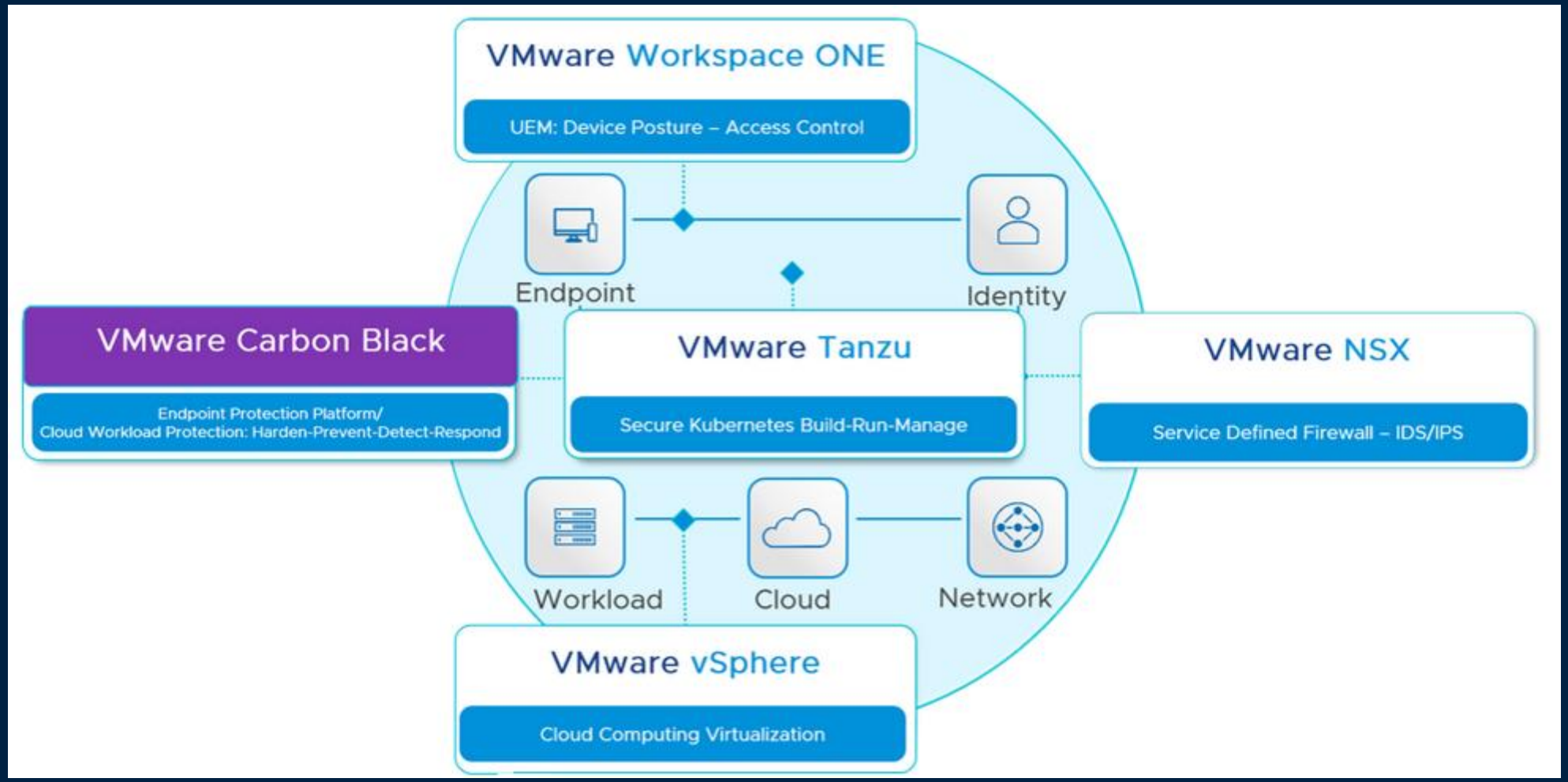
Solução Carbon Black

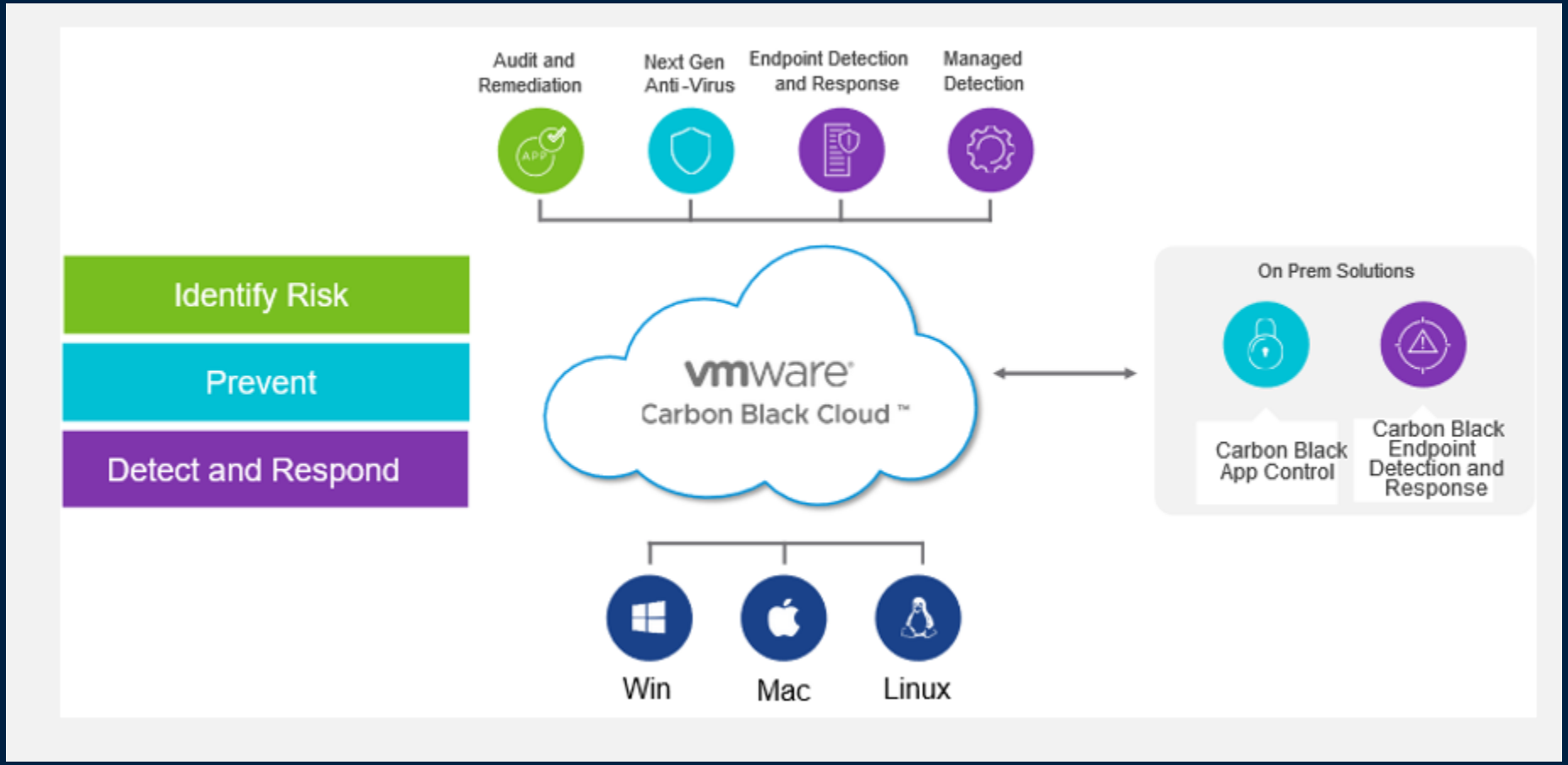
© Ingram Micro Inc.

