TD SYNNEX

Tobias Böckmann
Technical Presales,
Tobias.boeckmann@tdsynnex.com

TD SYNNEX

Agenda

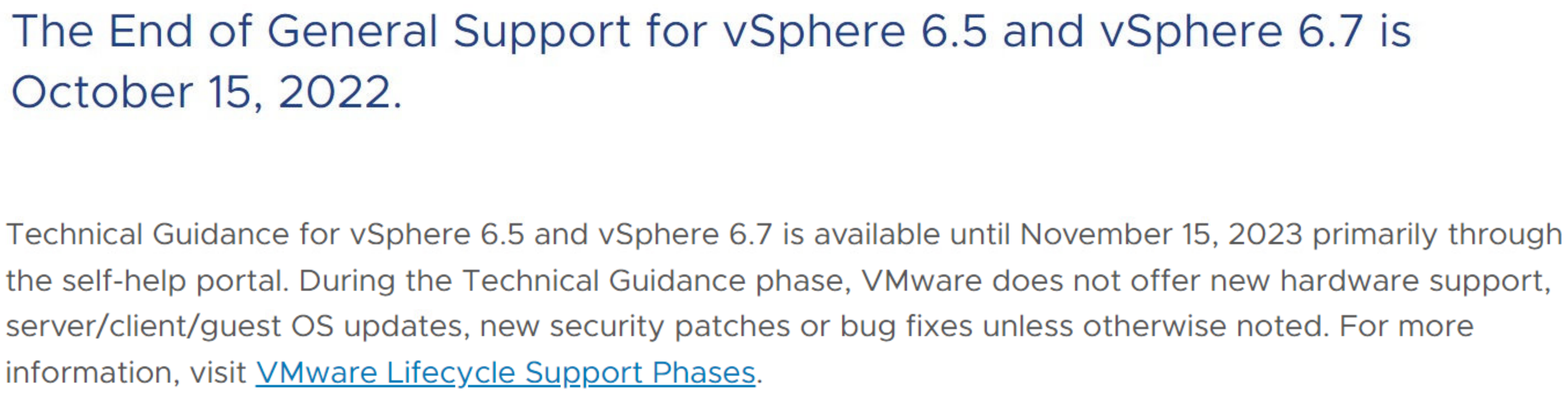
- Übersicht vSphere 8
- Übersicht vSAN 8
- Was ist VMware Aria
- VMware Carbon Black Cloud

TD SYNNEX

VMware vSphere 8

verfügbar seit 11.10. 2022

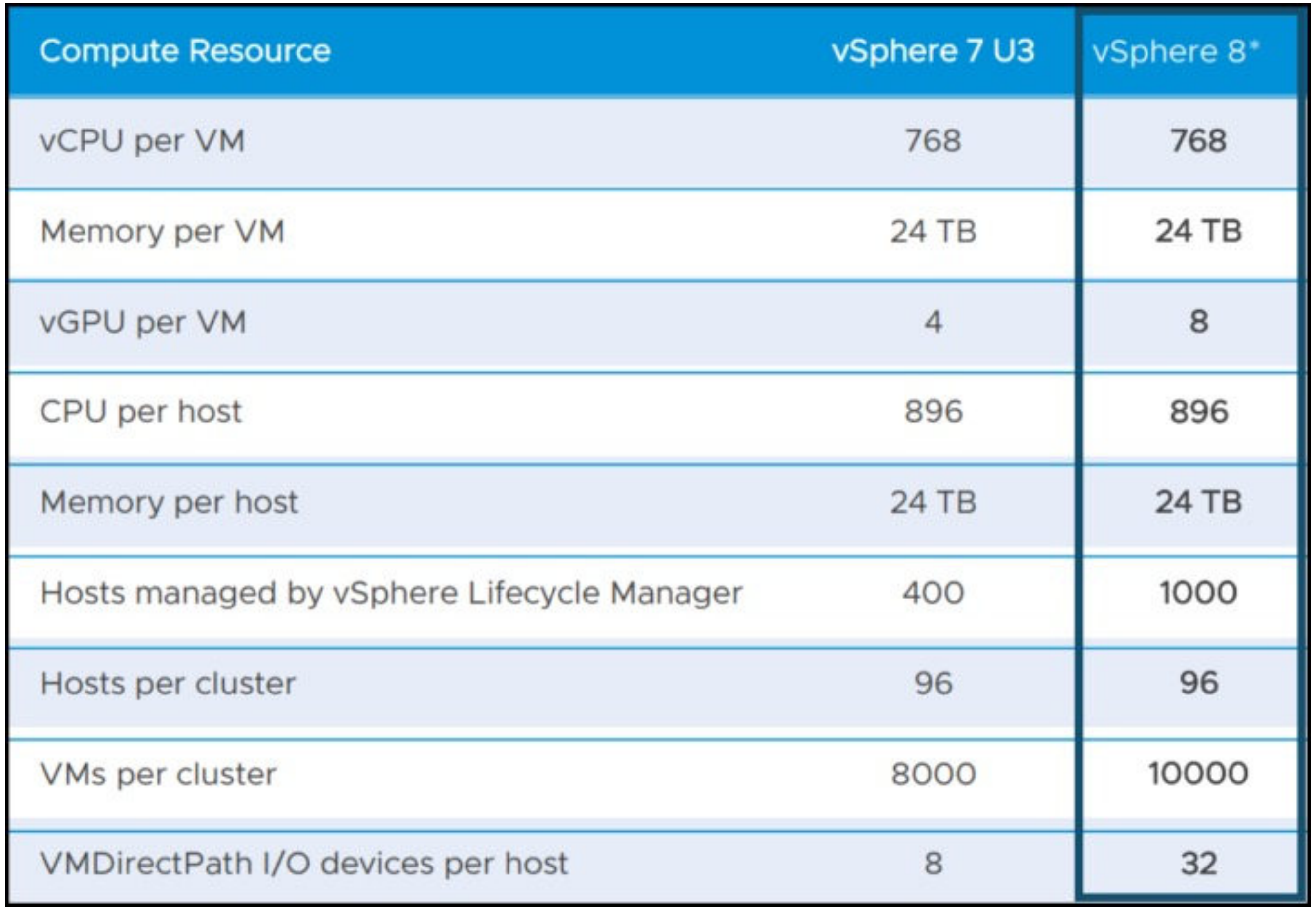
Ende des General Supports für vSphere 6.5 und 6.7!



The End of General Support for vSphere 6.5 and vSphere 6.7 is October 15, 2022.

Technical Guidance for vSphere 6.5 and vSphere 6.7 is available until November 15, 2023 primarily through the self-help portal. During the Technical Guidance phase, VMware does not offer new hardware support, server/client/guest OS updates, new security patches or bug fixes unless otherwise noted. For more information, visit VMware Lifecycle Support Phases.

vSphere 8



Compute Resource	vSphere 7 U3	vSphere 8*
vCPU per VM	768	768
Memory per VM	24 TB	24 TB
vGPU per VM	4	8
CPU per host	896	896
Memory per host	24 TB	24 TB
Hosts managed by vSphere Lifecycle Manager	400	1000
Hosts per cluster	96	96
VMs per cluster	8000	10000
VMDirectPath I/O devices per host	8	32

Hardware Version 20

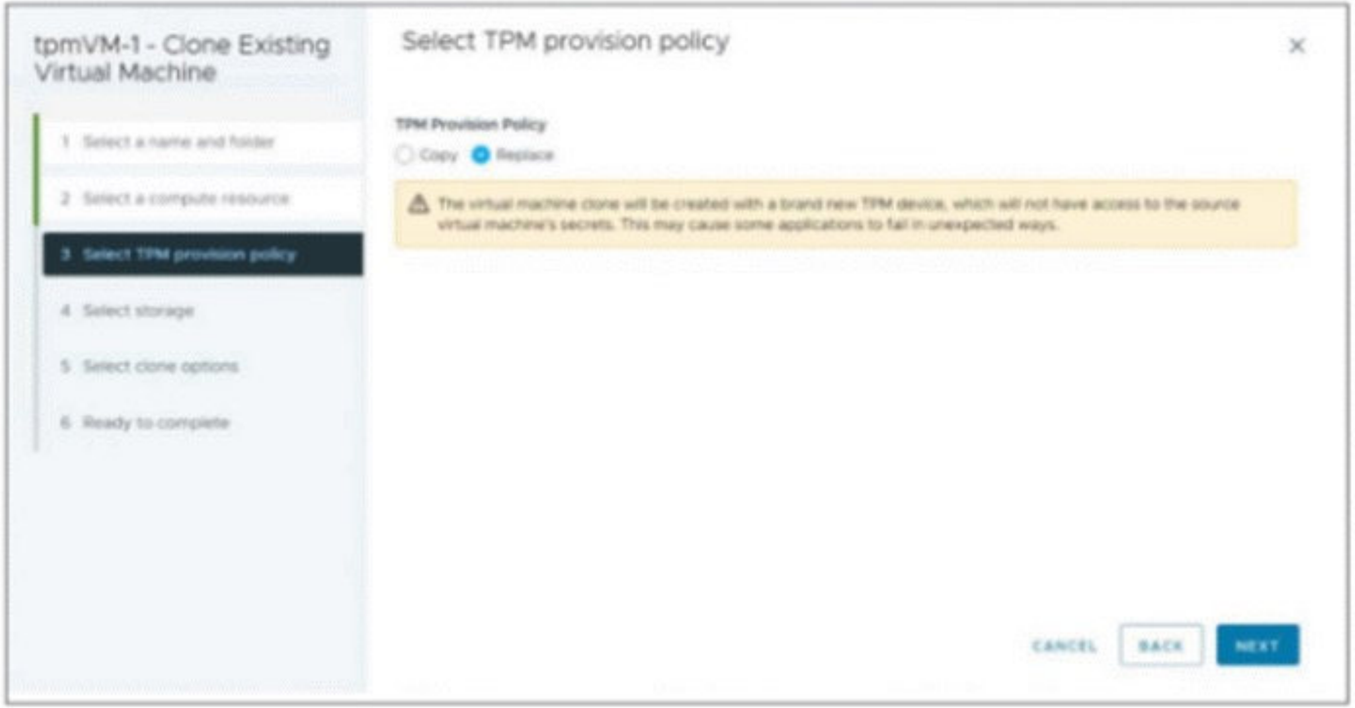
Clone für Windows 11 und vTPM (unique TPM device)

vSphere DataSets
Data is stored and moves with the VM

vSphere 8

Bereitstellungsrichtlinie für Windows 11 Virtual TPM

Introducing Virtual TPM Provisioning Policy


tpmVM-1 - Clone Existing Virtual Machine

1 Select a name and folder
2 Select a compute resource
3 Select TPM provision policy
4 Select storage
5 Select clone options
6 Ready to complete

