#1876

vmware EXPLORE 2022

Apply End-to-End Networking Security in Multi-Cloud for VMware Tanzu Users

Level 200

Tuan Nguyen & Stéphane List & Santosh Patel

Networking and Advanced Security Business Group, VMware

#vmwareexplore #1876

https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

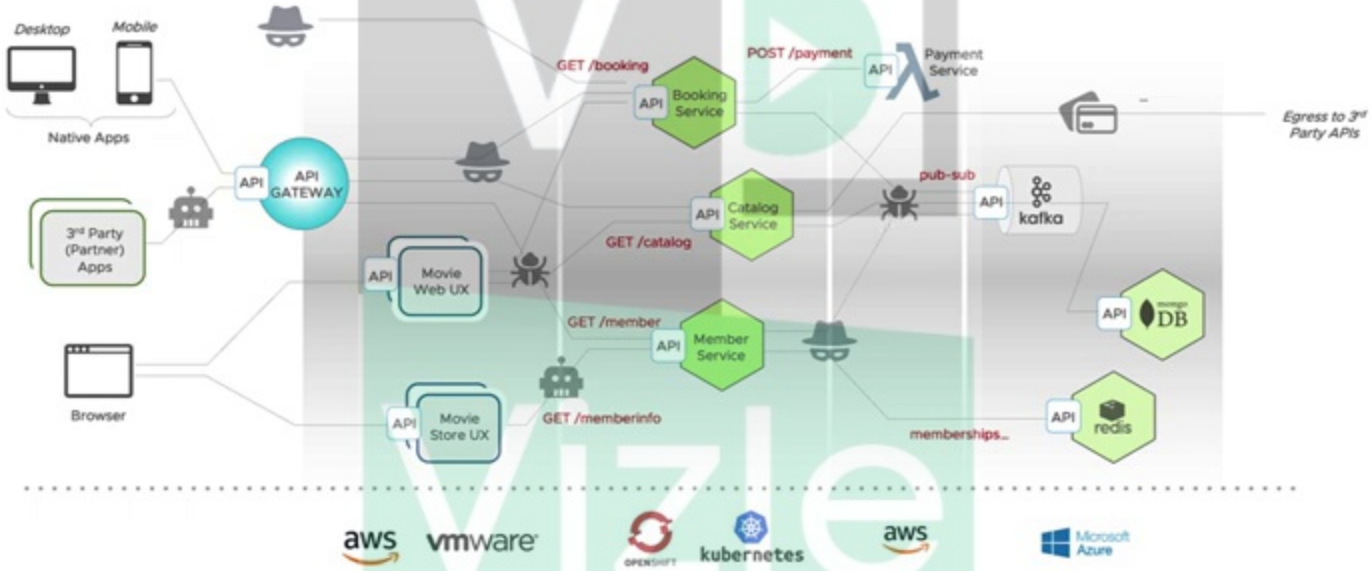
- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

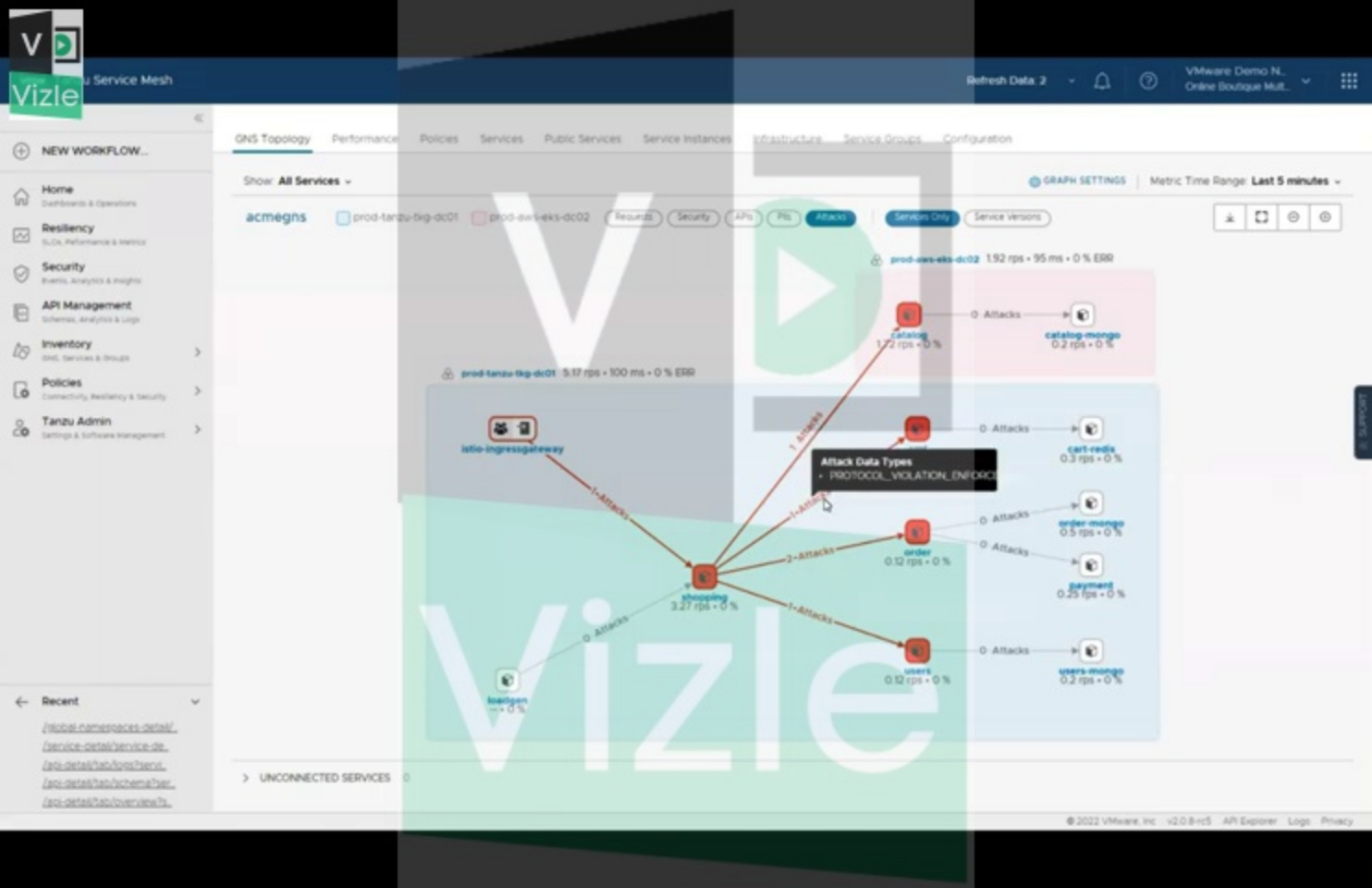
Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*