Proprietary information of Ingram Micro Inc. — Do not distribute or duplicate without Ingram Micro's express written permission.

VMware Foundational Solutions

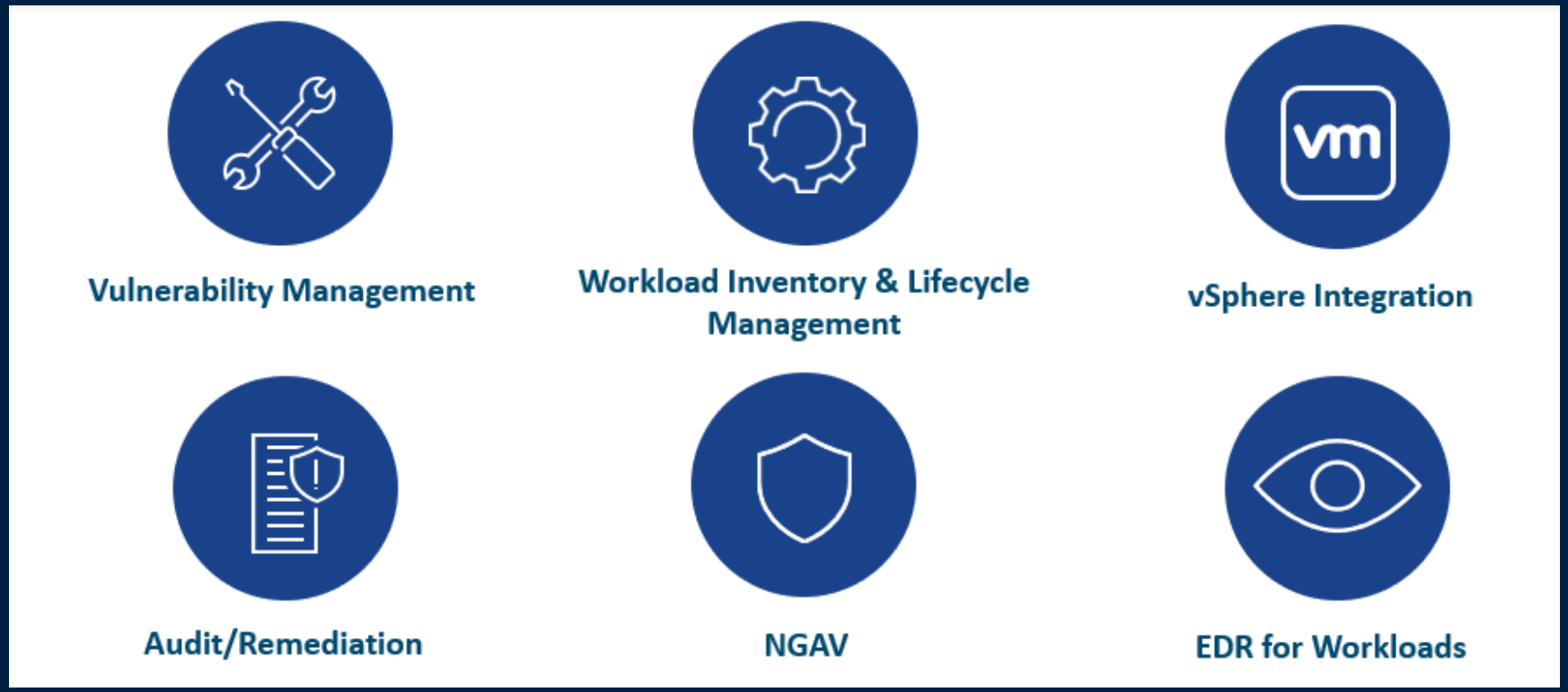


VMware Carbon Black Cloud



VMware Carbon Black's single-agent offering of all four core EPP capabilities

