# CARBON BLACK TECHNOLOGY

vmware

VMtalks México

# Carbon Black

## Seguridad end-to-end de siguiente generación con VMware Carbon Black

Hugo Ortiz,
hortiz@vmware.com

Ivan Anaya,
lanaya@vmware.com

18 Junio, 2020

vmware

# VMtalks México

## Analizando la red desde el servidor físico hasta el contenedor con VMware vRNI

Junio 23, 2020 – 10:00 A.M

**Expositores:**

Luis Daniel Retana, VMware Solution Engineer
Daniel Aguirre, VMware Solutions Engineer Networking & Security

VMware vRealize® Network Insight ofrece operaciones inteligentes para redes y seguridad definidas por software. Ayuda a los clientes a construir una infraestructura de red optimizada, altamente disponible y segura en entornos de múltiples nubes.

## Alcance las nubes con VMware SD-WAN

Junio 25, 2020 – 10:00 AM

**Expositores:**

Joel Rodríguez, VMware Solution Engineer
Alejandro Herrera, VMware Solution Engineer, Velocloud SD-WAN

Hoy, el negocio digital ya no es un concepto abstracto, es una realidad. A medida que más aplicaciones se trasladan a la nube, los usuarios comerciales confían cada vez más en ellas para hacer su trabajo.

Desde reuniones virtuales hasta el intercambio de archivos y la colaboración a través de herramientas como Skype, Slack y Office 365, incluido el tráfico de voz y video, requieren un ancho de banda consistente y de alta calidad,

vmware

# Difícil de resolver con enfoques heredados

## Demasiadas herramientas

**Maneja:**

- Complejidad
- Configuraciones erróneas.
- No alineadas
- Proyectos de integración

## Brechas de visibilidad

**Falta de visibilidad y contexto para:**

- Hardening
- Prevención
- Investigación
- Respuesta

## Brechas de detección

**Amenazas perdidas:**

- Sin malware
- Nuevo ransomware
- Movimiento lateral
- Ataques avanzados

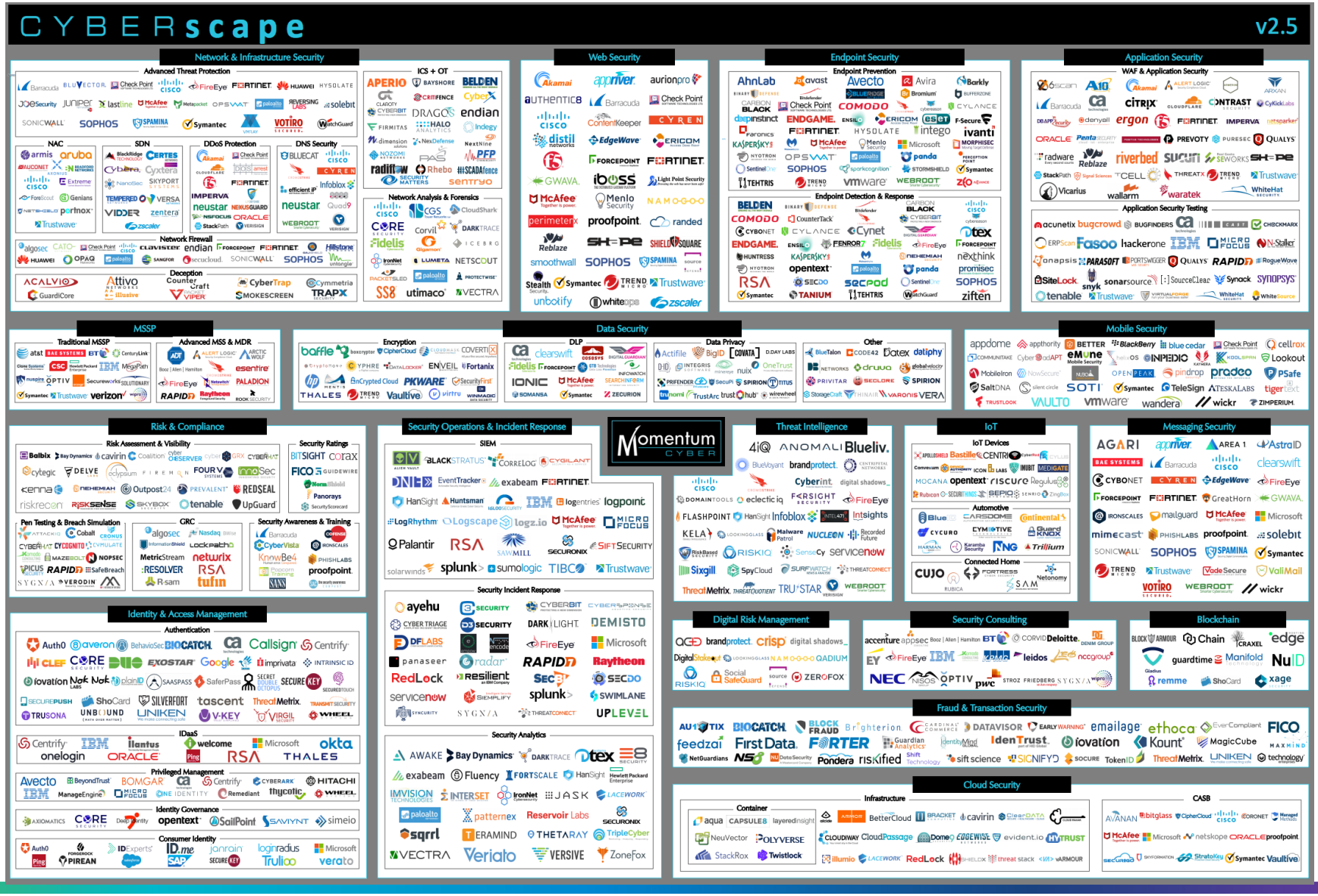
## Manejo de Silos

**Colaboración mínima entre:**

- Info Seguridad
- Infraestructura
- Red
- Servicios de escritorio

La cartera de seguridad tiene su propio desafío de complejidad.

vmware



# ¿Preguntas que se hacen los clientes?

## PREGUNTAS

¿Ya cuento con Firewalls / Firewall de Siguiente Generación, No necesito nada más?

¿Ya tengo el Antivirus actualizado y me está protegiendo los servidores de windows/Linux?

¿ Tengo en mi infraestructura con IDS/IPS?

