

VMware Security

VMware Carbon Black

Ivan Anaya
Security Specialist Mexico & NOLA



Confidential | © 2022 VMware, Inc.

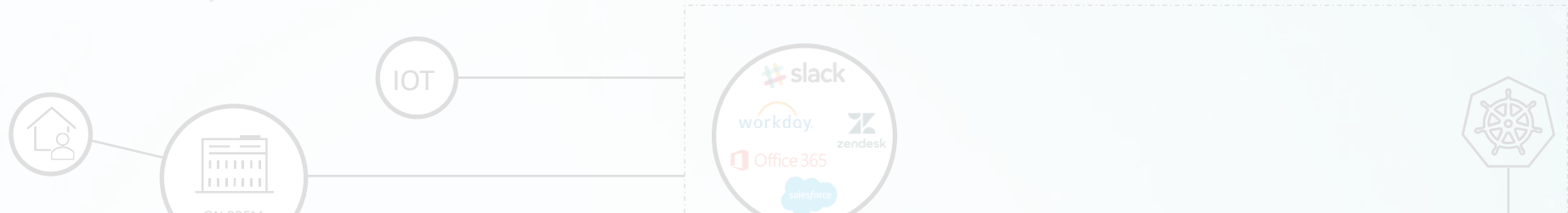


Para más información,
contácteme o visite kolbi.cr



The Modern Shape of Digital Business

The “trusted perimeter” has dissolved



Increased Attack Surface



Every
11 seconds

A New Org Falls
Victim

Cybersecurity Ventures (October 2019)

59%

Of All Attacks Involve
Double Extortion

IBM X-Force Threat Intelligence Index (March 2021)

>4000

Ransomware Attacks
Happen Daily

Justice.gov, *How to Protect Your Networks from Ransomware: Technical Guidance Document* (June 2016)

77%

Use RDP with either valid accounts or brute-
forced credentials to move laterally within
networks

2020 VMware Threat Landscape Report (May 2021)

Damage

2021 **\$20B**

2019 **\$11.5B**

2018 **\$8B**

Cybersecurity Ventures (October 2019)

Seguridad para Nubes, Workloads & Endpoints

Integraciones a SIEM, SOAR y Network Security para enriquecer Workflows

Identificar Riesgo

- Baseline/Visibilidad/Validación.
- Gestionar Vulnerabilidades, cambios de estado y configuraciones por medio de queries hacia Endpoints y Workloads.
- Aprovechamiento para tareas de hardening y contexto.
- Identifique los riesgos más fácilmente con un contexto compartido en todas las soluciones.



Prevenir

- Hardening y refuerzo de de Activos ante amenazas detectadas en el ecosistema.
- Prevenir malware, software y procesos no-deseados
- Prevenir acceso no autorizado con base a la postura de seguridad.
- Detener No-Malware y Ataques LoL

Detectar & Responder

- Zoom In: Detección (temprana/exacta)
- Zoom Out: Observar la “campana”
- Responder: Remediar y Prevenir
- Enriquecer las detecciones con mayor contexto de IOCs/Alertas correlacionadas
- Aprovechar el contexto compartido para automatizar procesos y respuesta

