BEST PRACTICES FOR IMPLEMENTING SECURITY IN AZURE

Stuart Green | Cloud Security Architect UK&I

Agenda

- Introduction to Check Point
- Securing Azure with Check Point
- Cloud Security Blueprint:
  - Concepts and Principles
  - Architectures and Solutions

25 Years of Recognition

Network: 20th time Security Leader in Magic Quadrant

Network: Customers' Choice for Unified Threat Management

Network: Highest cyber prevention score in NGFW

Endpoint: Top Product Scoring: 17.5 / 18

Endpoint: A leader in Endpoint Security

Mobile: Highest Mobile security value

Cloud: Dome9, a cool vendor in Cloud Security

Partnership with Microsoft

- One of Microsoft's **top Security ISVs WW in FY19**
- 2 **Marketplace** Offerings
- **M**icrosoft **I**ntelligent **S**ecurity **A**ssociation member
- Integrations with **Azure Security Center** and **Azure Sentinel**
- **First Security Vendor** for **Azure Stack**

Microsoft Azure Certified

Available on Microsoft Azure Marketplace

Member of Microsoft Intelligent Security Association

Microsoft

Best Practices for Architecting on Azure

Cloud advantages

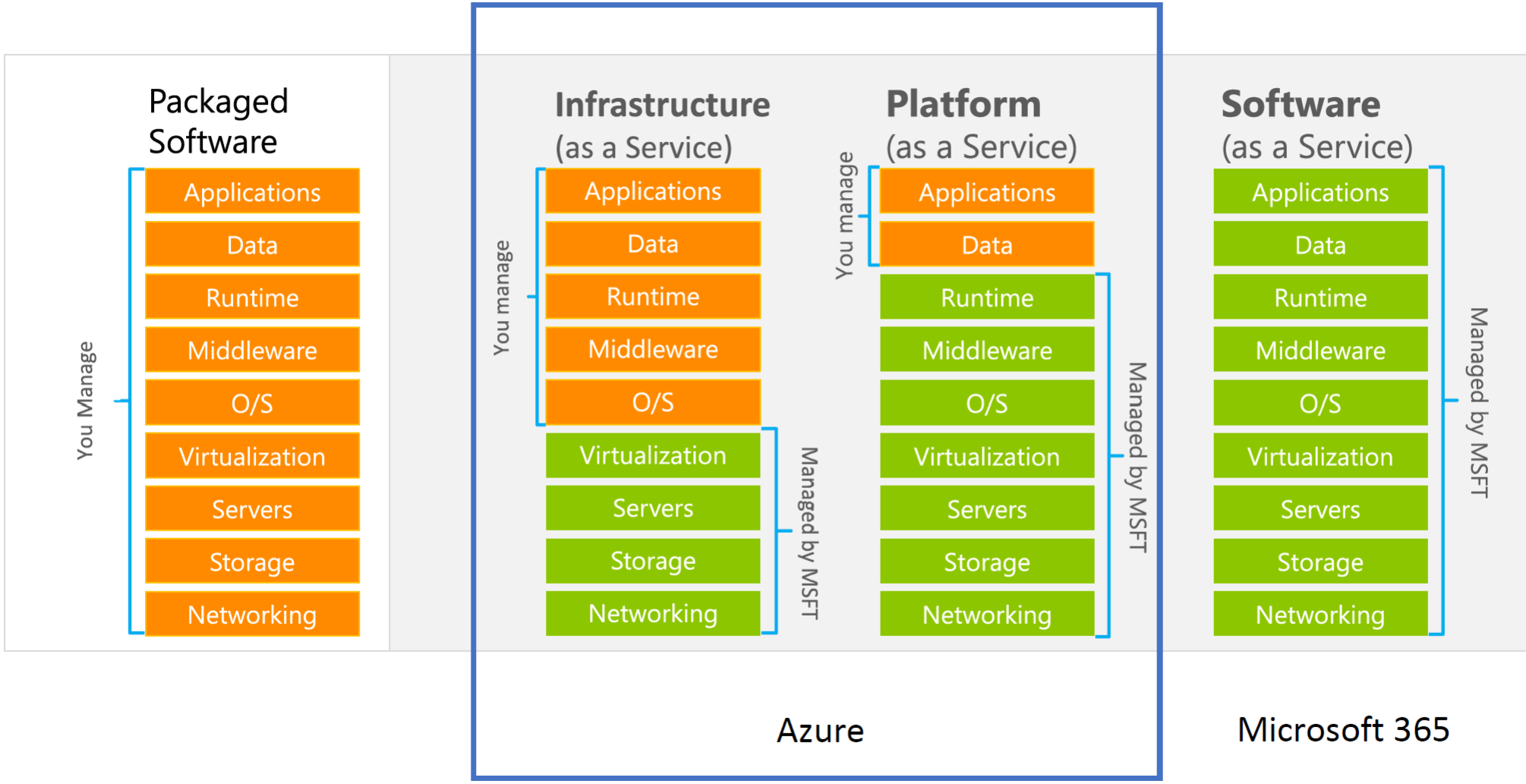
Agility — Faster time to market

Availability — Service backed by SLA
Redundancy across regions

Scalability — Ability to scale to demand
Scale up or down quickly

Cost Effecient — Pay as you go
Services provided at scale to enable low cost to customers

IaaS Overview

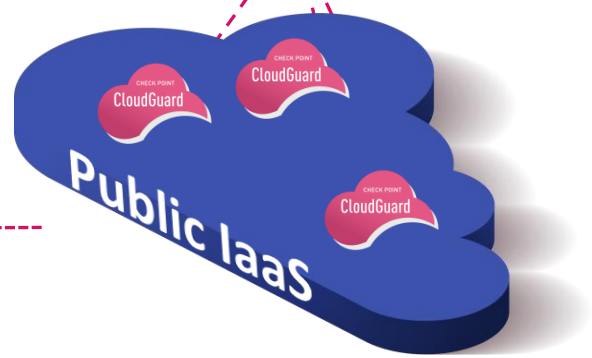


CloudGuard IaaS Portfolio

CloudGuard Gateway With NGTX

CloudGuard Controller Management

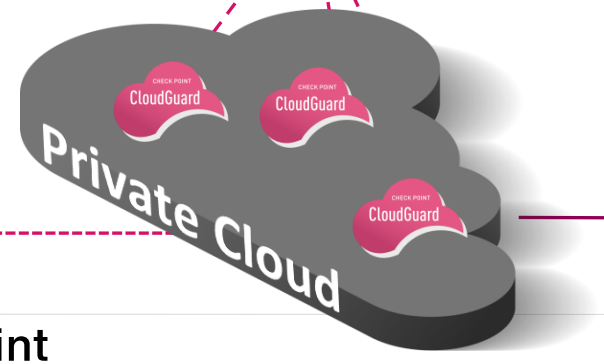
- AWS
- Azure
- GCP
- Alibaba Cloud
- Oracle



Mgmt.

Mgmt.