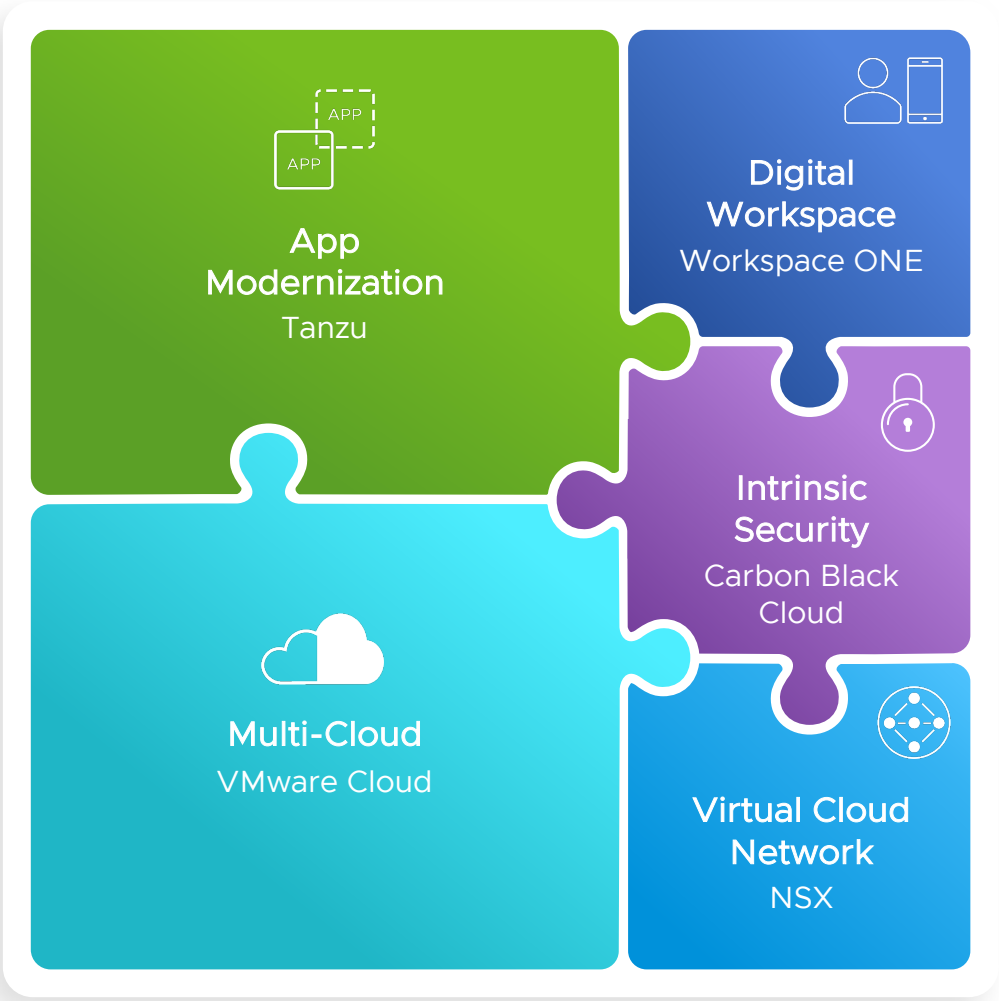
¿Tengo un mix de herramientas que me protegen?

vmware

# Demostración de un ataque

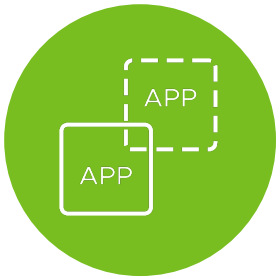
vmware

# Portafolio de VMware




vmware

# Portafolio de VMware

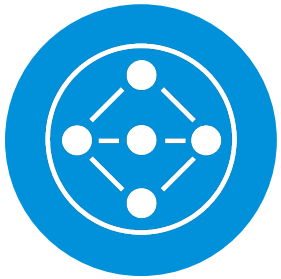



## App Modernization

- Tanzu
- PKS
- Bitnami
- Wavefront
- Pivotal Labs

## Multi-Cloud

- VMware Cloud Foundation
- VMware Cloud AWS
- vSphere, vSAN, NSX, vRealize
- CloudHealth
- Cloud Provider Platform
- SD-WAN by VeloCloud
- vCloud NFV



## Virtual Cloud Network

- NSX
- SD-WAN by VeloCloud
- NSX Advanced Load Balancer
- vRealize Network Insight
- Service Defined Firewall
- Uhana by VMware

## Digital Workspace

- Workspace ONE
- Horizon

## Intrinsic Security

- Carbon Black Cloud
- Service Defined Firewall
- Workspace Security
- Secure State

vmware

# ¿Qué es Seguridad intrínseca?

Aprovechar su infraestructura en cualquier aplicación, cualquier nube y cualquier dispositivo para proteger sus aplicaciones y datos en cualquier parte.


vmware

# Intrinsic Security

## Deja de sacrificar

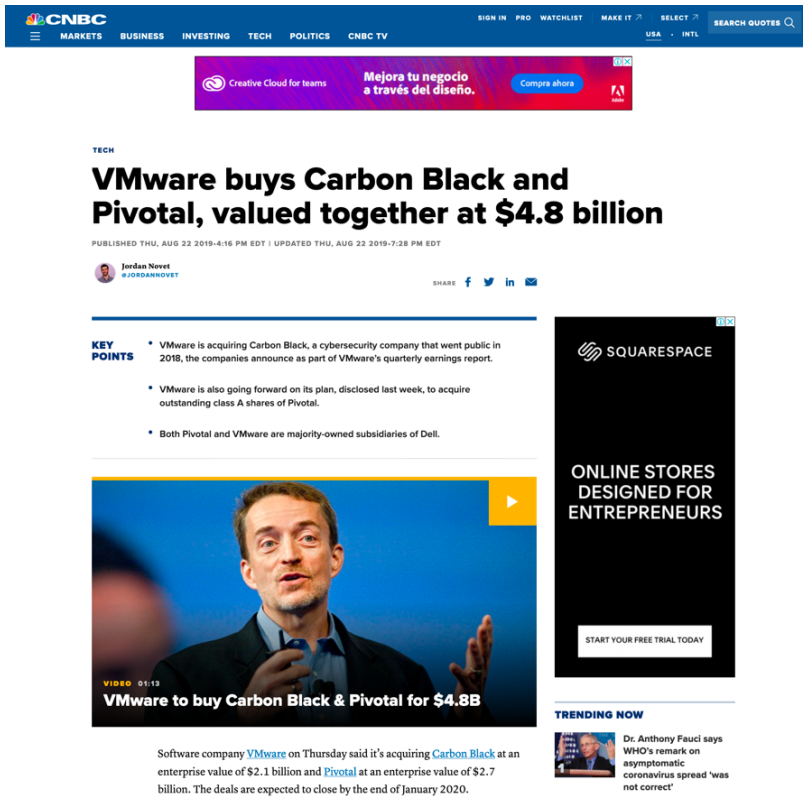
Producción
Computo

Dispositivo
Rendimiento

Usario
Experiencía

vmware

# Adquisición de Carbon Black



CNBC

MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

SIGN IN PRO WATCHLIST MAKE IT SELECT SEARCH QUOTES

USA · INTL



TECH

**VMware buys Carbon Black and Pivotal, valued together at $4.8 billion**

PUBLISHED THU, AUG 22 2019-4:16 PM EDT | UPDATED THU, AUG 22 2019-7:28 PM EDT

Jordan Novet
@JORDANNOVET

SHARE

**KEY POINTS**

- VMware is acquiring Carbon Black, a cybersecurity company that went public in 2018, the companies announce as part of VMware's quarterly earnings report.
- VMware is also going forward on its plan, disclosed last week, to acquire outstanding class A shares of Pivotal.
- Both Pivotal and VMware are majority-owned subsidiaries of Dell.

VIDEO 01:13
**VMware to buy Carbon Black & Pivotal for $4.8B**

Software company VMware on Thursday said it's acquiring Carbon Black at an enterprise value of $2.1 billion and Pivotal at an enterprise value of $2.7 billion. The deals are expected to close by the end of January 2020.