Modern Apps = Mesh of Services & APIs

APIs are a critical part of Modern Applications




Service Mesh
Refresh Data: 2
VMware Demo N..
Online Boutique Mult..
NEW WORKFLOW...
Home
Dashboards & Operations
Resiliency
SLOs, Performance & Metrics
Security
Events, Analytics & Insights
API Management
Schemas, Analytics & Logs
Inventory
DNS, Services & Groups
Policies
Connectivity, Resiliency & Security
Tanzu Admin
Settings & Software Management
Recent
GNS Topology
Performance
Policies
Services
Public Services
Service Instances
Infrastructure
Service Groups
Configuration
Show: All Services
GRAPH SETTINGS
Metric Time Range: Last 5 minutes
acmegns
prod-tanzu-tkg-dc01
prod-aws-eks-dc02
Requests
Security
APIs
Pls
Attacks
Services Only
Service Versions
prod-aws-eks-dc02 1.92 rps • 95 ms • 0 % ERR
catalog
1.72 rps • 0 %
0 Attacks
catalog-mongo
0.2 rps • 0 %
prod-tanzu-tkg-dc01 5.17 rps • 100 ms • 0 % ERR
istio-ingressgateway
1 Attacks
0 Attacks
cart-redis
0.3 rps • 0 %
Attack Data Types
• PROTOCOL_VIOLATION_ENFORCE
1 Attacks
0 Attacks
order-mongo
0.5 rps • 0 %
2 Attacks
order
0.12 rps • 0 %
0 Attacks
payment
0.25 rps • 0 %
shopping
3.27 rps • 0 %
1 Attacks
0 Attacks
users
0.12 rps • 0 %
0 Attacks
users-mongo
0.2 rps • 0 %
loadgen
0 %
UNCONNECTED SERVICES
SUPPORT
© 2022 VMware, Inc
v2.0.8-rc5
API Explorer
Logs
Privacy

