



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

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

Gartner

Network: 20th time Security Leader in Magic Quadrant

Gartner

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

Gartner

Cloud: Dome9, a cool vendor in Cloud Security



Partnership with Microsoft

- One of Microsoft's **top Security ISVs WW in FY19**
- **2 Marketplace Offerings**
- **Microsoft Intelligent Security Association member**
- Integrations with **Azure Security Center** and **Azure Sentinel**
- **First Security Vendor for Azure Stack**



Best Practices for Architecting on Azure

15/11/2011 SEARCH...A01

Cloud advantages

Agility

Faster time to market

Availability

Service backed by SLA
Redundancy across regions

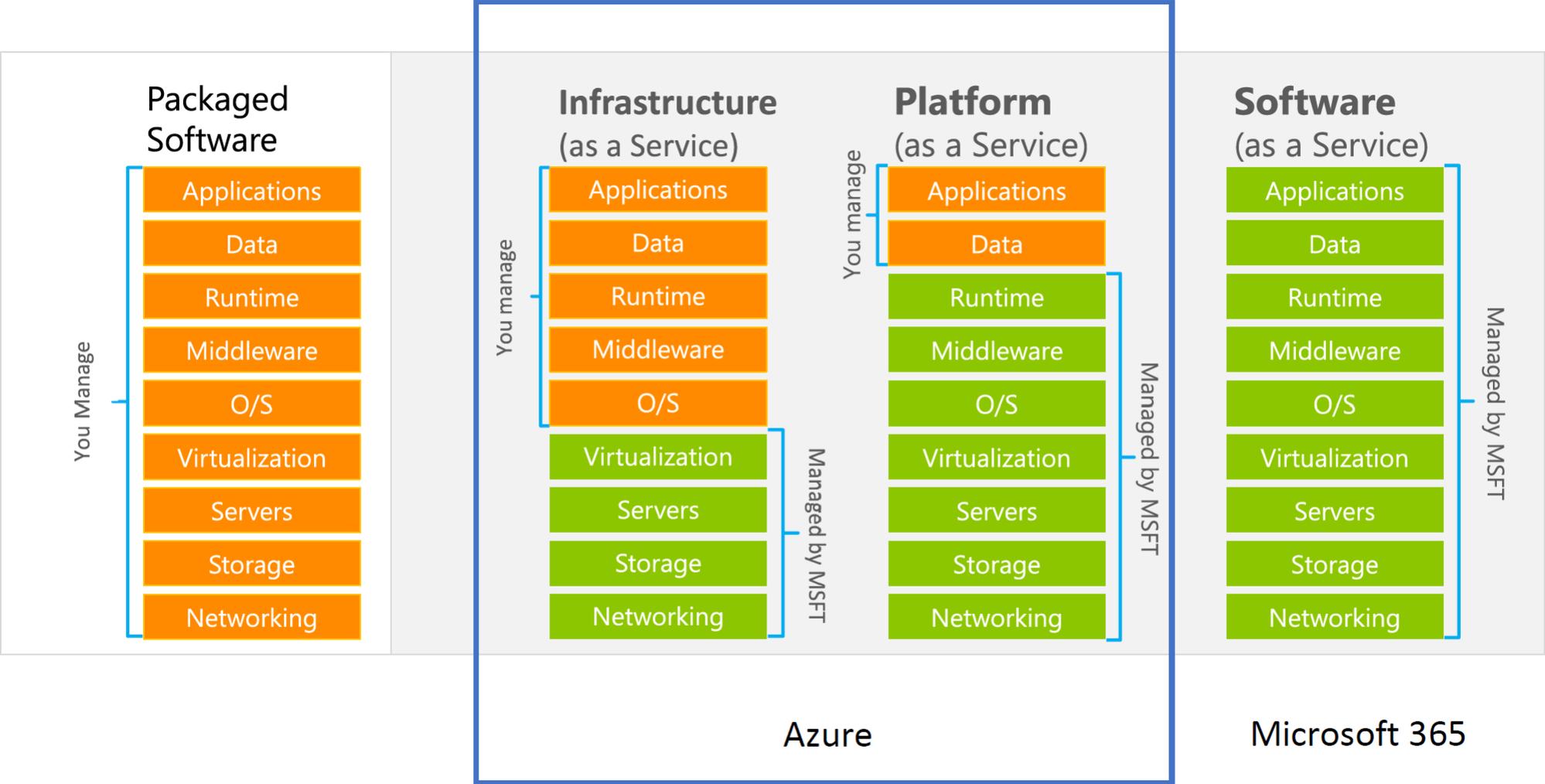
Scalability

Ability to scale to demand
Scale up or down quickly

Cost Efficient

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

IaaS Overview



CloudGuard IaaS Portfolio

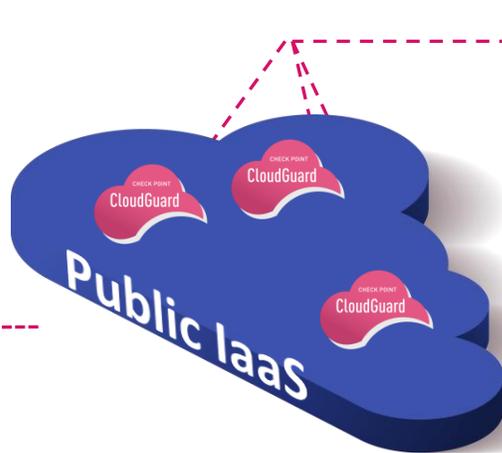


CloudGuard Gateway
With NGTX



CloudGuard Controller
Management

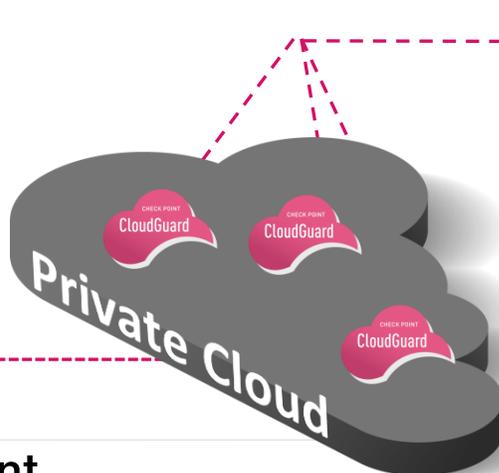
- ❑ AWS
- ❑ Azure
- ❑ GCP
- ❑ Alibaba Cloud
- ❑ Oracle



Mgmt.



- ❑ ESX
- ❑ Hyper-V
- ❑ KVM



Mgmt.



SDN Integration

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 IaaS / 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

Introducing the Hub-and-Spoke Model

When designing a secure cloud environment using CloudGuard IaaS, it is the hub-and-spoke model that was introduced in Blueprint 1.0. In order to maintain the architectural principles already described, in this model the environment connections are arranged like a bicycle wheel, in which all spokes are connected to a central hub. All traffic to and from the spokes traverses through a broker (hub). The blueprint shows one or multiple hubs, as shown in Figure 1.

