VMware Security

VMware Carbon Black

Ivan Anaya
Security Specialist Mexico & NOLA

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

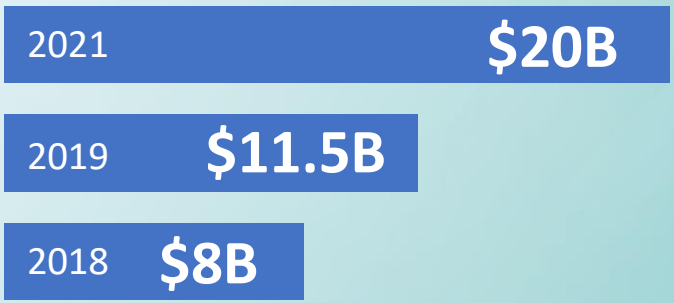
Justice.gov, *How to Protect Your Networks from Ransomware: Technical Guidance Document* (June 2016)

77%

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

2020 VMware Threat Landscape Report (May 2021)

Damage



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 Vulnerabiliades, 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.

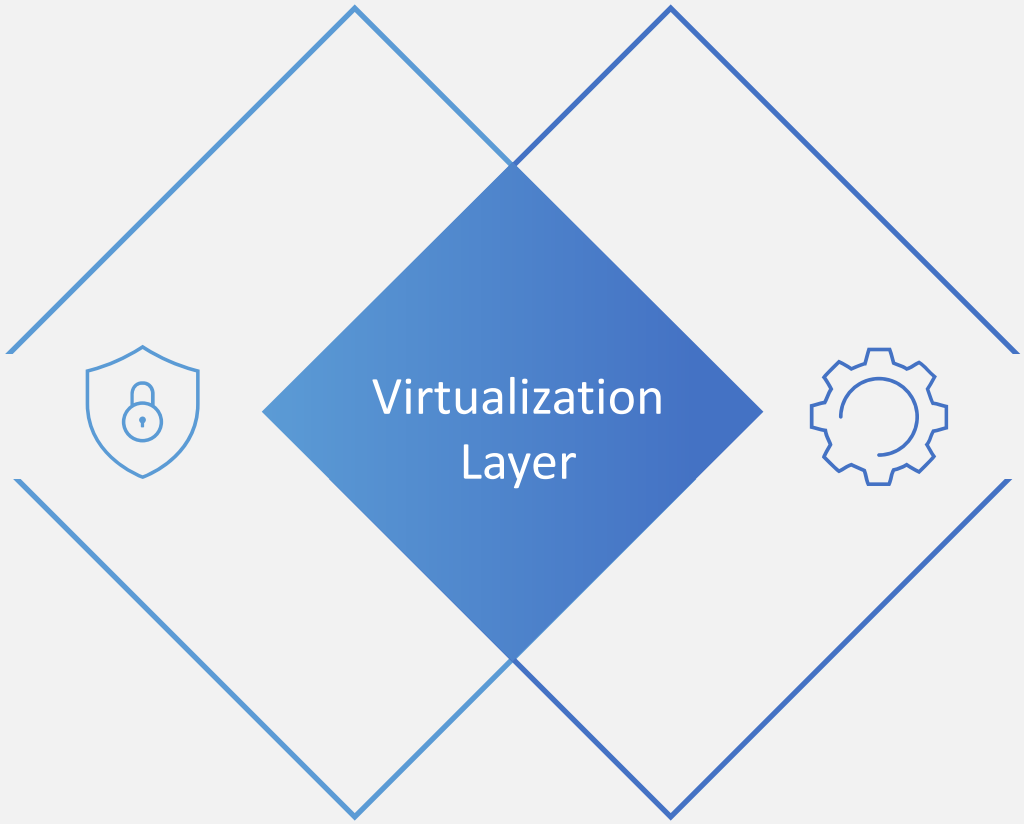
Prevenir

- 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

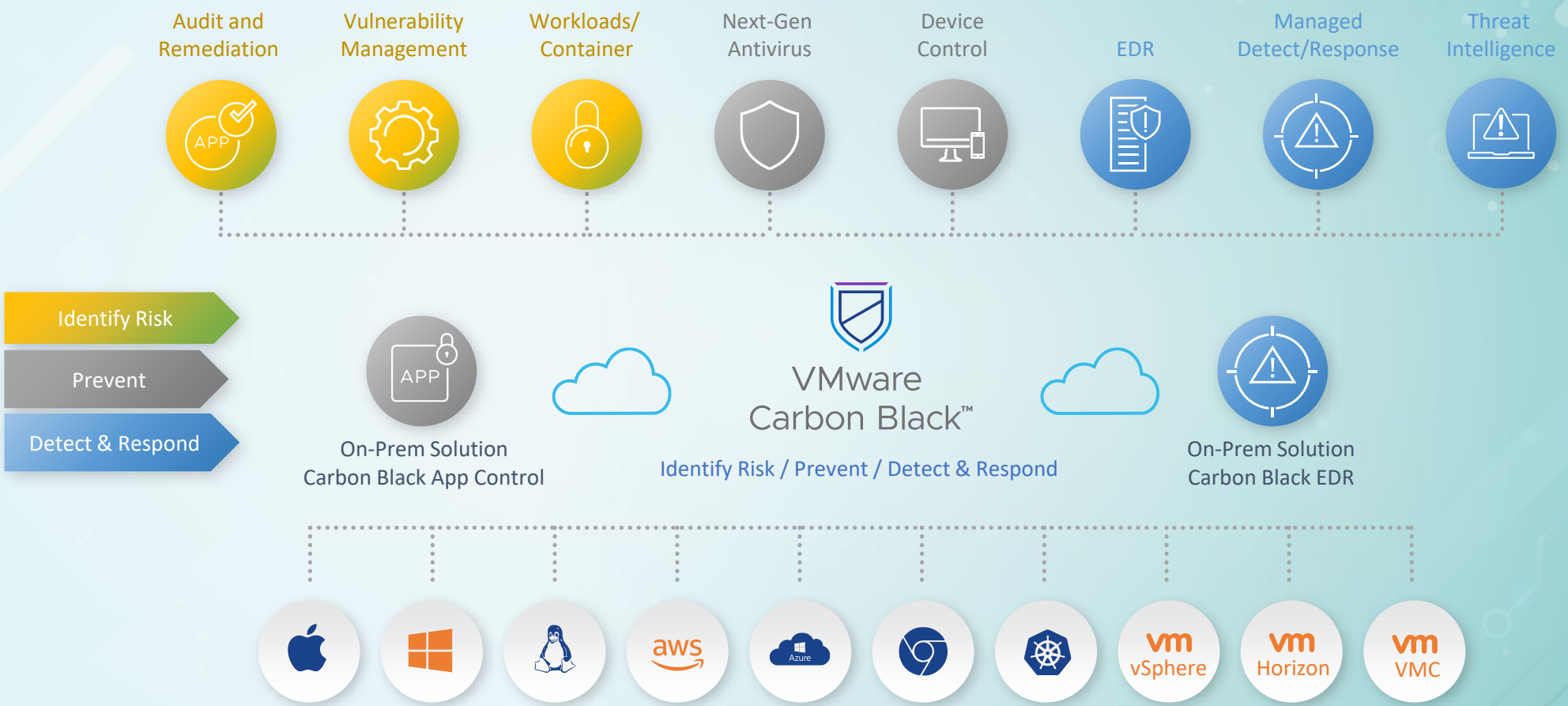
- Zoom In: Detección (temprana/exacta)
- Zoom Out: Observar la “campaña”
- Responder: Remediar y Prevenir
- Enriquecer las detecciones con mayor contexto de IOCs/Alertas correlacionadas
- Aprovechar el contexto compartido para automatizar procesos y respuesta