VMware Carbon Black Cloud Workload



Reduce Attack Surface

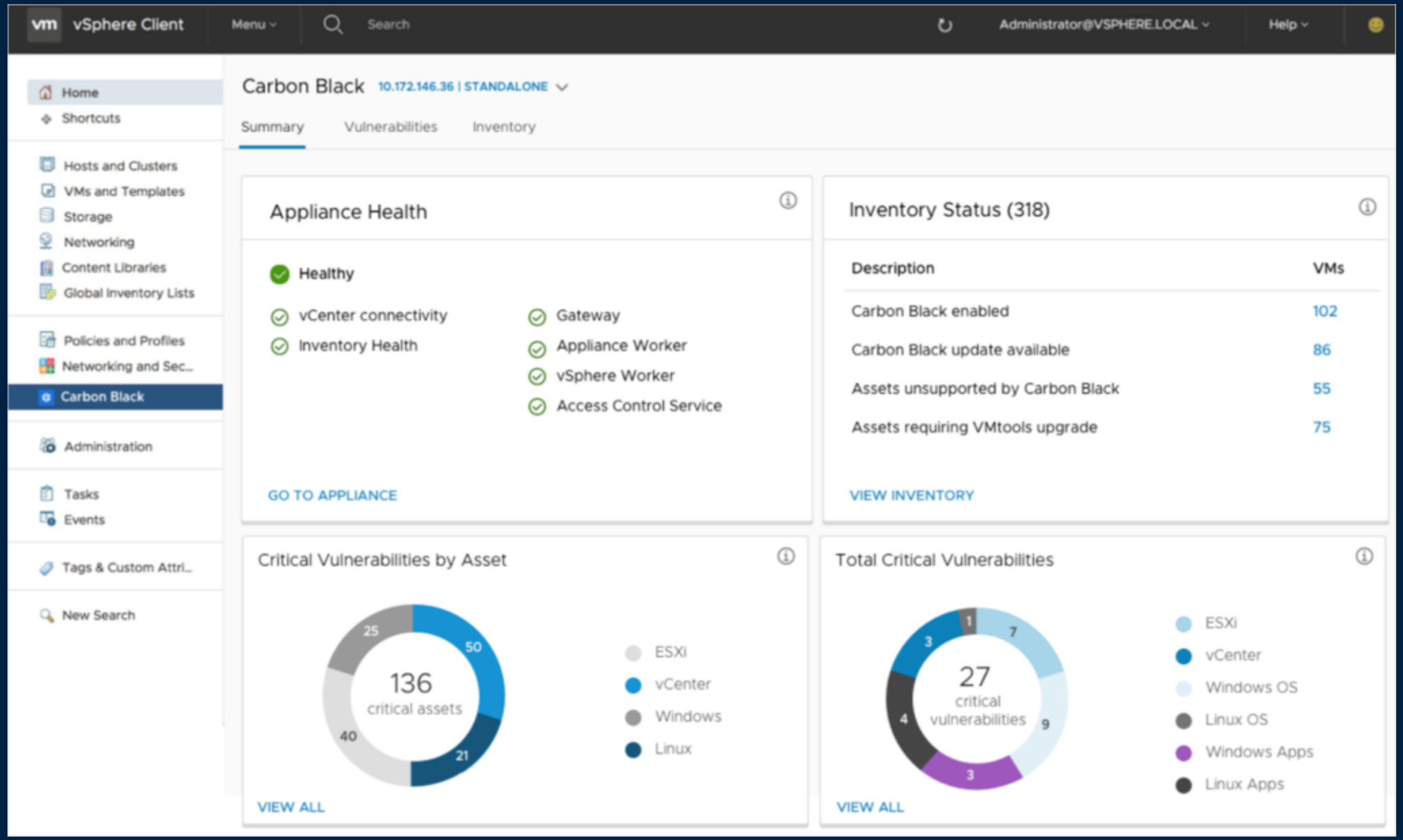
Identify risk and harden workloads against attack.

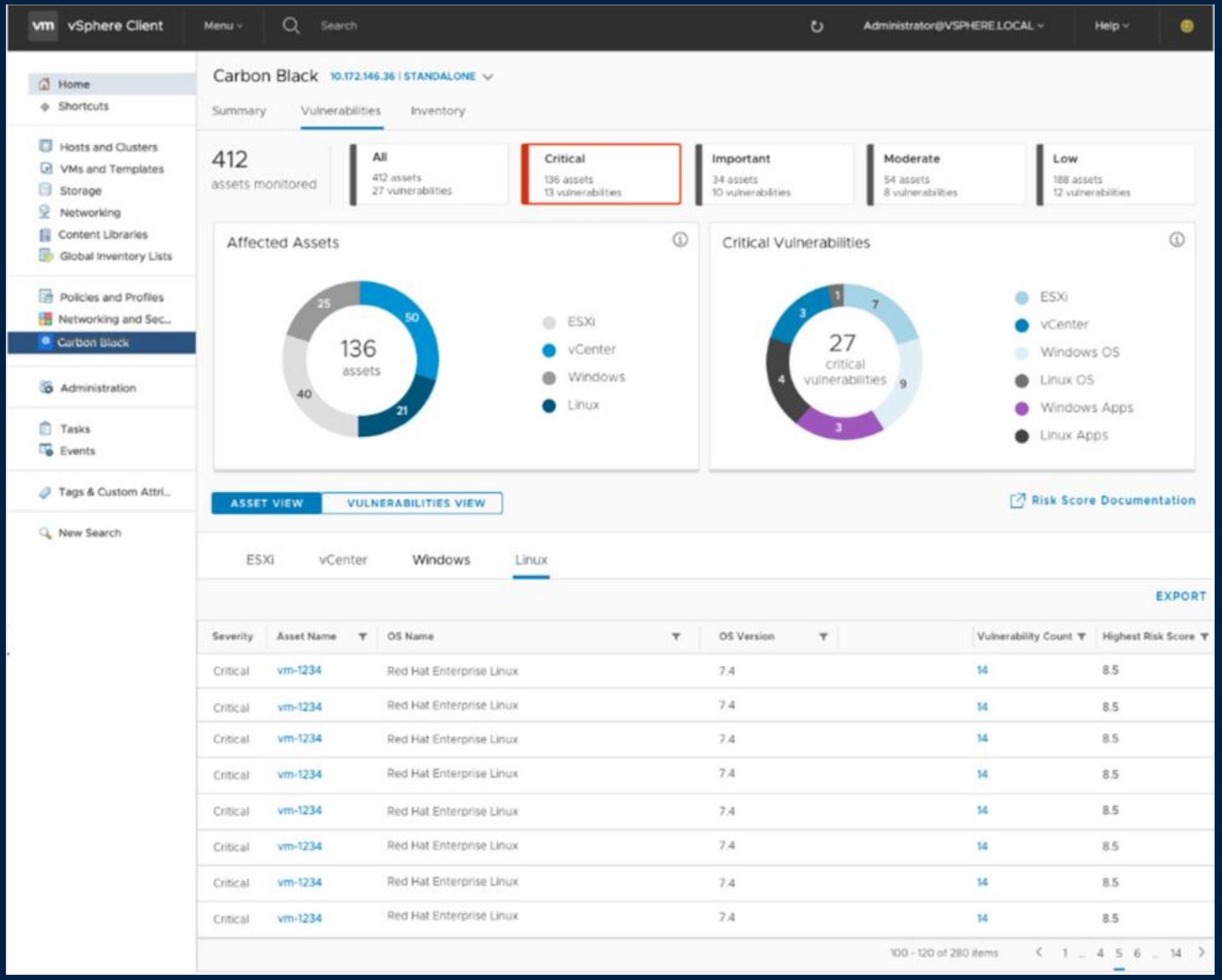
Increase Visibility

Easy to understand current state of workloads and vulnerabilities.