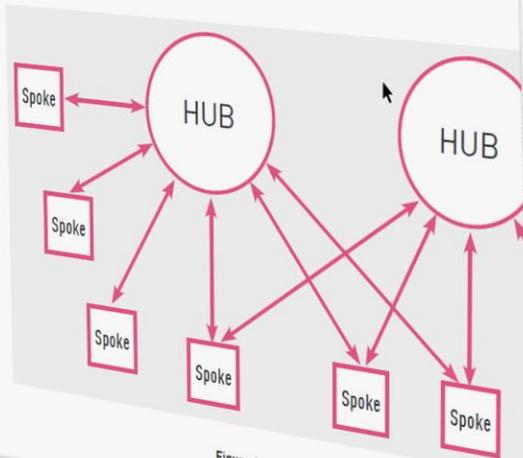
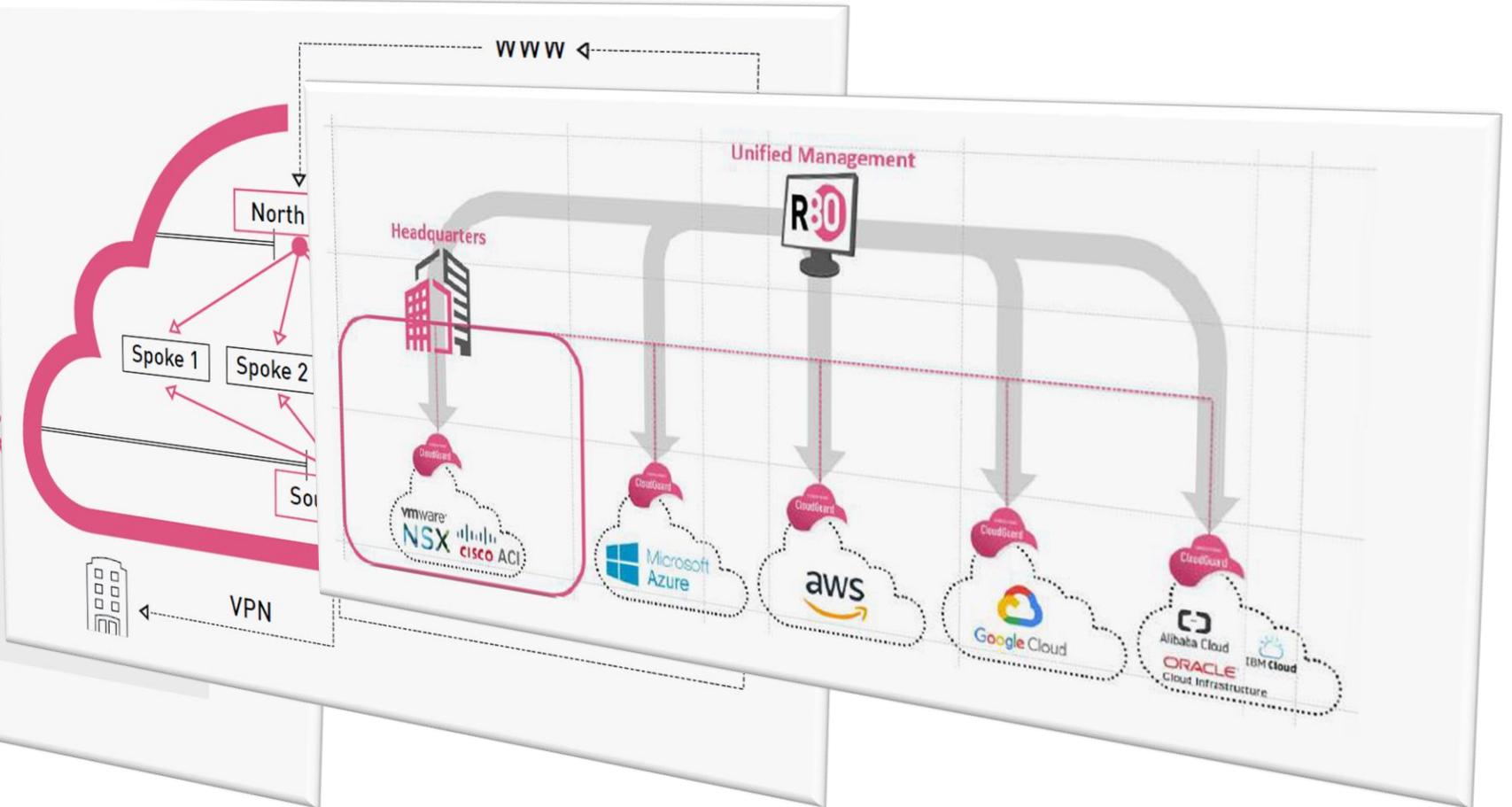
