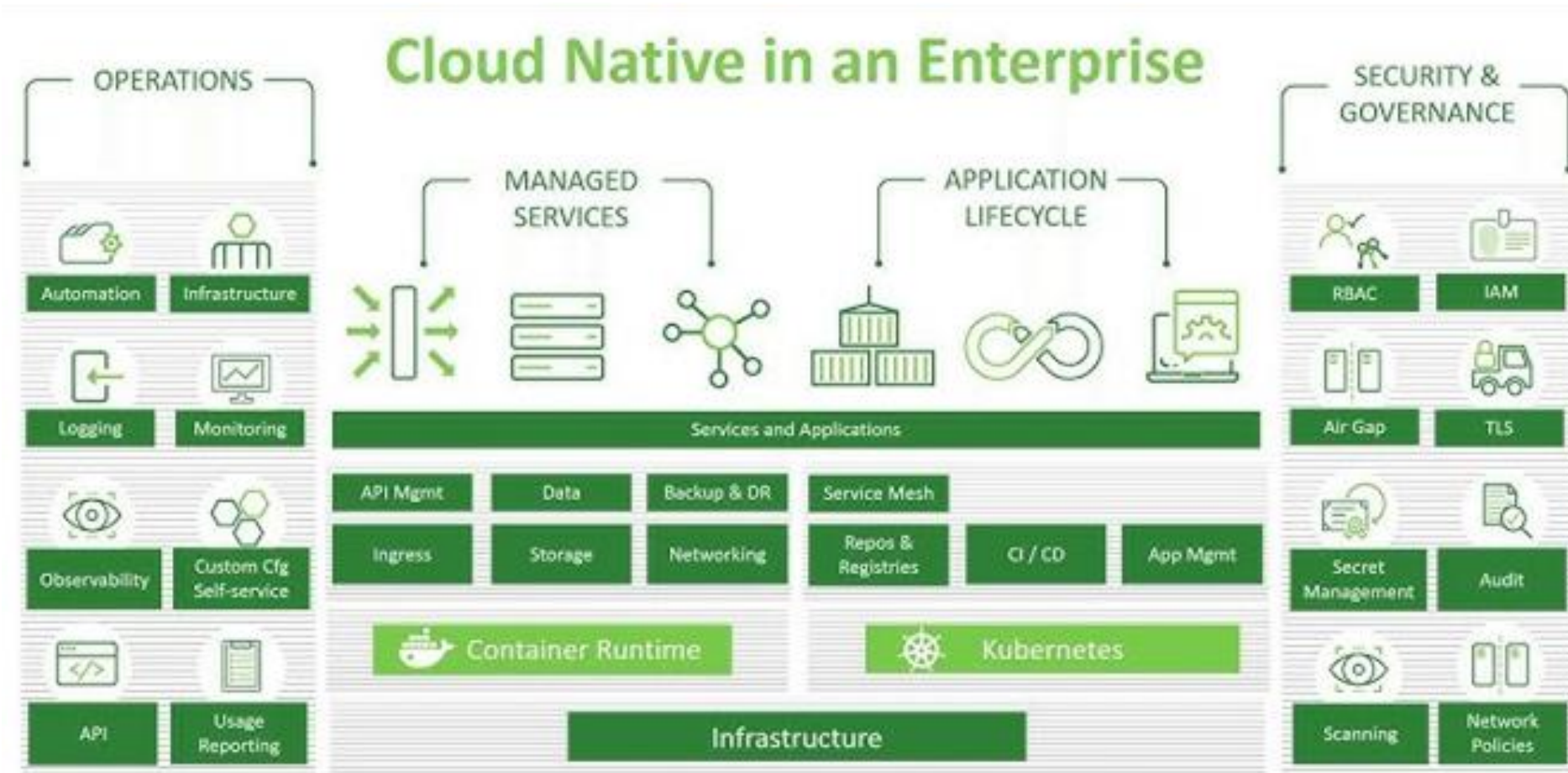
Cost/Benefit of Change



Incompatible Systems



Complicated Environments



Too Many Tools

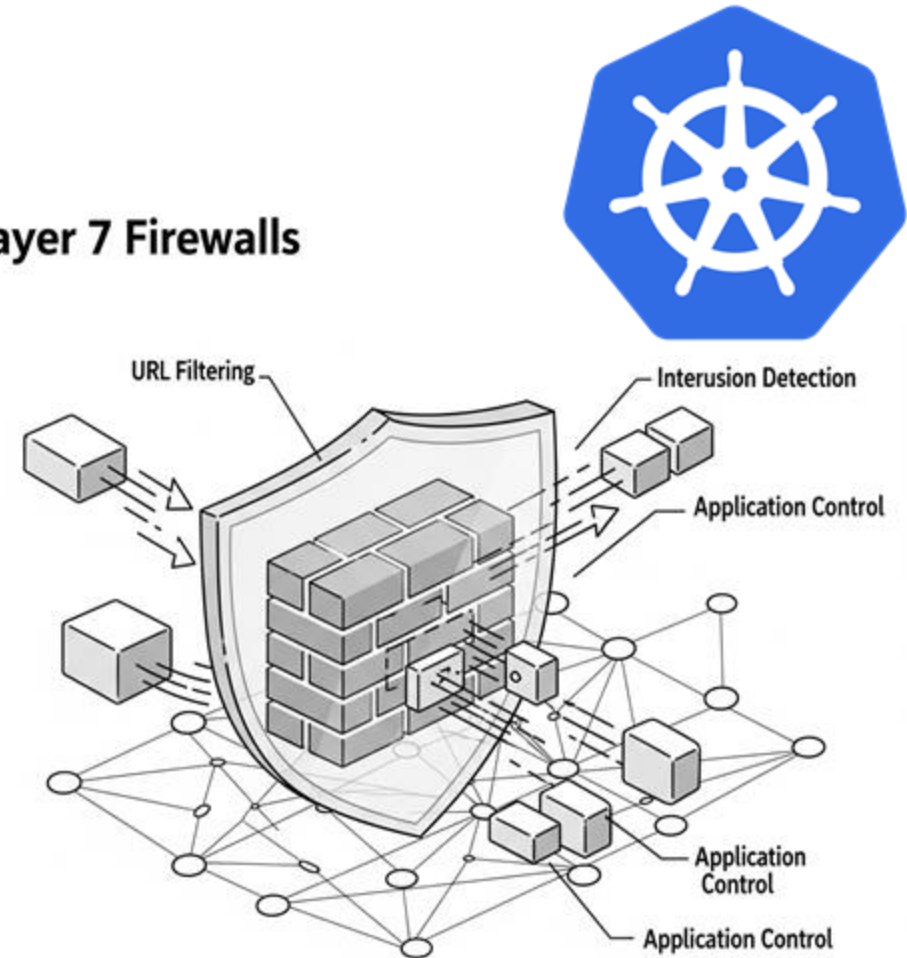


The Ideal Solution

