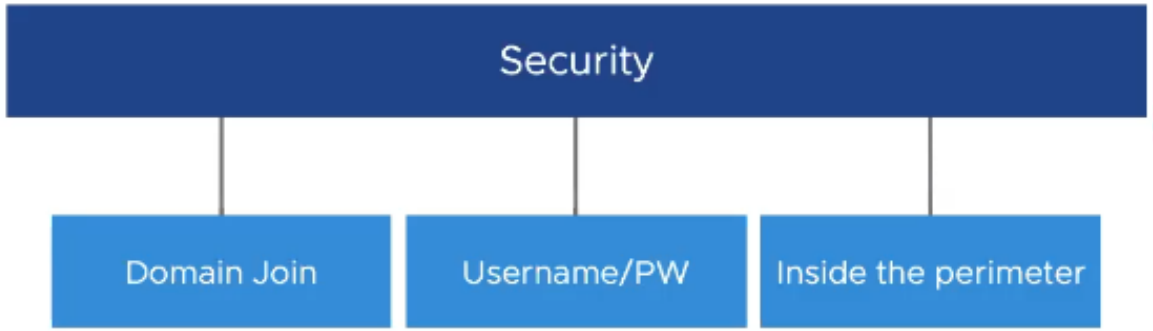
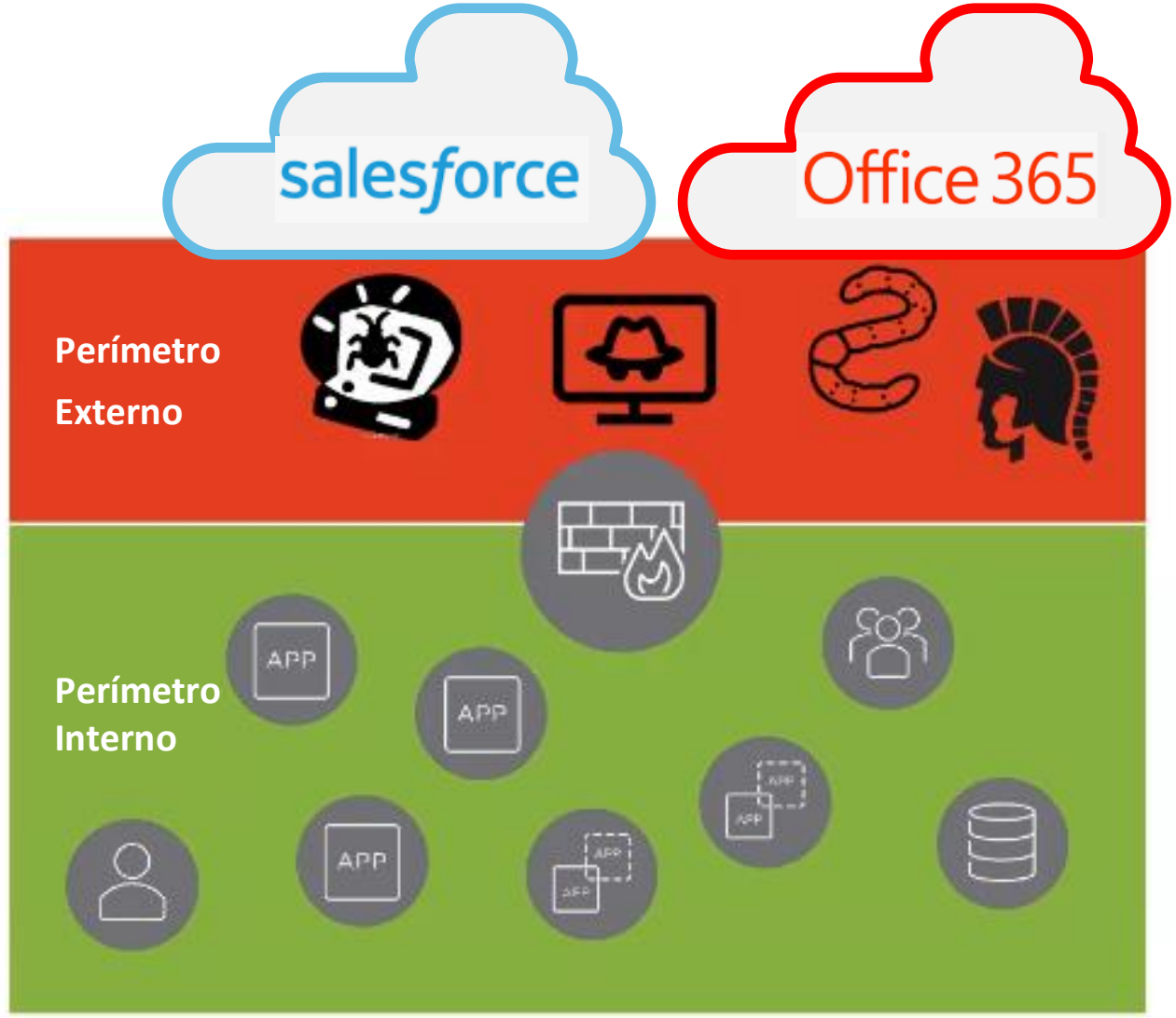
VMware Carbon Black