EFFECTIVE
security



EASIER
to operate

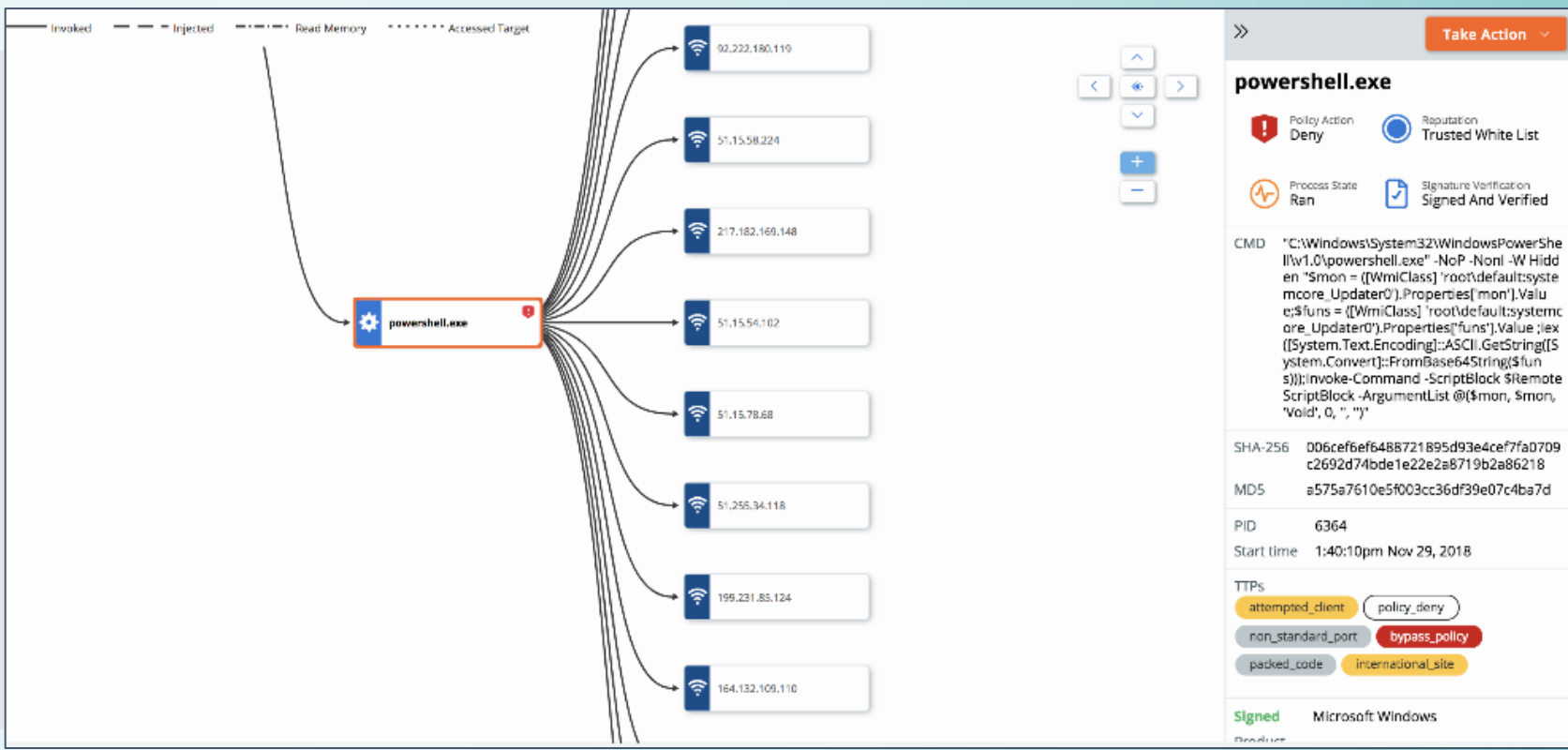
Seguridad Cloud, Workloads y Endpoints



Prevenir Ataques de Malware y Non-Malware

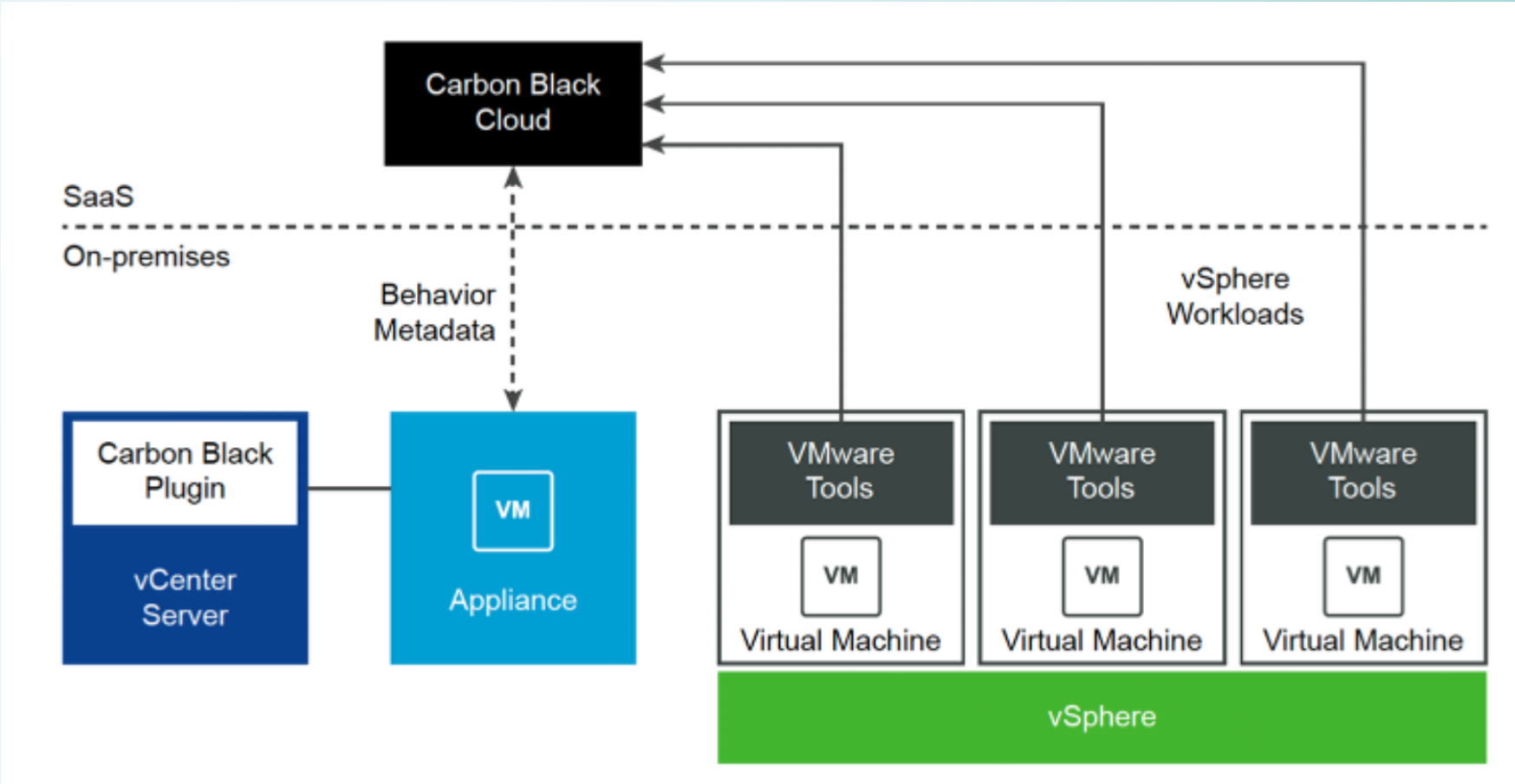
Multiple prevention techniques to stop each attack type