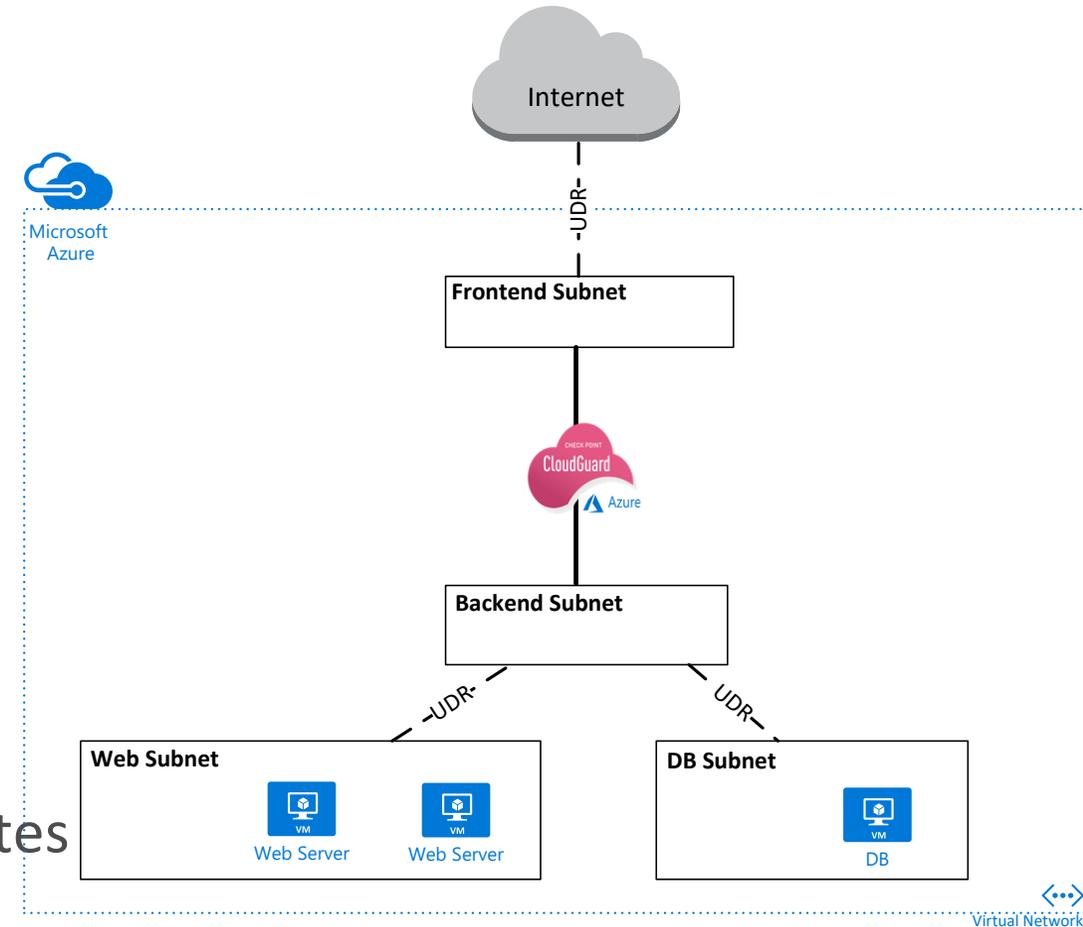