EFFECTIVE
security

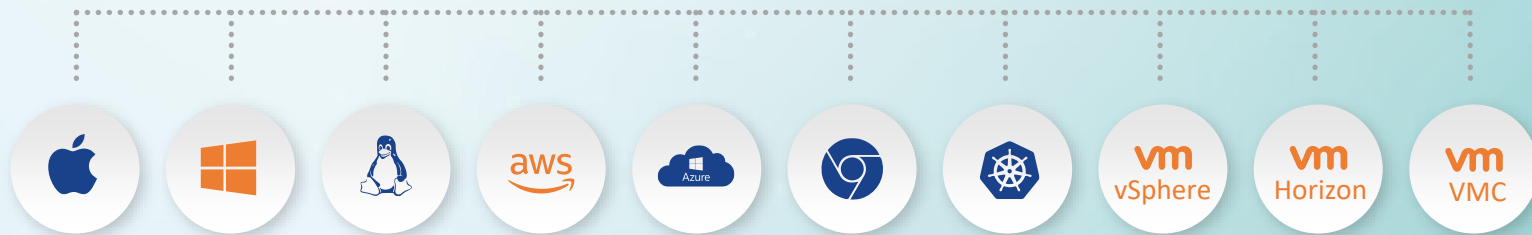
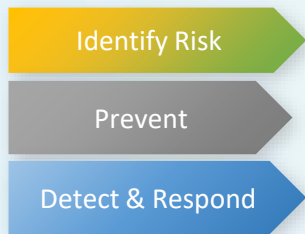
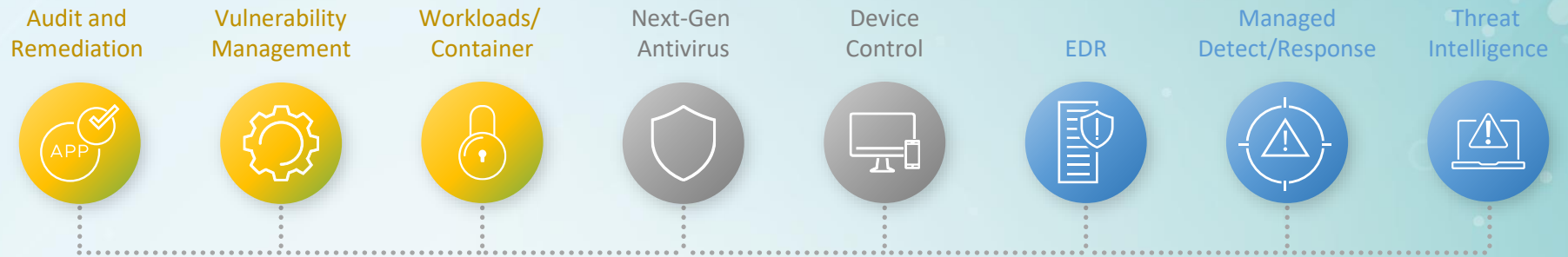


**Virtualization
Layer**



EASIER
to operate

Seguridad Cloud, Workloads y Endpoints



Prevenir Ataques de Malware y Non-Malware

Multiple prevention techniques to stop each attack type

- Reputación y ML para malware conocido y desconocido
- Prevención por comportamiento para ataques fileless y LOL
- Señuelos para Ransomware
- Una sola política

Invoked --- Injected --- Read Memory --- Accessed Target

powershell.exe

92.222.180.119
51.15.58.224
217.182.169.148
51.15.54.102
51.15.78.68
51.255.34.118
199.231.85.124
164.132.109.110

Take Action

powershell.exe

Policy Action Deny Reputation Trusted White List

Process State Ran Signatures Verification Signed And Verified

CMD "C:\Windows\System32\WindowsPowerShell\powershell.exe" -NoP -NonI -W Hidden "Smon = ([WmiClass] 'root\default\systemcore.Updates').Properties['mon'].Value;\$funs = ([WmiClass] 'root\default\systemcore.Updates').Properties['funs'].Value;(New-Object System.Text.Encoding::ASCII).GetString([System.Convert]::FromBase64String(\$funs));Invoke-Command -ScriptBlock \$RemoteScriptBlock -ArgumentList @(\$smon, \$smon, 'void', 0, '', '')"