Simplify Operations

Better collaboration and shared intelligence for IT and Security teams.


vSphere Client
Menu
Search
Administrator@VSPHERE.LOCAL
Help
Home
Shortcuts
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Global Inventory Lists
Policies and Profiles
Networking and Sec...
Carbon Black
Administration
Tasks
Events
Tags & Custom Attri...
New Search
Carbon Black 10.172.146.36 | STANDALONE
Summary
Vulnerabilities
Inventory
Appliance Health
Healthy
vCenter connectivity
Inventory Health
Gateway
Appliance Worker
vSphere Worker
Access Control Service
GO TO APPLIANCE
Inventory Status (318)
Description
VMs
Carbon Black enabled
102
Carbon Black update available
86
Assets unsupported by Carbon Black
55
Assets requiring VMtools upgrade
75
VIEW INVENTORY
Critical Vulnerabilities by Asset
136
critical assets
50
21
40
25
ESXi
vCenter
Windows
Linux
VIEW ALL
Total Critical Vulnerabilities
27
critical
vulnerabilities
7
9
3
4
3
1
ESXi
vCenter
Windows OS
Linux OS
Windows Apps
Linux Apps
VIEW ALL


vSphere Client
Menu
Search
Administrator@VSPHERE.LOCAL
Help
Home
Shortcuts
Hosts and Clusters
VMs and Templates
Storage
Networking
Content Libraries
Global Inventory Lists
Policies and Profiles
Networking and Sec...
Carbon Black
Administration
Tasks
Events
Tags & Custom Attri...
New Search
Carbon Black 10.172.146.36 | STANDALONE
Summary
Vulnerabilities
Inventory
412
assets monitored
All
412 assets
27 vulnerabilities
Critical
136 assets
13 vulnerabilities
Important
34 assets
10 vulnerabilities
Moderate
54 assets
8 vulnerabilities
Low
188 assets
12 vulnerabilities
Affected Assets
136
assets
50
21
40
25
ESXi
vCenter
Windows
Linux
Critical Vulnerabilities
27
critical
vulnerabilities
7
9
3
4
3
1
ESXi
vCenter
Windows OS
Linux OS
Windows Apps
Linux Apps
ASSET VIEW
VULNERABILITIES VIEW
Risk Score Documentation
ESXi
vCenter
Windows
Linux
EXPORT
Severity
Asset Name
OS Name
OS Version
Vulnerability Count
Highest Risk Score
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
Critical vm-1234 Red Hat Enterprise Linux 7.4 14 8.5
100 - 120 of 280 items
1 4 5 6 14

VMware Carbon Black Workspace Security

NGAV + EDR

Detects endpoint malware and behavioral threats and send to Intelligence.

Allows IT Ops and SecOps to get more depth of data on a compliance or security issue

Comprehensive Digital Workspace Security

Deliver zero trust security with Workspace ONE Intelligence continuous verification of user and device risk.

Combines broad WS1 Intelligence compliance & risk view w/ Carbon Black real-time threat

Manage Entire Device and App Lifecycle

Entitle, provision, and deploy apps easily across devices and enable DLP

Integrated insights, App analytics and Automation

Combines best-in-class behavior threat detection, NGAV, and digital workspace analytics & remediation solutions

Carbon Black Cloud

VMware Carbon Black Cloud Endpoint Standard

Certified to replace and extend traditional antivirus

Next-Gen Antivirus + EDR

ADAPTIVE PREVENTION

- Stops malware & fileless attacks
- Unique behavioral approach uses EDR data to stop unknown attacks
- Strongest ransomware protection – 100% efficacy in 3rd-party testing
- Online & offline protection
- Flexible policy configurations for advanced users

BEHAVIORAL EDR

- Clear, behavioral view of endpoint activity
- Visualize every stage of an attack and uncover root cause in minutes
- Easily search and investigate endpoints
- Live Response to fix issues in real time

GROWS WITH YOUR TEAM

- Out-of-box detection & prevention for less sophisticated teams
- Easily configured dashboard to reduce noise and complexity
- Real-time investigation for teams w/o dedicated IR practitioners

VMware Carbon Black Cloud Audit & Remediation

Ask questions and take action in real time

Real-time Query & Remediation

ON-DEMAND AUDIT

- Inspect endpoints on demand
- Remotely assess to understand current system state
- On-demand access to 1,500+ security artifacts
- Make quick decisions to reduce risk

REAL-TIME REMEDIATION

- Secure, remote shell into any protected endpoint
- Fix issues in real time
- Remotely perform full investigations and remediation
- Immediately resolve risky configurations and vulnerabilities

SIMPLIFIED OPERATIONS

- Built on a true security platform
- Single agent & single console
- Query results stored in the cloud
- Easy to manage
- No impact to users

VMware Carbon Black Cloud Enterprise EDR

Detect and respond to advanced attacks

Advanced Threat Hunting & IR

COMPLETE VISIBILITY

- Capture all endpoint activity
- Visualize the attack
- Identify root cause
- Aggregate custom threat intel
- Minimize resource impact

SCALE THE HUNT

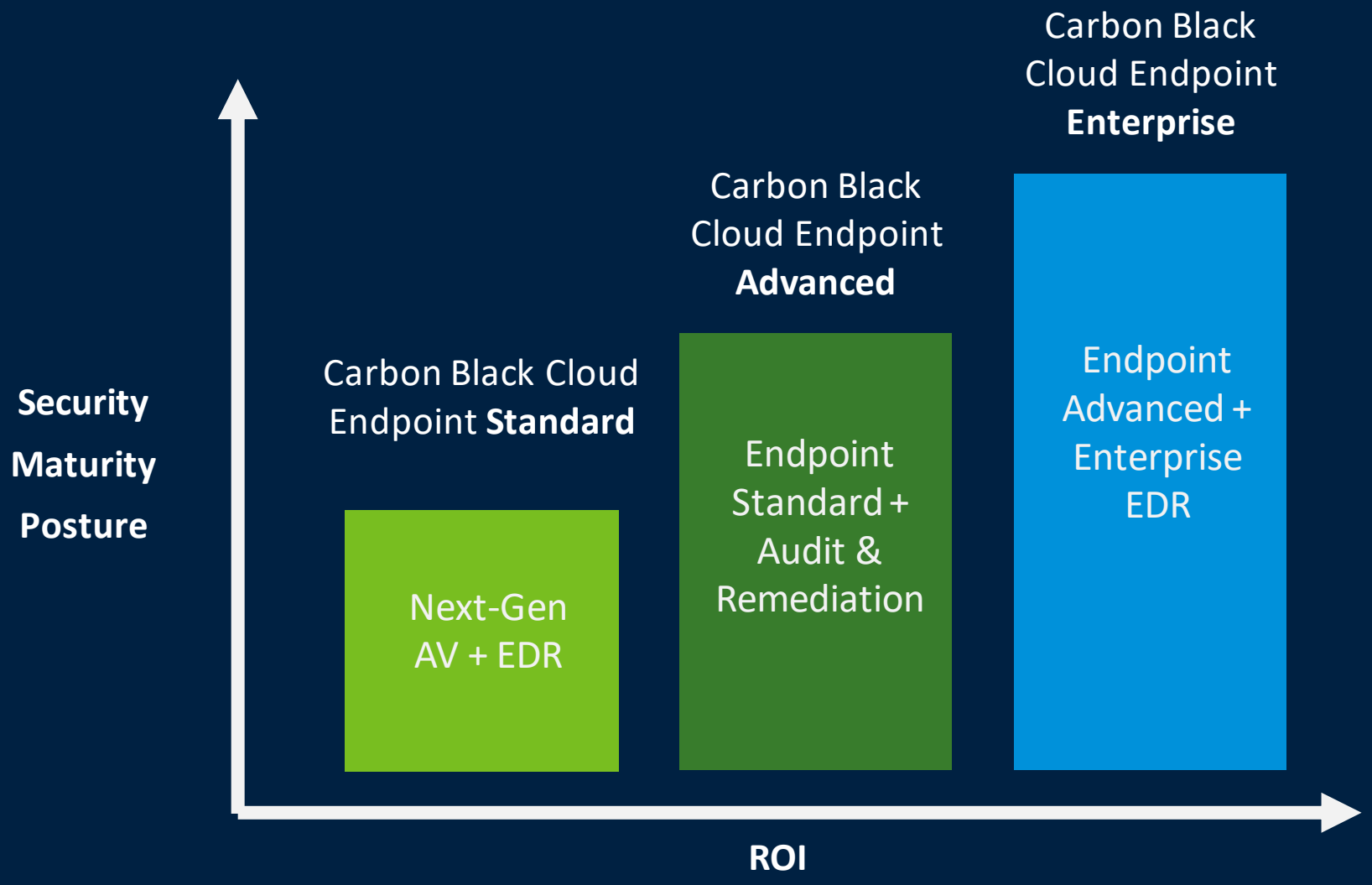
- Stop advanced threats
- Automate the hunt
- Reduce the attack surface
- Integrate defenses
- Leverage community experts