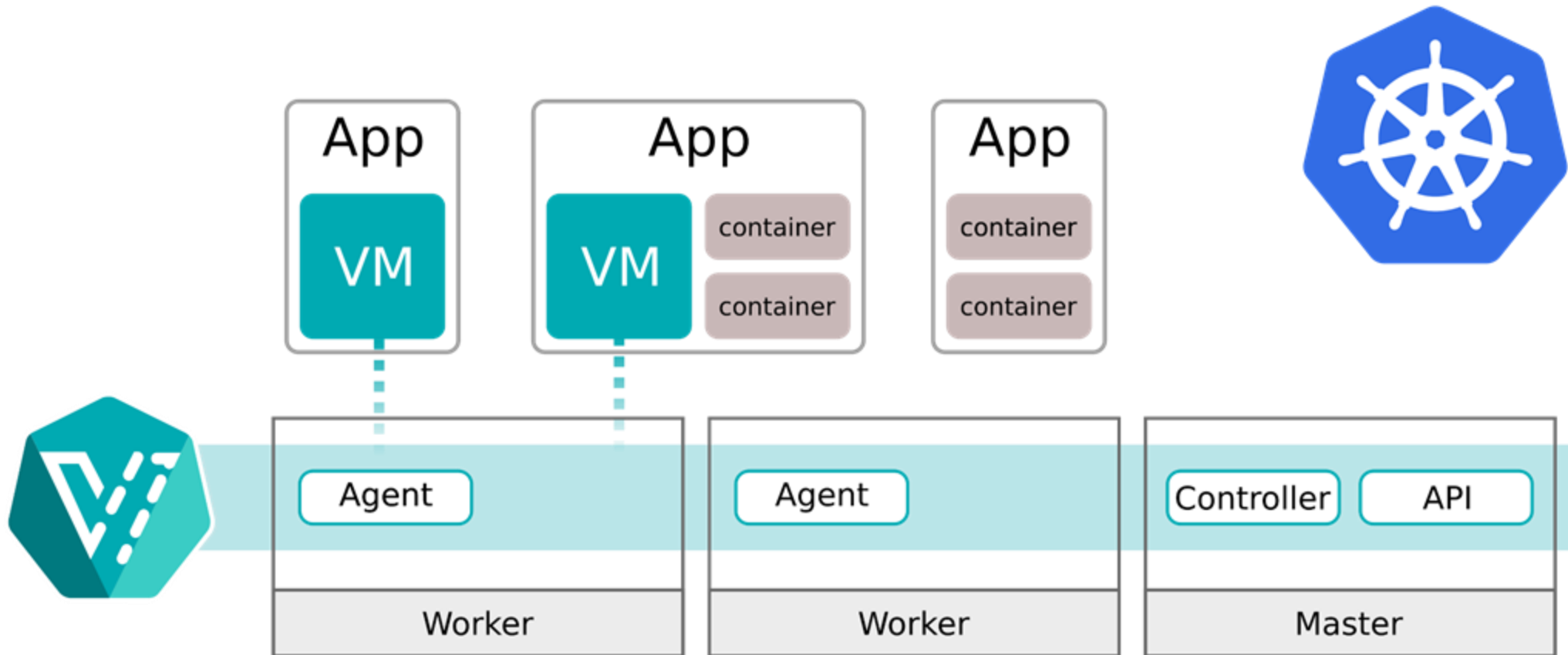
Modernized Zero Trust Concepts



Layer 7 Firewalls



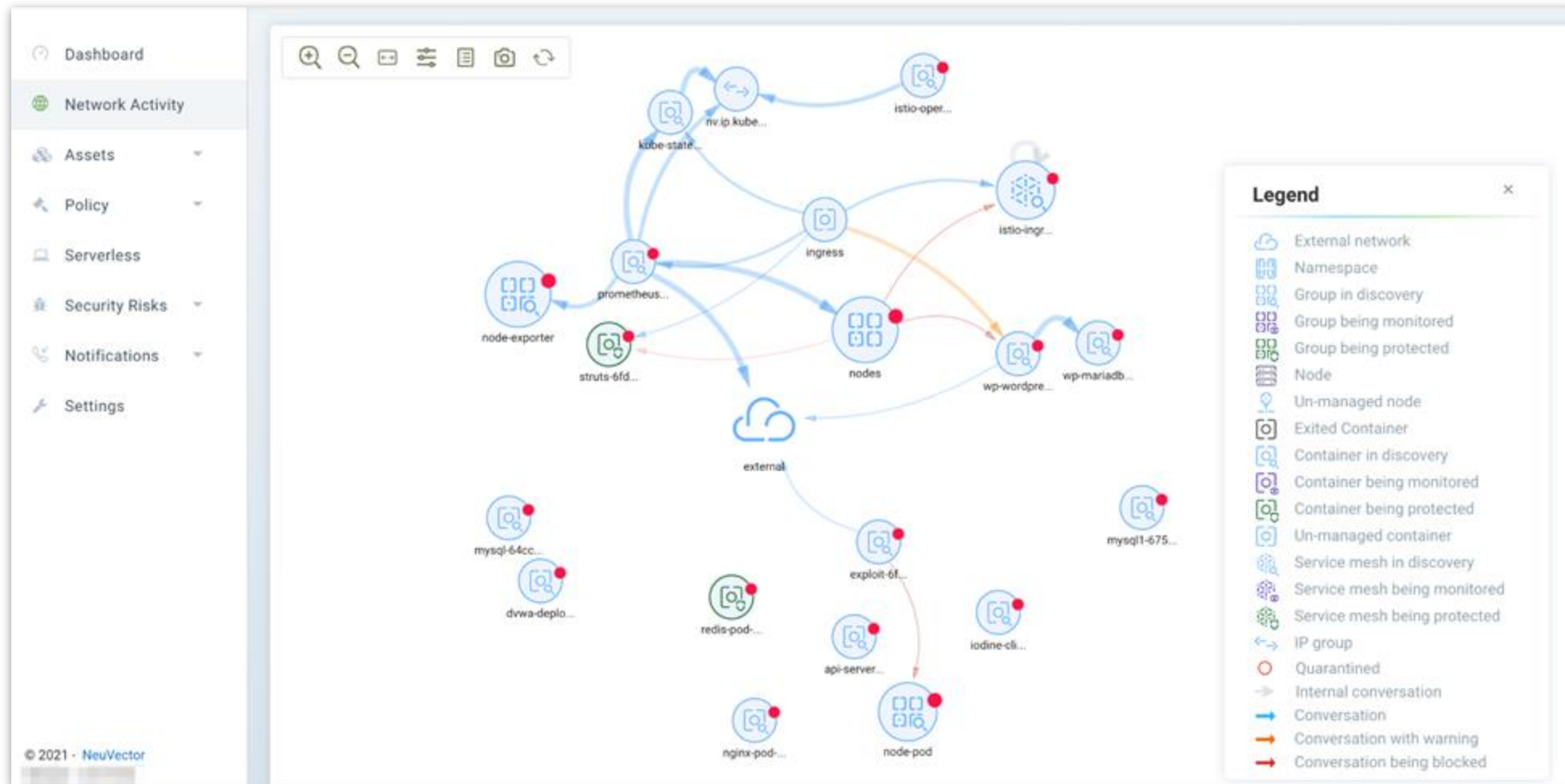
Homogenized Environments



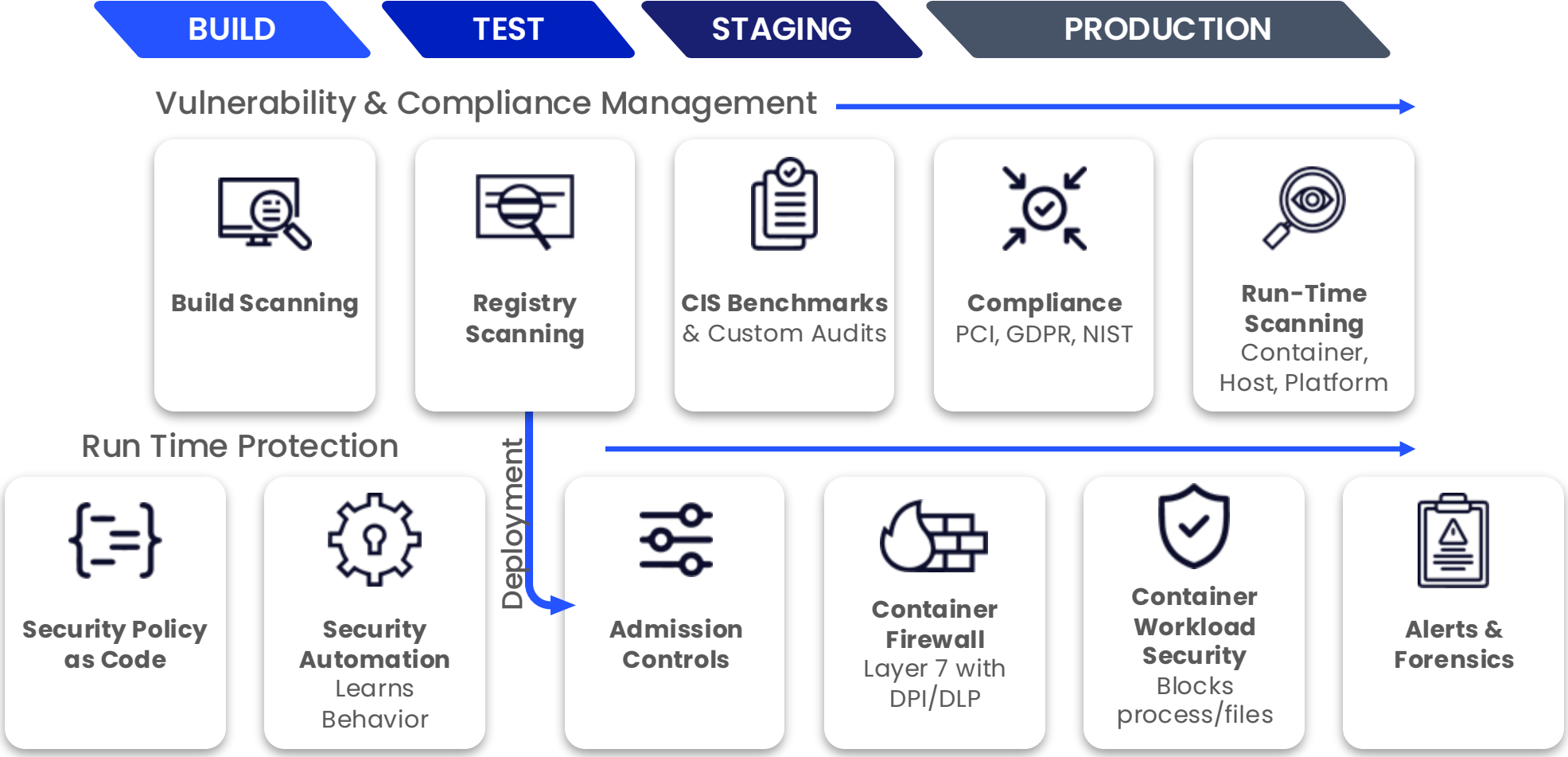
Available Anywhere and Everywhere



Understand Application Relationships



Secure the Pipeline and Runtime



Simplified, Batteries-Included Toolbox



How do get there?