SHA-256 006cef6ef6488721895d93e4cef7fa0709c2692d74bde1e22e2a8719b2a86218

MD5 a575a7610e5f003cc36df39e07c4ba7d

PID 6364

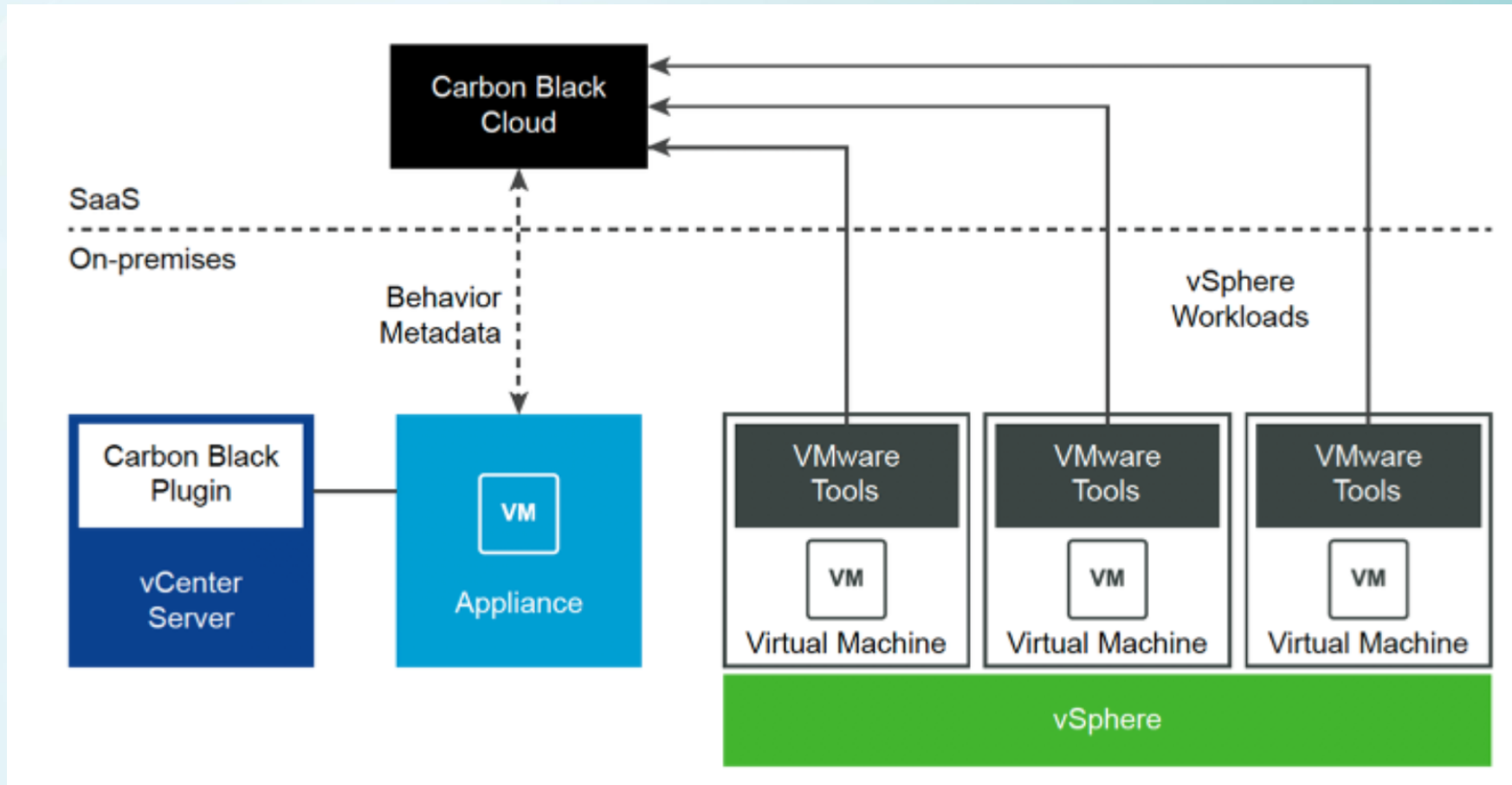
Start time 1:40:10pm Nov 29, 2018

TTPs attempted_client policy_deny non_standard_port bypass_policy packed_code internacional_site

Signed Microsoft Windows

vCenter Plugin & Appliance Architecture Overview

VMware Carbon Black Workload



Adaptarlo de manera única a su negocio

Traducir fácilmente la prevención por comportamiento en su ambiente

- Implementar prevención Flexible
- Definir listas de aprobación para comportamientos esperados
- Minimizar interrupción a usuarios

Carbon Black. Notificados 14 Help Ed Murphy (mitreval.carbonblack.com)

General | **Prevention** | Local Scan | Sensor

Use these rules to configure how sensors control process behavior

+ **Permissions** Allow specific operations or bypass application activity entirely. Takes precedence over blocking and isolation settings below.

— **Blocking and Isolation** Deny or terminate processes and applications.