- ESX
- Hyper-V
- KVM



SDN Integration

- AzureStack
- NSX
- ACI
- OpenStack

- vCenter
- NSX Manager
- OpenStack
- AzureStack
- Cisco APIC
- AWS
- Azure
- Google Cloud

Deployment Options

Azure Marketplace

- + Low effort
- + Up and running in a few clicks
- + Good for one-off deployments

- - Less customisation options
- - Not ideal for automated, repeated deployments

Template

- + Rapid deployment of customised environments.
- + Configure once, deploy many
- + Highly customisable

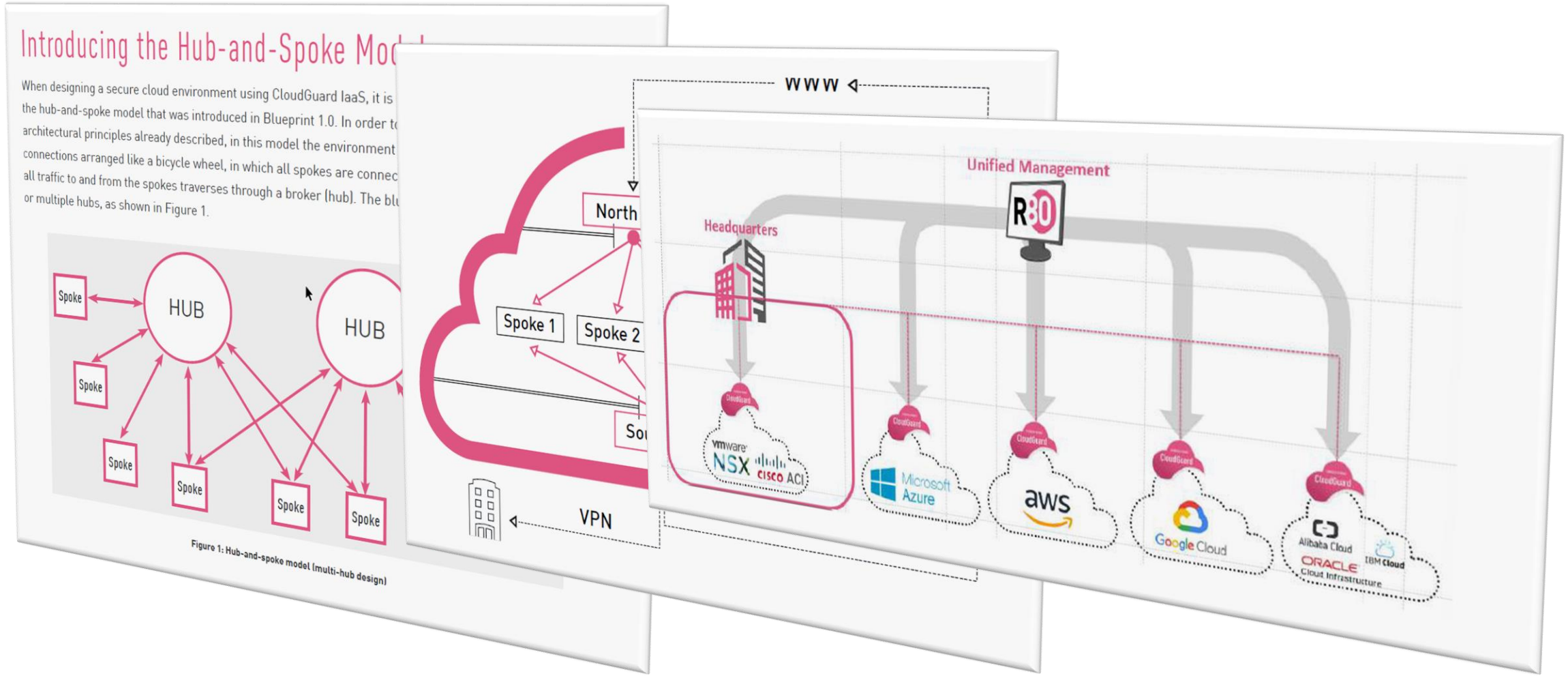
- - Tricky for beginners
- - Config overheads outweigh benefits for small deployments

Powershell / CLI

- + Ideal for IaaC / devops deployments
- + Perfect for automation
- + Policy management via API too

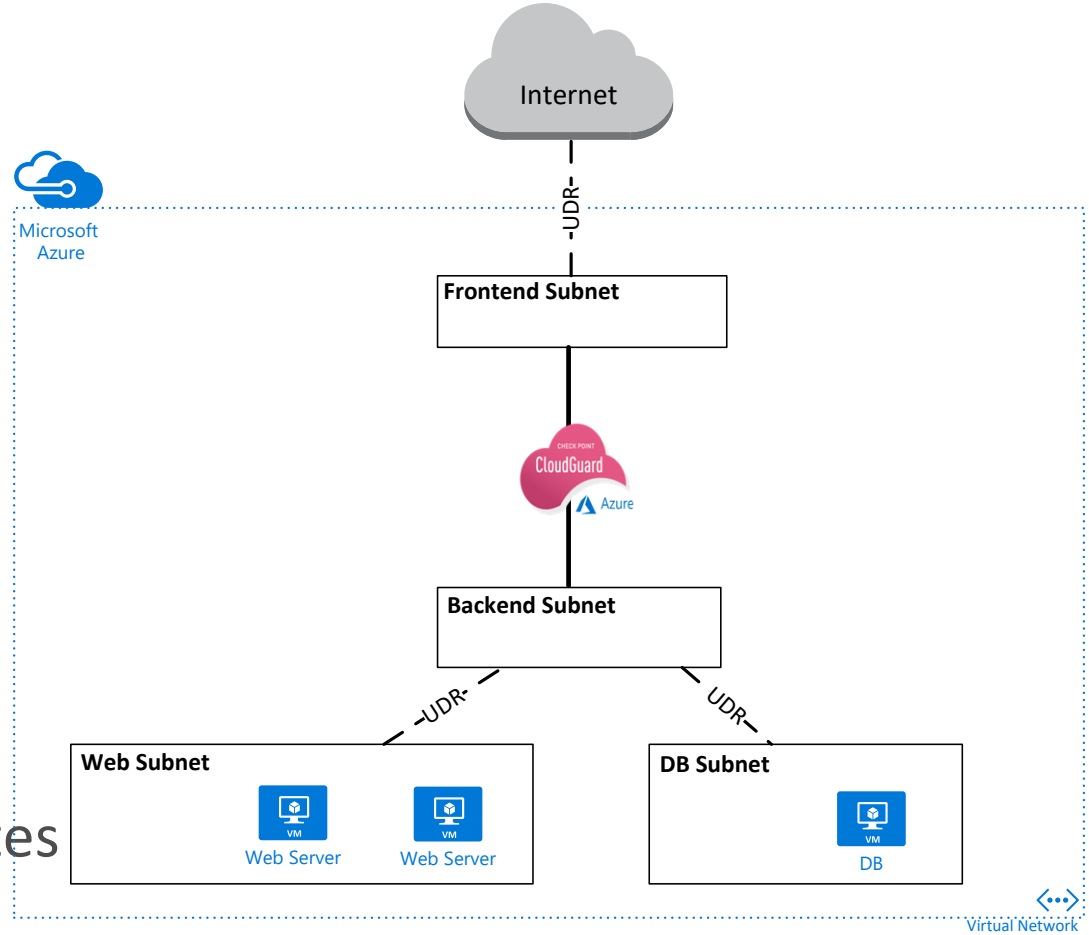
- - Tricky for beginners
- - Config overheads outweigh benefits for small deployments