Supply Chain – Sigstore Cosign Verification

The screenshot displays the 'Sigstore Verifiers' management interface. A modal window titled 'Add Signature Root of Trust' is open, allowing the user to add a new root of trust. The modal contains input fields for 'Name' and 'Comment', and radio buttons to select the 'Attribute' as either 'Private' or 'Public'. The 'Public' attribute is currently selected. Below the modal, a table lists existing verifiers.

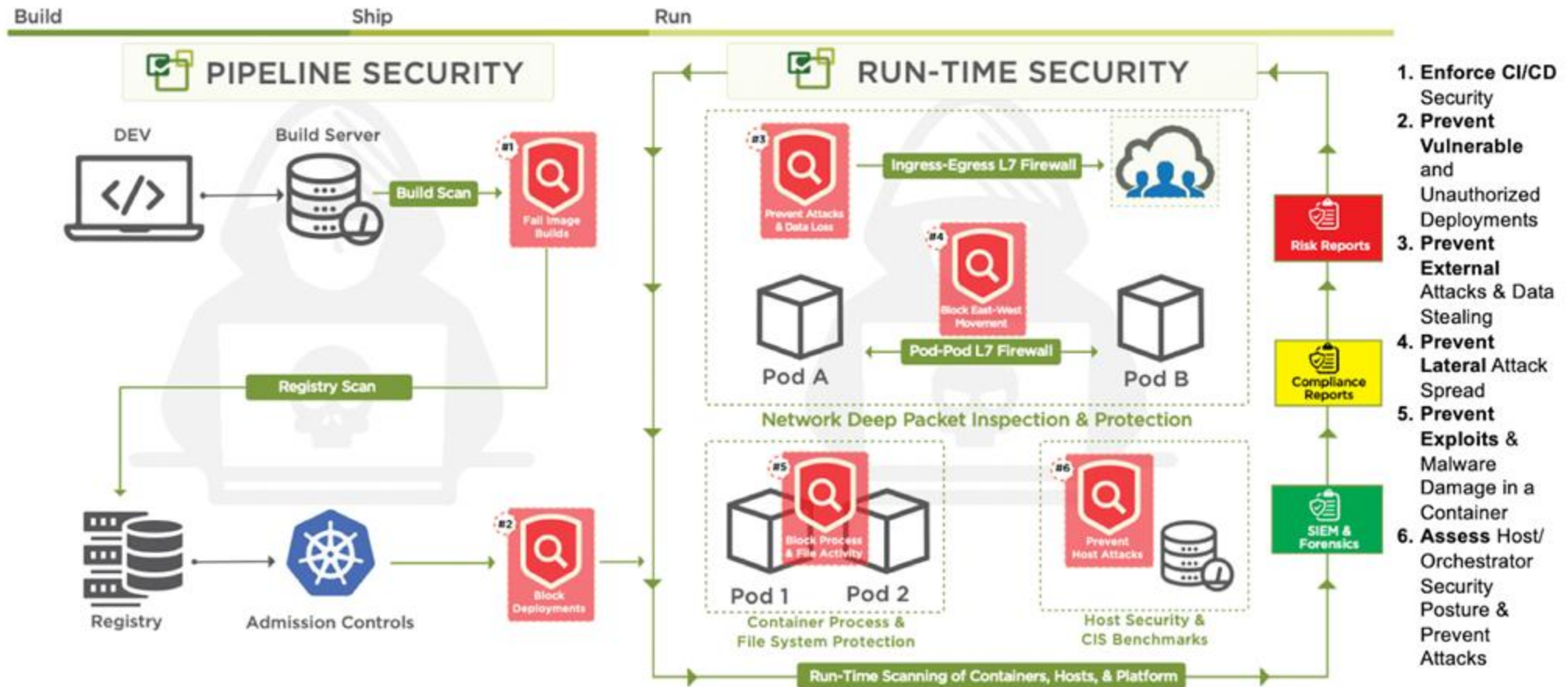
Sigstore Verifiers Table:

Sigstore Trust of Root Name	Comment	Attribute	Type
public_root_of_trust		Public	User Created
private-root-of-trust-v1	private root of trust	Private	User Created