Select TPM provision policy

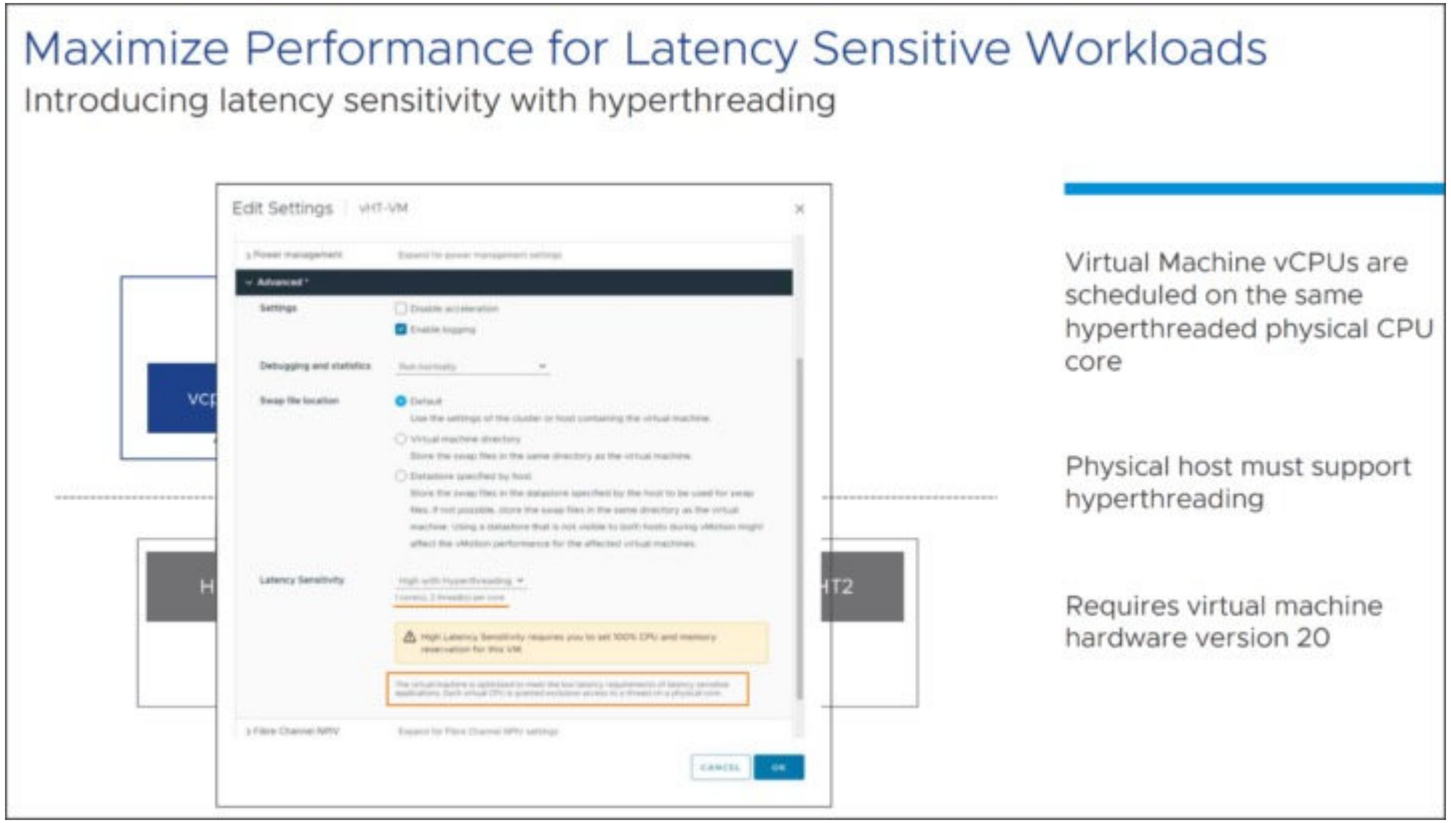
TPM Provision Policy
○ Copy ● Replace

⚠ The virtual machine clone will be created with a brand new TPM device, which will not have access to the source virtual machine's secrets. This may cause some applications to fail in unexpected ways.

Das Klonen von VMs mit TPM kann ein Sicherheitsrisiko darstellen. Deswegen können Admins in vSphere 8 angeben kann, ob sie das TPM-Gerät kopieren oder ersetzen möchte.

Wählt man die Option *Ersetzen* aus, dann wird der VM-Klon wird mit einem brandneuen TPM-Gerät erstellt, das keinen Zugriff auf die Geheimnisse der Quell-VM hat.

vSphere 8



Maximize Performance for Latency Sensitive Workloads

Introducing latency sensitivity with hyperthreading

Edit Settings | vHT-VM

› Power management — Expand for power management settings

⌄ Advanced *

Settings: □ Disable acceleration ☑ Enable logging

Debugging and statistics: Run normally

Swap file location:
● Default — Use the settings of the cluster or host containing the virtual machine.
○ Virtual machine directory — Store the swap files in the same directory as the virtual machine.
○ Datastore specified by host — Store the swap files in the datastore specified by the host to be used for swap files. If not possible, store the swap files in the same directory as the virtual machine. Using a datastore that is not visible to both hosts during vMotion might affect the vMotion performance for the affected virtual machines.

Latency Sensitivity: High with Hyperthreading
1 core(s), 2 thread(s) per core

⚠ High Latency Sensitivity requires you to set 100% CPU and memory reservation for this VM

The virtual machine is optimized to meet the low latency requirements of latency sensitive applications. Each virtual CPU is granted exclusive access to a thread on a physical core.

› Fibre Channel NPIV — Expand for Fibre Channel NPIV settings

Virtual Machine vCPUs are scheduled on the same hyperthreaded physical CPU core

Physical host must support hyperthreading

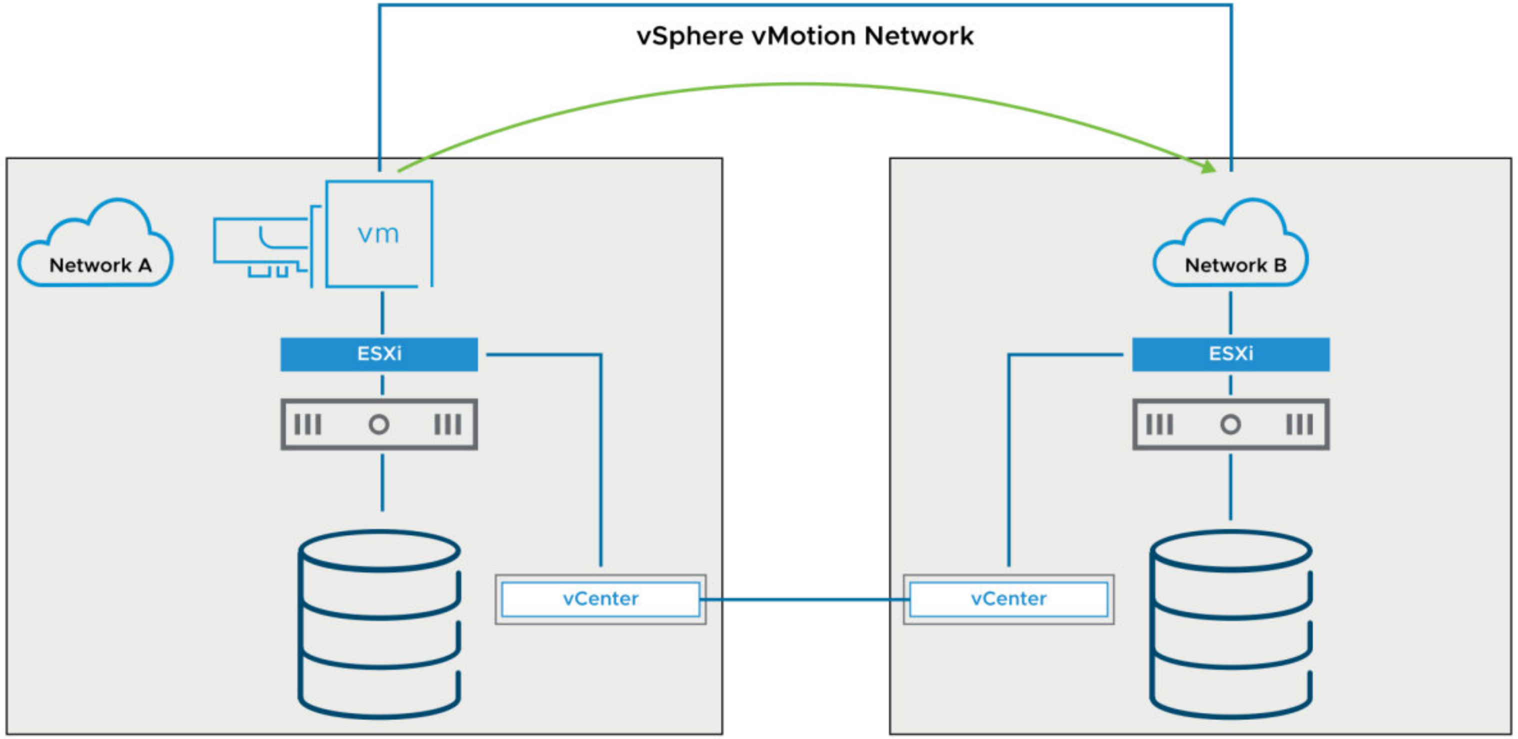
Requires virtual machine hardware version 20

New latency sensitivity with hyperthreading will allow VM's vCPUs scheduling on the same hyperthreaded physical CPU core. The physical host must support hyperthreading. This feature needs the latest virtual hardware 20. You'll also need to set 100% CPU and memory reservation for this VM. The VM is optimized to meet the low latency requirements of latency-sensitive applications. Each virtual CPU is granted exclusive access to a thread on a physical core.

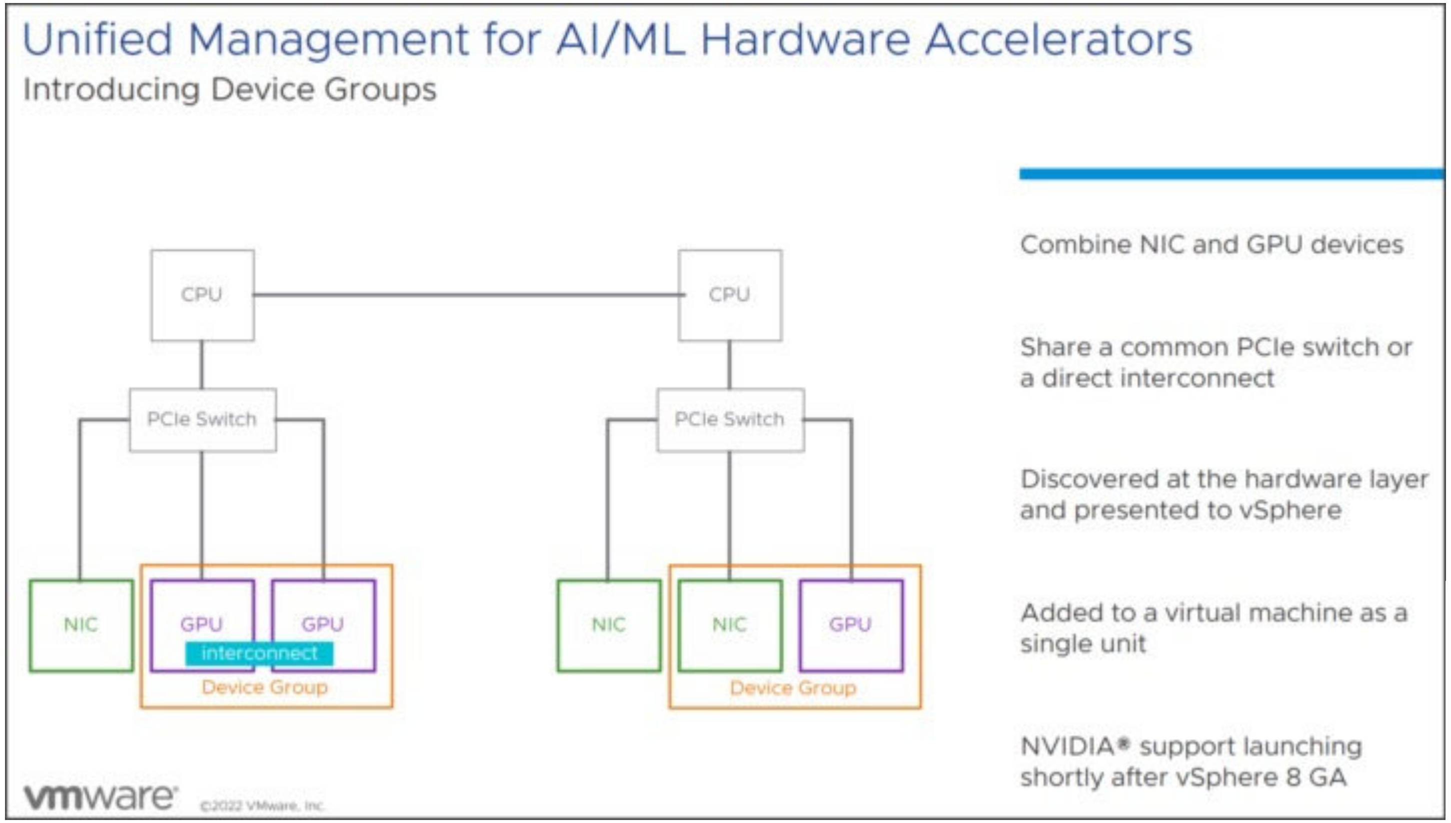
Cross vCenter Migration Requirements

Cross vCenter migrations have the following requirements:

- Hosts must be time-synchronized.
- Both vCenter instances can be in the same or different vCenter Single Sign-On domain.



vSphere 8



Unified Management for AI/ML Hardware Accelerators

Introducing Device Groups

Combine NIC and GPU devices

Share a common PCIe switch or a direct interconnect

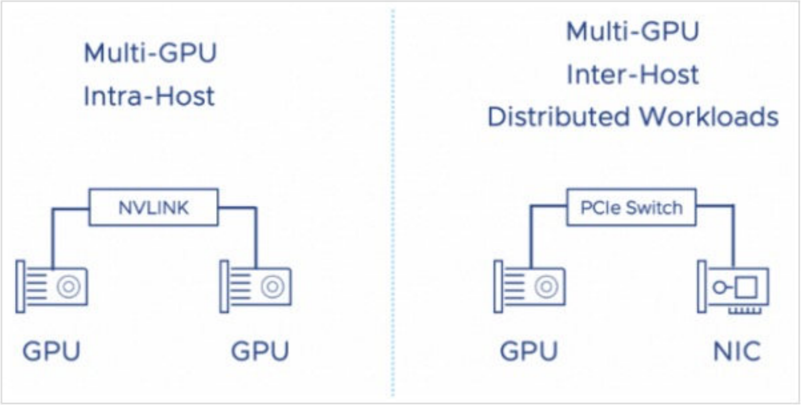
Discovered at the hardware layer and presented to vSphere

Added to a virtual machine as a single unit

NVIDIA® support launching shortly after vSphere 8 GA

vmware ©2022 VMware, Inc.

vSphere HA and DRS are aware of device groups so they'll work together and they'll make sure that the VM will be placed on a appropriate host that can satisfy the device group.