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



vCenter Plugin & Appliance Architecture Overview

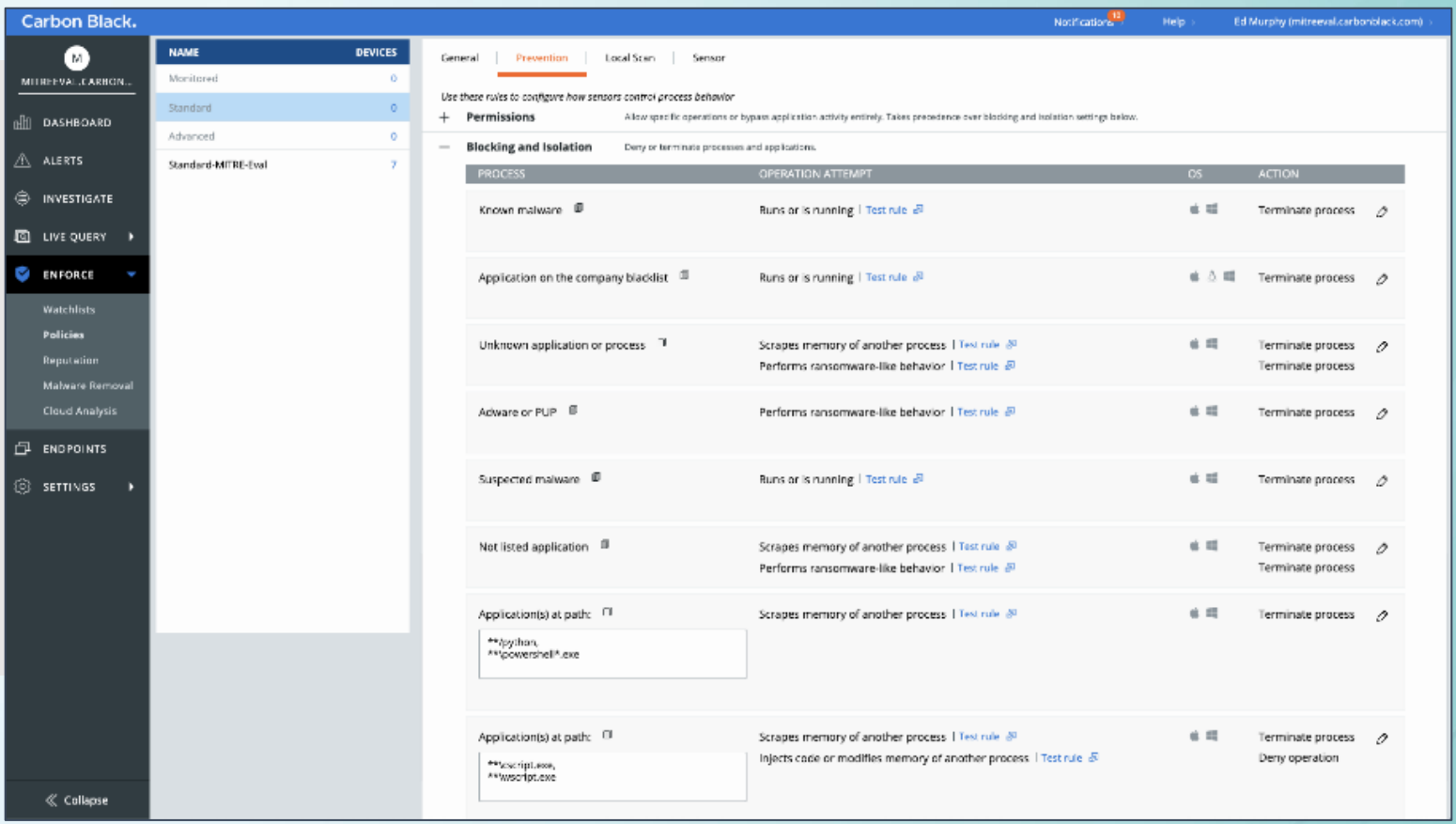
VMware Carbon Black Workload



Adaptarlo de manera única a su negocio

Traducir fácilmente la prevención por comportamiento en su ambiente

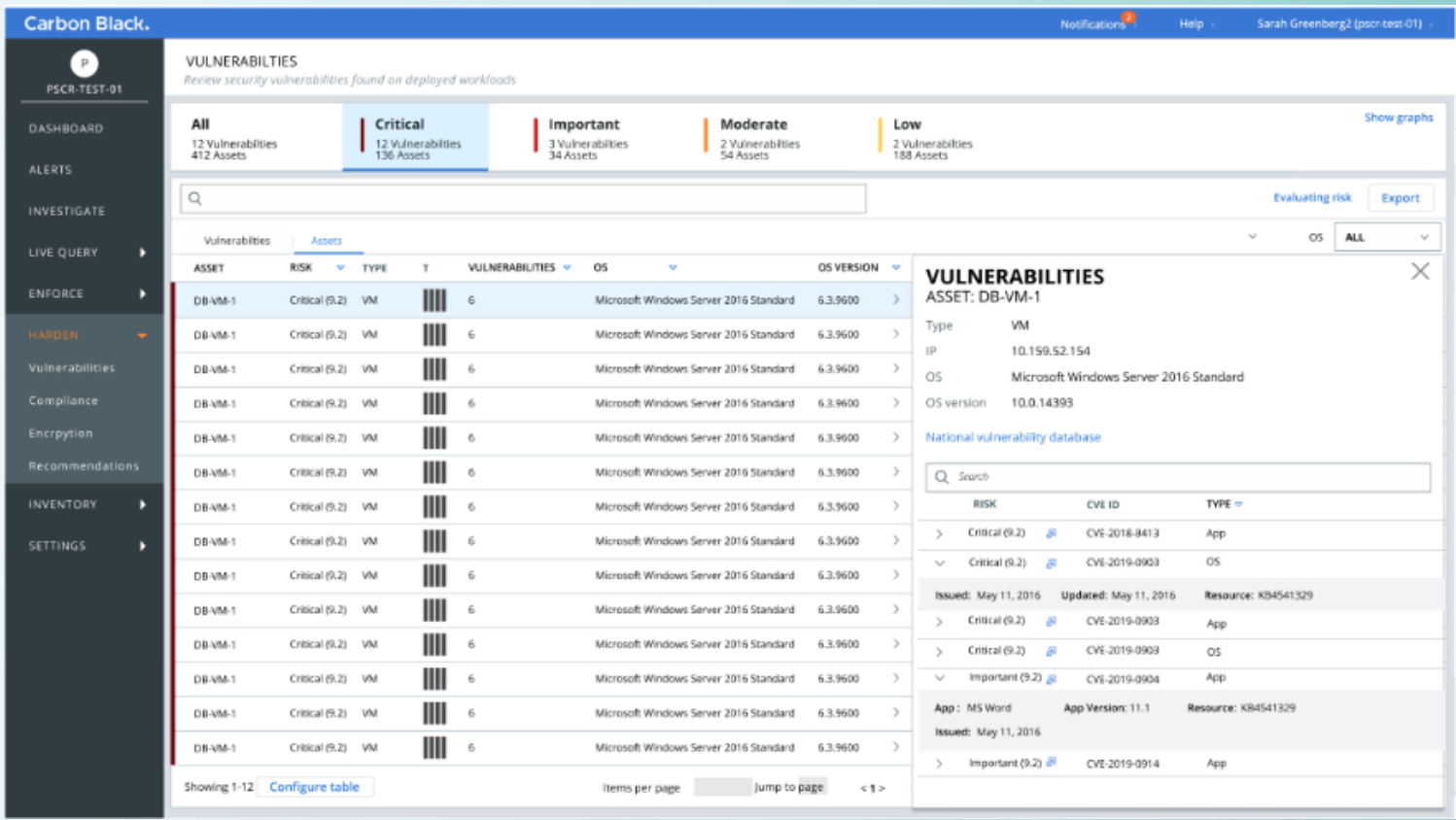
- Implementar prevención Flexible
- Definir listas de aprobación para comportamientos esperados
- Minimizar disrupción a usuarios