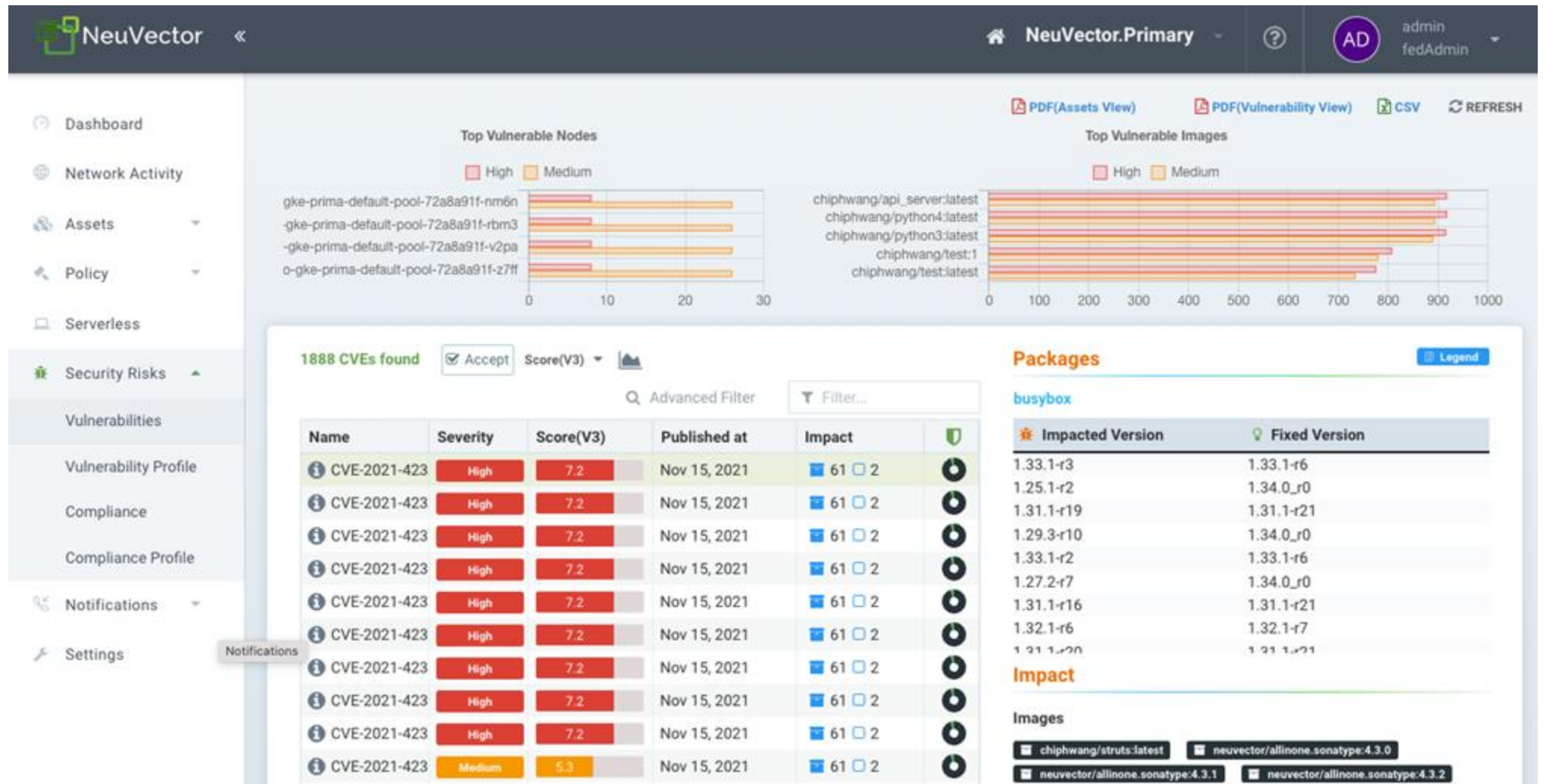
Verifiers Table (Visible Below Modal):

Verifier Name	Comment	Verifier Type	Public Key	Certificate Issuer	Certificate Subject
keyless-verifier	keyless-verifier	keyless		https://accounts.google.com	echen@gcpiz.geekos.io
keypair-verifier	keypair-verifier	keypair	-----BEGIN PUBLIC KEY-----...		

Pipeline Security



Vulnerability Scanning



Registry Scanning

Dashboard

Network activity

Assets

Platforms

Nodes

Containers

Registries

Controllers

Enforcers

Policy

Notifications

Settings

Registries

+ ADD REGISTRY

EDIT REGISTRY

DELETE REGISTRY

REFRESH

3 registries found

Filter...

Name	Registry	Filter	User name	Scan status	Queued	Finished	Failed
chip	https://registry.hub.docker.co	chiphwang/*	chiphwang	Idle	0	67	0
jfrog-xray	https://jfrogtraining-docker-nv	*	neuvector-user	Idle	0	4	0
nv-demo	https://registry.hub.docker.co	nvbeta/*	gkosaka	Idle	0	8	0

Start scan

Stop scan

https://registry.hub.docker.com/

Filter...

Repository	Tag	Image id	OS	Scan status	High	Medium	Scanned at
nvbeta/dns-client2	latest	bbaf66962c55...	ubuntu:14.04	Finished	41	619	Oct 31, 2019 07:40:35
nvbeta/dns_client2	latest	bbaf66962c55...	ubuntu:14.04	Finished	41	619	Oct 31, 2019 07:40:35
nvbeta/exploit_1_21	latest	151d24053798...	kali:2018.4	Finished	20	230	Oct 31, 2019 07:40:02
nvbeta/iodine	latest	beea85ab47d1...	ubuntu:18.04	Finished	0	15	Oct 31, 2019 07:38:53

Automated Runtime Scanning

Dashboard

Network activity

Assets

Platforms

Nodes

Containers

Registries

Controllers

Enforcers

Policy

Notifications

Settings

Containers

Auto scan ⓘ HIDE SYSTEM CONTAINER REFRESH

40 pods found

Filter...