Verteilte GPU-Arbeitslasten via NVLINK (nVidia) oder das Kombinieren von NIC und GPU (PCIe-Switch)

vSphere 8

- Applications that are migration-aware (VMotion)

- Certain applications cannot tolerate the stun that happens during vMotion operation. Applications can be written now to support migrations and vMotion operation. Applications can be notified that migration will take a place, and in this case, there might be some services that need to be gracefully shut down before the migration, or performing a failover operation.
- The application itself can delay the migration until a configurable timeout, but it cannot stop the migration from occurring. This could be some Time-sensitive applications, VoIP, or clustered applications.

About Images

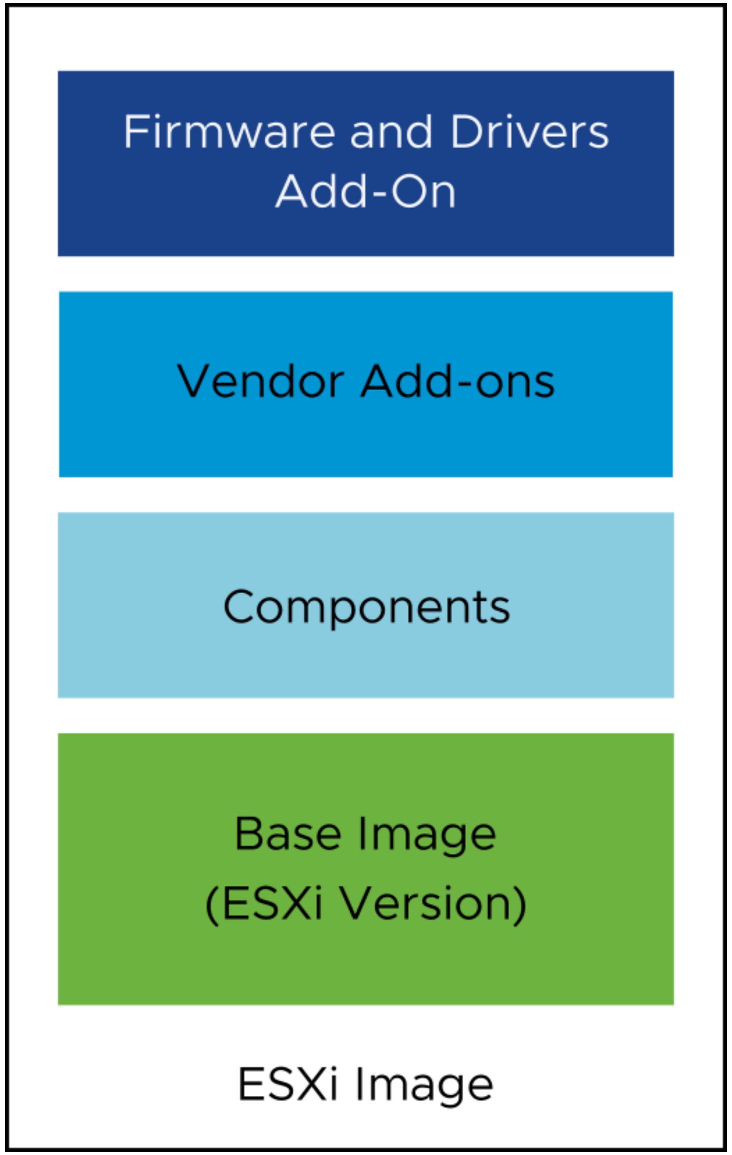
Managing clusters with images helps to standardize the software running on your ESXi hosts.

An ESXi image consists of several elements:

- ESXi base image: An update that provides software fixes and enhancements
- Components: A logical grouping of one or more VIBs (vSphere Installation Bundles) that encapsulates functionality in ESXi
- Vendor add-ons: Sets of components that OEMs create and distribute
- Firmware and Drivers Add-On: Firmware and driver bundles that you can define for your cluster image
  - Requires the Hardware Support Manager plug-in for the desired server family

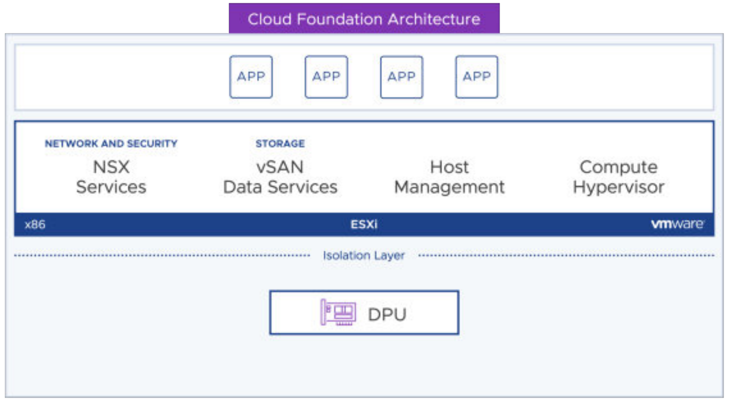
To maintain consistency, you apply a single ESXi image to all hosts in a cluster.

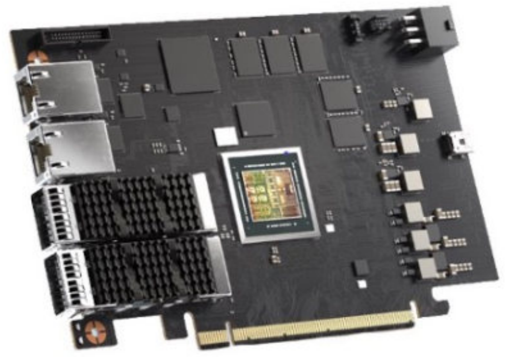
vSphere Lifecycle Manager
paralleler Update von Hosts



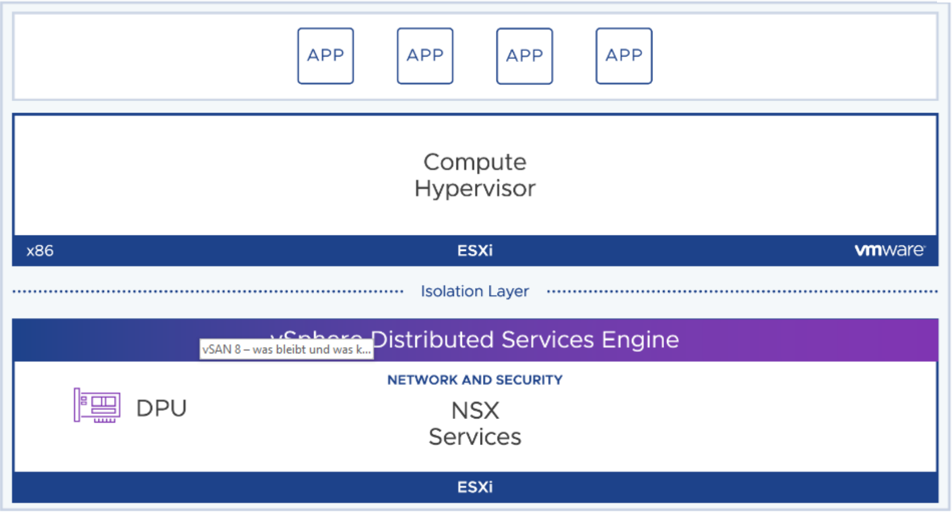
vSphere 8

vSphere Distributed Services Engine (ehemals Project Monterey)



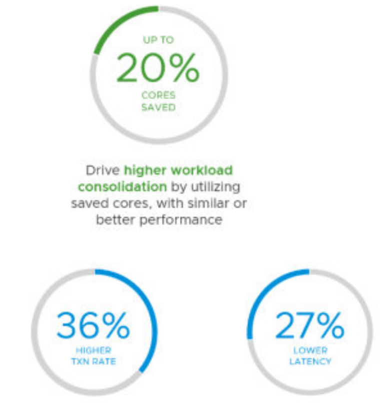


Mit GA -> NSX OFFLOAD



vSphere 8: Redis Performance Comparison

vSphere on DPUs Supercharges Workload Performance



Drive higher workload consolidation by utilizing saved cores, with similar or better performance

Supercharge performance by leveraging freed CPU cores and better cache locality to drive more workload traffic, while benefitting from vMotion & DRS

ESXi läuft auf der DPU

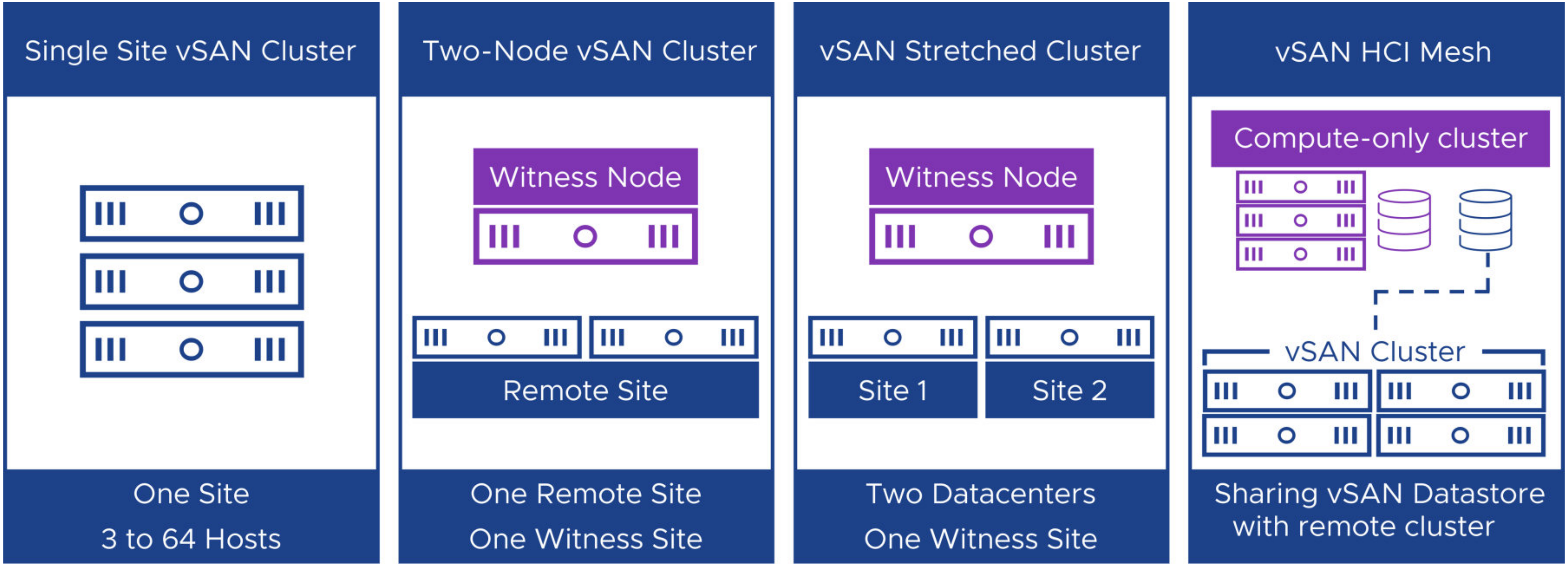
TD SYNNEX

VMware vSAN 8

verfügbar seit 11.10. 2022

vSAN Cluster Types

vSAN provides four types of deployment architectures to meet enterprise needs.