PROCESS	OPERATION ATTEMPT	OS	ACTION
Known malware	Runs or is running Test rule	Windows	Terminate process
Application on the company blacklist	Runs or is running Test rule	Windows	Terminate process
Unknown application or process	Scrapes memory of another process Test rule Performs ransomware-like behavior Test rule	Windows	Terminate process Terminate process
Adware or PUP	Performs ransomware-like behavior Test rule	Windows	Terminate process
Suspected malware	Runs or is running Test rule	Windows	Terminate process
Not listed application	Scrapes memory of another process Test rule Performs ransomware-like behavior Test rule	Windows	Terminate process Terminate process
Application(s) at path:	Scrapes memory of another process Test rule	Windows	Terminate process
**ipython, **powershell*.exe			
Application(s) at path:	Scrapes memory of another process Test rule Injects code or modifies memory of another process Test rule	Windows	Terminate process Deny operation
**cmd.exe, **powershell.exe			

Visibilidad para InfoSec

Gestión de Vulnerabilidades integrada en Carbon Black Cloud

- Priorización basada en riesgo sobre todas las vulnerabilidades existentes en el ambiente
- Entender el contexto de Vulnerabilidades con calificaciones de riesgo y links hacia la NVD
- Habilitar a InfoSec para colaborar con vAdmins y resolver las vulnerabilidades

The screenshot displays the Carbon Black Cloud interface for vulnerability management. The top navigation bar includes 'Carbon Black.', 'Notifications', 'Help', and the user 'Sarah Greenberg2 (pscr-test-01)'. The main section is titled 'VULNERABILITIES' with the subtitle 'Review security vulnerabilities found on deployed workloads'. It features a summary of vulnerability counts by severity: All (12 Vulnerabilities, 412 Assets), Critical (12 Vulnerabilities, 136 Assets), Important (3 Vulnerabilities, 34 Assets), Moderate (2 Vulnerabilities, 54 Assets), and Low (2 Vulnerabilities, 188 Assets). A search bar and 'Evaluating risk' button are present. Below is a table of vulnerabilities with columns for ASSET, RISK, TYPE, T, VULNERABILITIES, OS, and OS VERSION. A detailed view for 'ASSET: DB-VM-1' is shown on the right, including fields for Type, IP, OS, and OS version, and a list of associated CVEs with their risk levels and types.

ASSET	RISK	TYPE	T	VULNERABILITIES	OS	OS VERSION
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600
DB-VM-1	Critical (9.2)	VM		6	Microsoft Windows Server 2016 Standard	6.3.9600

VULNERABILITIES
ASSET: DB-VM-1

Type VM
IP 10.159.52.154
OS Microsoft Windows Server 2016 Standard
OS version 10.0.14393