Name	Namespace	Node name	Applications	State	Scan status	High	Medium	Scanned at
nginx-pod-6bbc5fb4c	demo	gke-chip-gke-1-default-p	HTTP, nginx	Monitor	Finished	0	0	Oct 15, 2019 17:25:45
nginx-pod	demo	gke-chip-gke-1-default-p	nginx	Monitor	Finished	157	440	Oct 15, 2019 17:25:52
node-pod-77756f657	demo	gke-chip-gke-1-default-p	HTTP	Protect	Finished	0	0	Oct 15, 2019 17:25:46
node-pod	demo	gke-chip-gke-1-default-p	TCP/8888	Protect	Finished	65	527	Oct 15, 2019 17:25:37
node-pod-77756f657	demo	gke-chip-gke-1-default-p	HTTP	Protect	Finished	0	0	Oct 15, 2019 17:25:40

CONTAINER DETAILS

COMPLIANCE

VULNERABILITIES

PROCESS

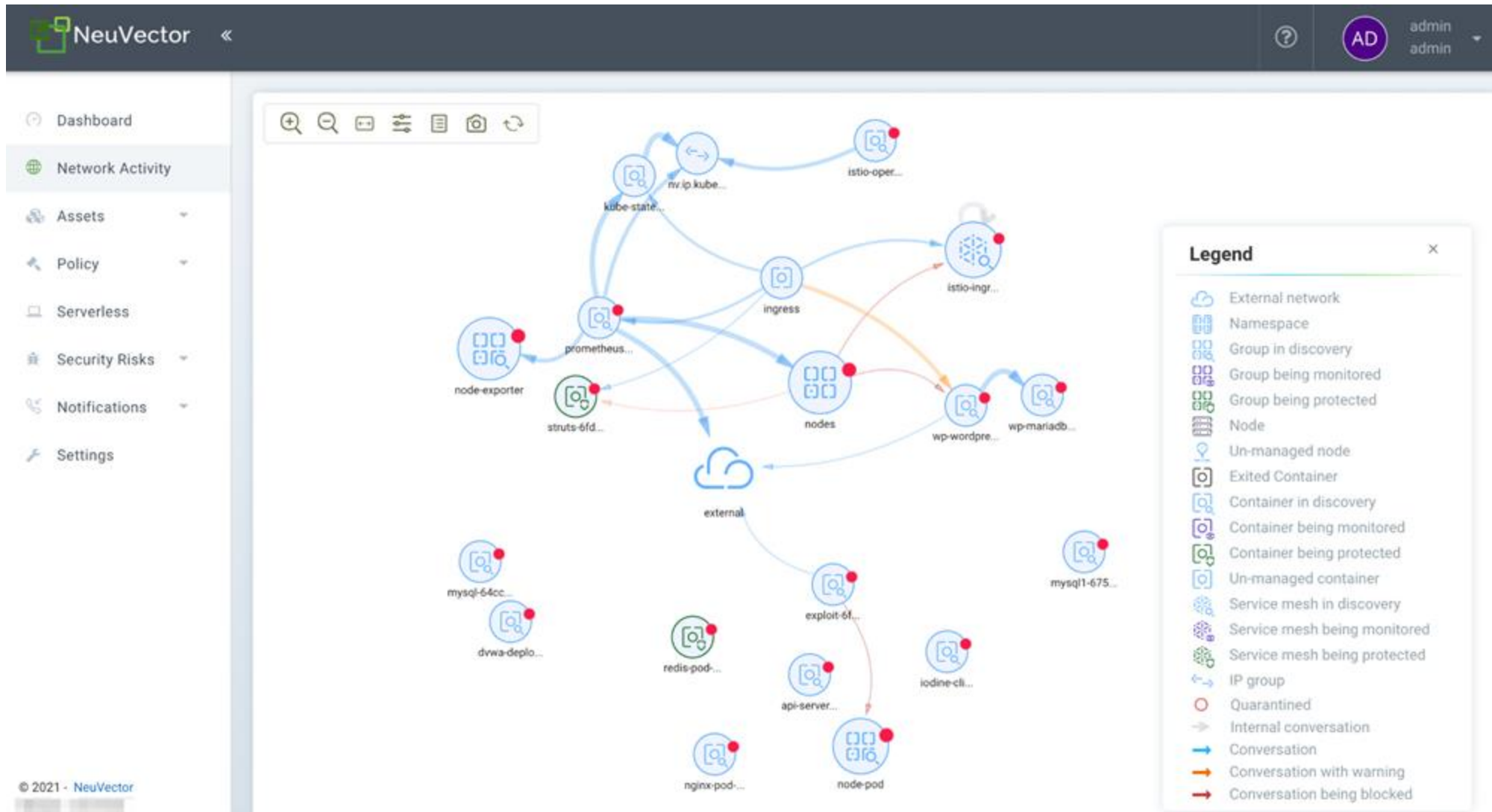
CONTAINER STATS

CVE DB Version 1.655

DOWNLOAD CSV SCAN Filter...

Name	Urgency	Score(V3)	Package	Version	Fixed version
CVE-2017-5754	High	4.7(5.6)	linux-libc-dev	3.13.0-125.174	3.13.0-139.188
CVE-2019-3462	High	9.3(8.1)	apt	1.0.1ubuntu2.14	1.0.1ubuntu2.19
CVE-2016-1252	High	4.3(5.9)	apt	1.0.1ubuntu2.14	1.0.1ubuntu2.17
CVE-2019-3462	High	9.3(8.1)	apt-transport-https	1.0.1ubuntu2.17	1.0.1ubuntu2.19

Network Activity



Network Security Rules

NeuVector

IKS-1

AD

admin

Dashboard

Network Activity

Assets

Policy

Admission Control

Groups

Network Rules

Response Rules

DLP Sensors

WAF Sensors

Serverless

Security Risks

Notifications

Settings

Groups

51 groups found Selected Group: 1 Add

EXPORT GROUP POLICY SWITCH MODE SCORABLE Filter...

Name	Namespace	Policy Mode	Type	Memb	Discover	Monitor	Protect	Response Rules
☐ nv.metrics-server.kube-system	kube-system	Discover	Learned	1				0
☐ nv.mysql1.demo	demo	Discover	Learned	1				0
☐ nv.nginx-pod.demo	demo	Discover	Learned	1	9			0
☒ nv.node-pod.demo	demo	Discover	Learned	3	10			0
☐ nv.olm-operator.ibm-system	ibm-system	Discover	Learned	1	1			0
☐ nv.prometheus.istio-system	istio-system	Discover	Learned	1	34			0
☐ nv.public-crbtmimbaw08dig9ddjo80-alb1.kube-system	kube-system	Discover	Learned	2	4			0
☐ nv.redis-pod.demo	demo	Discover	Learned	1	12			0

nv.node-pod.demo

MEMBERS CUSTOM CHECK PROCESS PROFILE RULES FILE ACCESS RULES NETWORK RULES RESPONSE RULES DLP WAF

Filter...