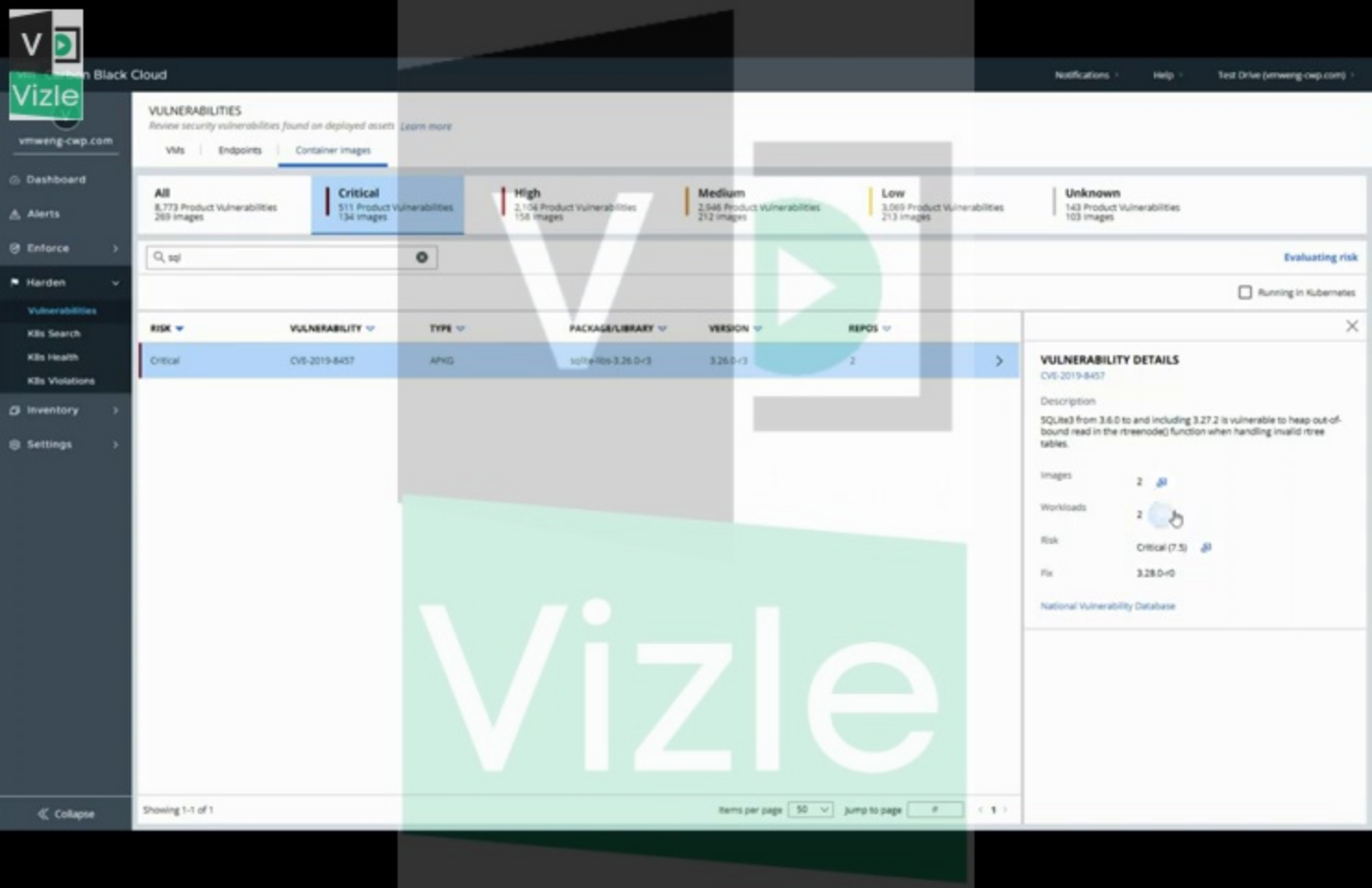
Admission Controller and Workload Hardening

- Admission Controllers Apply Policy to K8S Resource Definitions
- Validating ACs can deny the deployment of resources
- Mutating ACs can modify resources before deployment to conform with policy

K8S provides a basic built-in security admission controller

```
apiVersion: apiserver.config.k8s.io/v1
kind: AdmissionConfiguration
plugins:
- name: PodSecurity
  configuration:
    apiVersion: pod-security.admission.config.k8s.io/v1beta1
    kind: PodSecurityConfiguration
    defaults:
      enforce: "baseline"
      enforce-version: "latest"
      warn: "restricted"
      warn-version: "latest"
    exemptions:
      # Array of authenticated usernames to exempt.
      usernames: []
      # Array of runtime class names to exempt.
      runtimeClasses: []
      namespaces: ["kube-system"]
```

```
apiVersion: v1
kind: Namespace
metadata:
  name: test-ns
  labels:
    pod-security.kubernetes.io/enforce: baseline
    pod-security.kubernetes.io/audit: restricted
    pod-security.kubernetes.io/warn: restricted
```


Black Cloud
Notifications
Help
Test Drive (vmweng-cwp.com)
vmweng-cwp.com
Dashboard
Alerts
Enforce
Harden
Vulnerabilities
K8s Search
K8s Health
K8s Violations
Inventory
Settings
Collapse
VULNERABILITIES
Review security vulnerabilities found on deployed assets Learn more
VMs
Endpoints
Container images
All
8,773 Product Vulnerabilities
269 Images
Critical
511 Product Vulnerabilities
134 Images
High
2,104 Product Vulnerabilities
158 Images
Medium
2,946 Product Vulnerabilities
212 Images
Low
3,069 Product Vulnerabilities
213 Images
Unknown
143 Product Vulnerabilities
103 Images
sql
Evaluating risk
Running in Kubernetes
RISK
VULNERABILITY
TYPE
PACKAGE/LIBRARY
VERSION
REPOS
Critical
CVE-2019-8457
APKG
sqlite-libs-3.26.0-r3
3.26.0-r3
2
VULNERABILITY DETAILS
CVE-2019-8457
Description
SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.
Images
2
Workloads
2
Risk
Critical (7.5)
Fix
3.28.0-r0
National Vulnerability Database
Showing 1-1 of 1
Items per page
50
Jump to page
1

https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*