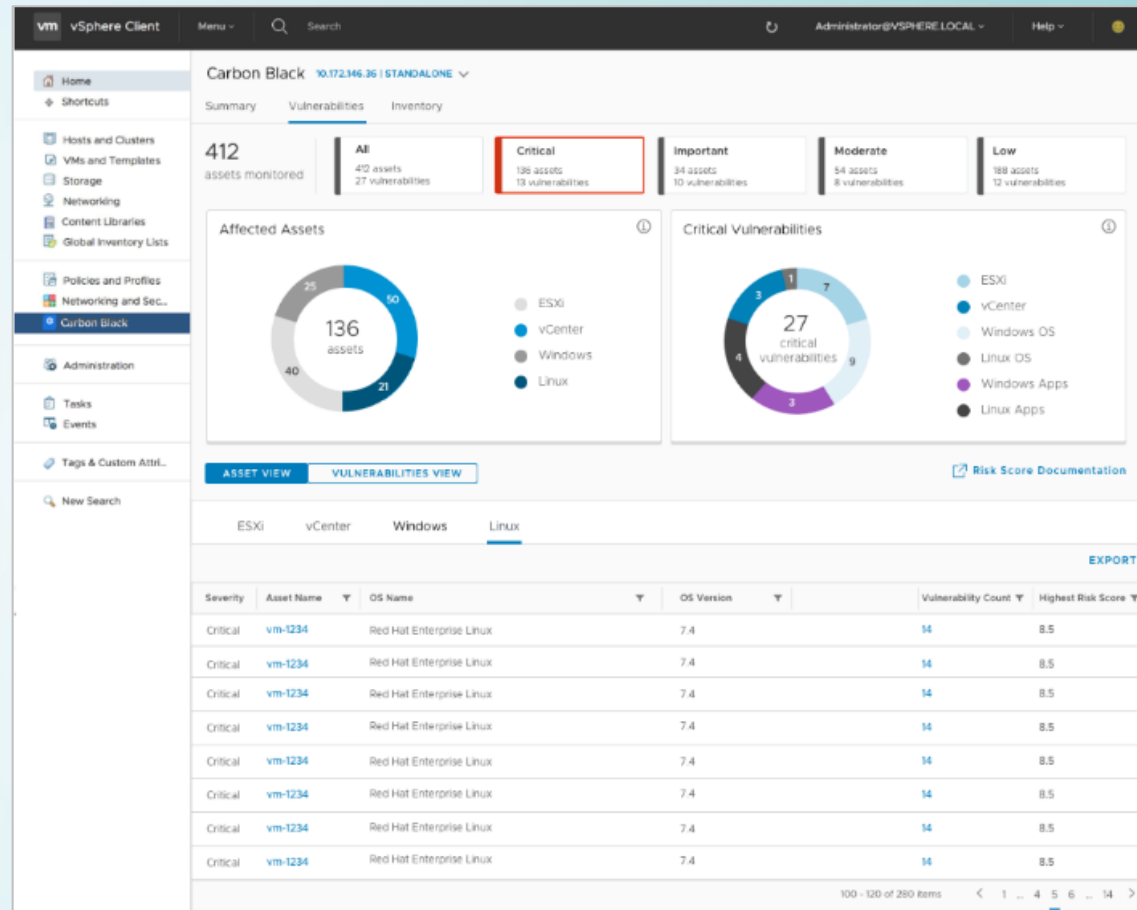
National vulnerability database

RISK	CVE ID	TYPE
Critical (9.2)	CVE-2018-8413	App
Critical (9.2)	CVE-2019-0903	OS
Issued: May 11, 2016	Updated: May 11, 2016	Resource: KB4541329
Critical (9.2)	CVE-2019-0903	App
Critical (9.2)	CVE-2019-0903	OS
Important (9.2)	CVE-2019-0904	App
App: MS Word	App Version: 11.1	Resource: KB4541329
Issued: May 11, 2016		