Visibilidad para InfoSec

Gestión de Vulnerabiidades integrada en Carbon Black Cloud

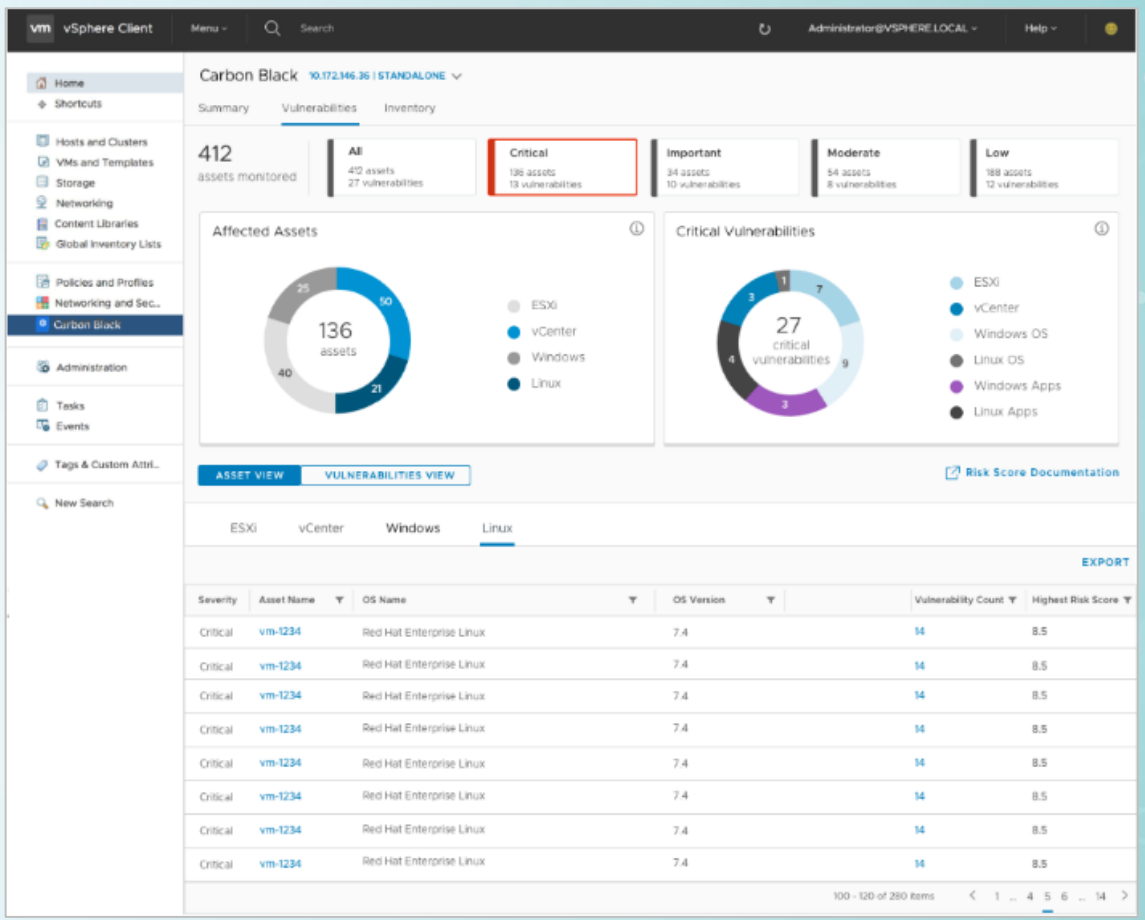
- **Priorización basada en riesgo** sobre todas las vulnerabilidades existentes en el ambiente
- **Entender el contexto de Vulnerabilidades** con calificaciones de riesgo y links hacia la NVD
- **Habilitar a InfoSec para colaborar** con vAdmins y resolver las vulnerabilidades