TRENDING NOW

Dr. Anthony Fauci says WHO's remark on asymptomatic coronavirus spread 'was not correct'

vmware | Security & Compliance Blog

// INTRINSIC SECURITY

## VMware Announces Intent to Acquire Carbon Black

Tom Corn, SVP/GM Security Products, VMware

Posted August 22, 2019

0 Comments

vmware | Carbon Black.

https://www.cnbc.com/2019/08/22/vmware-earnings-q2-2020-acquires-carbon-black-pivotal.html
https://blogs.vmware.com/security/2019/08/vmware-announces-intent-to-acquire-carbon-black.html

vmware

# 6,300+
Clientes

# 1/3
Fortune 100

# Reconocido por los principales analistas y publicaciones

Gartner peerinsights™

## MOST 5-STAR RATINGS

A Gartner Peer Insights Elección de los clientes para soluciones EDR Enero de 2019

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2019

## BEST PRODUCT ENDPOINT SECURITY

Cyber Defense Magazine 2019 InfoSec Awards

MITRE ATT&CK™

## LEADER IN DETECTING THREATS

MITRE ATT & CK Evaluación Noviembre 2018

Gartner®

## A VISIONARY

Cuadrante mágico de Gartner para plataformas de protección de puntos finales 2019

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2019

## BEST CYBERSECURITY COMPANY & BEST ENDPOINT SECURITY SOLUTION

Premios a la excelencia en ciberseguridad 2019

FORRESTER®

## STRONG PERFORMER

Las suites Forrester Wave ™ Endpoint Security 2019

vmware®

# ¿Por qué estamos aquí?

## Los desafíos que impulsan VMware Carbon Black

### Análisis y detección localizados

- Los empleados son remotos.
- El contexto es limitado.
- Análisis de amenazas aislado en un entorno.

### Las herramientas de seguridad son de talla única

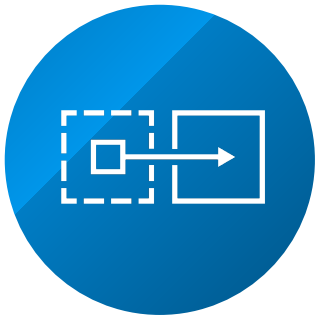
- Cada org es diferente
- Los parches tienen excepciones
- Uso del sistema no considerado

### La mayoría de los ataques abusan de las herramientas legítimas

- Software no todo en blanco y negro
- Actividad oculta en la memoria.
- El movimiento lateral es frecuente

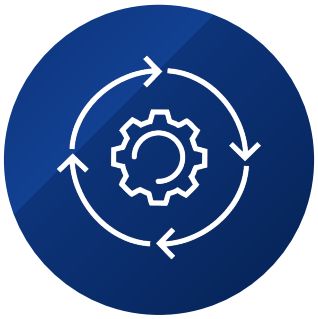
Docenas de agentes, docenas de consolas, docenas de verdades