Important (9.2)	CVE-2019-0914	App

Visibilidad para Admins de vSphere

Gestión de Vulnerabilidades integrada a vSphere

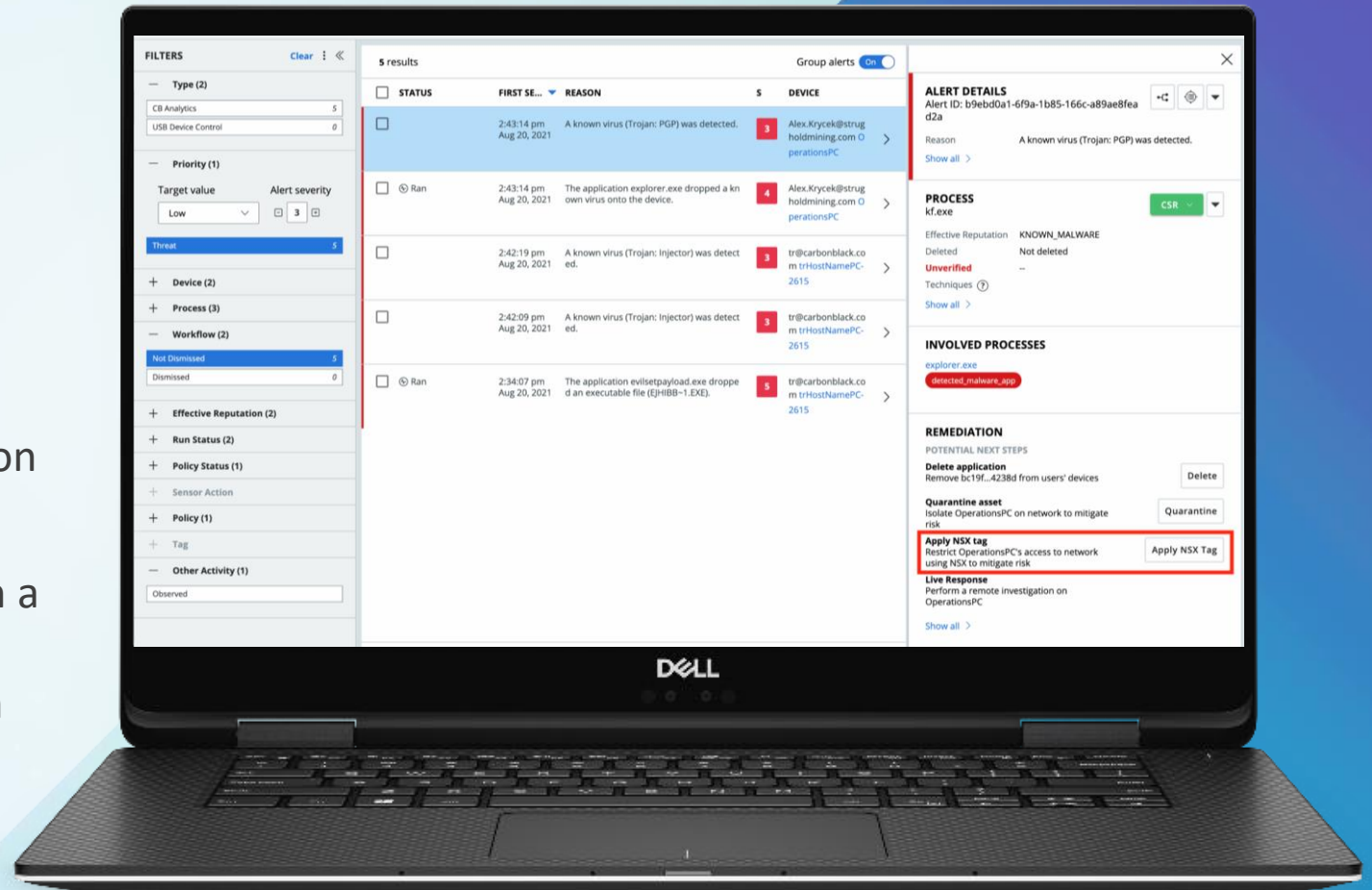
- Priorización basada en riesgo sobre todas las vulnerabilidades existentes en el ambiente de vSphere
- Proveer conciencia de riesgo a Admins de vSphere
- Investigar y remediar de manera directa las VMs por medio de vSphere Client