RESPOND IMMEDIATELY

- Isolate infected systems
- Ban malicious files
- Collect forensic data
- Remotely remediate devices

Carbon Black Cloud Endpoint Packages

Security Posture vs ROI



CBC Endpoint Standard provides Next-Gen AV + EDR

CBC Endpoint Advanced comes with Endpoint Standard + Audit & Remediation

CBC Endpoint Enterprise comes with Endpoint Advanced + Enterprise EDR

VMware Carbon Black Cloud Managed Detection

Prevent breaches with expert threat hunters at your side

Managed Alert Triage

Expert Threat Validation

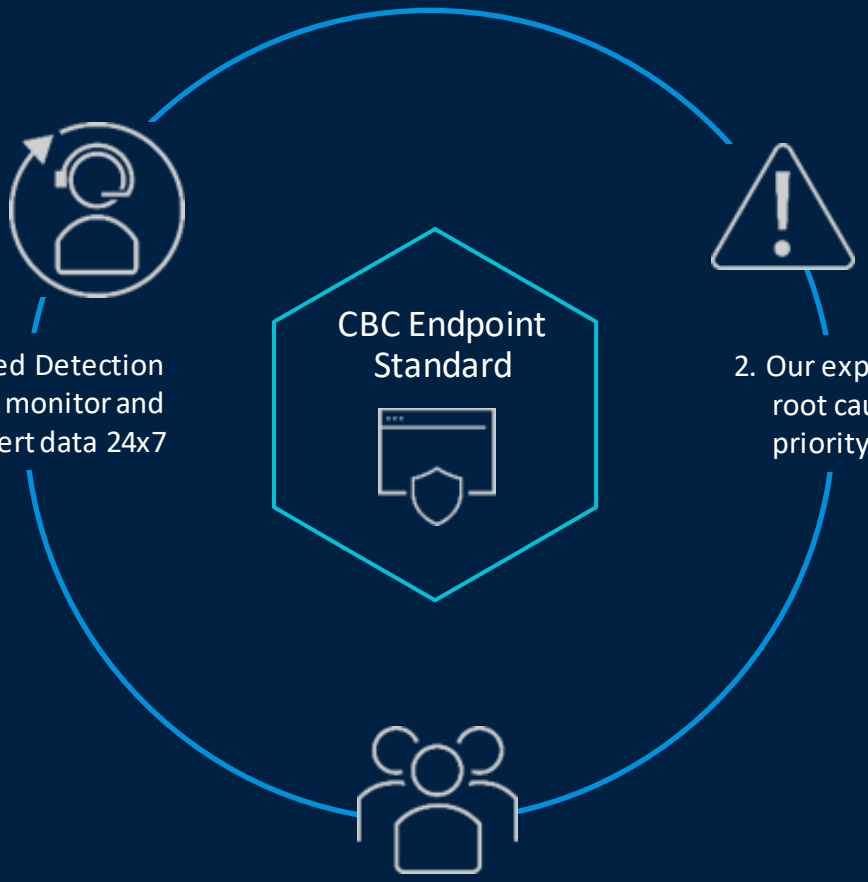
Analyzes, validates, and prioritizes alerts so that nothing is missed

Early Warning System

Identifies trends and proactively sends advisories to ensure a confident response

Roadmap to Root Cause

Provides additional context to streamline investigations and root cause analysis



1. CBC Managed Detection experts monitor and analyze alert data 24x7
2. Our experts validate alerts, analyze root cause, and notify you of high-priority threats
3. Armed with contextual data, your team can confidently take action directly from the CBC Endpoint Standard console

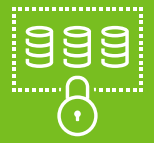
VMware Carbon Black App Control

Market-leading application control solution

Application Control

on-prem

LOCKDOWN SYSTEMS



- Strongest security possible
- Blocks malware, advanced attacks
- Prevents unwanted change
- Cross platform support

CONTINUOUS COMPLIANCE

- Enforce configuration integrity
- Monitor critical system activity
- Assess compliance risk
- Secure end-of-life systems

HIGH-PERFORMANCE & EASE OF MGMT

- Fast time to value
- Easy to manage
- Minimal impact to systems
- Low resource usage (<1 admin per 10,000 systems)

VMware Carbon Black EDR / Hosted EDR

Detect and respond to advanced attacks

SOC & Incident Response

COMPLETE VISIBILITY

- Capture all endpoint activity
- Visualize the attack
- Identify root cause
- Aggregate custom threat intel
- Minimize resource impact