Figure 1: Hub-and-spoke model (multi-hub design)



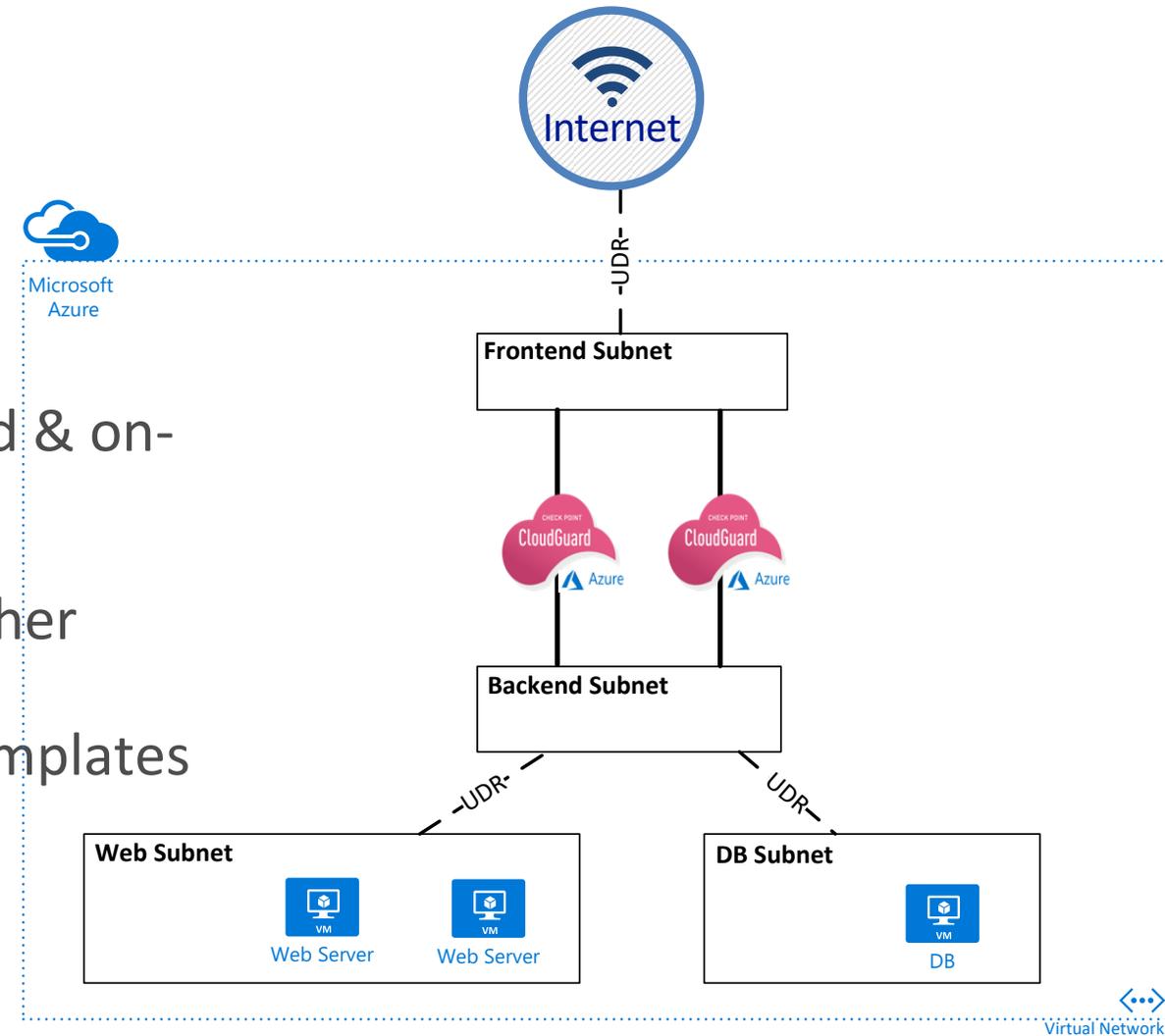
Architectures – Single gateway / standalone.