ID	From	To	Applications	Ports	Action	Type	Updated at
10428	nodes	nv.node-pod.demo	HTTP	any	Allow	Learned	Jan 06, 2022 12:42:35
10431	nv.node-pod.demo	nv.istiod.istio-system	any	tcp/15012	Allow	Learned	Jan 06, 2022 12:42:35
10434	nv.prometheus.istio-system	nv.node-pod.demo	any	tcp/15020	Allow	Learned	Jan 06, 2022 12:42:35
10435	nv.node-pod.demo	nv.coredns.kube-system	DNS	any	Allow	Learned	Jan 06, 2022 12:42:35
10494	nv.node-pod.demo	nv.redis-pod.demo	any	tcp/6379	Allow	Learned	Jan 06, 2022 12:42:35
10504	nv.node-pod.demo	nv.istiod.istio-system	SSL	any	Allow	Learned	Jan 06, 2022 12:51:00

Federation Management

Federation Management

REFRESH

Name	Type	Server	Port	Hosts	Running Pods	CVE DB Version	Score	Status	Action
GKE-ONE	Master	130.211.209.91	11443	5	48	2.237	58 POOR	ACTIVE	  
IBM-NV-SE-Demo-Toror	Managed	169.55.189.171	10443	4	64	2.237	42 FAIR	SYNCED	   
aks-remote	Managed	104.209.44.237	10443	3	24	2.237	42 FAIR	SYNCED	   

GKE-ONE

Platform
Kubernetes

Hosts
5

Controllers
3

CVE DB Version
2.237

Namespaces
7

Running Pods
48

Enforcers
5

Services
29

Total Workloads
124

Scanners
3

Web Application Firewall (WAF)

WAF Sensors

IMPORT
 EXPORT
 REFRESH

5 WAF sensors found
 Add

Sensor Name	Comment	Groups	Type	
☐ glen-test	test		CRD	
☐ sensor.cross	to detect cross site scripting attempt	demo-group	CRD	
☒ sensor.execution	arbitrary command execution attempt	demo-group	CRD	
☐ sensor.injection	to detect injection attempt	demo-group	CRD	
☐ sensor.traversal	to detect directory traversal attempt	demo-group	CRD	

sensor.execution

Rule Name	
Alchemy	
CCBill	
DotNetNuke	
HNAP	
Log4j	

Have/Not have	Pattern	Context
Have	\\$\{\{((\\${\ \\s lower upper \:- \\})*[jJ](\\${\ \\s lower upper \:- \\})*[nN](\\${\ \\s lower upper \:- \\})*[dD](\\${\ \\s lower upper \:- \\}) header	

Data Loss Prevention (DLP)

NeuVector

IKS-1

AD

admin

admin

Dashboard

Network Activity

Assets

Policy

Admission Control

Groups

Network Rules

Response Rules

DLP Sensors

WAF Sensors

Serverless

Security Risks

Notifications

Settings

DLP Sensors

2 DLP sensors found

Add

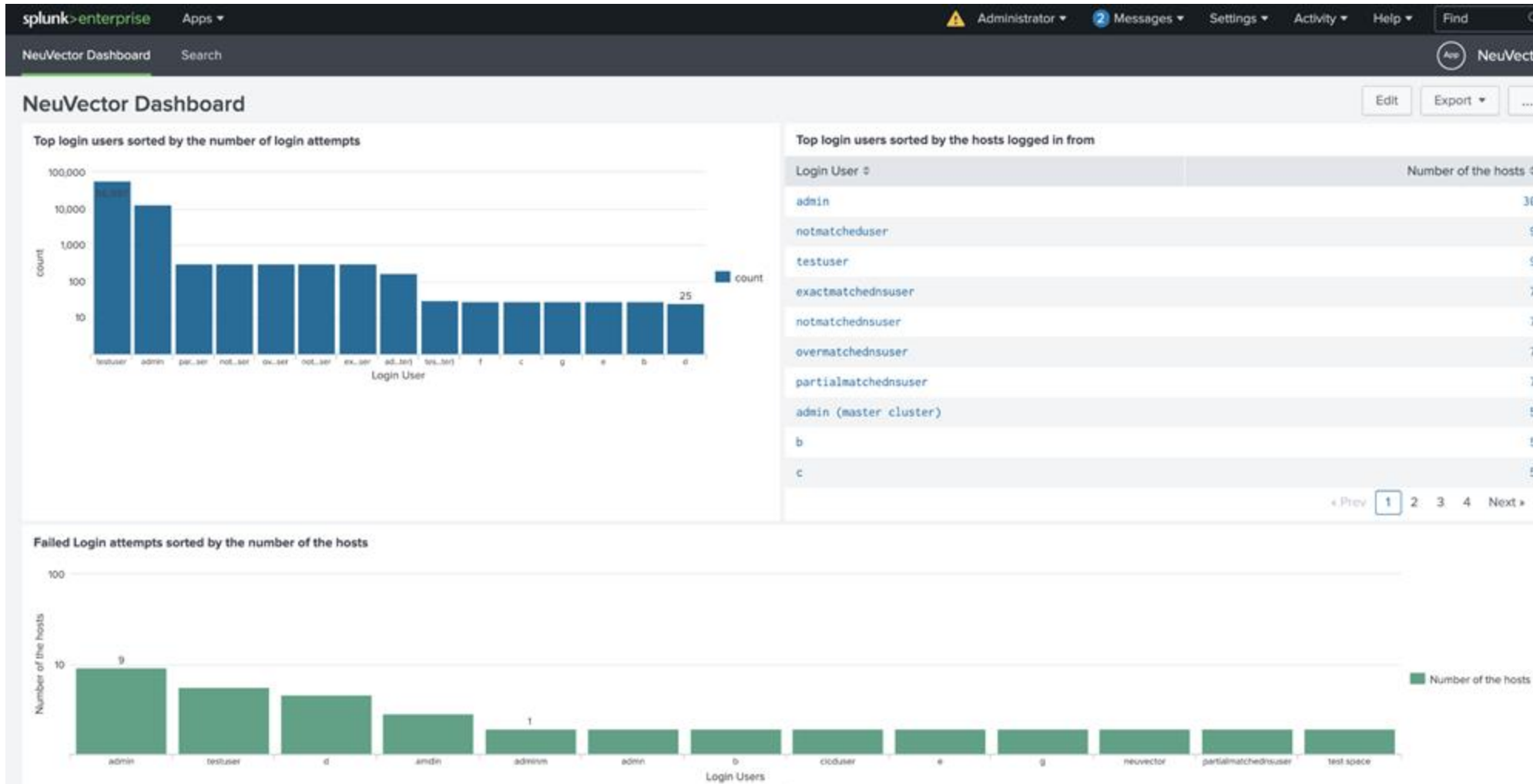
Filter...