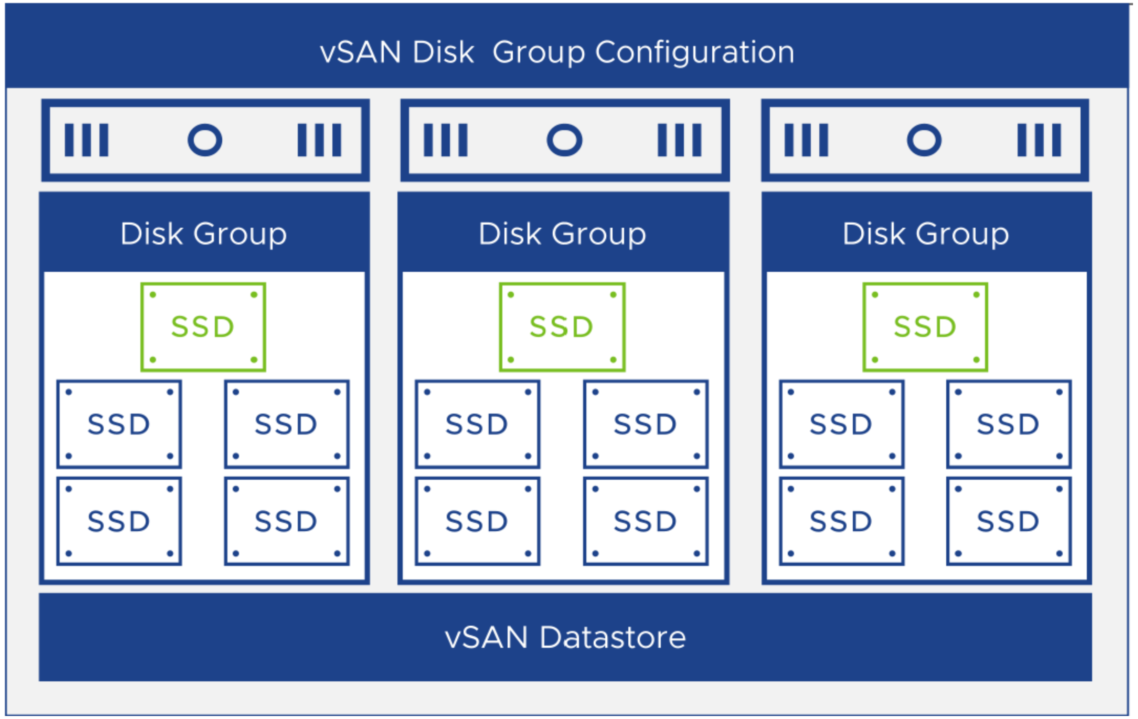


vSAN Disk Configuration

vSAN uses a two-tier model where the disk first docks onto a cache device to take advantage of caching speed, then trickles down to the larger capacity tier.

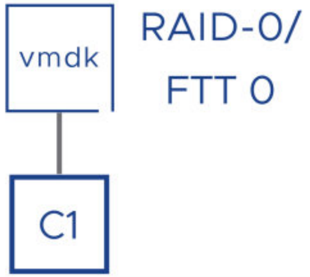
Two tier disk construct a disk group which supports Hybrid and All-Flash configurations.

A maximum of five disk Groups can be created per vSAN node.



vSAN Storage Policy Space Consumption Comparison

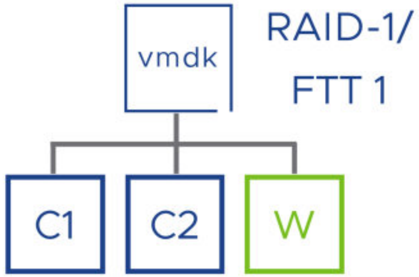
To store a 100 GB VMDK on vSAN datastore, you can compare between the storage space consumed with the different types of storage policies.



No Redundancy

RAID-0/FTT0

- 1 Host
- 100 GBs of Storage



Mirroring

RAID-1/FTT1

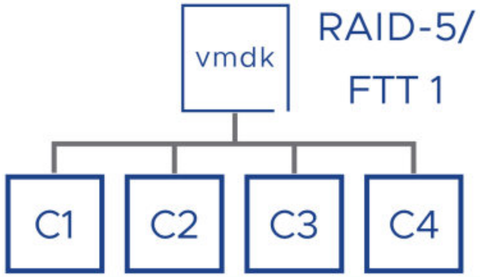
- 3 Hosts
- 200 GBs of Storage

RAID-1/FTT2

- 5 Hosts
- 300 GBs of Storage

RAID-1/FTT3

- 7 Hosts
- 400 GBs of Storage



Erasure Coding

RAID-5/FTT1(3+1)

- 4 Hosts
- 133 GBs of Storage

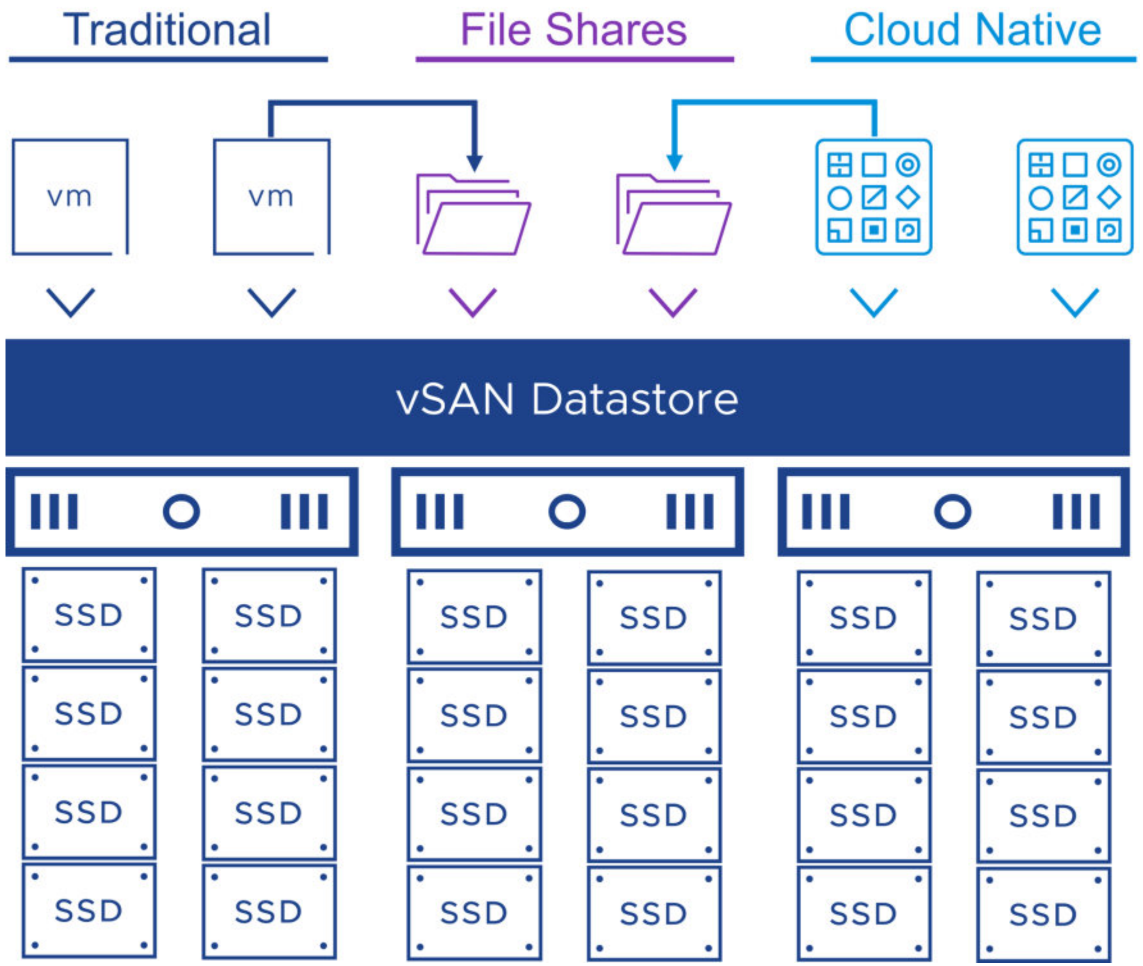
RAID-6/FTT2 (4+2)

- 6 Hosts
- 150 GBs of Storage

vSAN File Service Overview

vSAN File Service (vSAN FS) allows an administrator to create file shares backed by vSAN Datastore.

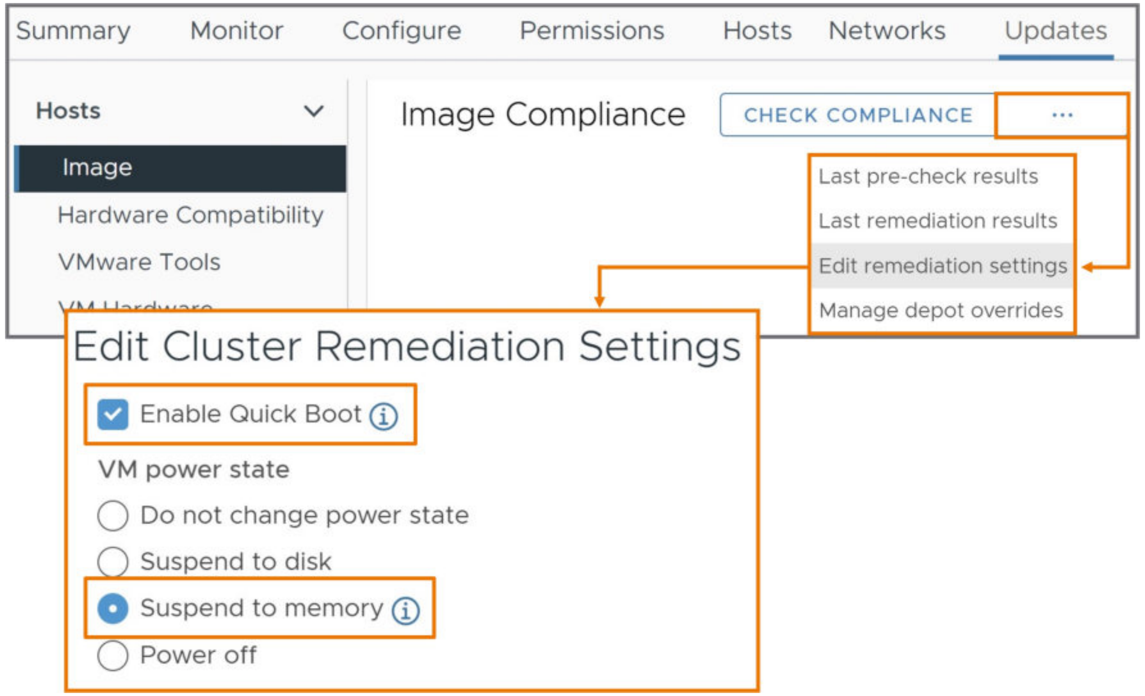
- Designed for Cloud Native Applications and traditional workloads
- Supports SMBv2.1 and v3
- Supports NFSv3 and NFSv4.1
- Assigns file share quotas
- Compatible with other vSAN services



Quick Boot Enhancement

Faster host restarts using Suspend VMs to Memory.