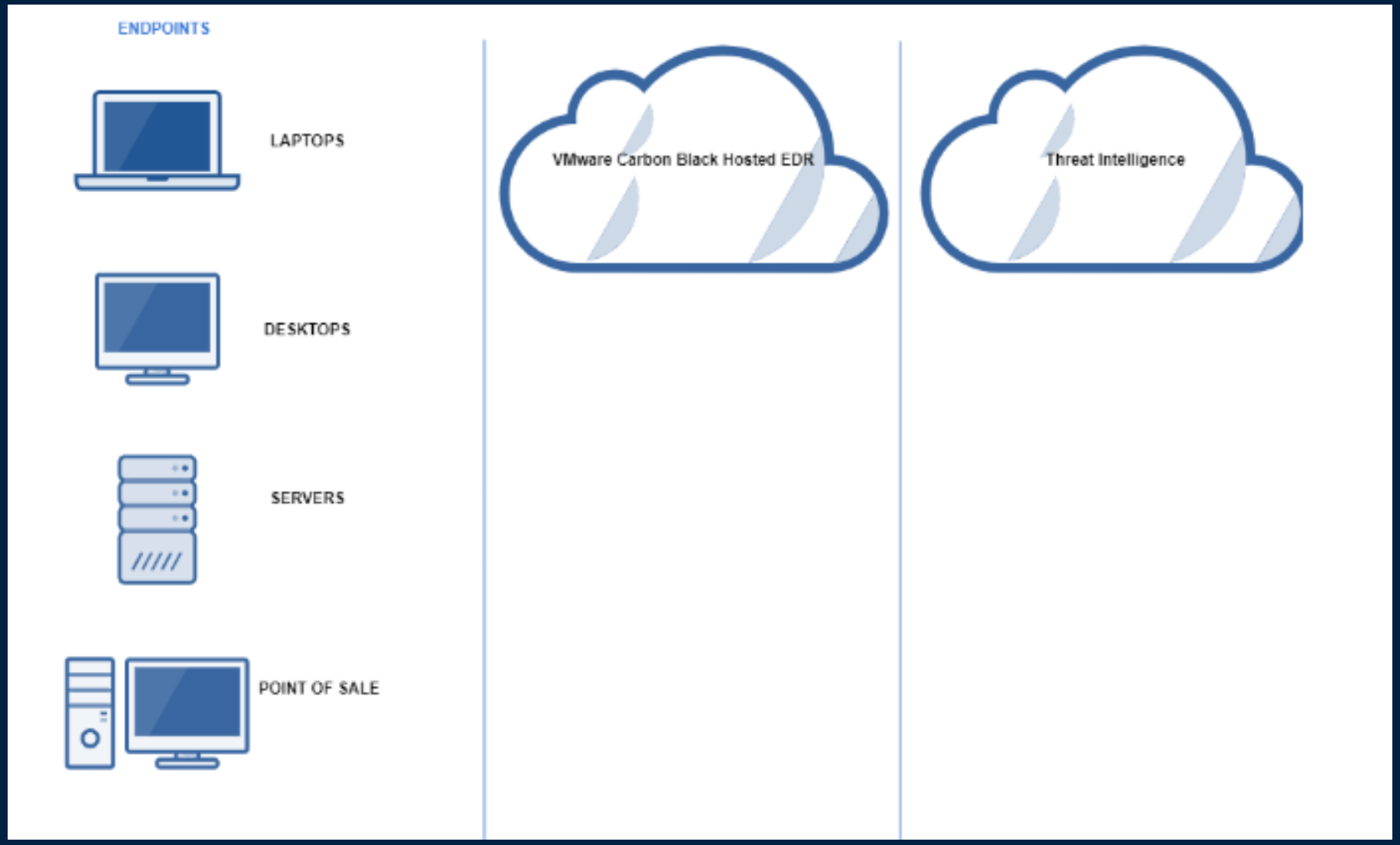
PROACTIVE THREAT HUNTING

- Automate the hunt
- Stop the “headline” breach
- Make the next attack harder
- Integrate defenses
- Leverage community experts

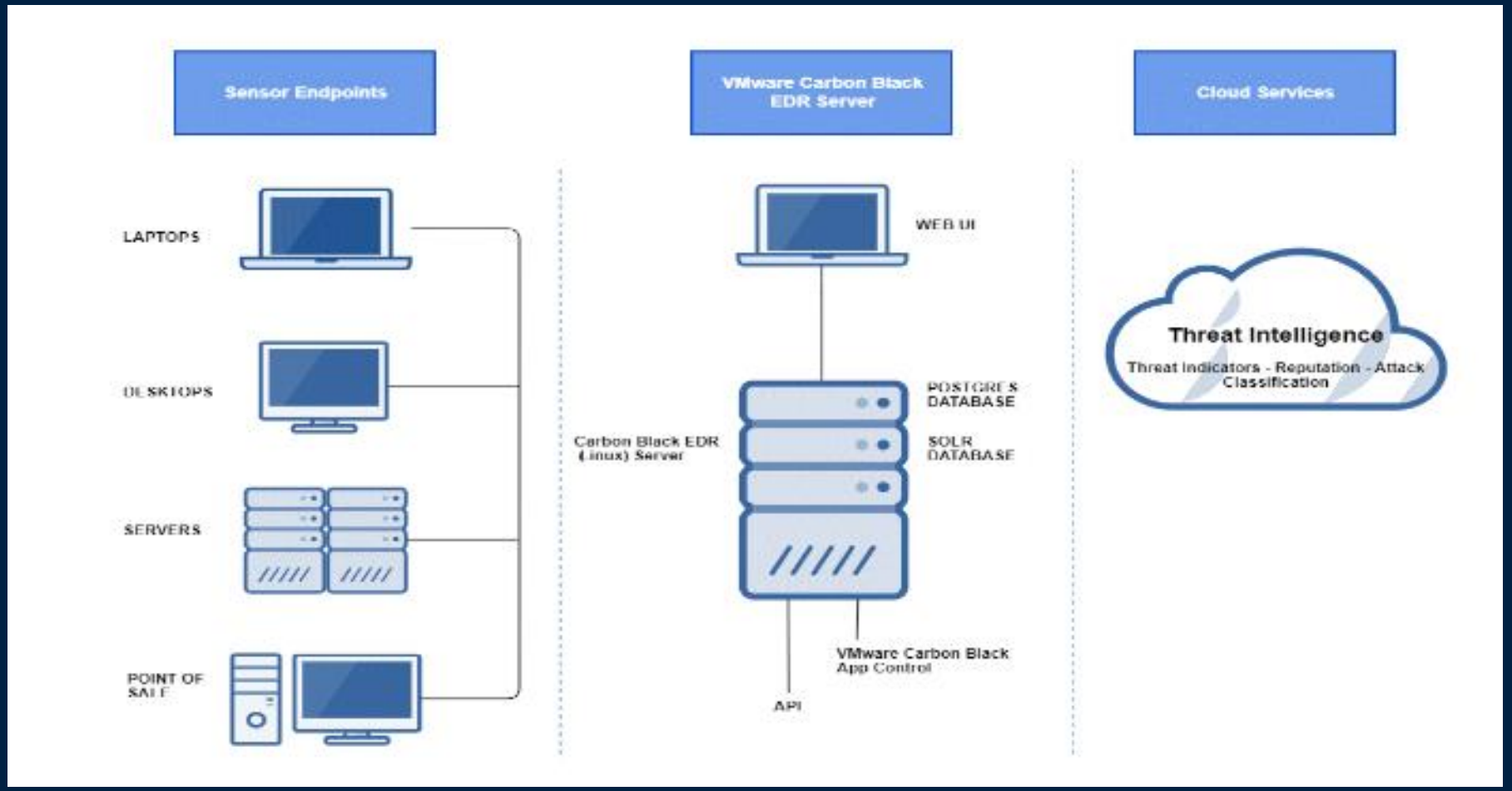
RESPOND IMMEDIATELY

- Isolate infected systems
- Collect forensic data
- Remediate infected devices
- Prevent future attacks