Check Point Cloud Security Blueprint



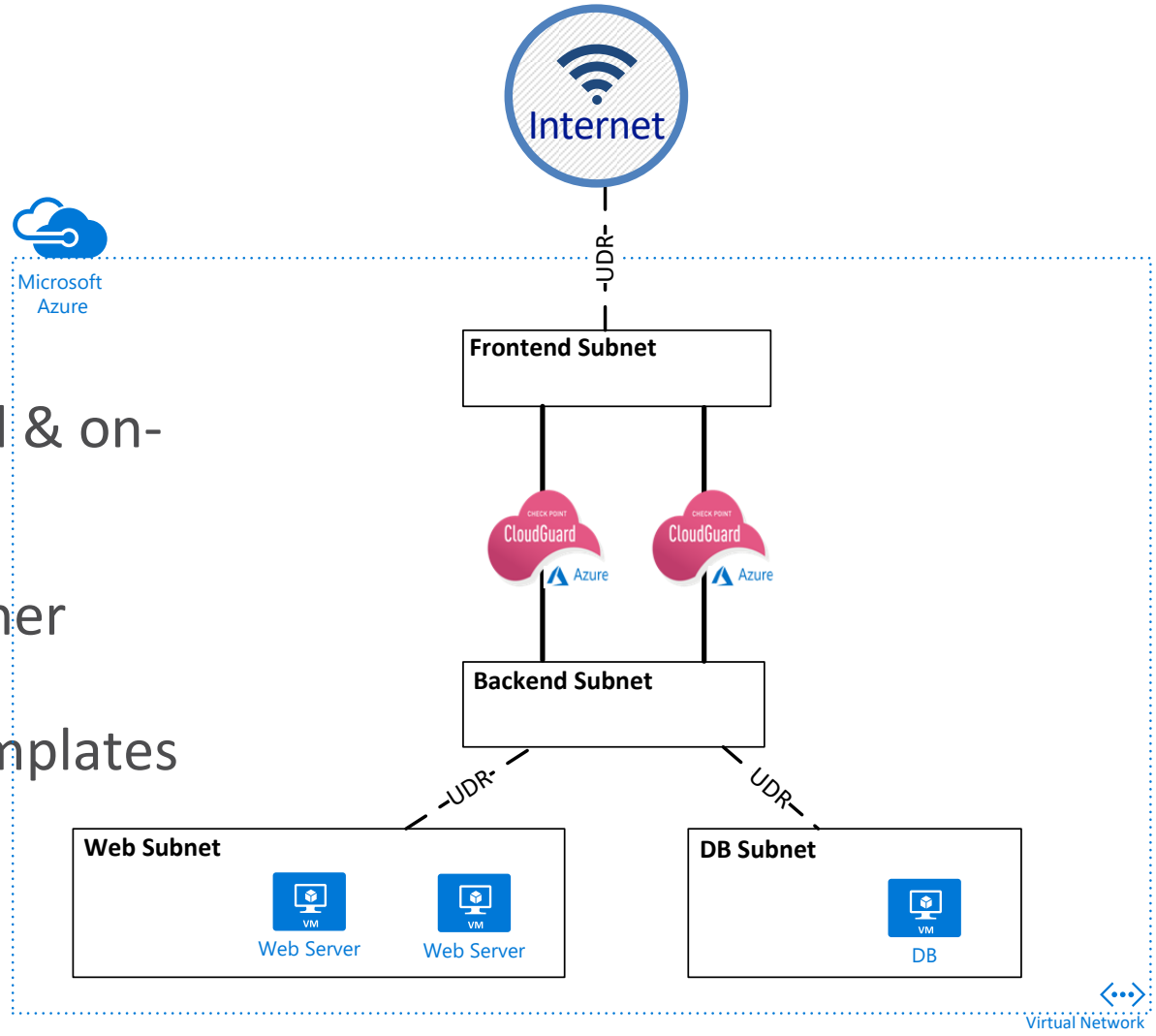
Architectures – Single gateway / standalone.

- Small deployment adjusted to specific applications
- R80 management with adaptive policy for cloud & on-premise
- Acts as perimeter & Datacenter Gateway together
- Automated deployment with Azure solution templates