- Avoids time needed to vMotion VMs during a rolling upgrade
- Faster host restarts = less resyncs
- New power option added, **Suspend to Memory**
- Cluster wide setting
- Requires to **Enable Quick Boot**
- Results in VM/application interruption



Edit Cluster Remediation Settings

☑ Enable Quick Boot ⓘ

VM power state

○ Do not change power state

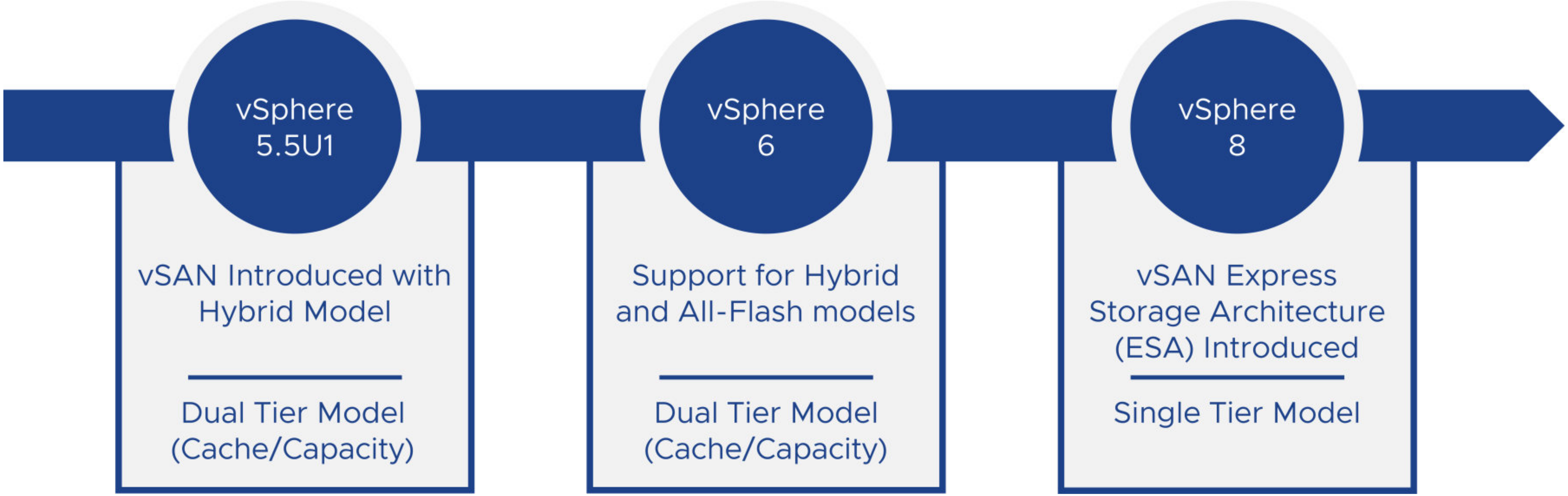
○ Suspend to disk

● Suspend to memory ⓘ

○ Power off

vSAN Express Storage Architecture

vSAN 8 introduces Express Storage Architecture, designed to support high-performance storage devices resulting in greater performance and efficiency.



vSphere 5.5U1

vSAN Introduced with Hybrid Model

Dual Tier Model (Cache/Capacity)

vSphere 6

Support for Hybrid and All-Flash models

Dual Tier Model (Cache/Capacity)

vSphere 8

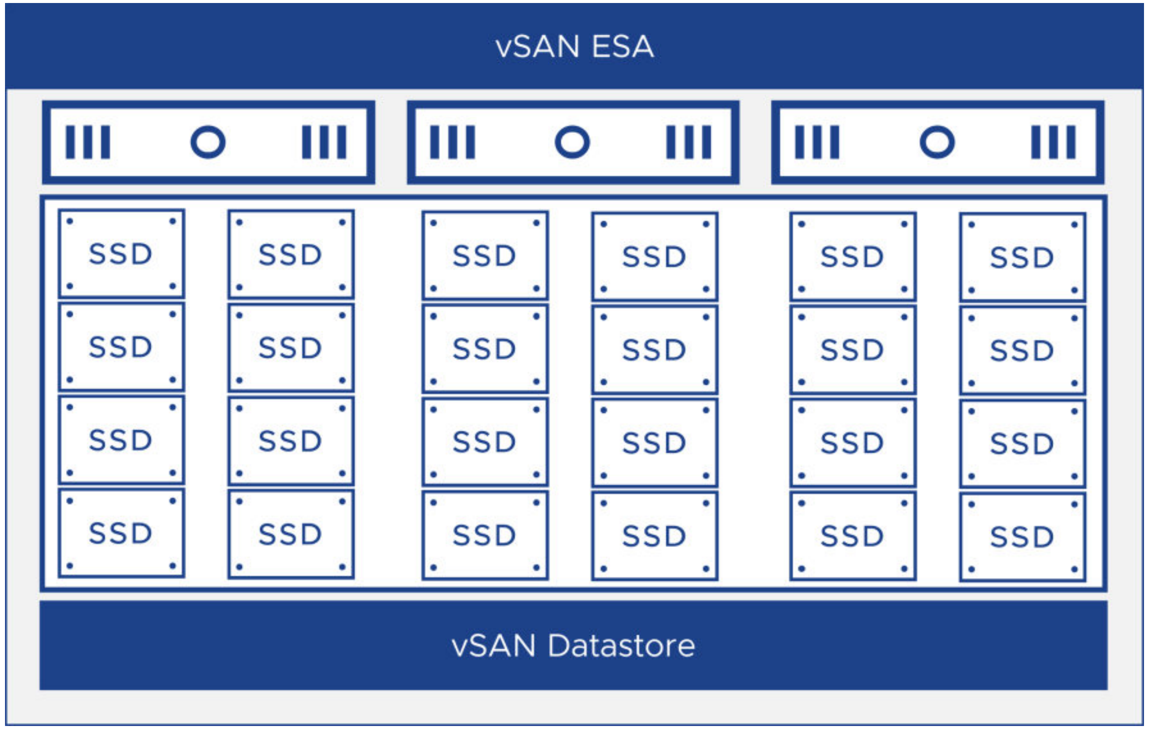
vSAN Express Storage Architecture (ESA) Introduced

Single Tier Model

vSAN ESA Requirements

ESA supports an All-Flash only configuration and has different requirements compared to vSAN OSA

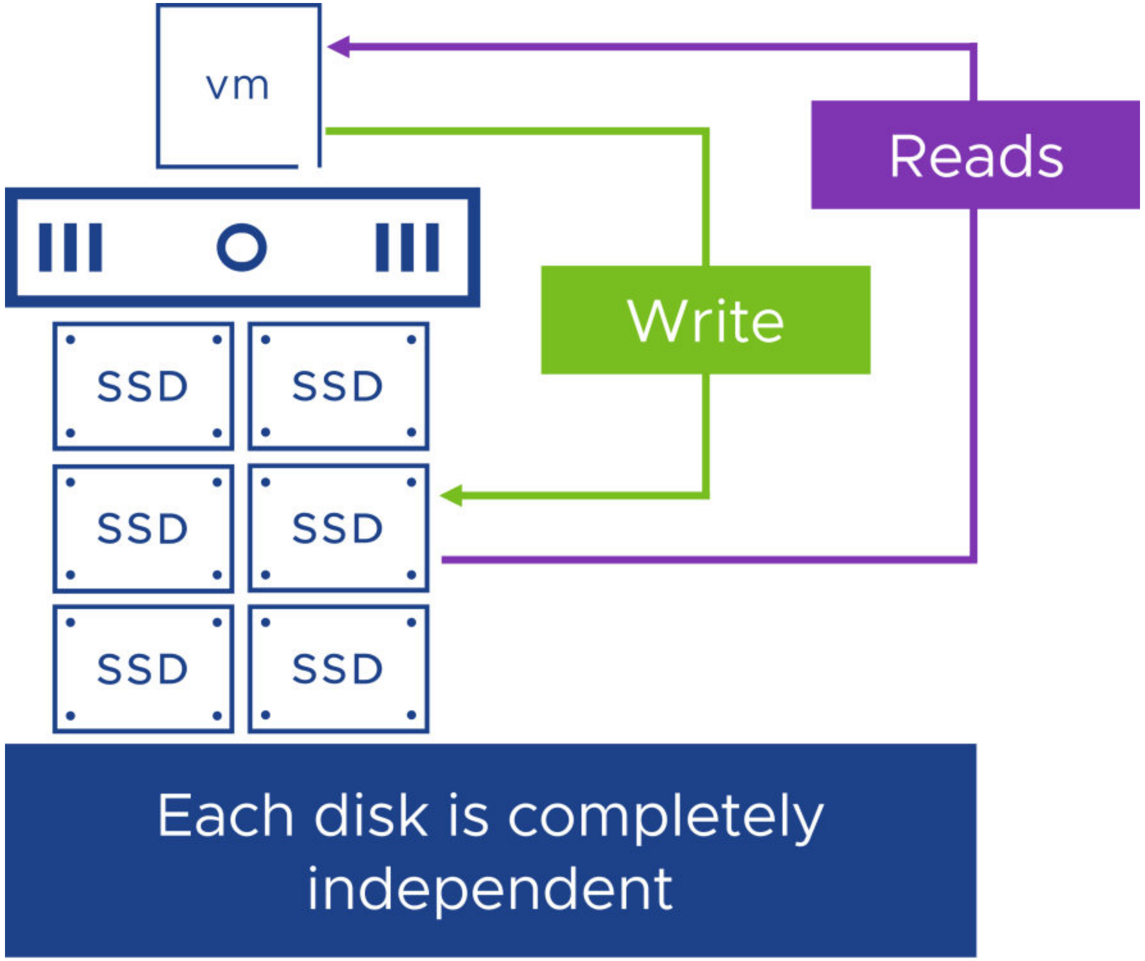
- vSAN ReadyNodes
- One 25 Gbps or faster NIC for vSAN
- One 1 Gb of faster NIC for VMs and management
- Minimum of 32 GBs of RAM
- Minimum of four SSDs or NVMe per host
- Disks at least 1.6 TBs in size



vSAN ESA Storage Pool

vSAN ESA uses the new disk configuration architecture, Storage Pool:

- Single-Tier architecture
- Only supports All-Flash
- Pool of independent disks
- Reduced I/O flow (No two-tier architecture)
- Number of disk slots define max number of disks
- Requires at least 25 Gbps network connectivity between nodes



TD SYNNEX

VMware vSphere +

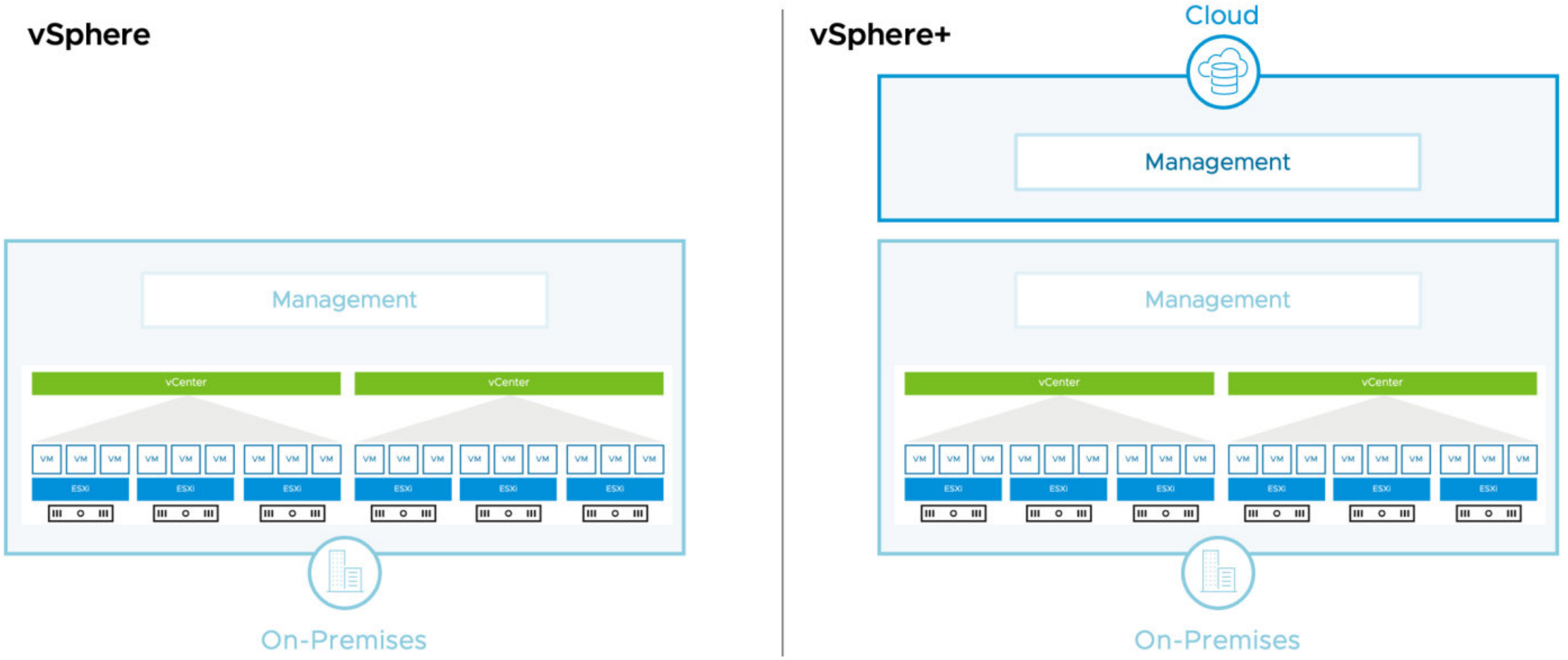
Subscription Lizenz

About vSphere+

VMware vSphere+ is a subscription-based offering that brings the benefits of cloud to on-premises workloads.