Visibilidad para Admins de vSphere

Gestión de Vulnerabilidades integrada a vSphere

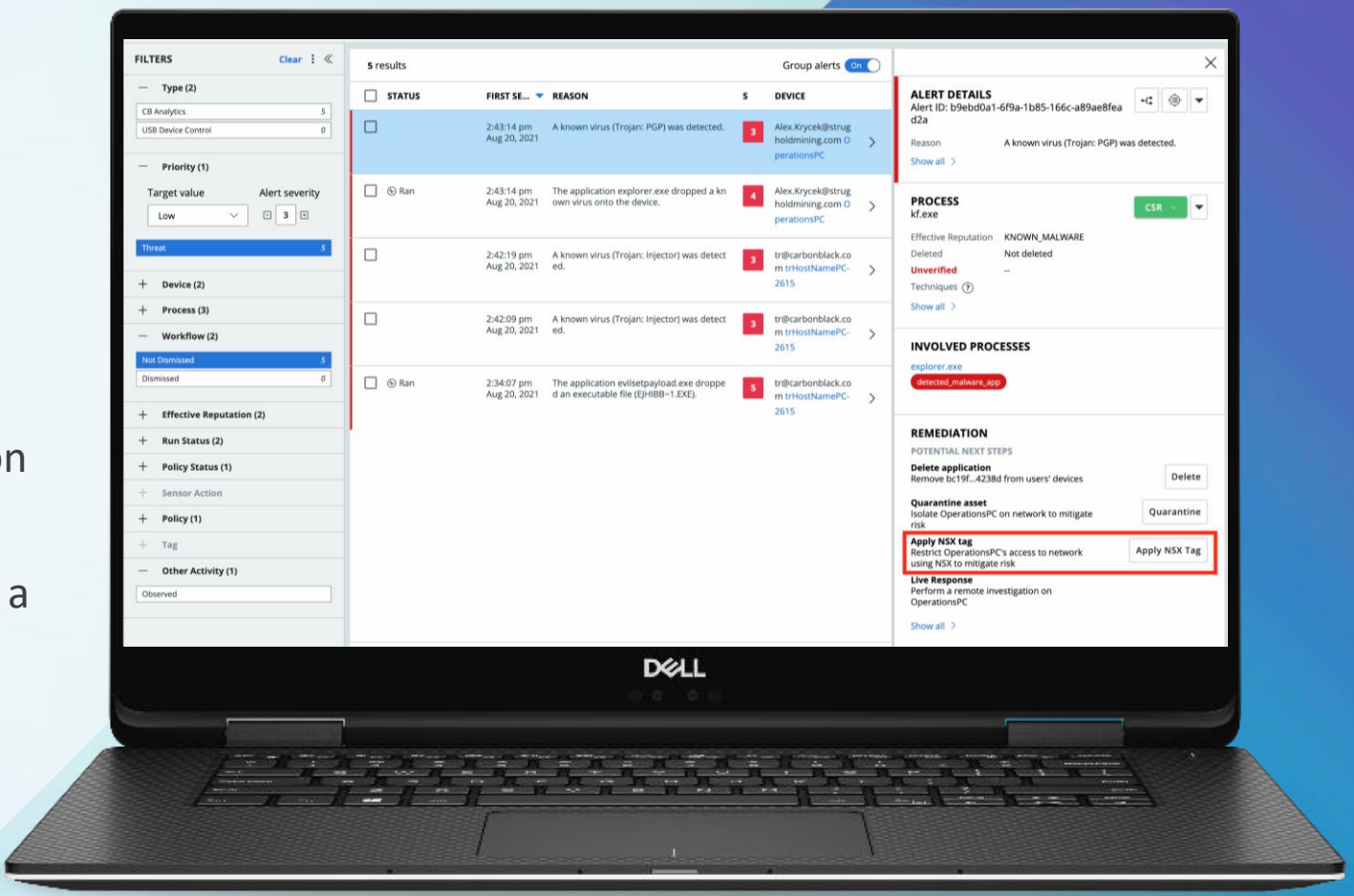
- **Priorización basada en riesgo** sobre todas las vulnerabilidades existentes en el ambiente de vSphere
- **Proveer conciencia de riesgo** a Admins de vSphere
- **Investigar y remediar de manera directa** las VMs por medio de vSphere Client