- 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



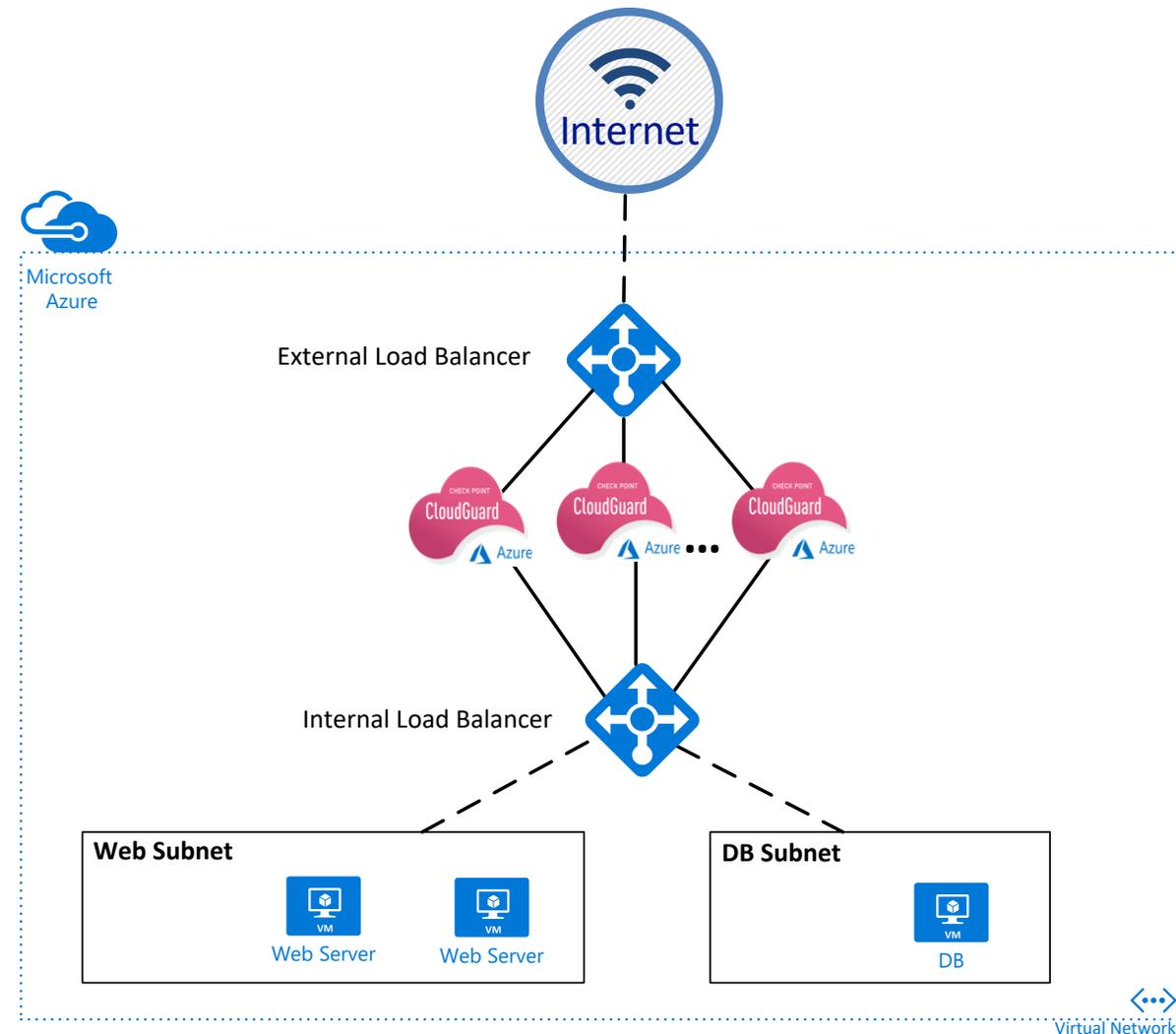
Architectures – High Availability

- 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

Virtual Core / year

NGTX

Virtual Core / year

Incl. Product, Subscriptions & Support



PER HOUR (Pay-As-You-Go)

Sold through marketplaces

Cloudguard Gateway (starting from)

NGTP

\$/h

NGTX

\$/h

Incl. Product, Subscriptions & Support



Smart Center¹

5-GW

\$/h

25-GW

\$/h

Incl. SmartEvent and Compliance blades & Support



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!