Sensor Name	Comment	Groups
sensor.creditcard	Sensor for Credit Card detection, Credit Card includes visa, master, discover, american express, diner and jcb	
sensor.ssn	Sensor for SSN detection	

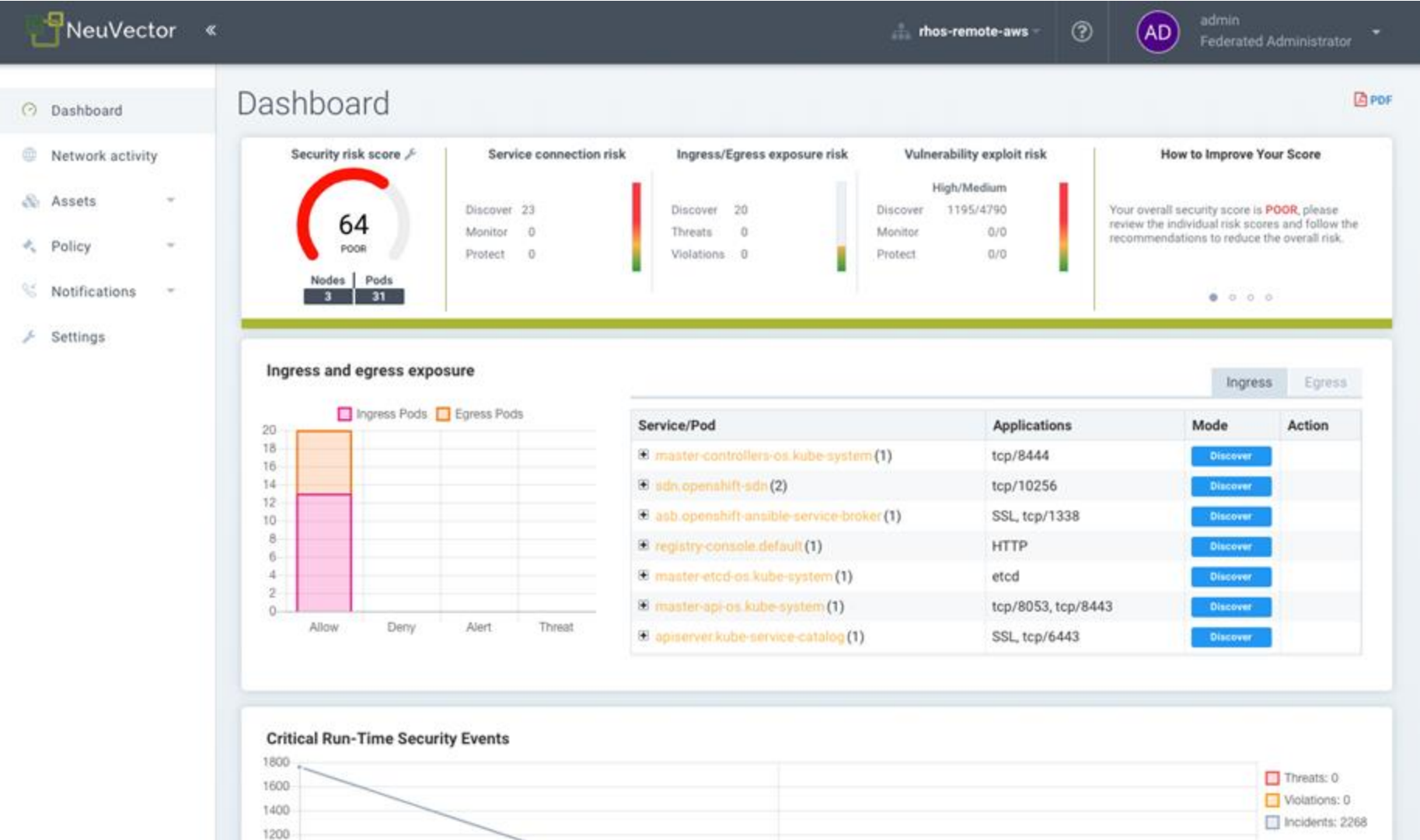
sensor.creditcard

Rule Name	Have/Not have	Pattern	Context
rule.americanexpress	Have	\b3[47]\d{2}([])?(\d{5} 123456 234567 345678)\d{6}\1(?!(\d{3} 12345 56789)\d{5})\b	body
rule.diner1			
rule.diner2			
rule.discover			
rule.jcb			
rule.master			
rule.visa			

Integrations – Trust but Verify



RGS Security (NeuVector)



Thank You