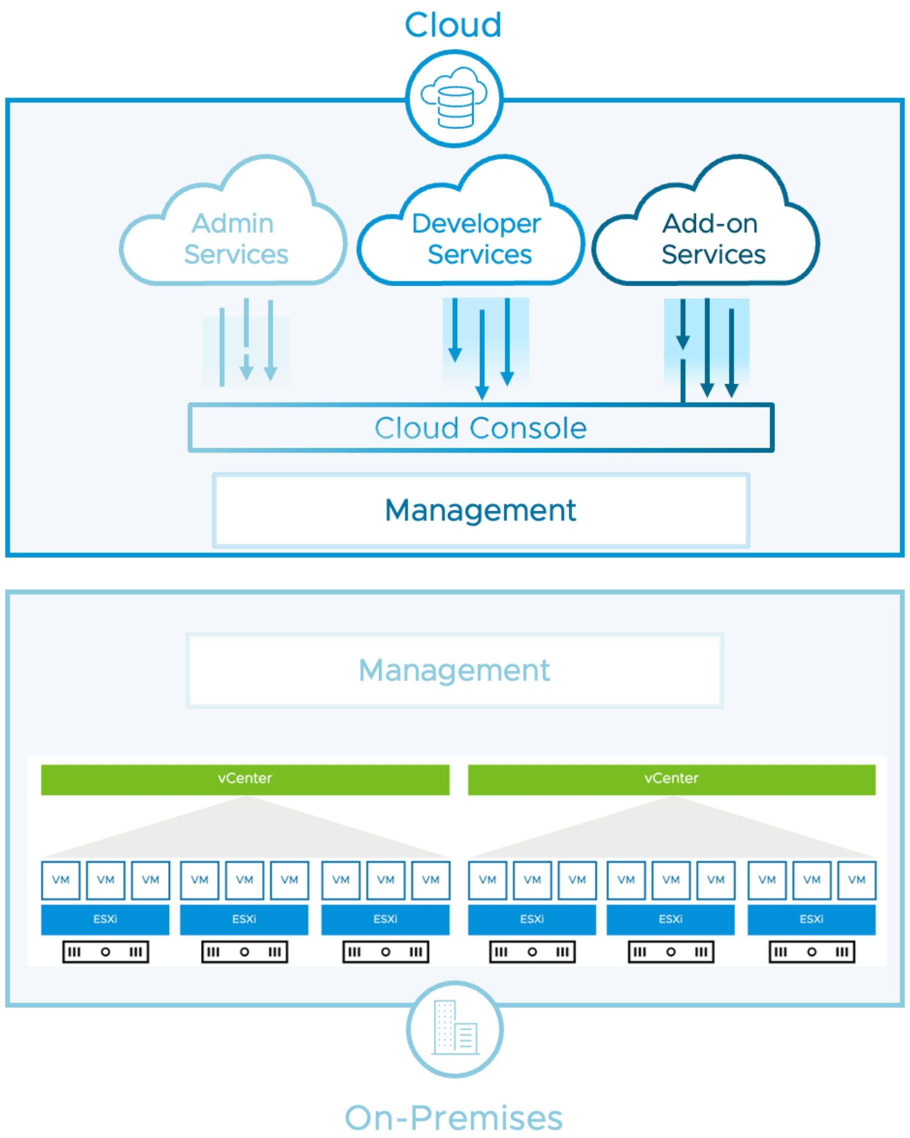
vSphere+ consists of on-premises and cloud components that interact with each other.

vSphere+ lets you centrally manage your on-premises workloads from a cloud console, with access to cloud services.



vSphere+ lets you access cloud services to augment and enhance on-premises capabilities

- Admin Services
  - Inventory management
  - Events and alerts management
  - VM provisioning
  - Lifecycle management
  - Configuration management
- Developer Services
  - Tanzu Kubernetes Grid
  - Tanzu integrated services
- Add-On Services
  - Disaster recovery



vSphere + - vSphere Enterprise Plus + vCenter

- Beispiel 36 Monate – Perpetual 10 CPU Lizenzen

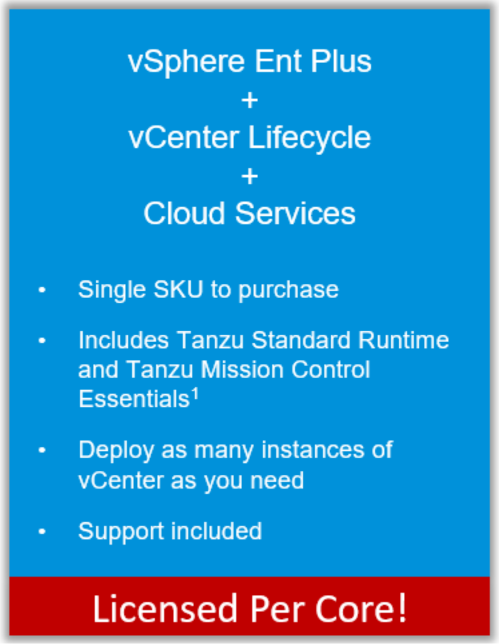
- 16 Cores pro Prozessor = 160 Cores = 48.000€

- 10 CPU Enterprise Plus mit SNS 36 Monate = 66.844€
- 1 vCenter Standard mit SNS 36 Monate = 10.426€
- Kein Tanzu usw. dabei Gesamt: 77.270€

Was ist in vSphere + enthalten / Lizensierung

- vSphere Enterprise Plus
- Beliebige Anzahl an vCenter Standard
- Tanzu Standard

- Subscription Minimum 16 Cores werden pro CPU gerechnet
- Nutzung von mehr Cores. Kunden erwerben weitere Cores per Subscription (Stand 18.10.22)



vSphere Ent Plus
+
vCenter Lifecycle
+
Cloud Services

- Single SKU to purchase
- Includes Tanzu Standard Runtime and Tanzu Mission Control Essentials[1]
- Deploy as many instances of vCenter as you need
- Support included

Licensed Per Core!

TD SYNNEX

VMware Aria

VMware Aria

Number of Tiers 2
Number of VMs 0
DiscoverySource FLOW_BASED_DISCOVERY
LastModifiedTime Thu Aug 25 2022
SupportsCuration false

- **VMware Aria Automation** (formerly, vRealize Automation)
- **VMware Aria Automation for Secure Clouds** (formerly, CloudHealth Secure State)
- **VMware Aria Operations** (formerly, vRealize Operations)
- **VMware Aria Operations for Networks** (formerly, vRealize Network Insight)
- **VMware Aria Operations for Logs** (formerly, vRealize Log Insight)
- **VMware Aria Cost powered by CloudHealth** (formerly, CloudHealth)

TD SYNNEX

VMware Carbon Black

TD SYNNEX

General Attack Situation

Every

11 seconds

A New Org Falls
Victim Every

59%

Of All Attacks Involve
Double Extortion

Source: IBM X-Force Threat Intelligence Index 2021

>4000

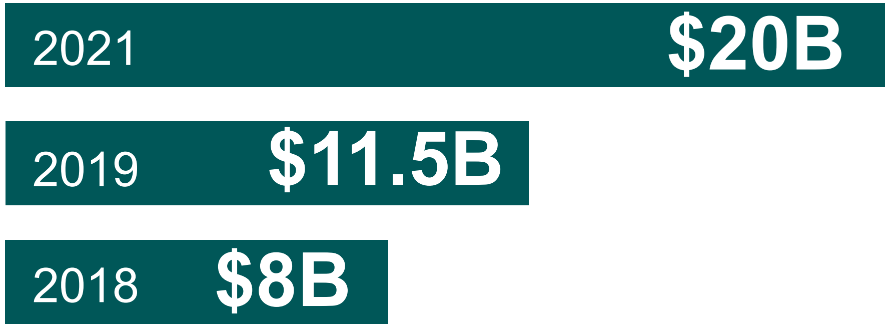
Ransomware Attacks
Happen Daily

Full Funded
Adversary Syndicates

Ransomware

As-A-Service

Damage



Security Must Be Transformed

Built-in	Unified	Context-centric
Bolted-on	Siloed	Threat-centric

Securing Endpoints Requires Dozens of Siloed Tools

And the problem is only getting worse

47

Different cybersecurity tools are deployed by a company on average

70%

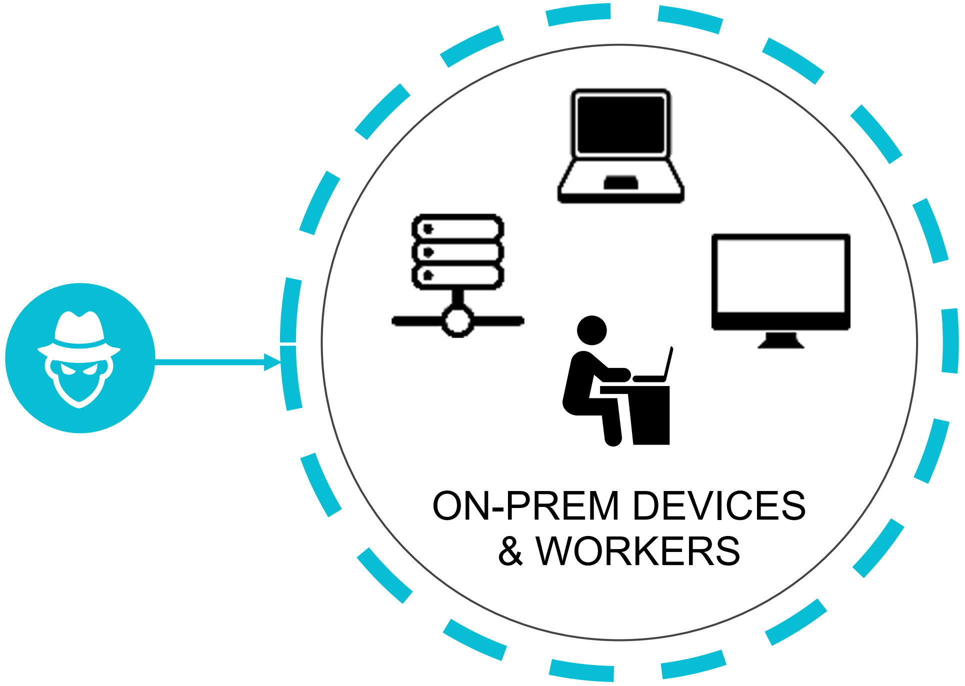
Have invested in more than five technologies in the past year alone

95%

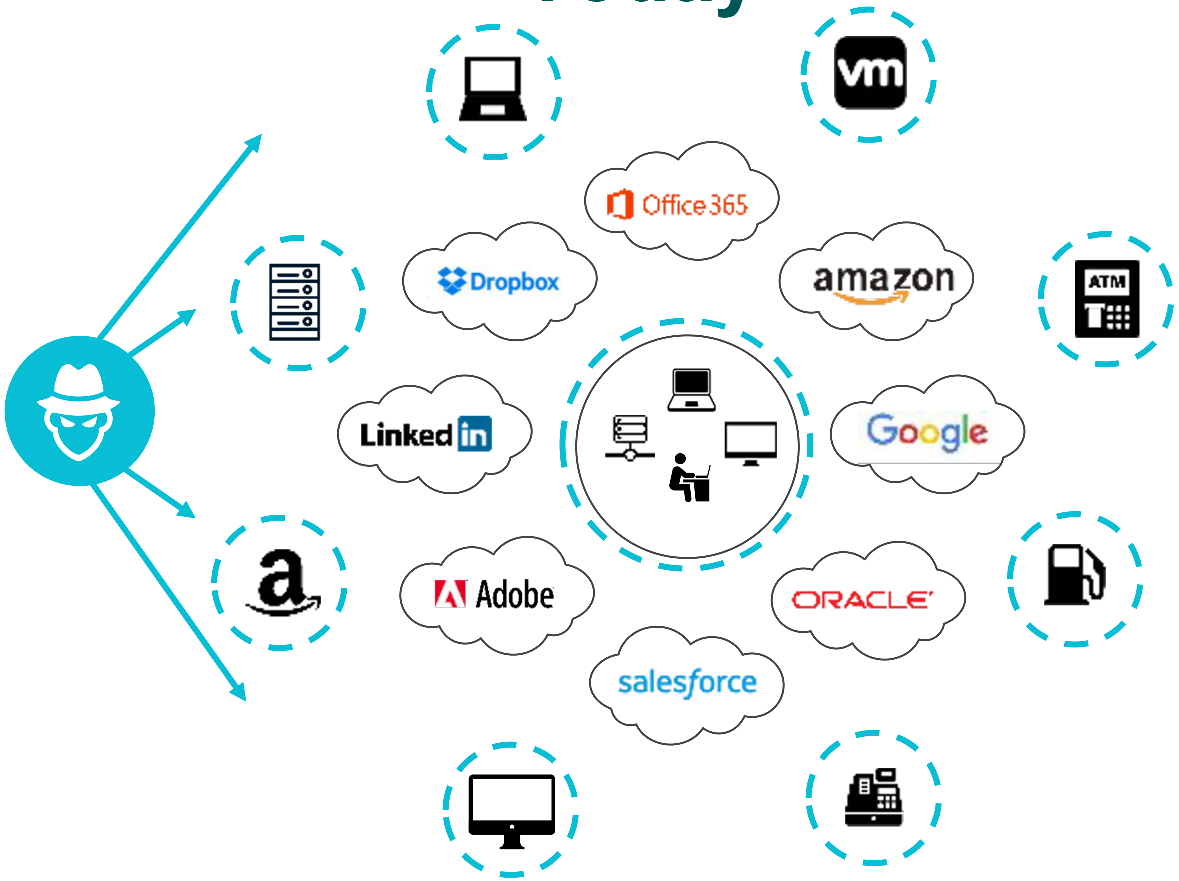
Of compromises leverage misconfiguration and misalignment of controls