Subscriptions - Microsoft Azure | Check Point Infinity Portal

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

SHIFT | SHIFT-Demo4

Shay Levin

CHECK POINT INFINITY PORTAL

ACCOUNT

ASSETS

SHIFT GATEWAYS

LOGS & EVENT

GLOBAL SETTINGS

+ Connect | Search account by name

CONNECT ACCOUNT

Azure Credentials
Service Principal with contributor permission is required.

Account Name *
checkmystie

Client ID *
261afef0-ac24-4f7f-86e0-b09f45442eee

Client Secret *
.....

Directory ID *
ad625cb3-9b23-4525-b340-36f9ba7ef2c5

Subscription *
6808449c-057b-434b-8434-a2c6e0338d40

CANCEL | CONNECT

YET

```

:
261afef0-ac24-4f7f-86e0-b09f45442eee
Directory (tenant) ID
:
ad625cb3-9b23-4525-b340-36f9ba7ef2c5
client secret: n0f-fkuh67qD5C7W/V-LmDAZCNGx:4k1

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

```

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

Protect Refresh Search...

Status	Name	Type	Account	Vendor	Location	Resource Group	Virtual Network	Private IP	Public IP
	Spoke-01	Virtual Machine	checkmystie	Azure	East US	Spoke-01	vNet-Spoke-01	172.16.0.4	spoke-01-pub (52.142.24.208)
	Win-mng	Virtual Machine	checkmystie	Azure	East US	Manage	vNet-Spoke-02	192.168.0.6	
	nginx-spoke-02	Virtual Machine	checkmystie	Azure	East US	Spoke-02	vNet-Spoke-02	192.168.0.4	nginx-spoke-02-ip (40.117.17...
	LB-Internal	Internal Load Balancer	checkmystie	Azure	East US	Spoke-02-vmss	vNet-Spoke-02	192.168.0.5	

Protect Refresh Search...

Status	Name	Type	Account	Vendor	Location	Resource Group	Virtual Network	Private IP	Public IP
	Spoke-01							72.16.0.4	spoke-01-pub (52.142.24.208)
	Win-mng							92.168.0.6	
	nginx-spoke-02							92.168.0.4	nginx-spoke-02-ip (40.117.17...
	LB-Internal							92.168.0.5	

PROTECT ASSET: SPOKE-01

- 1 VMSS DEPLOYMENT
- 2 INBOUND PROTECTION
- 3 REVIEW & CONFIRM

Deploying a new Shift VMSS

Protecting asset for the first time in East US

New Resource Group Name:

New Virtual Network Name:

New Virtual Network Address Space:

New VMSS Name: VMSS MIN/MAX: -

NEXT

ACCOUNT
ASSETS
SHIFT GATEWAYS
LOGS & EVENT
GLOBAL SETTINGS

Status	Name	Type	Account	Vendor	Location	Resource Group	Virtual Network	Private IP	Public IP
	Spoke-01							172.16.0.4	spoke-01-pub (52.142.24.208)
	Win-mng							92.168.0.6	
	nginx-spoke-02							92.168.0.4	nginx-spoke-02-ip (40.117.17...
	LB-Internal							92.168.0.5	

PROTECT ASSET: SPOKE-01

- 1 VMSS DEPLOYMENT
- 2 INBOUND PROTECTION
- 3 REVIEW & CONFIRM

Protect Inbound Traffic

HTTP (80) HTTPS (443)

HTTPS inspection server Certificate

No Certificate Imported
[Import...](#) [Select existing...](#)

Allow Inbound Traffic

SSH RDP

Forward traffic to the following asset's private IP

172.16.0.4

Publish the asset with the following public IP

Use Asset's IP

spoke-01-pub (52.142.24.208)

Public IP: 52.142.24.208 HTTPS

SHIFT-checkmystie-vmss-eastus-1

SHIFT-vnet 10.0.0.0/26

SHIFT-vmss 1-15

Spoke-01

IP Addresses: 172.16.0.4, 52-142-24-208

CHECK POINT PROTECTION

PROTECTED ASSETS

BACK NEXT

Status	Name	Type	Account	Vendor	Location	Resource Group	Virtual Network	Private IP	Public IP
	Spoke-01							72.168.0.4	spoke-01-pub (52.142.24.208)
	Win-mng							92.168.0.6	
	nginx-spoke-02							92.168.0.4	nginx-spoke-02-ip (40.117.17...
	LB-Internal							92.168.0.5	

PROTECT ASSET: SPOKE-01

- ✓ VMSS DEPLOYMENT
- ✓ INBOUND PROTECTION
- 3 REVIEW & CONFIRM

Shift will deploy a new CloudGuard IaaS VMSS solution in your environment, see deployment details below.