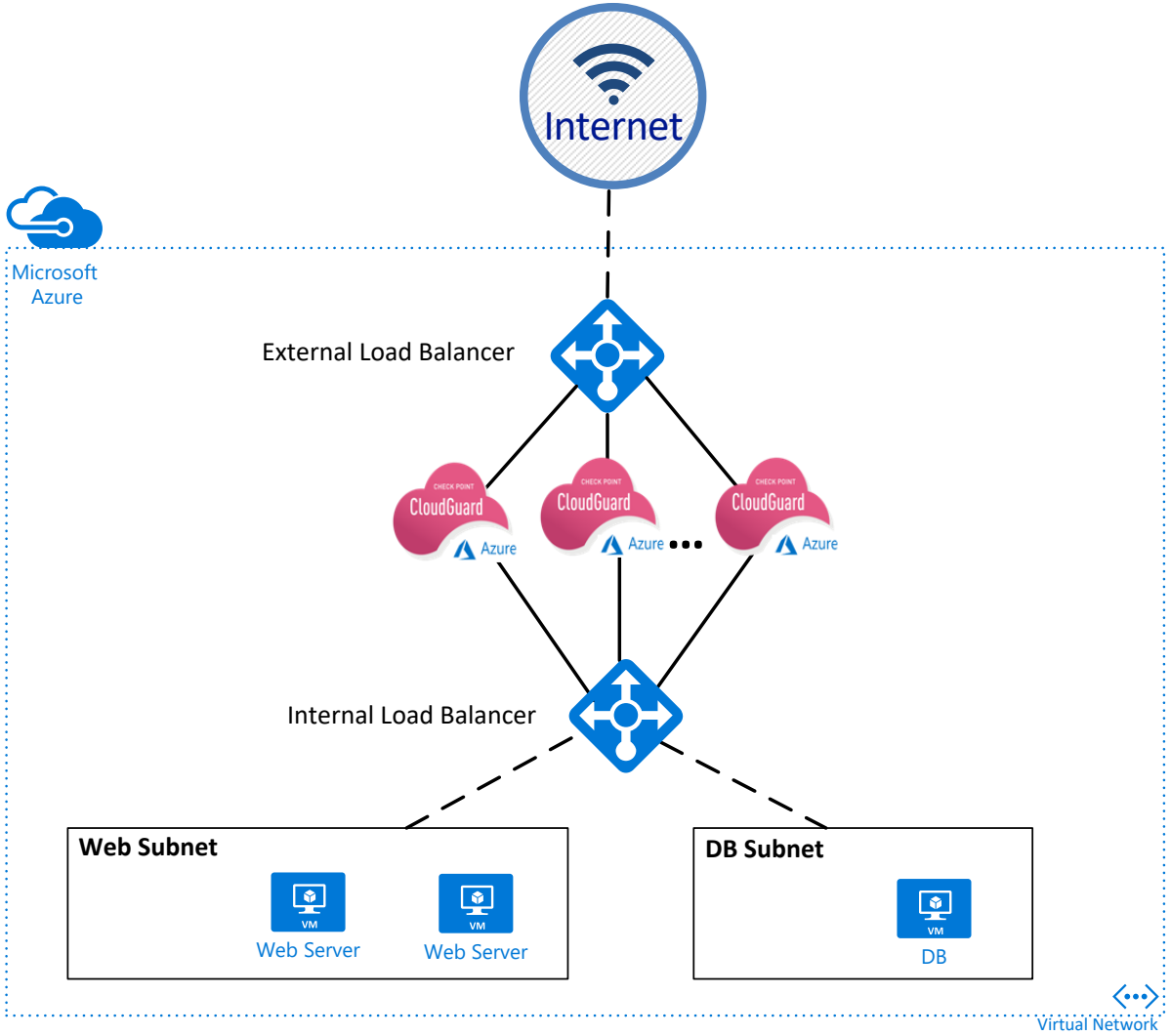
Architectures – High Availability

- Small – medium deployments.
  Dedicated management recommended
- R80 management with adaptive policy for cloud & on-premise
- Acts as perimeter & Datacenter Gateway together
- Automated deployment with Azure solution templates
- For customers that require HA with availability sets / zones



Architectures – Virtual Machine Scale Sets (VMSS)

- Scales dynamically based on custom metrics (CPU, network, schedule)
- Allows dynamic security inline with elastic workloads
- Reduced operational costs (PAYG Licensing)



Licensing options

YEARLY

Sold through Check Point and Partners

CloudGuard Gateway

NGTP	NGTX
Virtual Core / year	Virtual Core / year

Incl. Product, Subscriptions & Support

Microsoft Hyper-V · vmware vSphere · KVM · aws · Microsoft Azure · Google Cloud Platform

PER HOUR (Pay-As-You-Go)

Sold through marketplaces

Cloudguard Gateway (starting from)

NGTP	NGTX
$/h	$/h

Incl. Product, Subscriptions & Support

aws · Microsoft Azure · Google Cloud Platform

Smart Center[1]

5-GW	25-GW
$/h	$/h

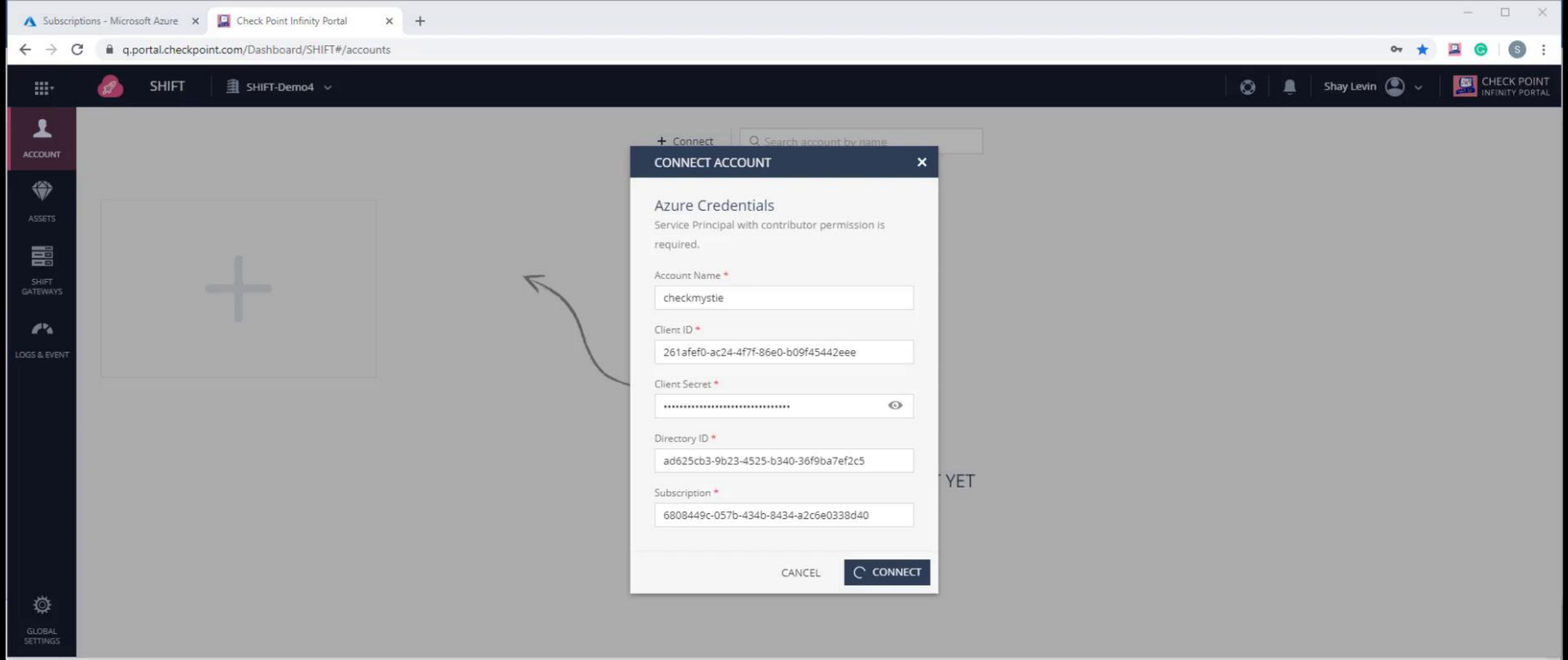
Incl. SmartEvent and Compliance blades & Support