Carbon Black Hosted EDR



Carbon Black EDR



- **VMware Workspace Security™** - The VMware Workspace Security offerings may include certain VMware Carbon Black Cloud functionality in combination with VMware Workspace ONE® and/or VMware Horizon® Service capabilities.
  For details on the Workspace ONE offerings, see the Service Description at:
  https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/workspace-one-service-description.pdf
  For details on the Horizon Service offerings, see the Service Description at:
  https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/downloads/eula/vmw-horizon-service-description.pdf
- **VMware Advanced Security™ for VMware Cloud Foundation™** – VMware Carbon Black Workload Advanced, plus VMware NSX® Advanced Load Balancer™ and VMware NSX® Advanced Threat Prevention™ add-on.

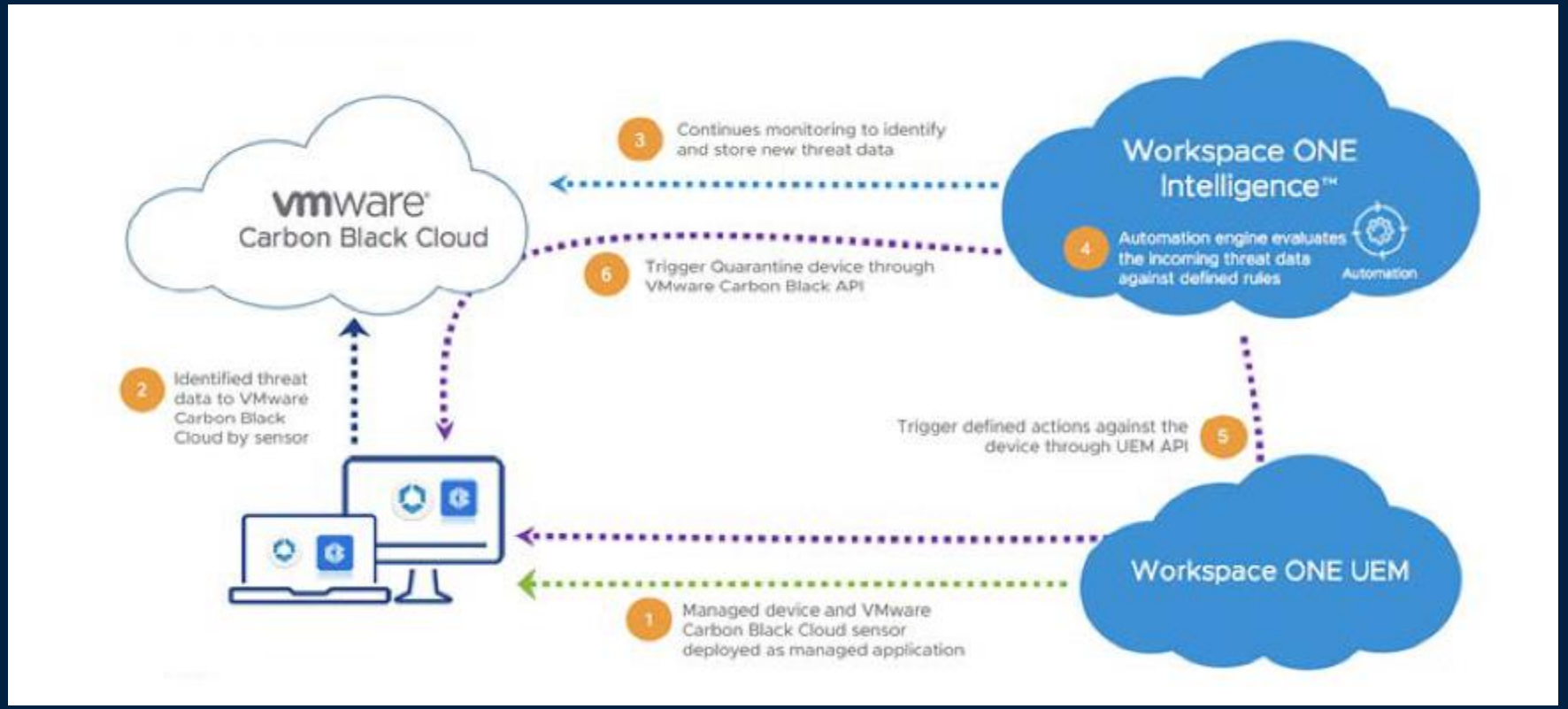
Announcing the General Availability of Container Security in the VMware Carbon Black Cloud

Octarine

Carbon Black Workspace Security

VMware Workspace Security

Combines best-in-class behavior threat detection, NGAV, and digital workspace analytics & remediation solutions



https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-workspace-security-solutions.pdf

VMware Workspace Security

Combines best-in-class behavior threat detection, NGAV, and digital workspace analytics & remediation solutions