# La seguridad debe ser transformada



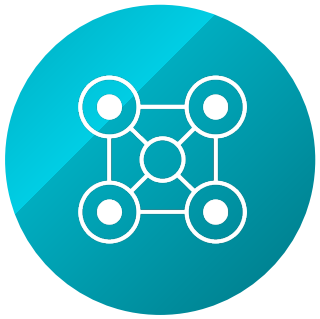
Incluído

Construído



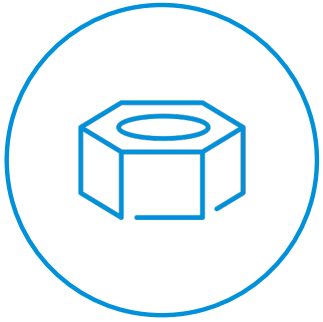
Proactivo

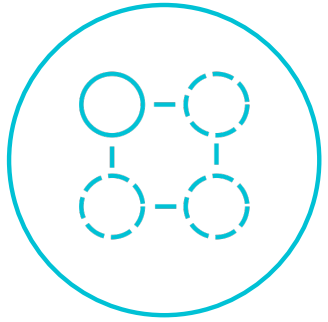
Reactivo



Alineado

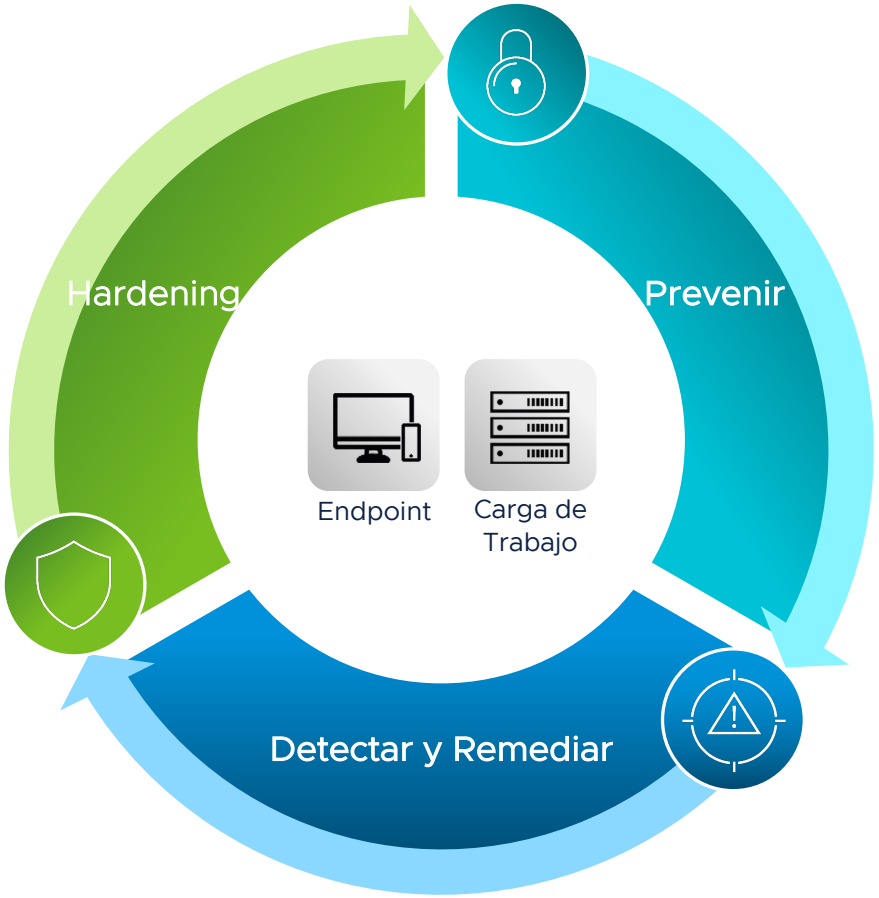
Aislado





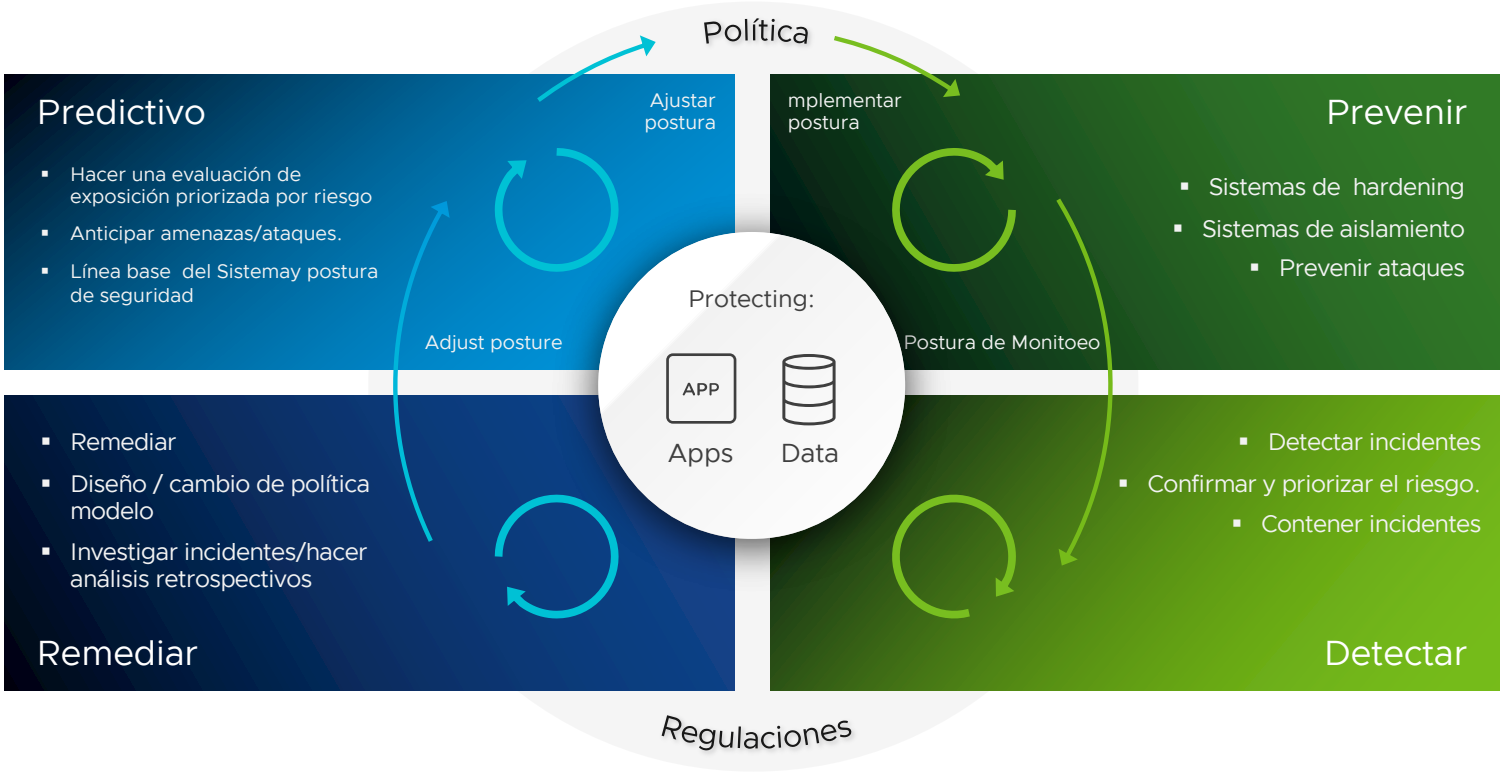
vmware

# Seguridad en los End Points y en las Cargas de Trabajo




vmware

# Arquitectura adaptativa de protección contra ataques




ID: 377791

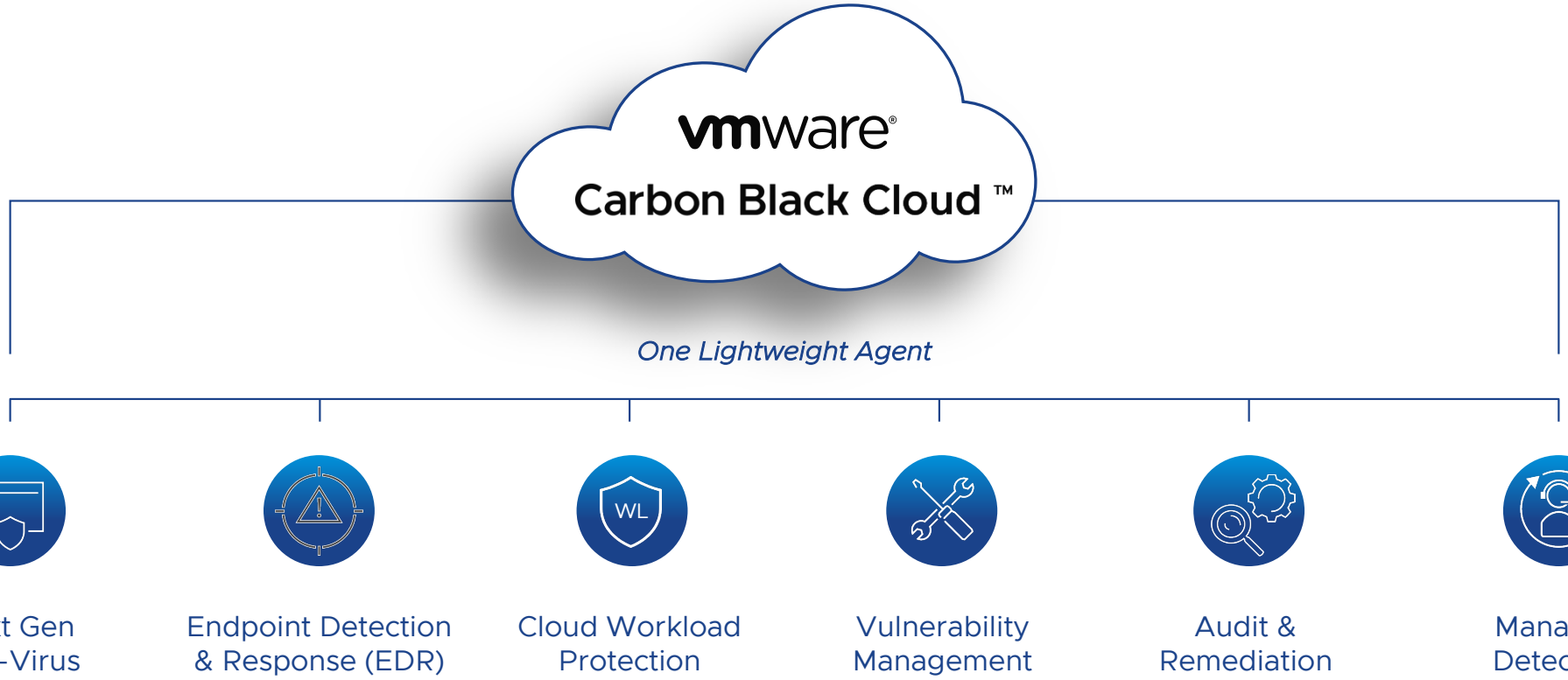
Source: Gartner (December 2018)