Account: checkmysite

Location: East US

New Components To Be Deployed

- CloudGuard IaaS VMSS (1 to 15 Instances)
- Public Load Balancer (Standard SKU)
- Virtual Network: SHIFT-vnet
- Resource Group: SHIFT-checkmysite-vmss-eastus-1

Existing Architecture Changes

- VNET vNet-Spoke-01 will be peered with VNET SHIFT-vnet
- Public IP will be detached from Spoke-01 and attached as frontend IP to the public load balancer.

Shift Additional Changes

- A new NAT rule will be created to allow inbound traffic to Spoke-01
- A new access rule will be created to allow inbound traffic to Spoke-01
- Install policy on CloudGuard IaaS VMSS SHIFT-vmss

Protection Information: The selected asset will be protected using Check Point IPS Software Blade.

BACK | CONFIRM & PROTECT

Subscriptions - Microsoft Azure | Check Point Infinity Portal | https://spoke-01.checkmystie.co

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

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

Protect Refresh Search...

Status	Name	Type	Account	Vendor	Location	Resource Group	Virtual Network	Private IP	Public IP
	Spoke-01							72.168.0.4	spoke-01-pub (52.142.24.208)
	Win-mng							92.168.0.6	
	nginx-spoke-02							92.168.0.4	nginx-spoke-02-ip (40.117.17...
	LB-Internal							92.168.0.5	

PROTECT ASSET: SPOKE-01

- ✓ VMSS DEPLOYMENT
- ✓ INBOUND PROTECTION
- 3 REVIEW & CONFIRM

Shift will deploy a new CloudGuard IaaS VMSS solution in your environment, see deployment details below.

Account: checkmystie

Location: East US

New Components To Be Deployed

- CloudGuard IaaS VMSS (1 to 15 Instances)
- Public Load Balancer (Standard SKU)
- Virtual Network: SHIFT-vnet
- Resource Group: SHIFT-checkmystie-vmss-eastus-1

Existing Architecture Changes

- VNET vNet-Spoke-01 will be peered with VNET SHIFT-vnet
- Public IP will be detached from Spoke-01 and attached as frontend IP to the public load balancer.

Shift Additional Changes

- A new NAT rule will be created to allow inbound traffic to Spoke-01
- A new access rule will be created to allow inbound traffic to Spoke-01
- Install policy on CloudGuard IaaS VMSS SHIFT-vmss

Protection Information: The selected asset will be protected using Check Point IPS Software Blade.

BACK CONFIRM & PROTECT

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

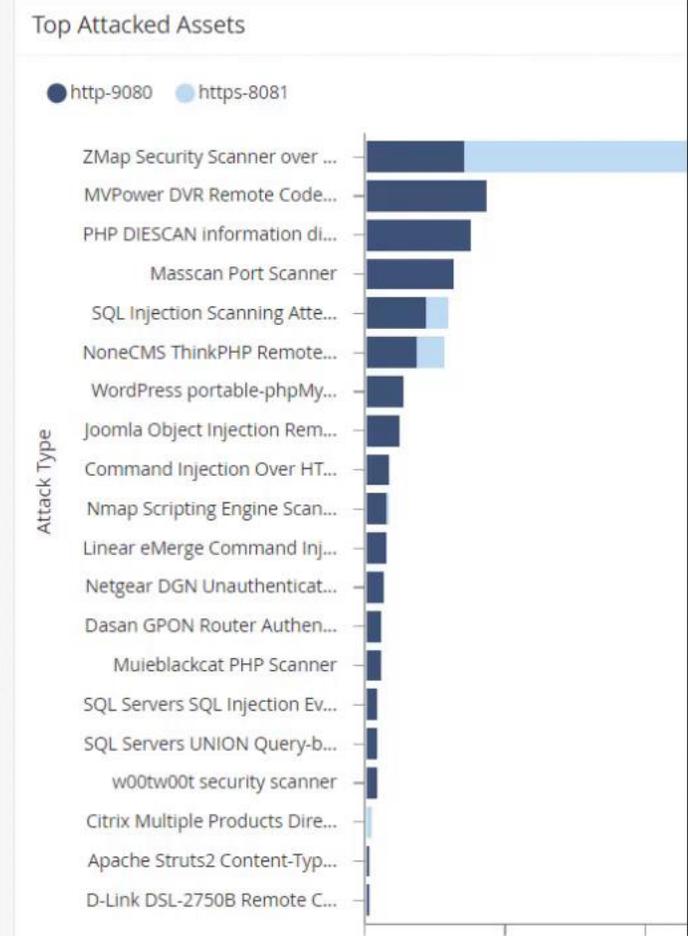
Cyber Attack View - IaaS

Attacks Allowed by Policy

- 0 Download/Upload Malicious Files
- 0 Attacked Cloud Assets
- 0 Scanned Cloud Assets