NSX-T Integration and Tagging

Apply Network Policy

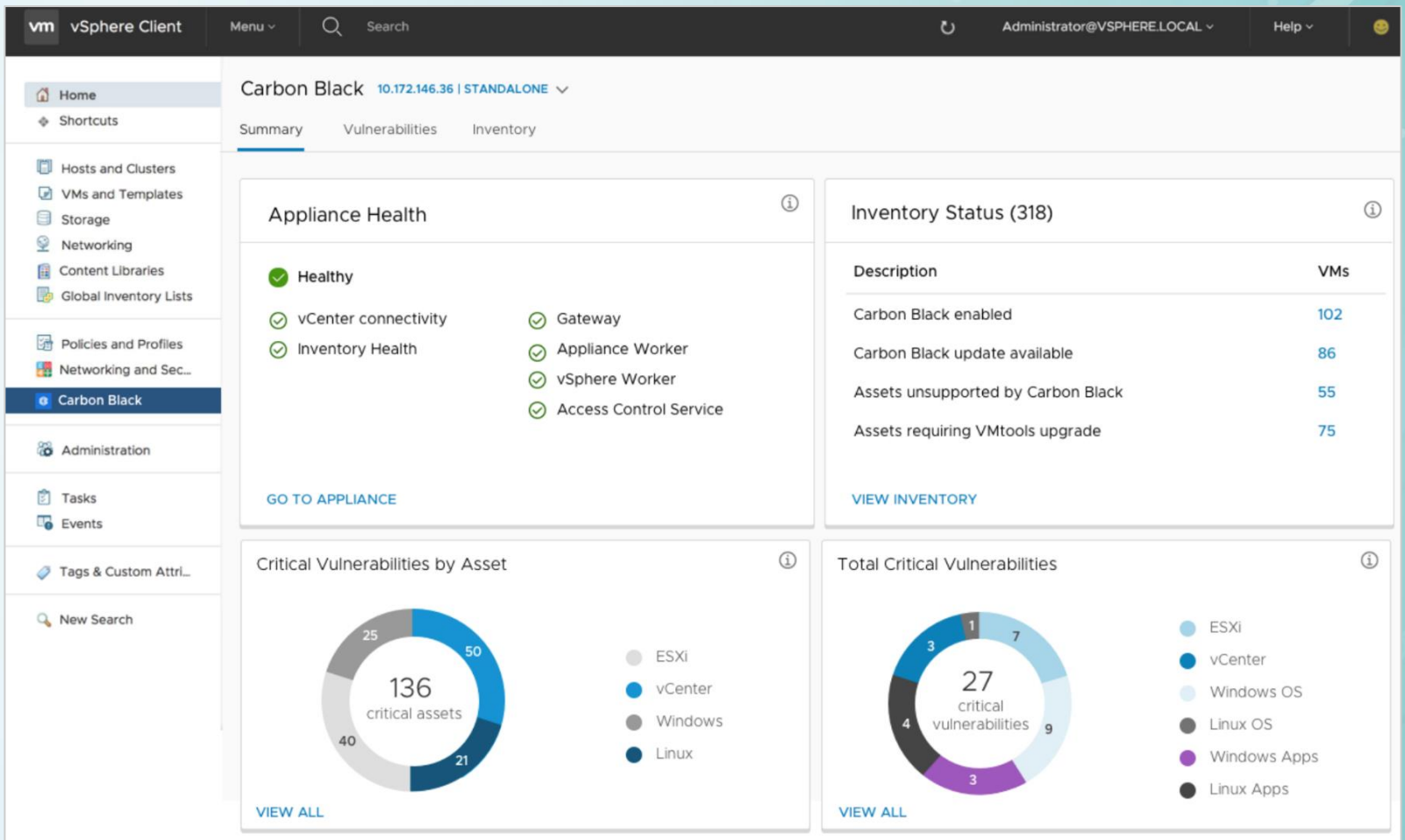
- Integrate with VMware NSX-T distributed firewall to provide protection for your VMs from the networking layer.
- Assign an NSX-T tag and associated firewall policy to a VM directly through the Carbon Black Cloud console.
- This action can be taken when a Carbon Black alert has been generated or from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