# Potal de Carbon Black

Demostración

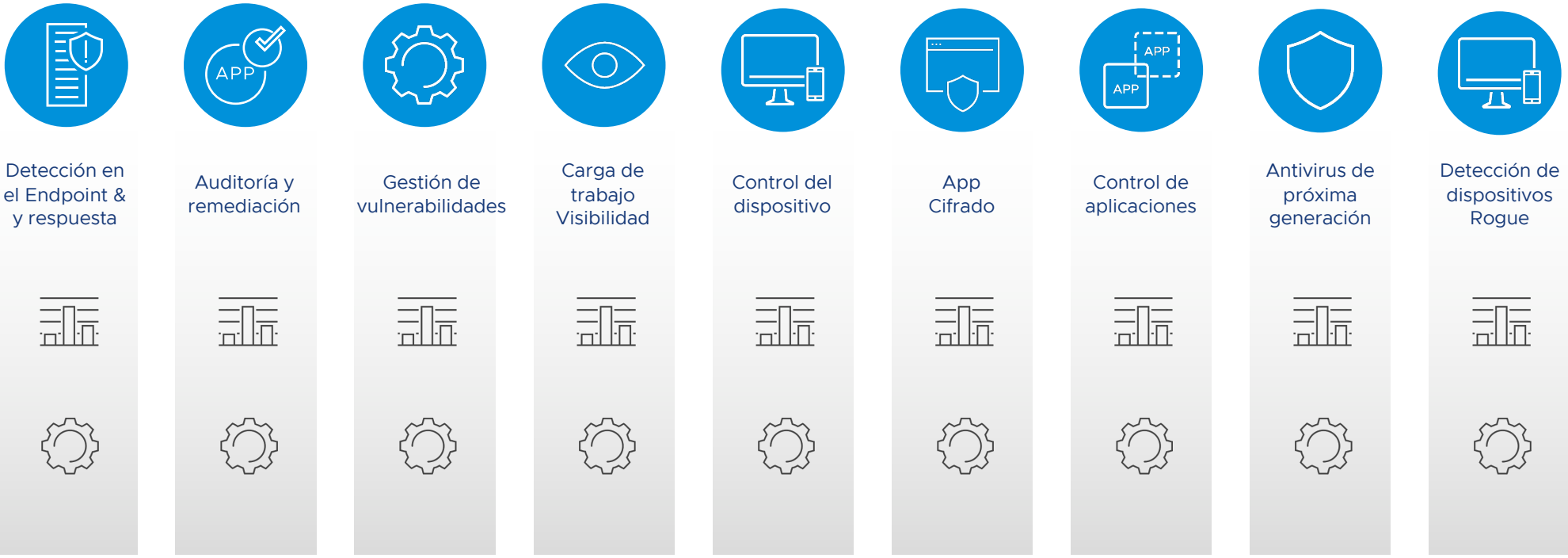
vmware

# Plataforma de protección de endpoints nativa de la nube



# Silos…

## Conjunto de herramientas fragmentado y en silicio con múltiples consolas, conjuntos de políticas, agentes …

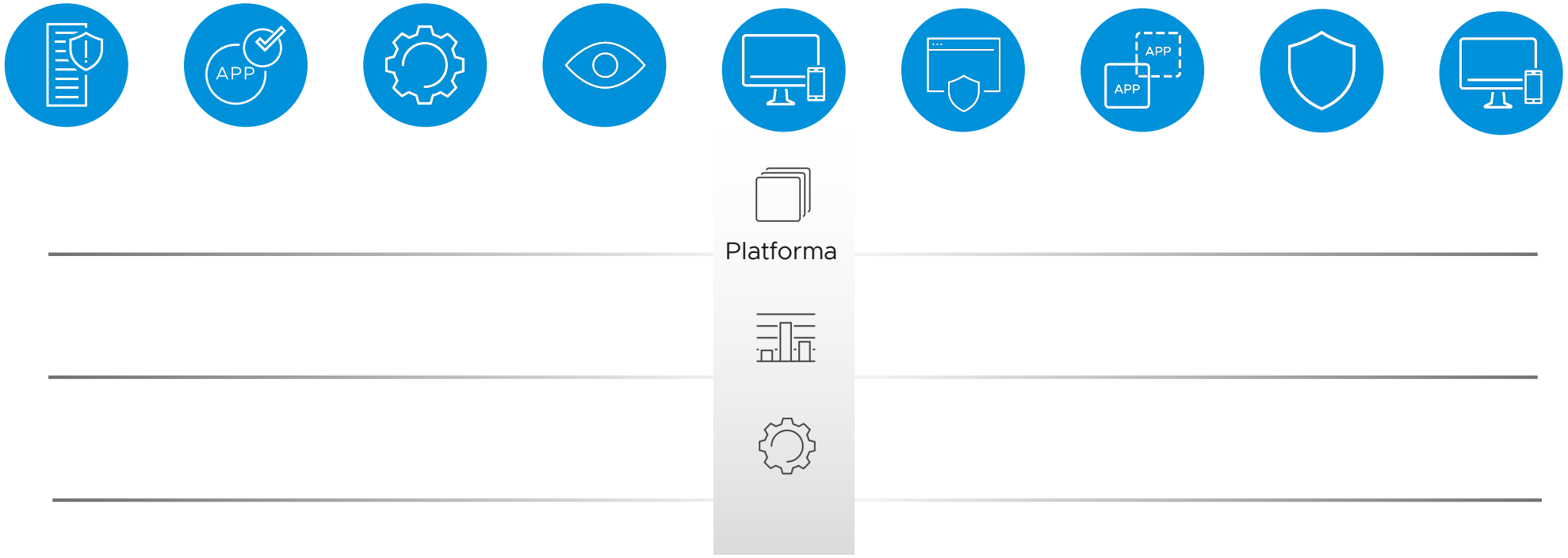



vmware

# A una plataforma unificada

## Casos de uso interconectados. Una sola consola, plataforma y agente

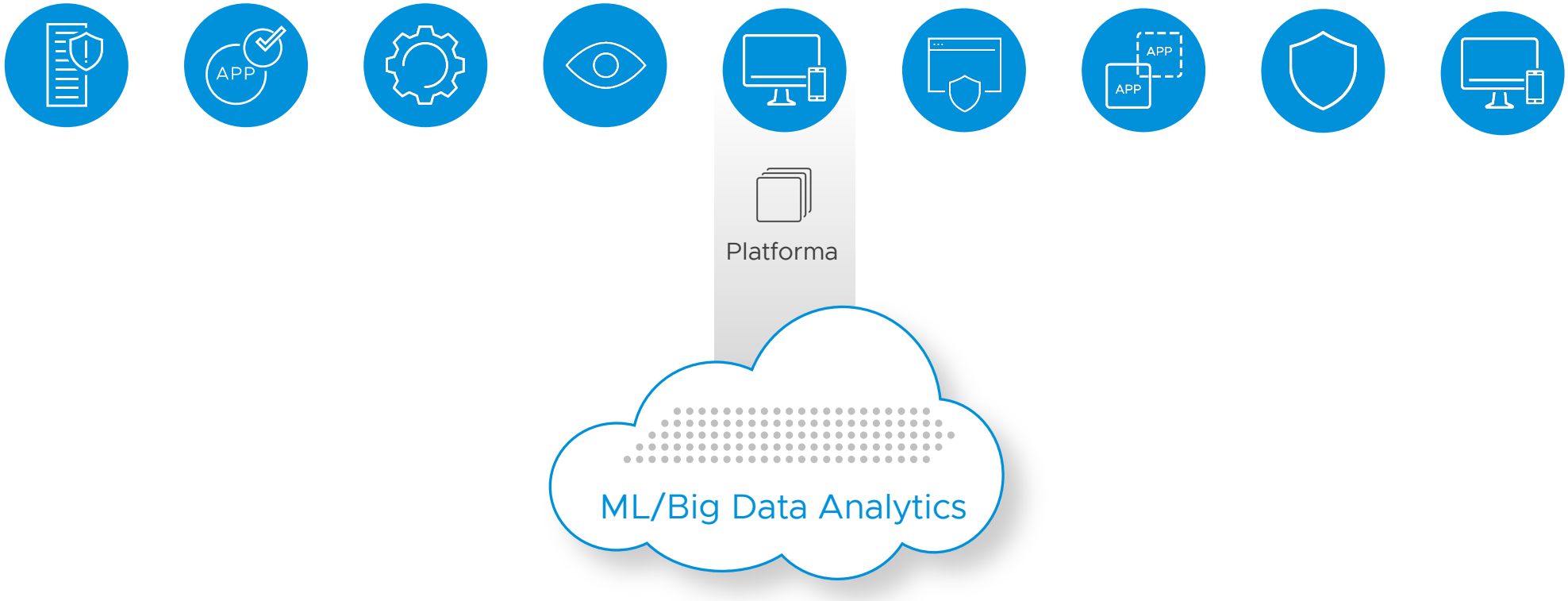
.