Attacks Prevented by Policy

- 0 Download/Upload Malicious Files
- 2 Attacked Cloud Assets
- 2 Scanned Cloud Assets



Cyber Attack Trends - Top 10 Attack Names

- Apache Struts2 Content-Type Remote Code Execution
- Citrix Multiple Products Directory Traversal (CVE-2019-19781)
- Command Injection Over HTTP
- D-Link DSL-2750B Remote Command Execution
- Dasan GPON Router Authentication Bypass
- GNU Bash Remote Code Execution
- Joomla Object Injection Remote Command Execution
- Linear eMerge Command Injection (CVE-2019-7256)
- MVPower DVR Remote Code Execution
- Masscan Port Scanner

Last 365 Days | Search | Query Sy

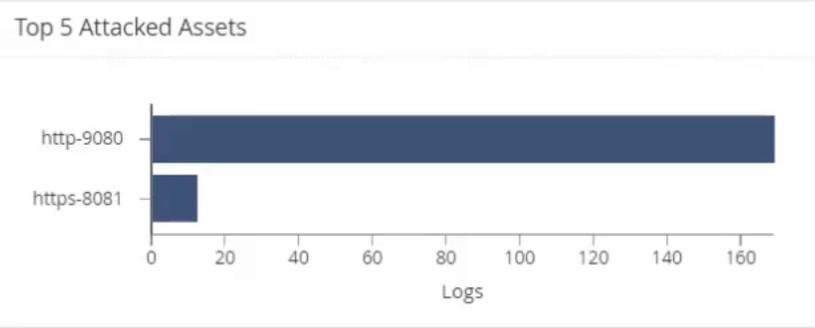
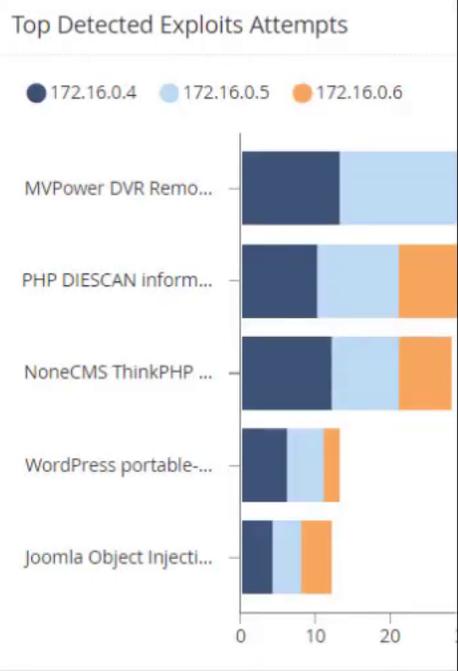
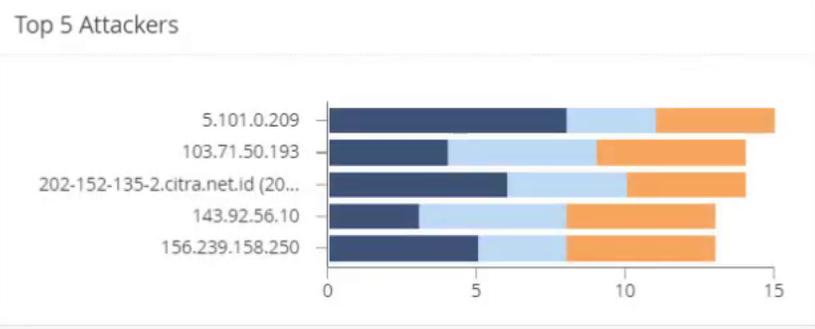
Cyber Attack View - IaaS > Attacked Cloud Assets

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



Exploit Attacks Timeline

- MVPower DVR Remote Code Execution
- PHP DIESCAN information disclosure
- NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)
- WordPress portable-phpMyAdmin Plugin Authentication Bypass
- Joomla Object Injection Remote Command Execution
- Command Injection Over HTTP
- Linear eMerge Command Injection (CVE-2019-7256)

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	



Check Point[®]
SOFTWARE TECHNOLOGIES LTD

QUESTIONS?

Stuart Green | Cloud Security Architect

stuartg@checkpoint.com