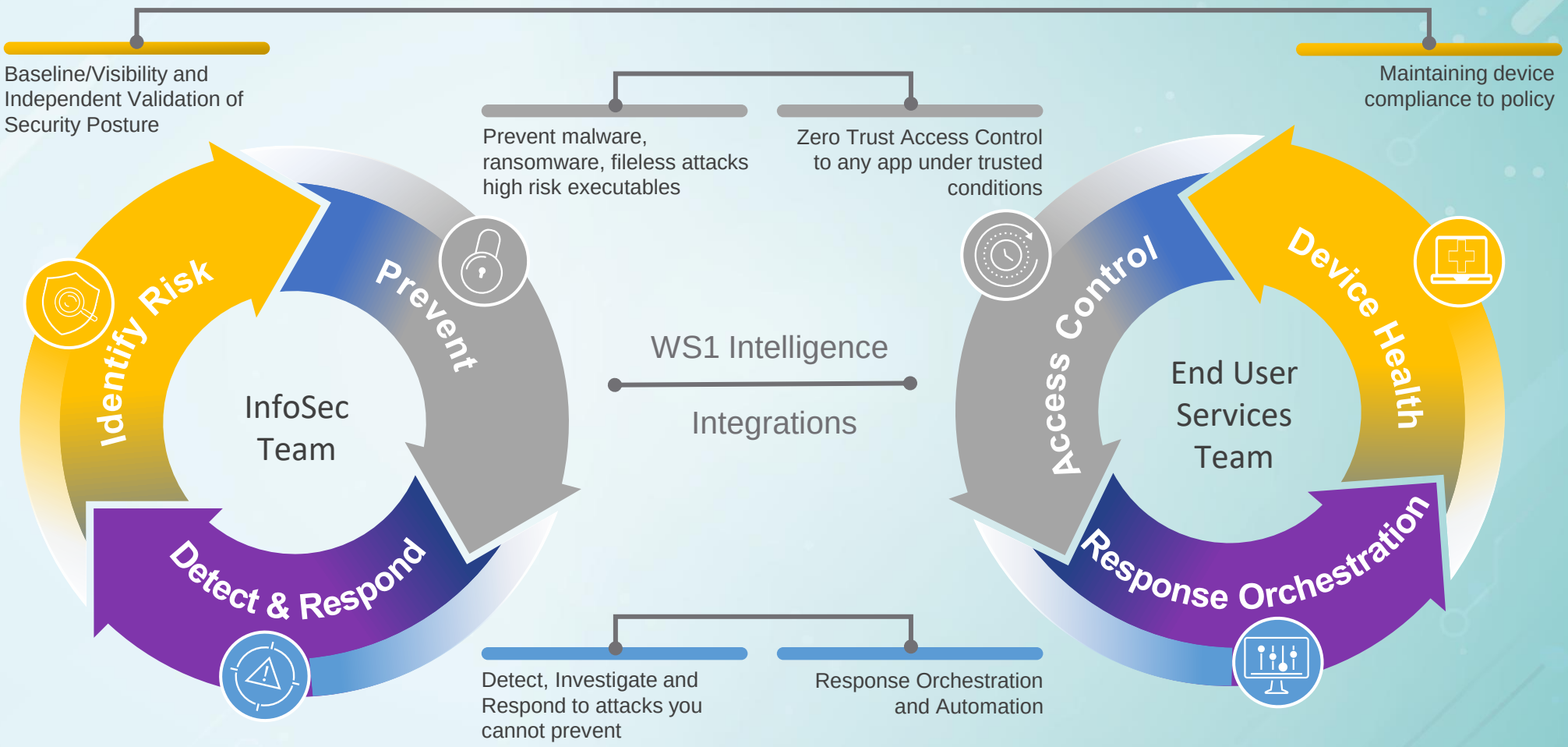
Lifecycle Management for VM Inventory

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

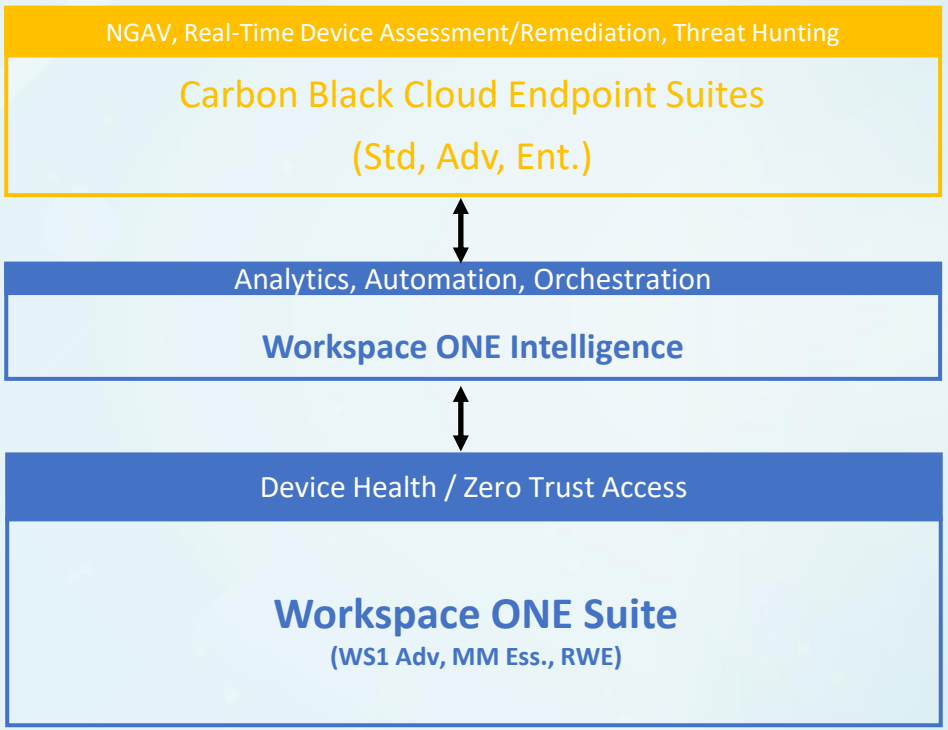


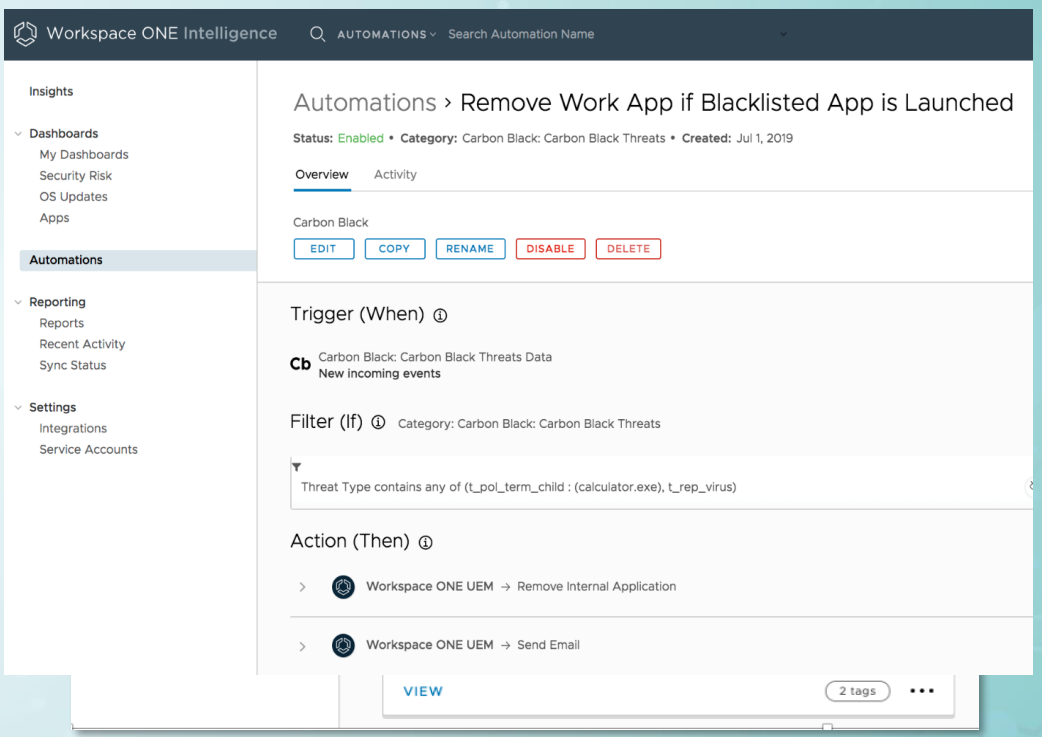
Workspace Security – Integrations strengthen the solutions



Integrations help differentiate the solution

Enhanced Protection with Workspace Security





DEMO

VMware Carbon Black en acción

Thank You