VMware Carbon Black Product Portfolio

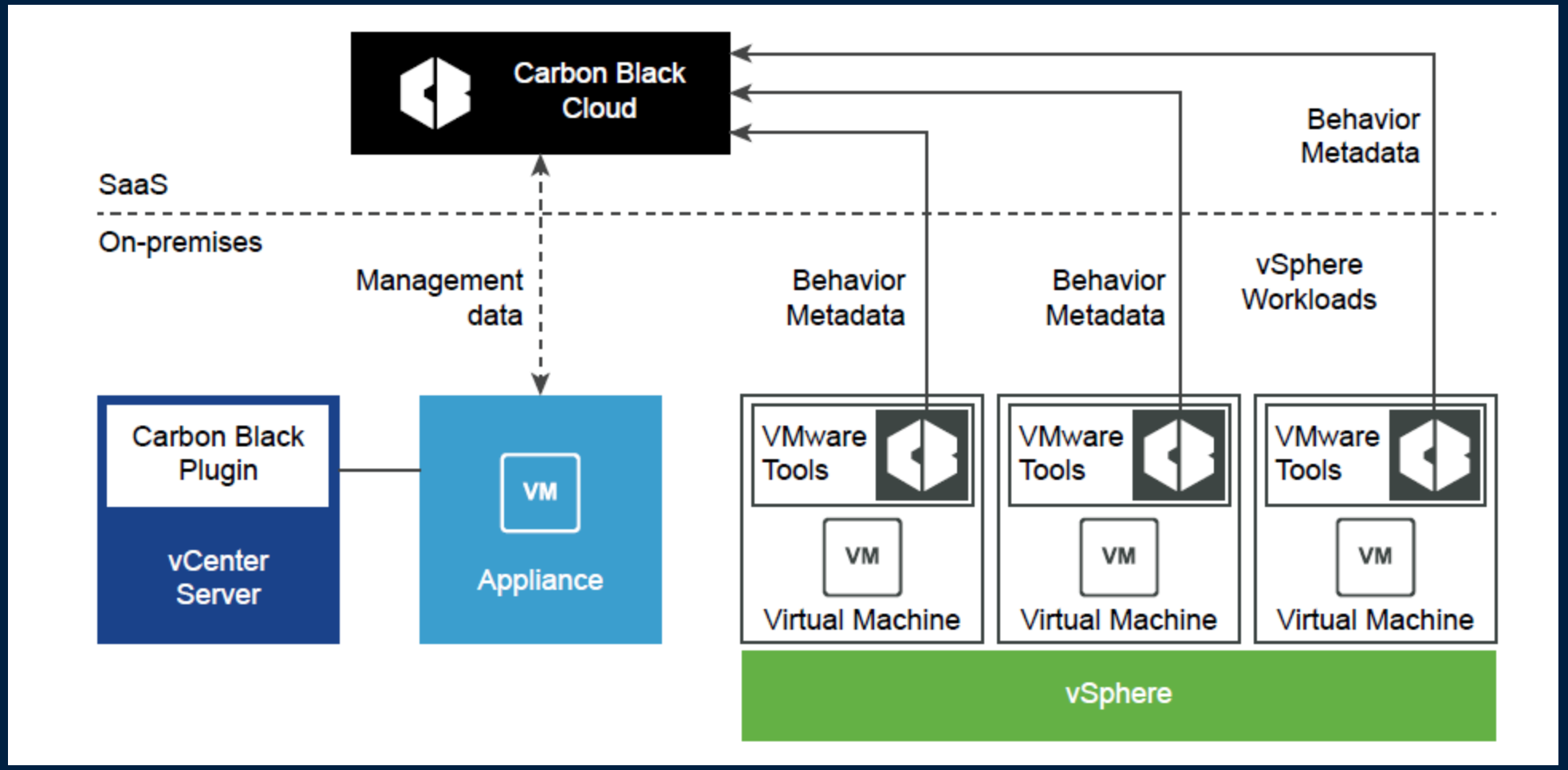
High Level

FUNCTION	VMware Carbon Black Endpoint			VMware Workspace Security
	STANDARD	ADVANCED	ENTERPRISE	
Next Gen AV	✓	✓	✓	✓
Endpoint detection and response (EDR)	✓	✓	✓	✓
Realtime endpoint audit and remediation		✓	✓	✓
Advanced threat hunting			✓	
Incident response			✓	
WorkspaceONE Compatible				✓

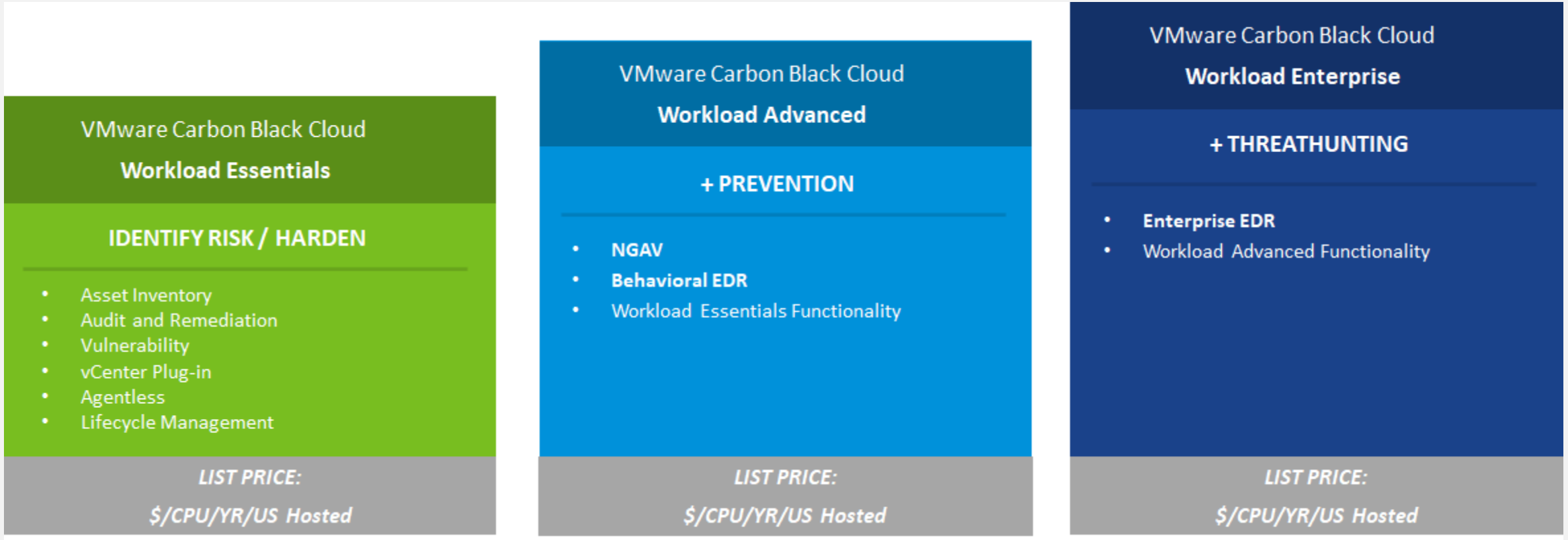
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-workspace-security-solutions.pdf

Carbon Black Cloud Workload

Carbon Black Cloud Workload



Carbon Black Cloud Workload



https://www.vmware.com/products/carbon-black-cloud/workload-protection-bundles.html

DEMONSTRAÇÃO

Demonstração

Demonstração do Carbon Black Endpoints console:

https://docs.hol.vmware.com/hol-isim/hol-2021/hol-isim-player.htm?isim=HOL-2236-01-ISM_module2_Introduction%20to%20the%20Carbon%20Black%20Cloud%20Console.json

Demonstração do Carbon Black Cloud Workload Protection

https://docs.hol.vmware.com/hol-isim/hol-2022/hol-isim-player.htm?isim=hol-2236-01-ism_module2_vcenter-plugin.json

Realize the Promise of Technology

Proprietary information of Ingram Micro Inc. — Do not distribute or duplicate without Ingram Micro's express written permission.