NSX-T Integration and Tagging

Apply Network Policy

- Integrate with VMware NSX-T distributed firewall to provide protection for your VMs from the networking layer.
- Assign an NSX-T tag and associated firewall policy to a VM directly through the Carbon Black Cloud console.
- This action can be taken when a Carbon Black alert has been generated or from the Carbon Black inventory view.



Lifecycle Management for VM Inventory

vCenter Plugin

- **Overview of inventory and security posture**
- **Inventory management for install and updates**
- **Enable CBC Workload as a feature on virtual machines**
- **Provide context for appliance health and install workflow**

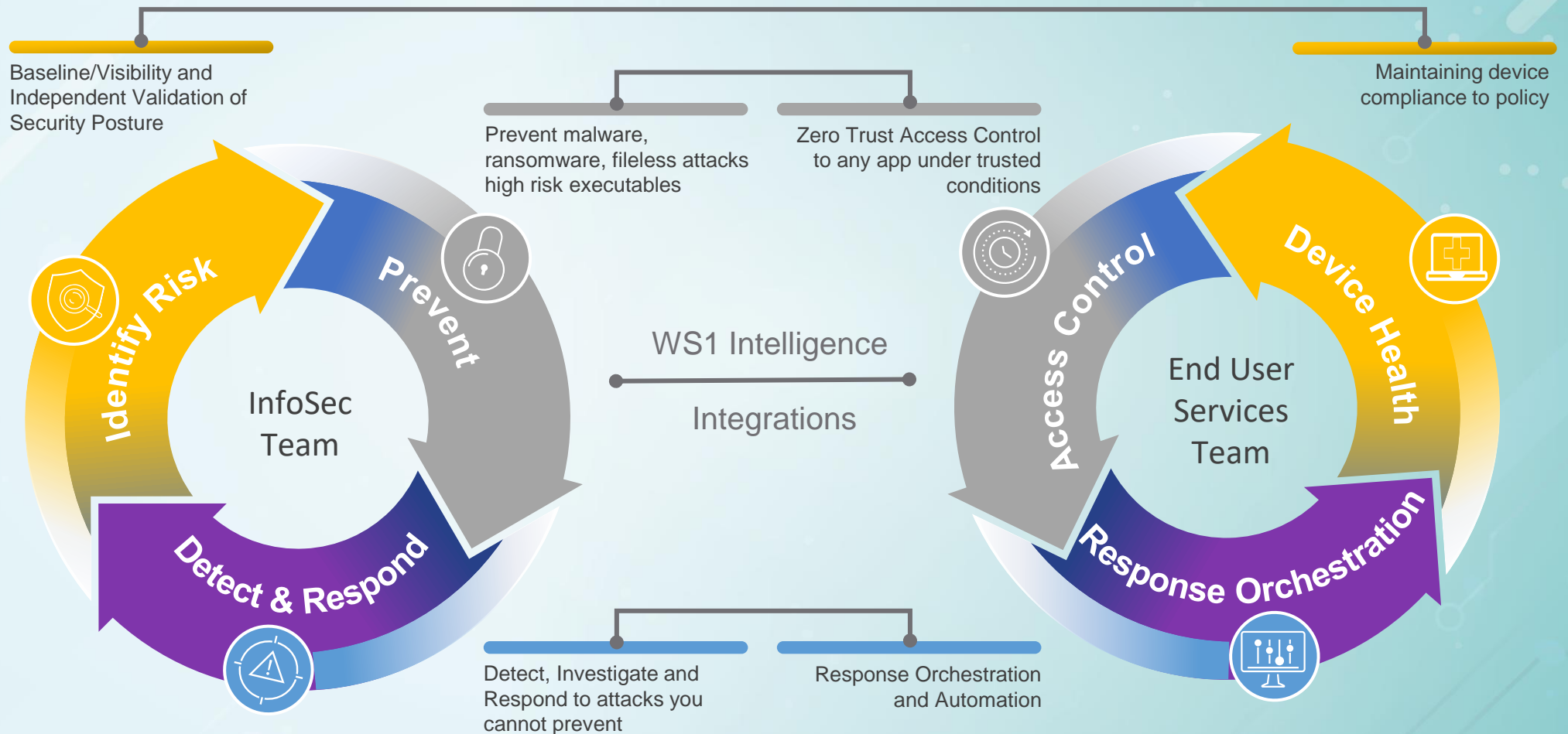
The screenshot displays the vSphere Client interface for a Carbon Black appliance. The left sidebar shows navigation options like Home, Shortcuts, Hosts and Clusters, VMs and Templates, Storage, Networking, Content Libraries, Global Inventory Lists, Policies and Profiles, Networking and Sec..., Carbon Black (selected), Administration, Tasks, Events, Tags & Custom Attr..., and New Search.

The main content area is titled "Carbon Black 10.172.146.36 | STANDALONE" and has tabs for Summary, Vulnerabilities, and Inventory. The "Summary" tab is active, showing:

- Appliance Health:** Overall status is "Healthy". Components include vCenter connectivity, Inventory Health, Gateway, Appliance Worker, vSphere Worker, and Access Control Service.
- Inventory Status (318):** A table listing various items and their counts:

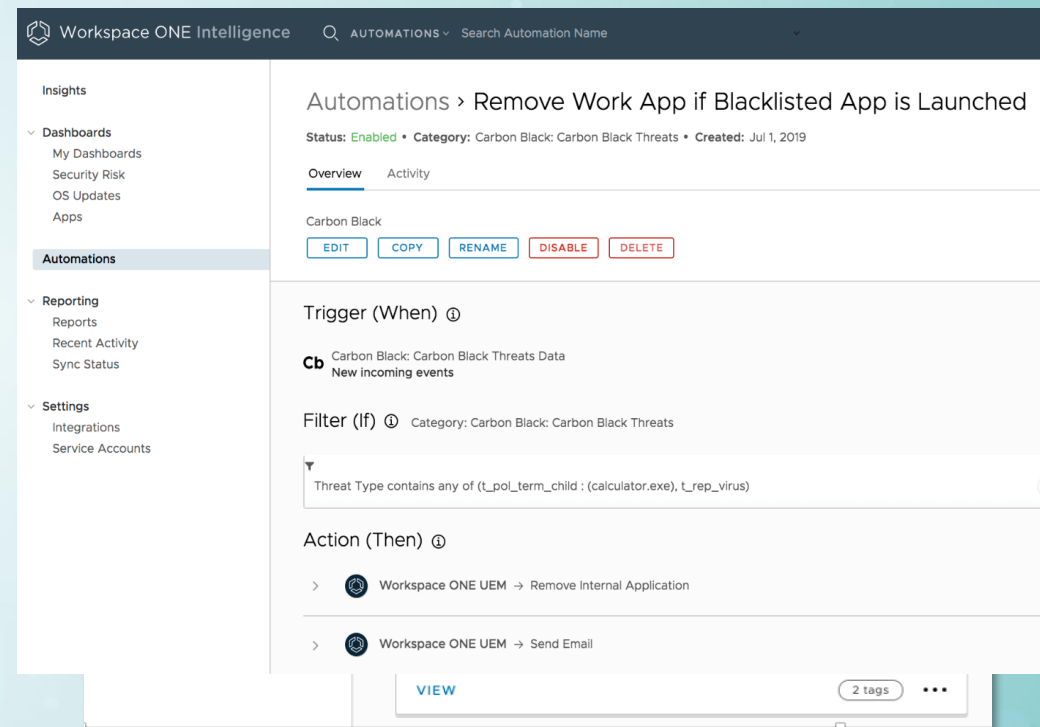
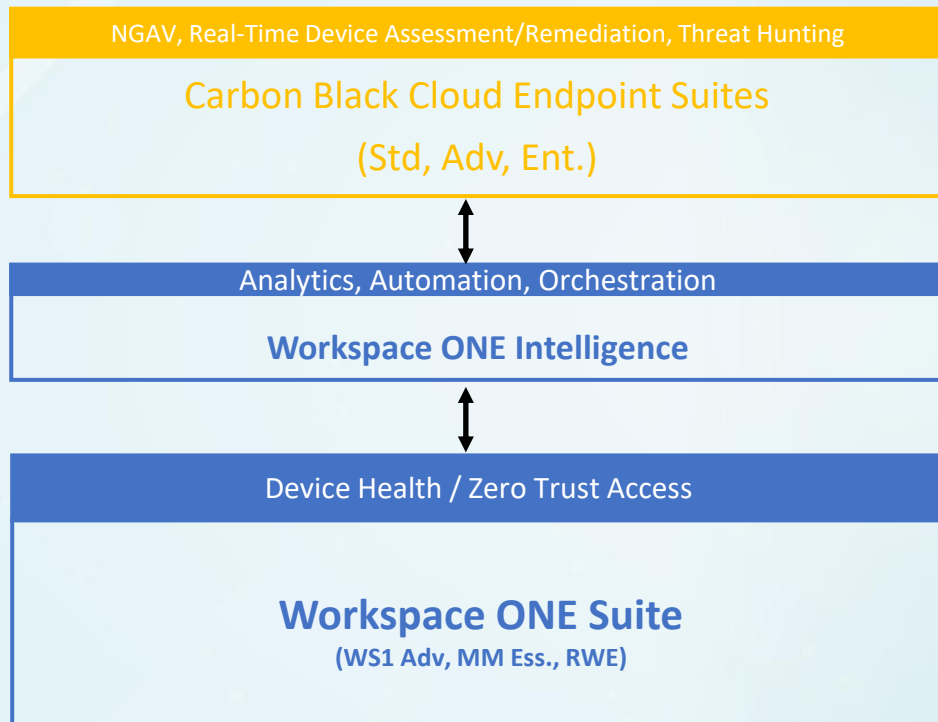
Description	VMs
Carbon Black enabled	102
Carbon Black update available	86
Assets unsupported by Carbon Black	55
Assets requiring VMtools upgrade	75
- Critical Vulnerabilities by Asset:** A donut chart showing 136 critical assets across ESXi (25), vCenter (50), Windows (40), and Linux (21).
- Total Critical Vulnerabilities:** A donut chart showing 27 total critical vulnerabilities across ESXi (7), vCenter (3), Windows OS (9), Linux OS (4), Windows Apps (3), and Linux Apps (1).

Workspace Security – Integrations strengthen the solutions



Integrations help differentiate the solution

Enhanced Protection with Workspace Security



DEMO

VMware Carbon Black en acción



Confidential | ©2022 VMware, Inc.



Para más información,
contácteme o visite kolbi.cr



Thank You



Confidential | ©2022 VMware, Inc.



Para más información,
contácteme o visite kolbi.cr