Mobility & Cloud Have Transformed Security

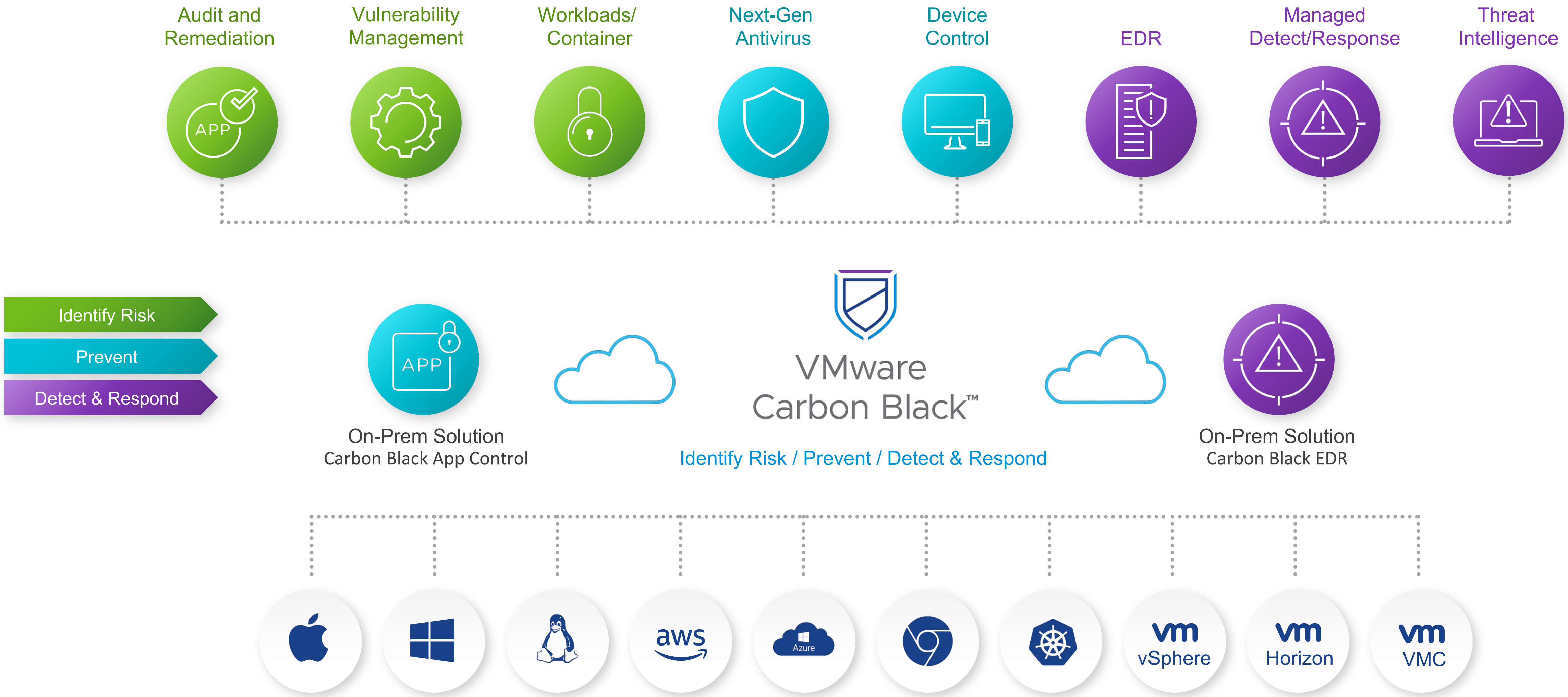
Before



Today



Carbon Black Security for Cloud, Workloads, and Endpoints



Audit and Remediation

Vulnerability Management

Workloads/ Container

Next-Gen Antivirus

Device Control

EDR

Managed Detect/Response

Threat Intelligence

Identify Risk

Prevent

Detect & Respond

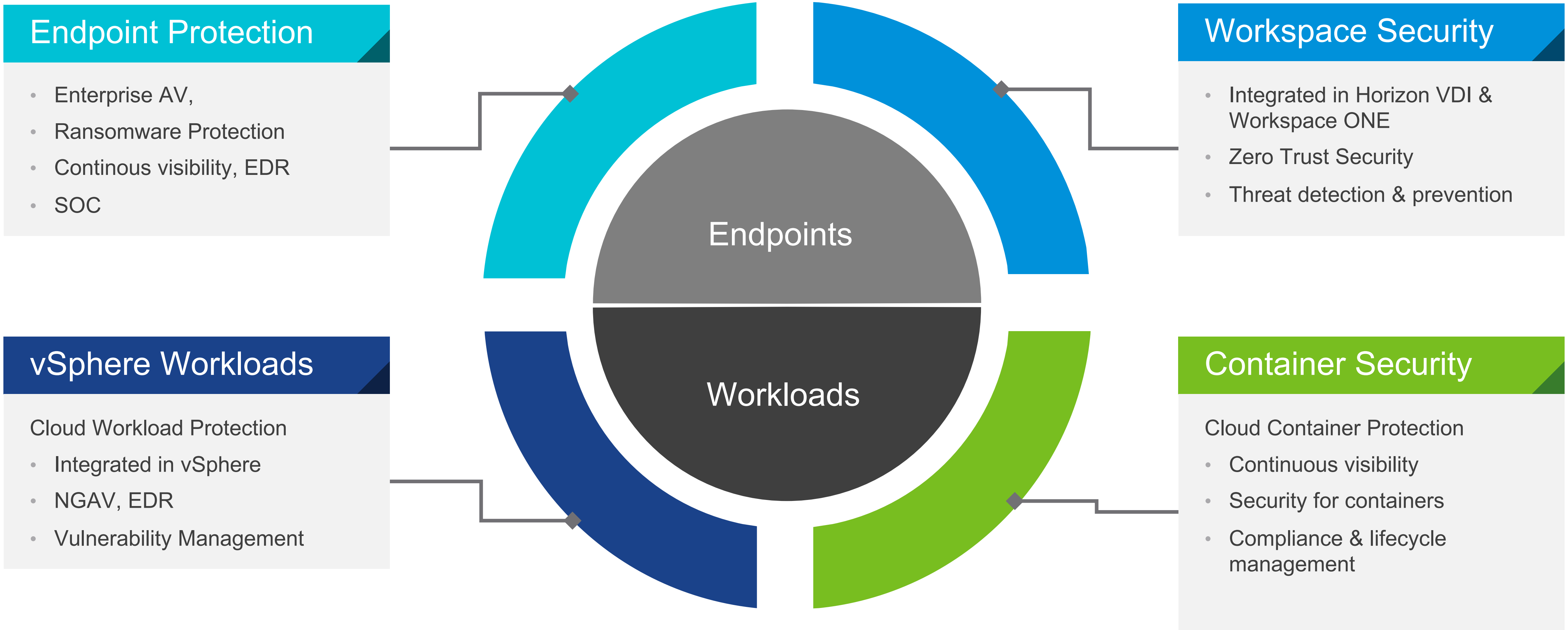
On-Prem Solution
Carbon Black App Control

VMware Carbon Black™

Identify Risk / Prevent / Detect & Respond

On-Prem Solution
Carbon Black EDR

Overview VMware Carbon Black



Endpoint Protection

- Enterprise AV,
- Ransomware Protection
- Continous visibility, EDR
- SOC

Workspace Security

- Integrated in Horizon VDI & Workspace ONE
- Zero Trust Security
- Threat detection & prevention

vSphere Workloads

Cloud Workload Protection

- Integrated in vSphere
- NGAV, EDR
- Vulnerability Management

Container Security

Cloud Container Protection

- Continuous visibility
- Security for containers
- Compliance & lifecycle management

The VMware Advantage

Increased Operational Confidence

Remote workforce, misalignment between IT and Security

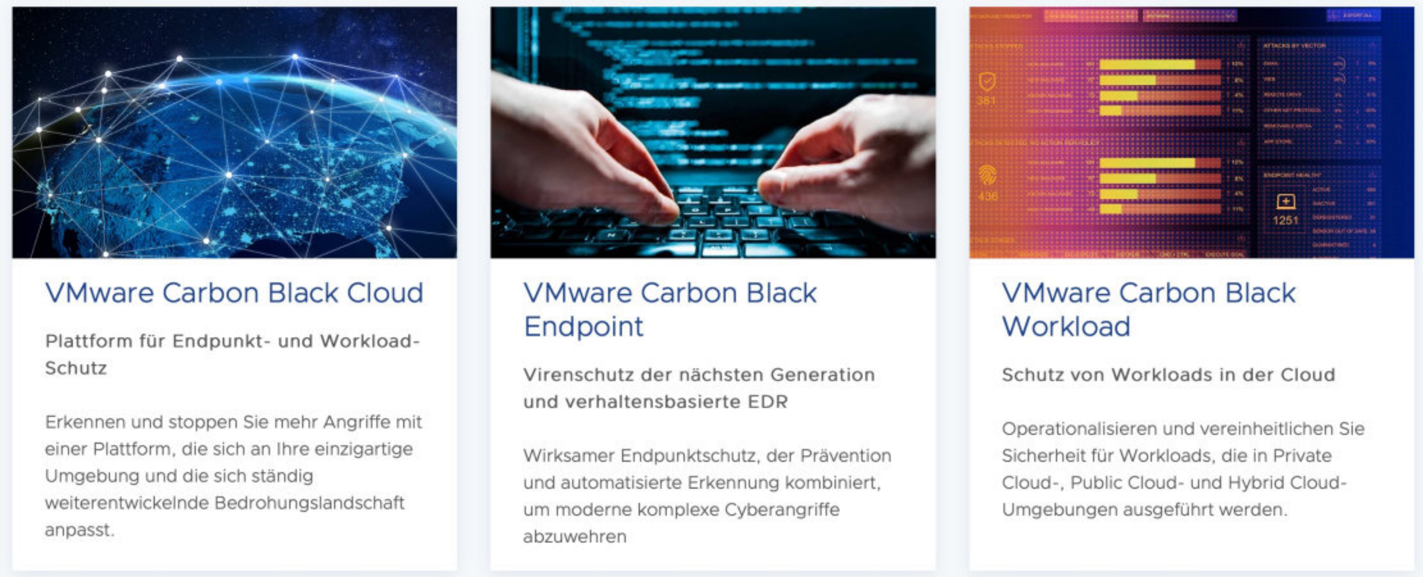
Reduced Time to Resolution

Overstretched IT/ security teams

Future-Ready Security

React quickly to the adversary, supports the transition to the cloud

Carbon Black Cloud – Übersicht



VMware Carbon Black Cloud

Plattform für Endpunkt- und Workload-Schutz

Erkennen und stoppen Sie mehr Angriffe mit einer Plattform, die sich an Ihre einzigartige Umgebung und die sich ständig weiterentwickelnde Bedrohungslandschaft anpasst.