aws · Microsoft Azure · Google Cloud Platform

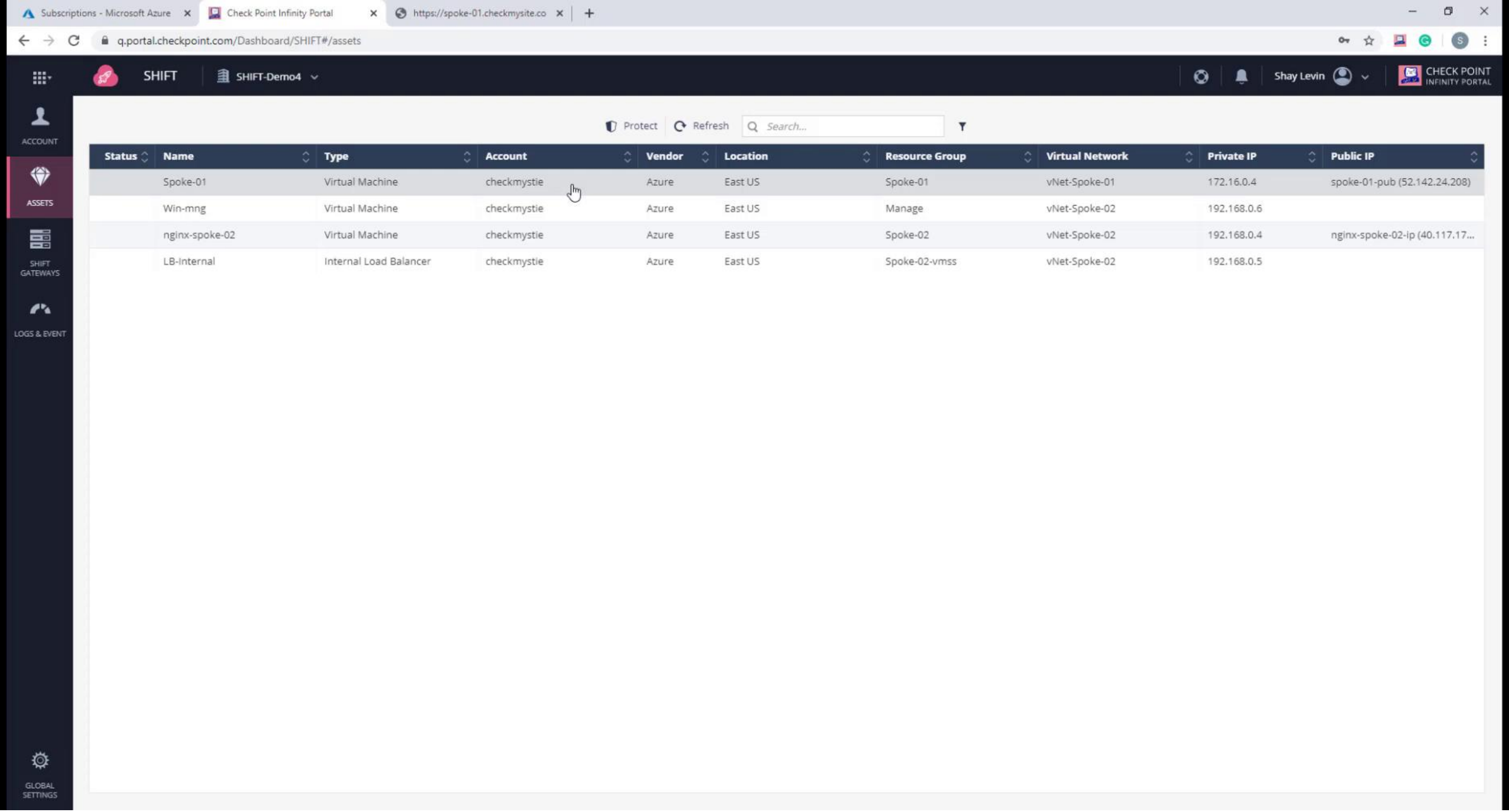
CloudGuard Express

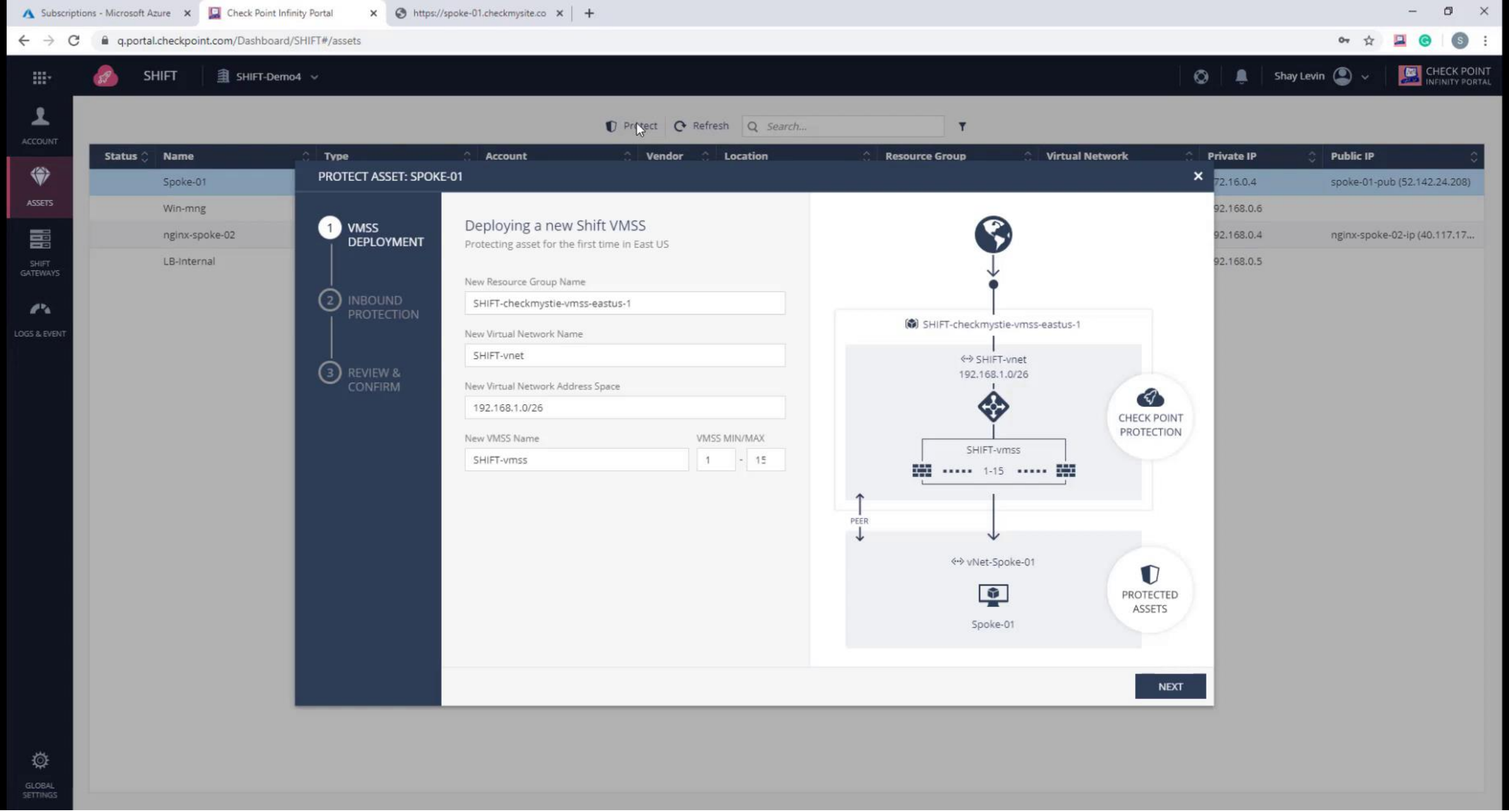
- Simple IaaS deployment – made simpler!
- Select your assets, deploy and go!
- API driven
- Part of the Check Point Infinity Portal