vmware

# Contexto

## Una plataforma basada en la nube que combina la amenaza, la infraestructura y el contexto de la aplicación




Monitoree millones de puntos finales y cargas de trabajo, analizando más de 540 TB de datos de punto final y más de 1.3 billones de eventos por día *

vmware

# ¿Por qué las empresas están cambiando a la seguridad nativa de la nube??

## Prevención sin perímetro y adaptación global más rápida

**Implementar y proteger**
en horas, no meses

**Contener ataques**,
incluso en redes domésticas

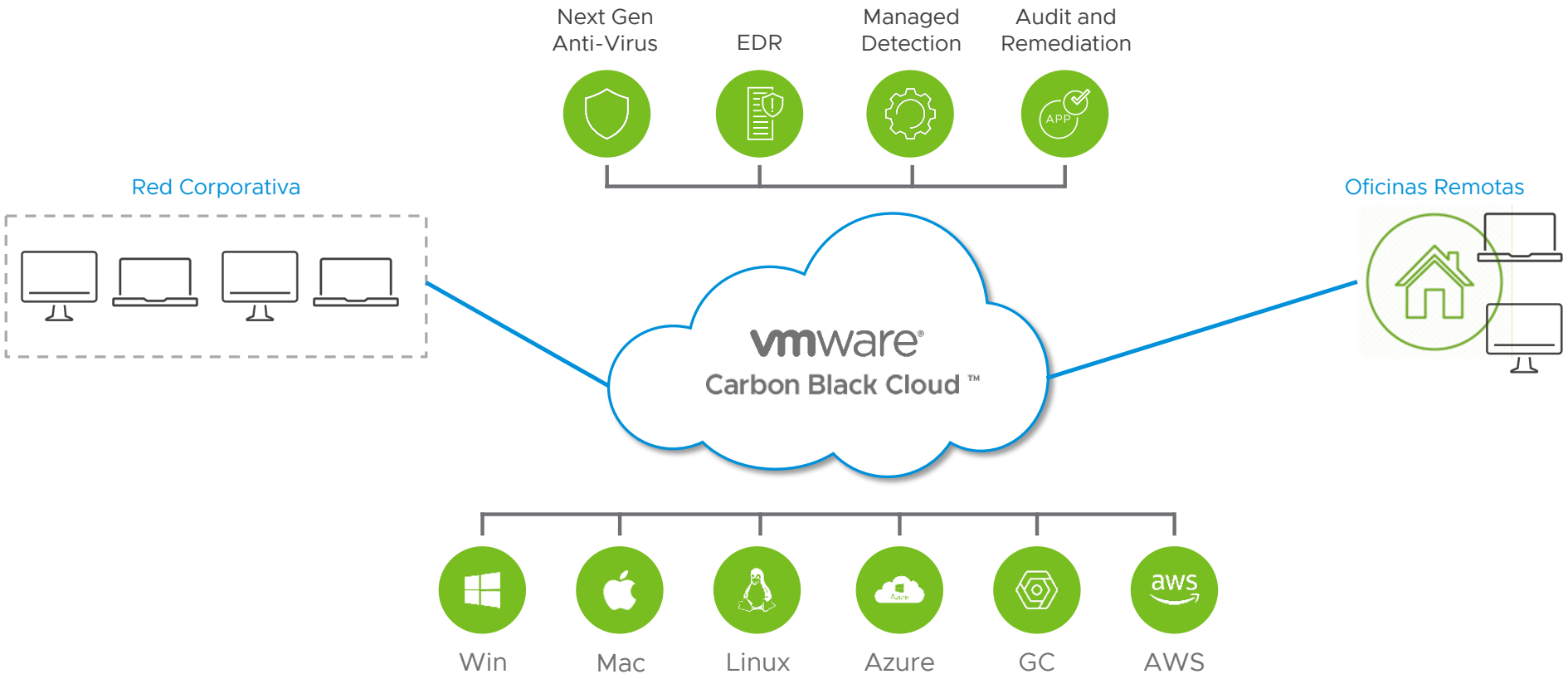
**Escala sin esfuerzo**
a millones de puntos finales

**Mejora la analítica**
como son los comportamientos visto a nivel mundial

vmware

# VMware Carbon Black Cloud

## Protección para ambientes corporativos y domésticos




vmware

# ¿Preguntas que tienen los clientes?

¿Cómo puedes accesar a la herramienta cuando tienes ya un virus en tu ambiente?

¿Qué pasa si tengo un ataque ahora, lo puedes detener?

¿Puedo analizar el ataque y lo puedo ver en tiempo real?

¿Qué acciones puedo realizar cuando detecto un ataque?

¿La herramienta cuenta con Alertas y Notificaciones?

¿Qué Sistemas Operativos soporta la herramienta actualmente?

¿ La herramieta cuenta con una consola centralizada y fácil de manejar?

¿Cómo filtras un ataque?

¿Exite integraciones con terceros ó APIs abiertos?

# Endpoint Standard

## Antivirus de próxima generación y EDR basada en el comportamiento

### CASOS DE USO

Reemplace y extienda las soluciones de antivirus (AV) tradicionales

Investigue ataques en tiempo real

Consolide múltiples agentes en un único endpoint

Oficinas remotas seguras y fuerza de trabajo móvil

### VENTAJAS

Protección contra ataques conocidos y desconocidos

Alertas claras y priorización de ataques potenciales

Investigación más sencilla de los incidentes de seguridad

Tiempo promedio de resolución más corto

• Reducción de costos generales; no se requiere infraestructura

# Endpoint Detection and Response (EDR)

## Persecución de amenazas y respuesta ante incidentes para implementaciones híbridas

### CASOS DE USO

Persecución de amenazas

Respuesta ante incidentes

Preparación ante infracciones

Validación y evaluación de alertas

Análisis de la causa principal

Investigaciones forenses

Aislamiento de hosts

### VENTAJAS

Respuesta y corrección integrales y más rápidas

Respuesta ante incidentes acelerada y persecución de amenazas con visibilidad continua del endpoints

Identificación rápida de las actividades y la causa principal del atacante

Acceso remoto seguro a los endpoints infectados para una investigación en profundidad

# App Control

## Control de aplicaciones y protección de infraestructura crítica

### CASOS DE USO

Bloqueo de sistemas críticos

Dispositivos de función fija: terminales de punto de venta, cajeros automáticos, sistemas de control industrial, dispositivos médicos

Endpoints de alto riesgo: escritorios corporativos, computadoras portátiles de ejecutivos

**Servidores:** controladores de dominio, servidores de correo electrónico y aplicaciones web, entornos de datos de tarjetas, plataformas de negociación financiera

### VENTAJAS

Detenga el malware, el ransomware y los ataques de próxima generación

Elimine el tiempo fuera de servicio no planificado de los sistemas críticos

Consolide agentes de endpoints

Evite cambios no deseados en la configuración del sistema

Proteja los sistemas legacy que se ejecutan en sistemas operativos no compatibles

vmware

# Integración en sus soluciones de seguridad existentes

## API abiertas y más de 100 integraciones de productos con proveedores de seguridad líderes


vmware

# Integración en sus soluciones de seguridad existentes

## Más de 500 socios de productos y servicios

### SIEM

*Correlacione alertas de amenazas y acciones de respuesta en una sola plataforma*

sumologic
splunk>
IBM Security QRadar
exabeam

### SOAR

*Automatizar/organizar la respuesta a incidentes y acciones correctivas*

Resilient an IBM Company
splunk> phantom
DEMISTO
SWIMLANE


### Intelligence

*Mejora la detección*

INTEL471
IBM X-Force
Recorded Future
KENNA Security

### Perimeter

*Conecte la red y los datos y acciones del punto final*

zscaler
netskope
paloalto NETWORKS
Check Point SOFTWARE TECHNOLOGIES LTD.