VMware Carbon Black Endpoint

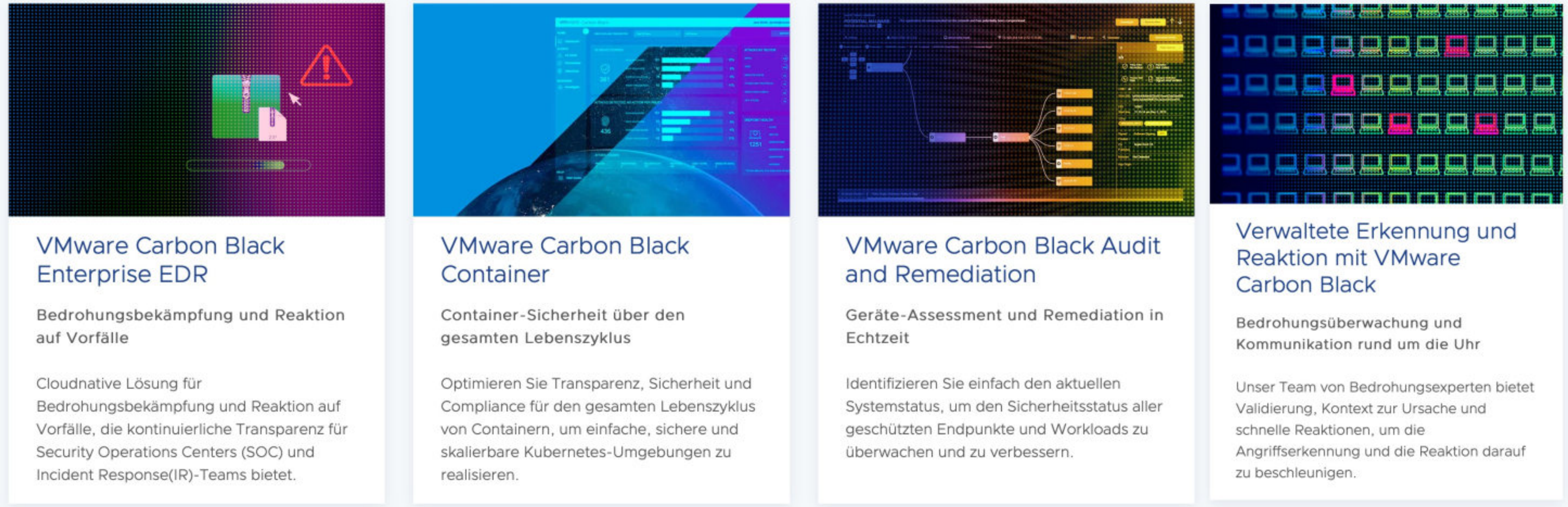
Virenschutz der nächsten Generation und verhaltensbasierte EDR

Wirksamer Endpunktschutz, der Prävention und automatisierte Erkennung kombiniert, um moderne komplexe Cyberangriffe abzuwehren

VMware Carbon Black Workload

Schutz von Workloads in der Cloud

Operationalisieren und vereinheitlichen Sie Sicherheit für Workloads, die in Private Cloud-, Public Cloud- und Hybrid Cloud-Umgebungen ausgeführt werden.



VMware Carbon Black Enterprise EDR

Bedrohungsbekämpfung und Reaktion auf Vorfälle

Cloudnative Lösung für Bedrohungsbekämpfung und Reaktion auf Vorfälle, die kontinuierliche Transparenz für Security Operations Centers (SOC) und Incident Response(IR)-Teams bietet.

VMware Carbon Black Container

Container-Sicherheit über den gesamten Lebenszyklus

Optimieren Sie Transparenz, Sicherheit und Compliance für den gesamten Lebenszyklus von Containern, um einfache, sichere und skalierbare Kubernetes-Umgebungen zu realisieren.

VMware Carbon Black Audit and Remediation

Geräte-Assessment und Remediation in Echtzeit

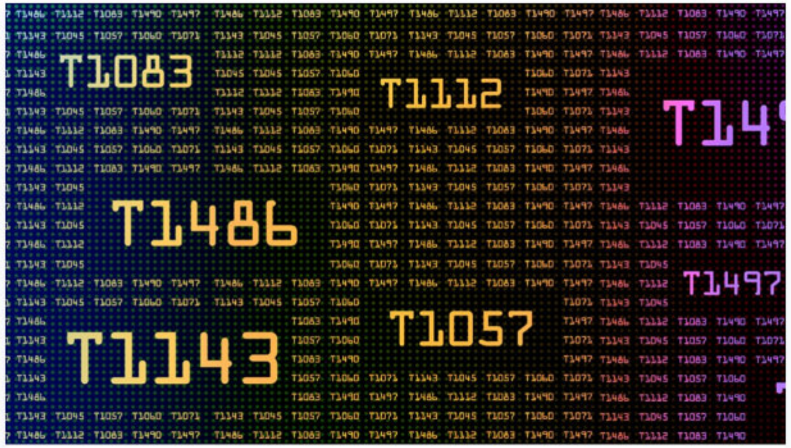
Identifizieren Sie einfach den aktuellen Systemstatus, um den Sicherheitsstatus aller geschützten Endpunkte und Workloads zu überwachen und zu verbessern.

Verwaltete Erkennung und Reaktion mit VMware Carbon Black

Bedrohungsüberwachung und Kommunikation rund um die Uhr

Unser Team von Bedrohungsexperten bietet Validierung, Kontext zur Ursache und schnelle Reaktionen, um die Angriffserkennung und die Reaktion darauf zu beschleunigen.

Carbon Black On-Premises – Übersicht

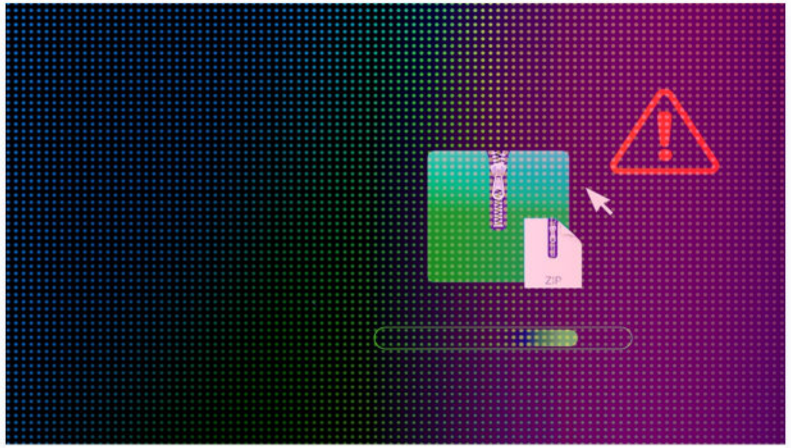


VMware Carbon Black App Control

Anwendungskontrolle und Schutz kritischer Infrastrukturen

Sperren Sie Server und kritische Systeme, verhindern Sie unerwünschte Änderungen und stellen Sie kontinuierliche Compliance mit gesetzlichen Bestimmungen sicher.

- Unterstützen Sie eine detailliertere Kontrolle Ihrer Sicherheitsrichtlinien mit inhaltsbasierter Prüfung.



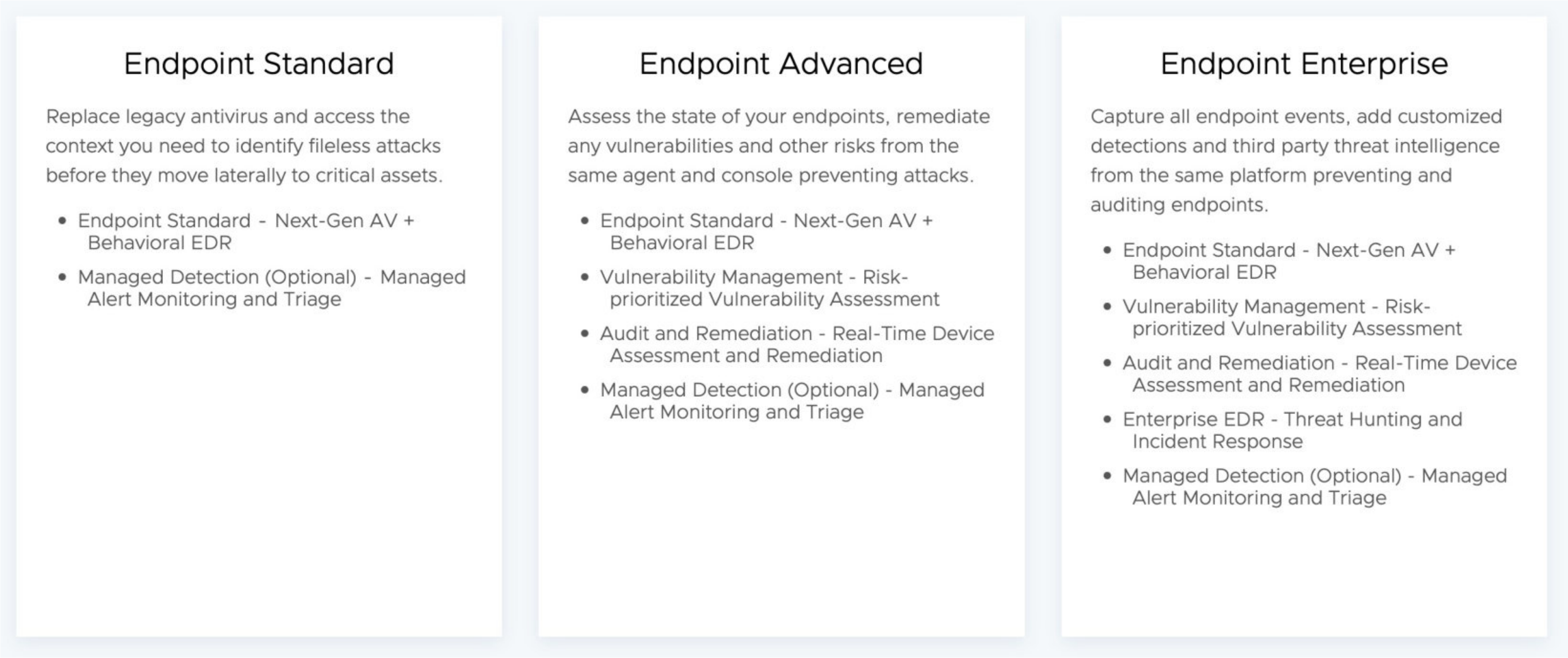
VMware Carbon Black EDR

Umfassende Erkennung und Reaktion auf komplexe Angriffe

Bedrohungsbekämpfung und Reaktion auf Vorfälle (Incident Response, IR) bieten kontinuierliche Transparenz für hybride Bereitstellungen.

- Erfassen Sie umfassende Telemetriedaten mit Informationen zu kritischen Bedrohungen, um verdächtiges Verhalten automatisch zu erkennen.
- Isolieren Sie infizierte Systeme und entfernen Sie bösartige Dateien mithilfe von detaillierten forensischen Daten für Untersuchungen nach einem Vorfall.

Carbon Black Endpoint Protection Bundles



Endpoint Standard

Replace legacy antivirus and access the context you need to identify fileless attacks before they move laterally to critical assets.

- Endpoint Standard - Next-Gen AV + Behavioral EDR
- Managed Detection (Optional) - Managed Alert Monitoring and Triage

Endpoint Advanced

Assess the state of your endpoints, remediate any vulnerabilities and other risks from the same agent and console preventing attacks.

- Endpoint Standard - Next-Gen AV + Behavioral EDR
- Vulnerability Management - Risk-prioritized Vulnerability Assessment
- Audit and Remediation - Real-Time Device Assessment and Remediation
- Managed Detection (Optional) - Managed Alert Monitoring and Triage

Endpoint Enterprise

Capture all endpoint events, add customized detections and third party threat intelligence from the same platform preventing and auditing endpoints.

- Endpoint Standard - Next-Gen AV + Behavioral EDR
- Vulnerability Management - Risk-prioritized Vulnerability Assessment
- Audit and Remediation - Real-Time Device Assessment and Remediation
- Enterprise EDR - Threat Hunting and Incident Response
- Managed Detection (Optional) - Managed Alert Monitoring and Triage

Carbon Black Endpoint – Editionsvergleich 1/2

Funktionen	CBC Standard	CBC Advanced	CBC Enterprise
Virenschutz und Malware	X	X	X
EDR	X	X	X
Warnmeldungen	X	X	X
Quarantäne	X	X	X
Remotekonsole	X	X	X
Regel vor der Einführung testen	X	X	X
Abstimmbare Prävention	X	X	X
Drittanbietern Threat Detection			X
Benutzerdefinierte Warnmeldungen			X
Integration von API	X	X	X
Abfragesprache	X	X	X

Carbon Black Endpoint – Editionsvergleich 2/2

Funktionen	CBC Standard	CBC Advanced	CBC Enterprise
Virenschutzsignatur – erstmaliger vollständiger Scan	X	X	X
Geplante Virenscan			
Virenschutzsignaturprüfung beim Download	X	X	X
Untersuchen der IP-Adressensuche	X	X	X
Untersuchen der Nutzersuche	X	X	X
Untersuchen der Hash-Suche	X	X	X
USB-Gerätesteuerung	X	X	X
Vollständige Datenaufbewahrung (Tage)	30	30	30
Incident-Datenaufbewahrung (Tage)	180	180	180
Abfragen des Betriebssystems nach Informationen		X	X
Protokoll der geänderten Dateien			
Sandbox	X	X	X
Kontrollierte Veröffentlichung neuer Versionen	X	X	X

TD SYNNEX

Vielen Dank !