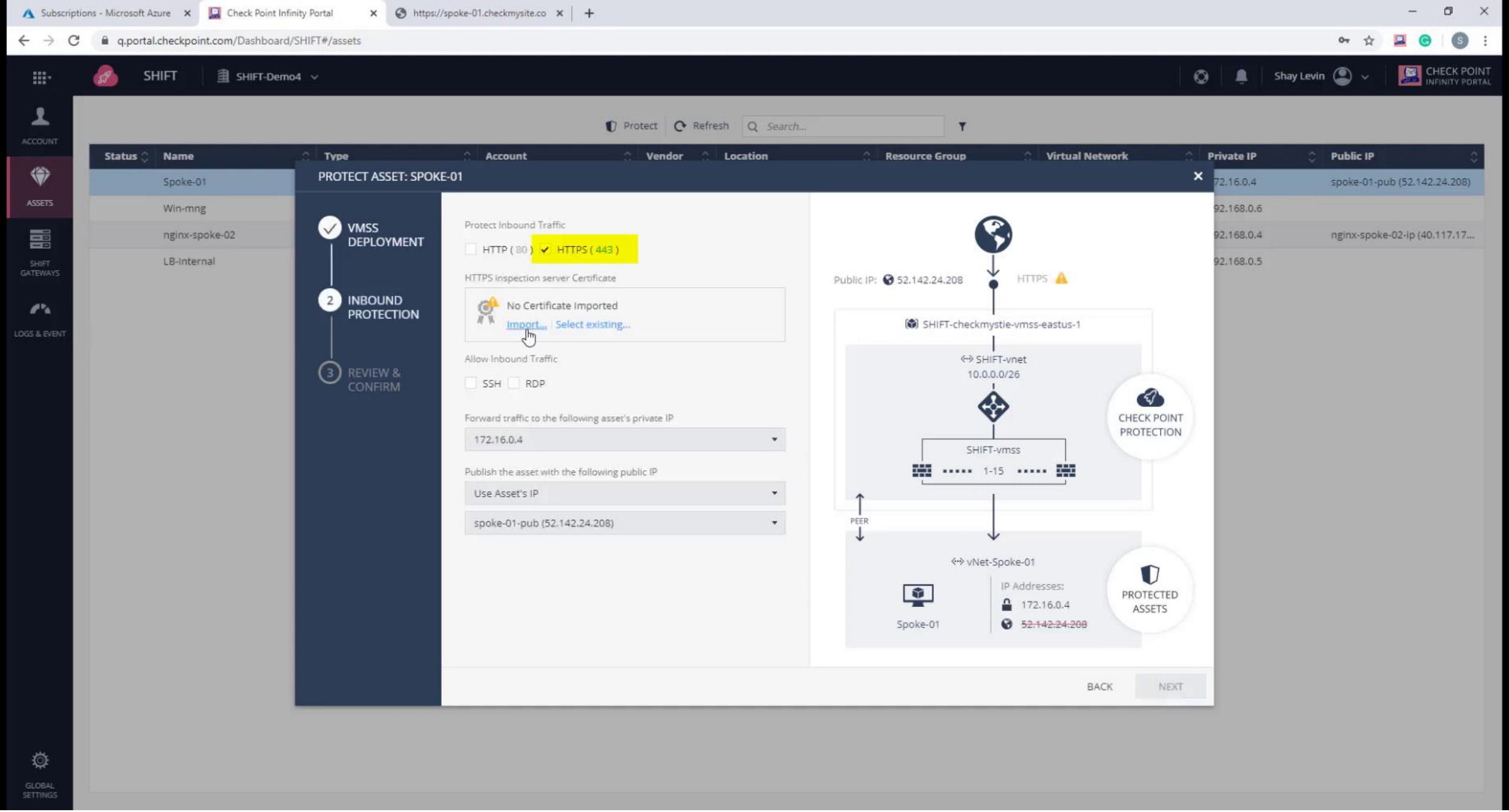
- Currently in EA – contact us if you would like to try!