# Demostración de Carbon Black

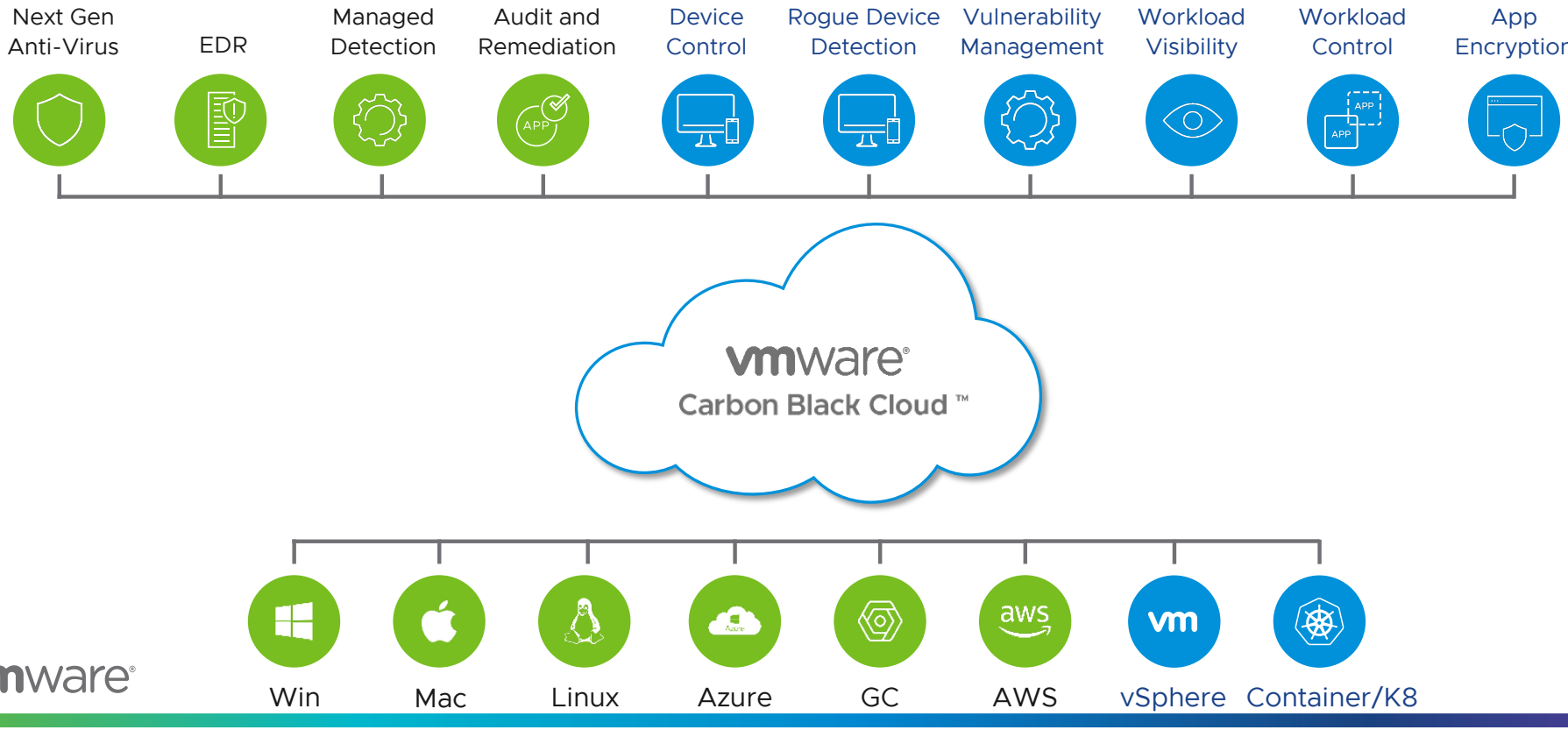
vmware

# VMware Carbon Black Cloud

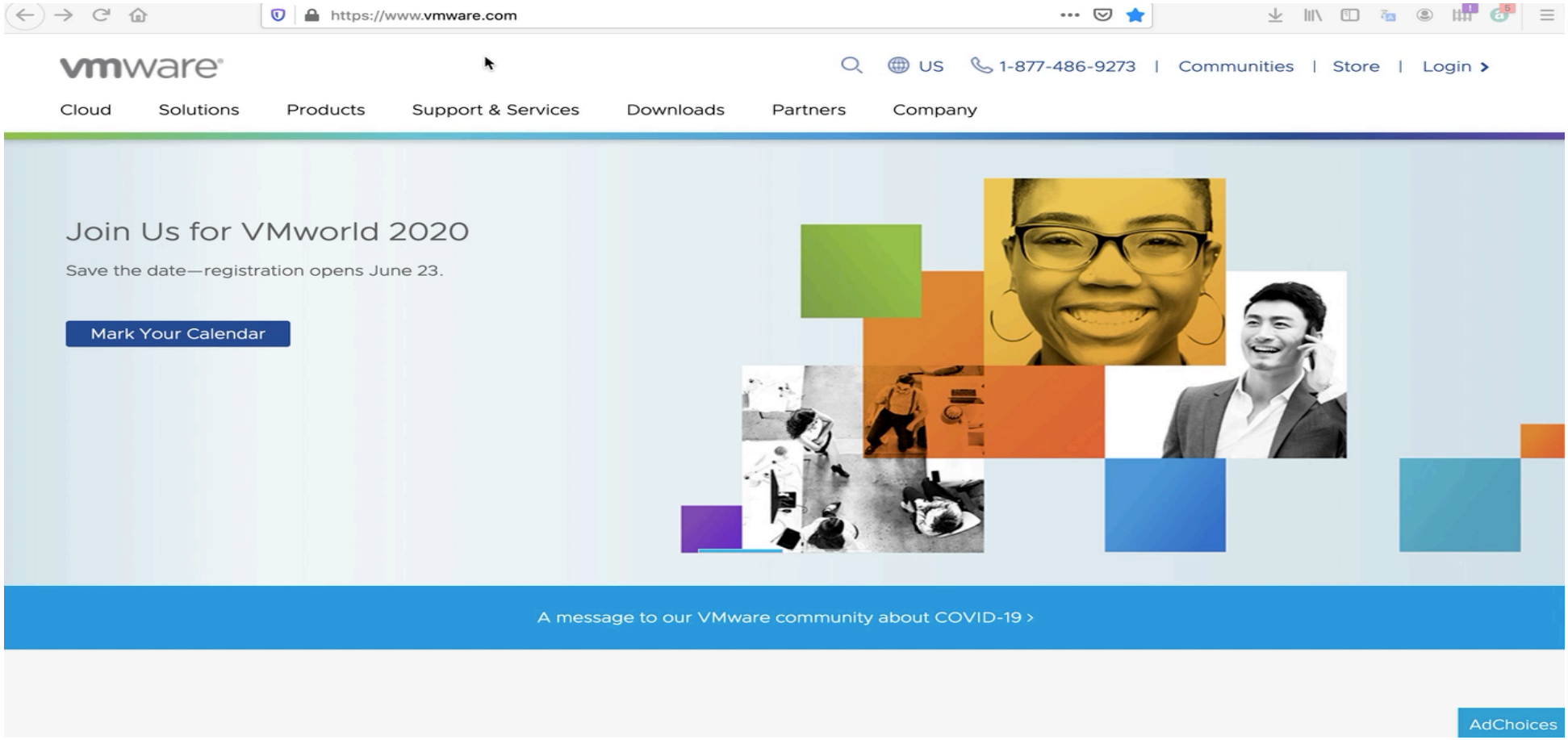
## Roadmap

En 2020, VMware planea expandir estas capacidades en gran medida con:

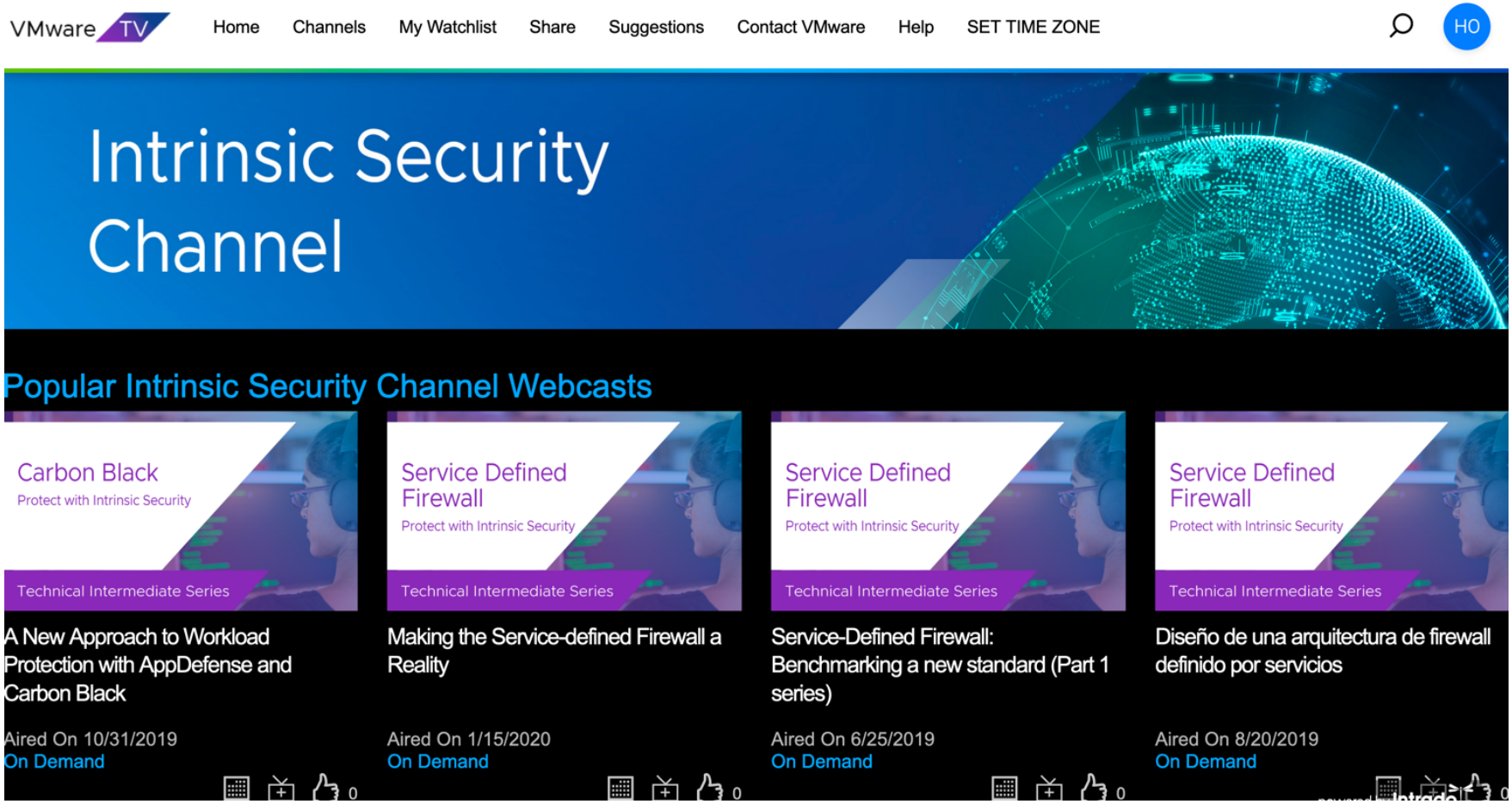
- Capacidades de protección de punto final heredadas, como Control de dispositivos y Detección de dispositivos no autorizados
- Capacidades clave de protección de la carga de trabajo y el endurecimiento, como la gestión automatizada de vulnerabilidades y el control de la carga de trabajo.
- Una expansión más allá de los puntos finales tradicionales, para proteger vSphere y los contenedores.



# Recursos


https://www.vmware.com
vmware
US
1-877-486-9273
Communities
Store
Login
Cloud
Solutions
Products
Support & Services
Downloads
Partners
Company
Join Us for VMworld 2020
Save the date—registration opens June 23.
Mark Your Calendar
A message to our VMware community about COVID-19 ›
AdChoices

# VMware TV


VMware TV
Home
Channels
My Watchlist
Share
Suggestions
Contact VMware
Help
SET TIME ZONE
HO
Intrinsic Security Channel
Popular Intrinsic Security Channel Webcasts
Carbon Black
Protect with Intrinsic Security
Technical Intermediate Series
A New Approach to Workload Protection with AppDefense and Carbon Black
Aired On 10/31/2019
On Demand
Service Defined Firewall
Protect with Intrinsic Security
Technical Intermediate Series
Making the Service-defined Firewall a Reality
Aired On 1/15/2020
On Demand
Service Defined Firewall
Protect with Intrinsic Security
Technical Intermediate Series
Service-Defined Firewall: Benchmarking a new standard (Part 1 series)
Aired On 6/25/2019
On Demand
Service Defined Firewall
Protect with Intrinsic Security
Technical Intermediate Series
Diseño de una arquitectura de firewall definido por servicios
Aired On 8/20/2019
On Demand

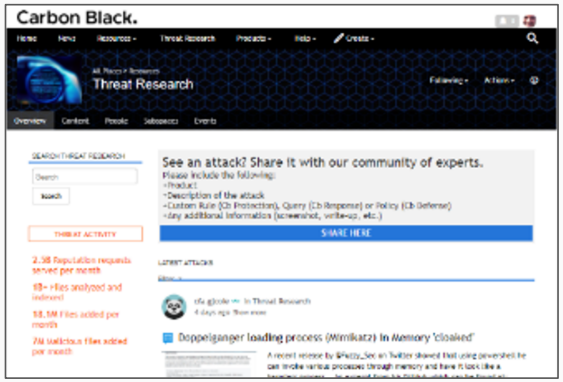
# Comunidad de seguridad

## Conéctese con miles de expertos en seguridad

Más de 20,000 miembros de la comunidad

A nivel global

## Reúna inteligencia de amenazas en tiempo real




Amenaza procesable Intel

COI, listas de observación y más

## Acceso directo a la unidad de análisis de amenazas de VMware Carbon Black


Análisis de amenazas avanzadas y alertas de amenazas

vmware

# Qué significa la nube de Carbón Black

## 1

### ESTAMOS EXTENDIENDO NUESTRAS OFERTAS AL PSC

El mejor lugar para análisis, excelencia operativa e innovación rápida

## 2

### ESTAMOS COMPROMETIDOS CON LA RESPUESTA DE CB ON PREMISE

Miles de clientes y docenas de socios.

## 3

### Cuando estés lista, podrás mudarte a PSC(femenino)

La migración es opcional, se puede hacer en el momento que usted elija y seremos facilitados por nosotros.

## 4

### LA RESPUESTA CB EN LA PREM SE BENEFICIARÁ DE PSC

El análisis de amenazas en la nube potenciará los feeds de amenazas de PSC y CB Response

vmware

# Mitigar el riesgo

Diseñado específicamente para su seguridad interna

Análisis de contexto enriquecido y aplicación gradual

# Preguntas

vmware


*Gracias por su Tiempo!!*