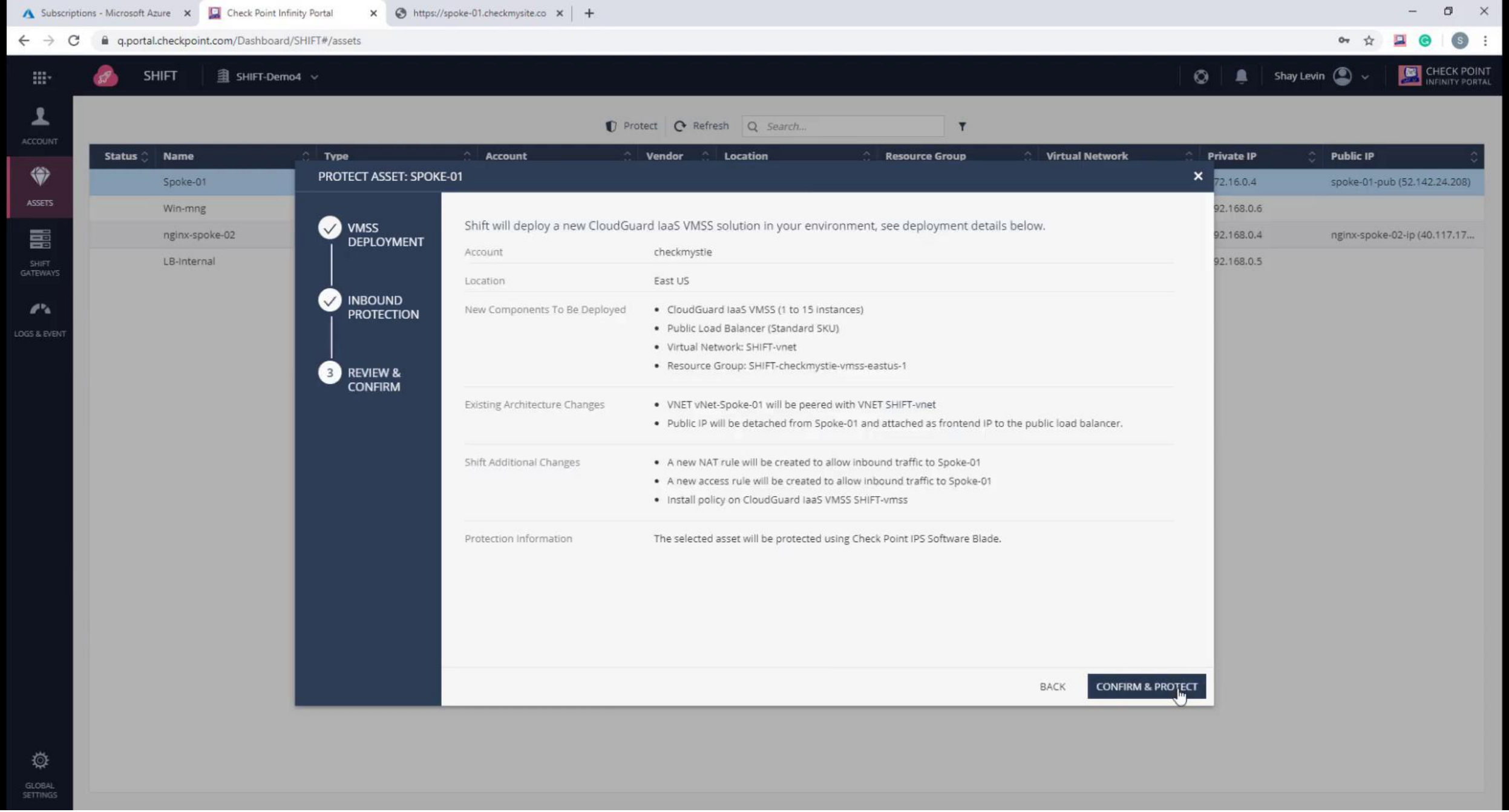


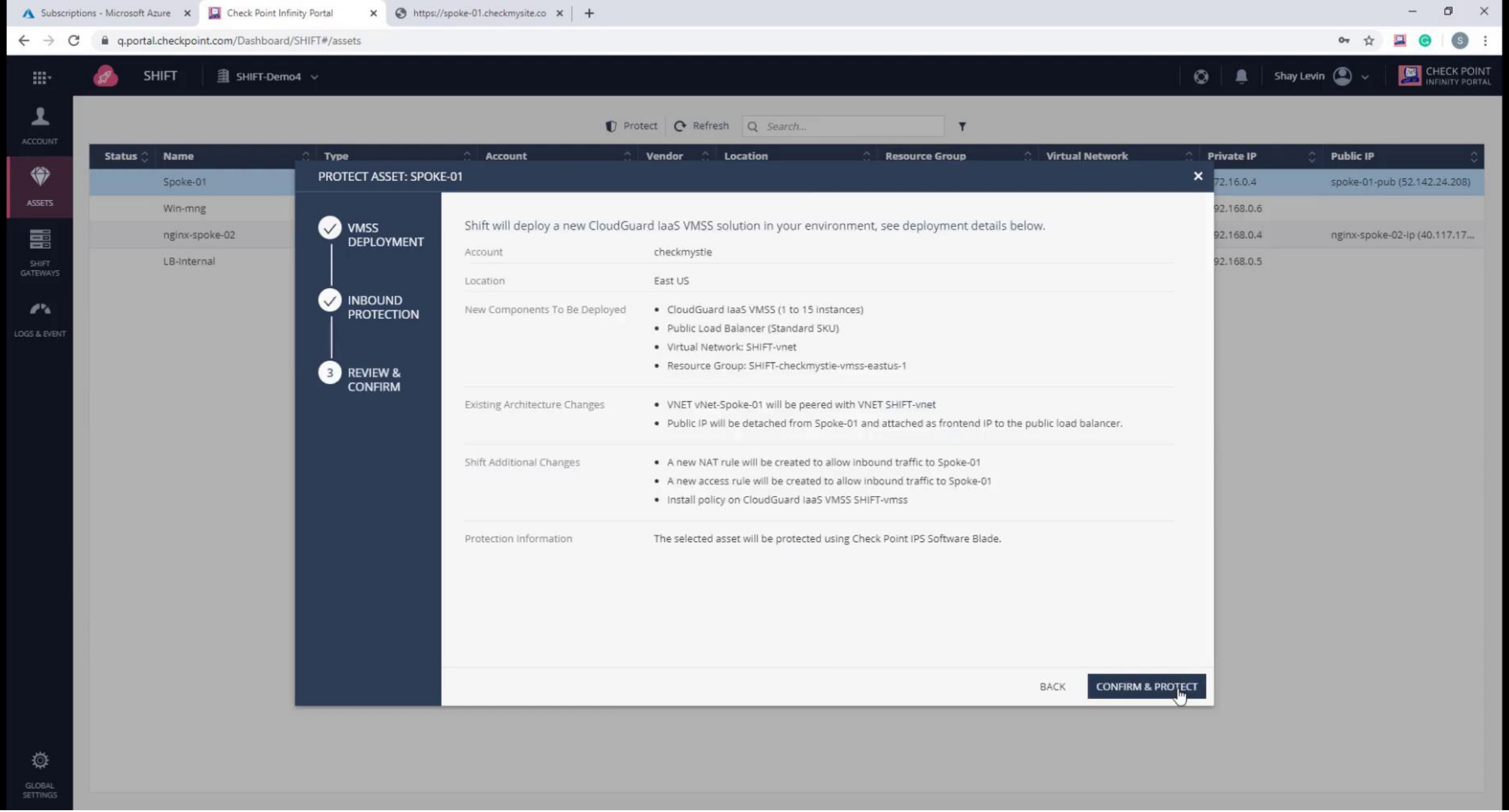

```
:
261afef0-ac24-4f7f-86e0-b09f45442eee
Directory (tenant) ID
:
ad625cb3-9b23-4525-b340-36f9ba7ef2c5
client secret: nOf-fkuh67qD5C7W/V-LmDAZCNGx:4k1

Subscription ID
:
6808449c-057b-434b-8434-a2c6e0338d4040
```

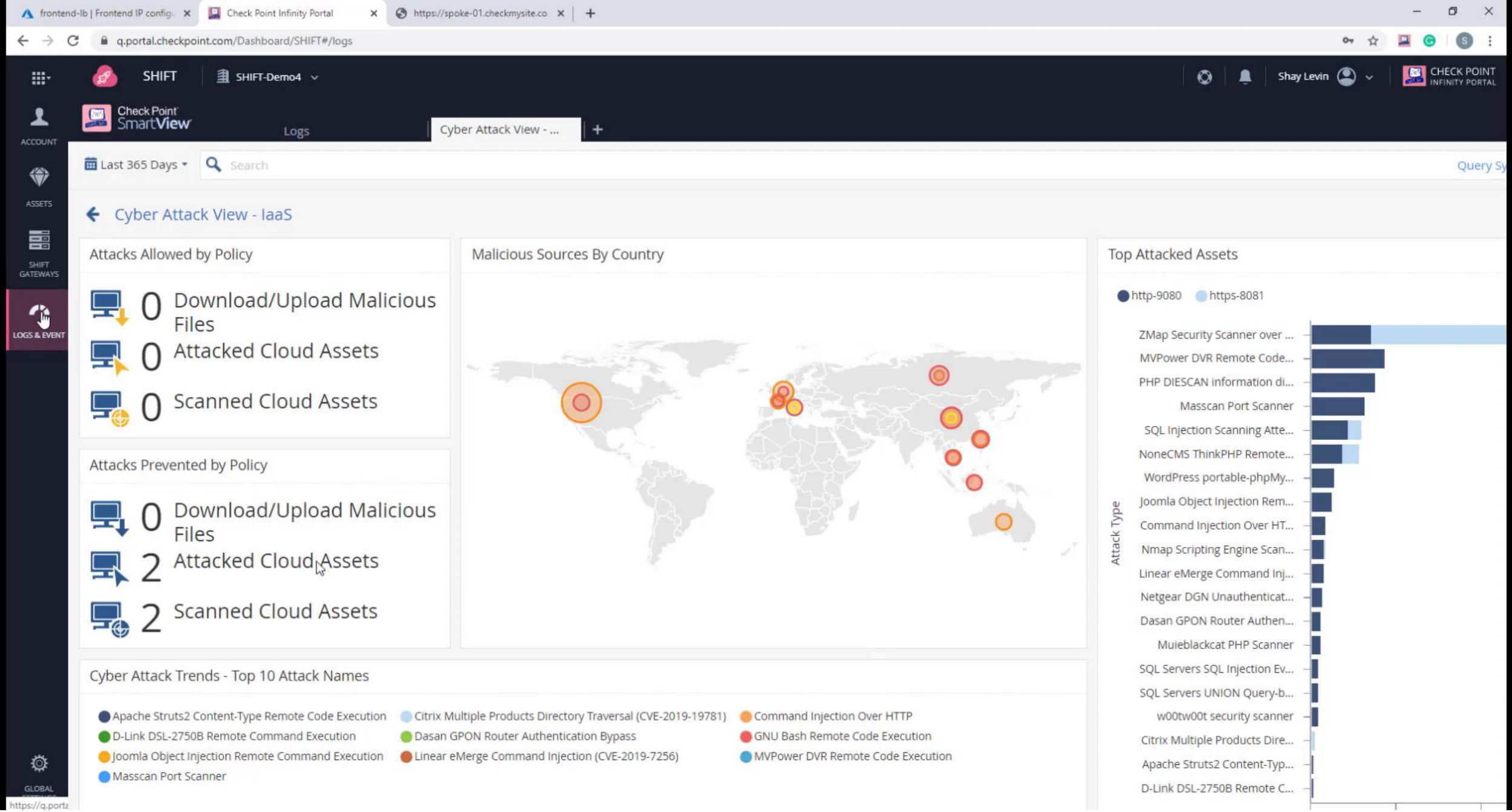












frontend-lb | Frontend IP config | Check Point Infinity Portal | https://spoke-01.checkmysite.co

q.portal.checkpoint.com/Dashboard/SHIFT#/logs

SHIFT | SHIFT-Demo4 | Shay Levin | CHECK POINT INFINITY PORTAL

Check Point SmartView | Logs | Cyber Attack View - ...

ACCOUNT | ASSETS | SHIFT GATEWAYS | LOGS & EVENT | GLOBAL SETTINGS

Last 365 Days | Search | Query Sy

Cyber Attack View - IaaS > Attacked Cloud Assets

Top Assets

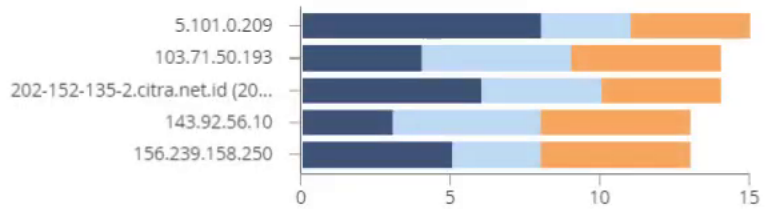
2 Total Targeted Assets

181 Total Exploit Attempts

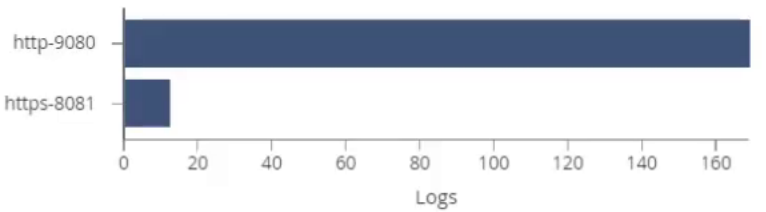
Top Detected Attacked Assets on the Network

Asset	Vulnerability Name	CVE	Number ...	Severity
http-9080	NoneCMS ThinkPHP Remote C...	CVE-2018-20...	18	
	WordPress portable-phpMyAd...	CVE-2012-54...	13	
	Joomla Object Injection Remot...	CVE-2015-85...	12	
	MVPower DVR Remote Code E...		43	
	PHP DIESCAN information discl...		37	
	16 Protections	12 Refer...	169	
https-8081	NoneCMS ThinkPHP Remote C...	CVE-2018-20...	10	
	Citrix Multiple Products Direct...	CVE-2019-19...	2	

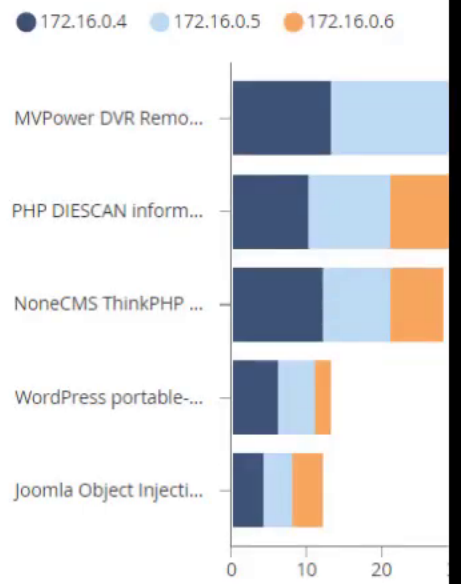
Top 5 Attackers



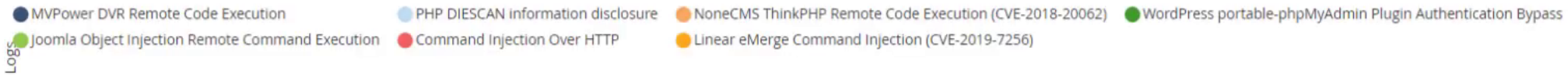
Top 5 Attacked Assets



Top Detected Exploits Attempts



Exploit Attacks Timeline



Check Point SmartView — Logs | Cyber Attack View - ...

Jan 5, 2020 - Feb 14, 2020 | (NOT product:"Firewall") | Query Syntax

Time	Blade	Action	Origin	Source	Destinat...	Service	R...	Access Rule Na...	Policy Na...	Descript...
Feb 14, 2020 2:51:15 AM	HTTPS Inspection	HTTPS Inspect	Azure...	209.17.97.18.rdns.cloudsystem...	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 2:21:03 AM	IPS	Prevent	Azure...	102.164.4.203	172.16...	http-9080		CPX-asset-VMSS	SHIFT_policy	
Feb 14, 2020 1:55:48 AM	HTTPS Inspection	HTTPS Inspect	Azure...	164.52.24.162	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:55:44 AM	HTTPS Inspection	HTTPS Inspect	Azure...	164.52.24.162	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:14:08 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:50 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:49 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:49 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:48 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:48 AM	IPS	Prevent	Azure...	47.92.172.245	172.16...	https-8081		CPX-asset-1	SHIFT_policy	
Feb 14, 2020 1:13:47 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:47 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:47 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:47 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:35 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:34 AM	HTTPS Inspection	Reject	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 1:13:34 AM	HTTPS Inspection	HTTPS Inspect	Azure...	47.92.172.245	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 14, 2020 12:55:13 ...	IPS	Accept	Azure...	45.152.6.58	172.16...	https-8081			SHIFT_policy	
Feb 14, 2020 12:02:28 ...	HTTPS Inspection	HTTPS Inspect	Azure...	165.22.202.29	172.16...	Spoke-01-49152			SHIFT_policy	
Feb 13, 2020 11:44:01 ...	IPS	Prevent	Azure...	156.239.158.250	172.16...	http-9080		CPX-asset-VMSS	SHIFT_policy	
Feb 13, 2020 11:44:00 ...	IPS	Prevent	Azure...	156.239.158.250	172.16...	http-9080		CPX-asset-VMSS	SHIFT_policy	

QUESTIONS?

Stuart Green | Cloud Security Architect

stuartg@checkpoint.com