Como podemos proteger os negócios dos clientes ?

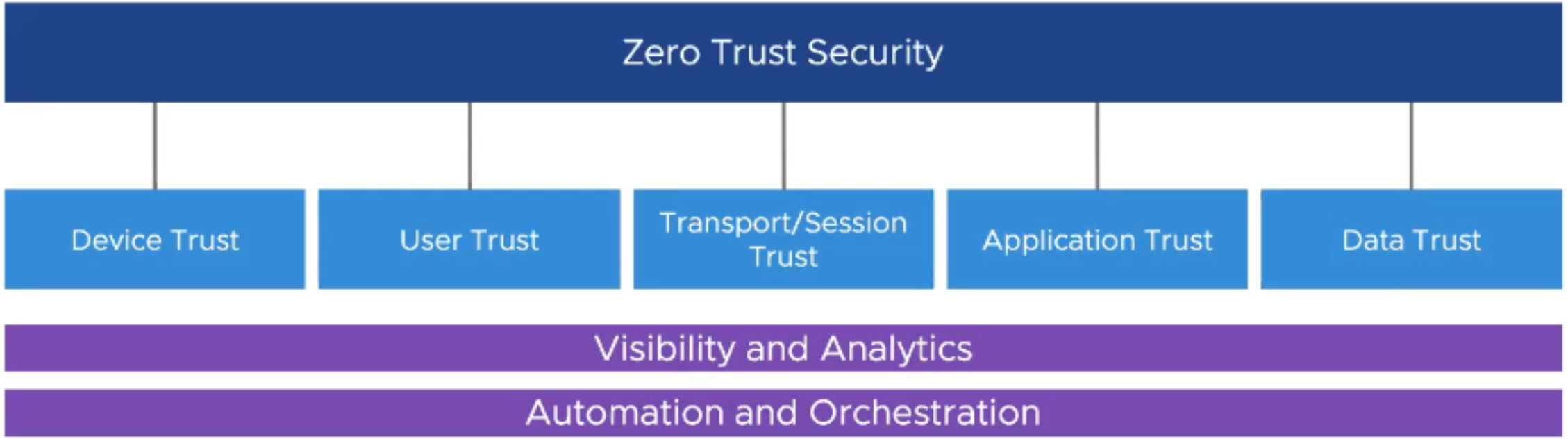
Segurança Tradicional



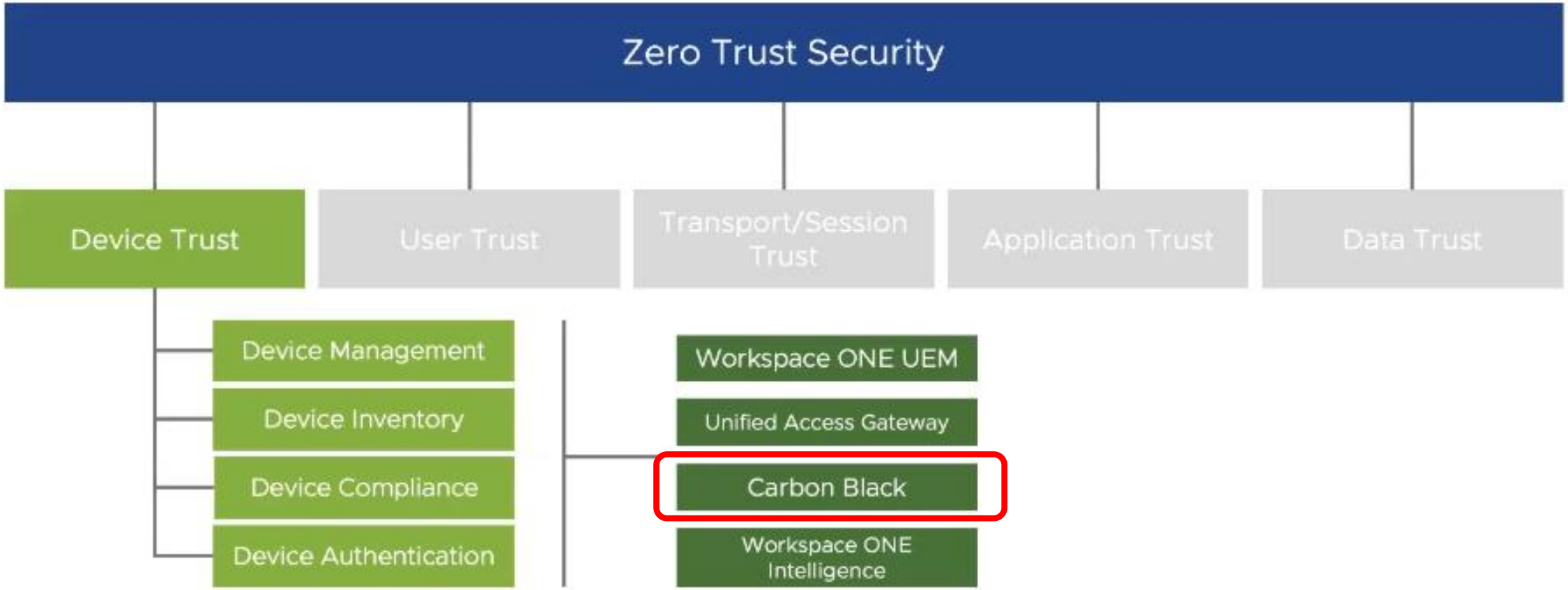


Conceito Zero Trust

Os cinco pilares da arquitetura Zero Trust



VMware Zero Trust



Zero Trust - Desafios

Fragmentação

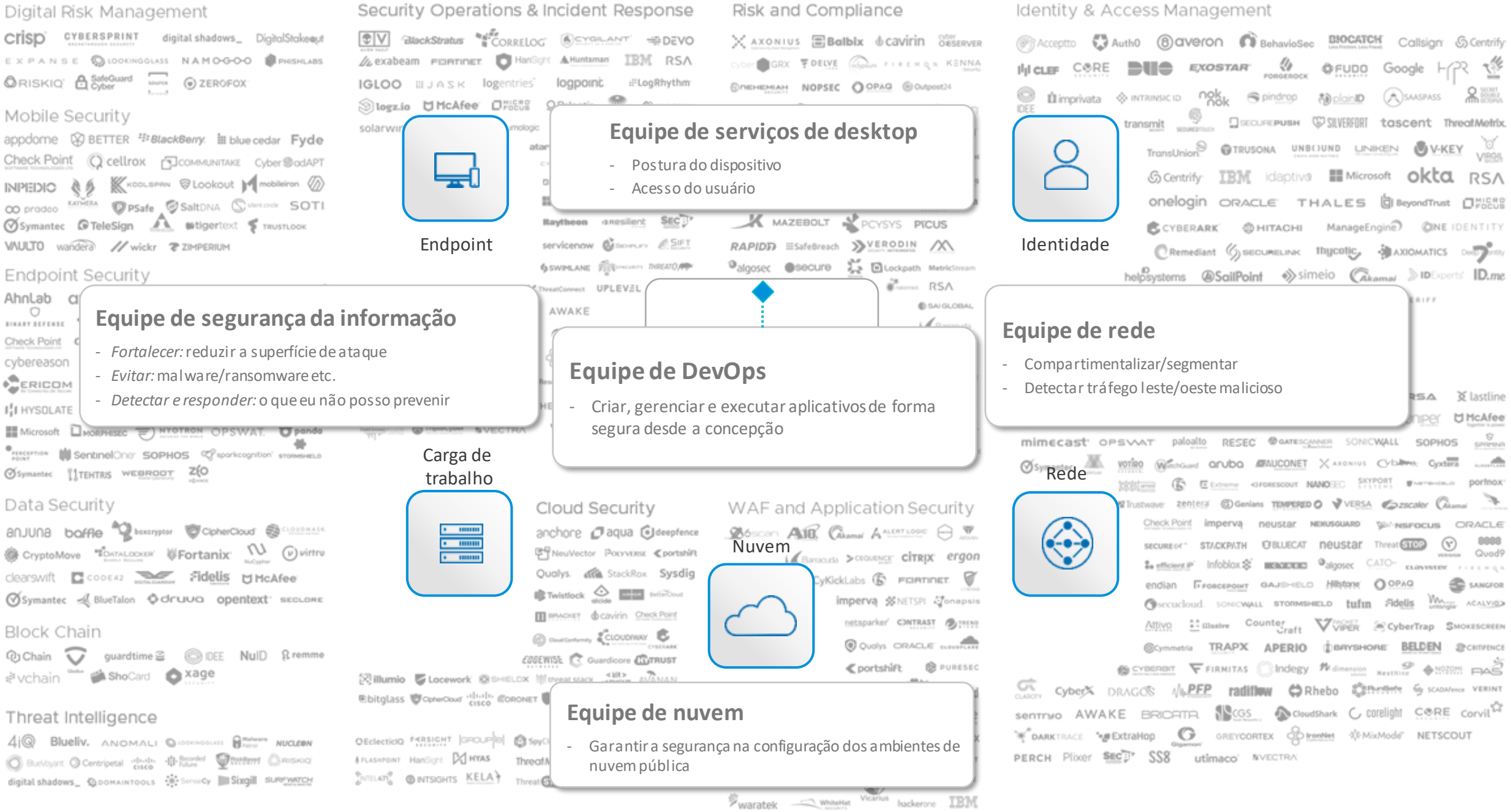
Os silos de TI
e de segurança dificultam
a colaboração e a
operacionalização da
proteção e correção

Foco nas ameaças

As equipes não têm contexto sobre os sistemas e a infraestrutura que estão sendo protegidos

Agregação

A quantidade excessiva de consoles, agentes, scripts etc. resultam em desalinhamento e erros de configuração


Digital Risk Management
Mobile Security
Endpoint Security
Data Security
Block Chain
Threat Intelligence
Security Operations & Incident Response
Risk and Compliance
Identity & Access Management
Cloud Security
WAF and Application Security
Equipe de serviços de desktop
- Postura do dispositivo
- Acesso do usuário
Endpoint
Identidade
Equipe de segurança da informação
- Fortalecer: reduzir a superfície de ataque
- Evitar: malware/ransomware etc.
- Detectar e responder: o que eu não posso prevenir
Equipe de DevOps
- Criar, gerenciar e executar aplicativos de forma segura desde a concepção
Equipe de rede
- Compartimentalizar/segmentar
- Detectar tráfego leste/oeste malicioso
Carga de trabalho
Nuvem
Rede
Equipe de nuvem
- Garantir a segurança na configuração dos ambientes de nuvem pública

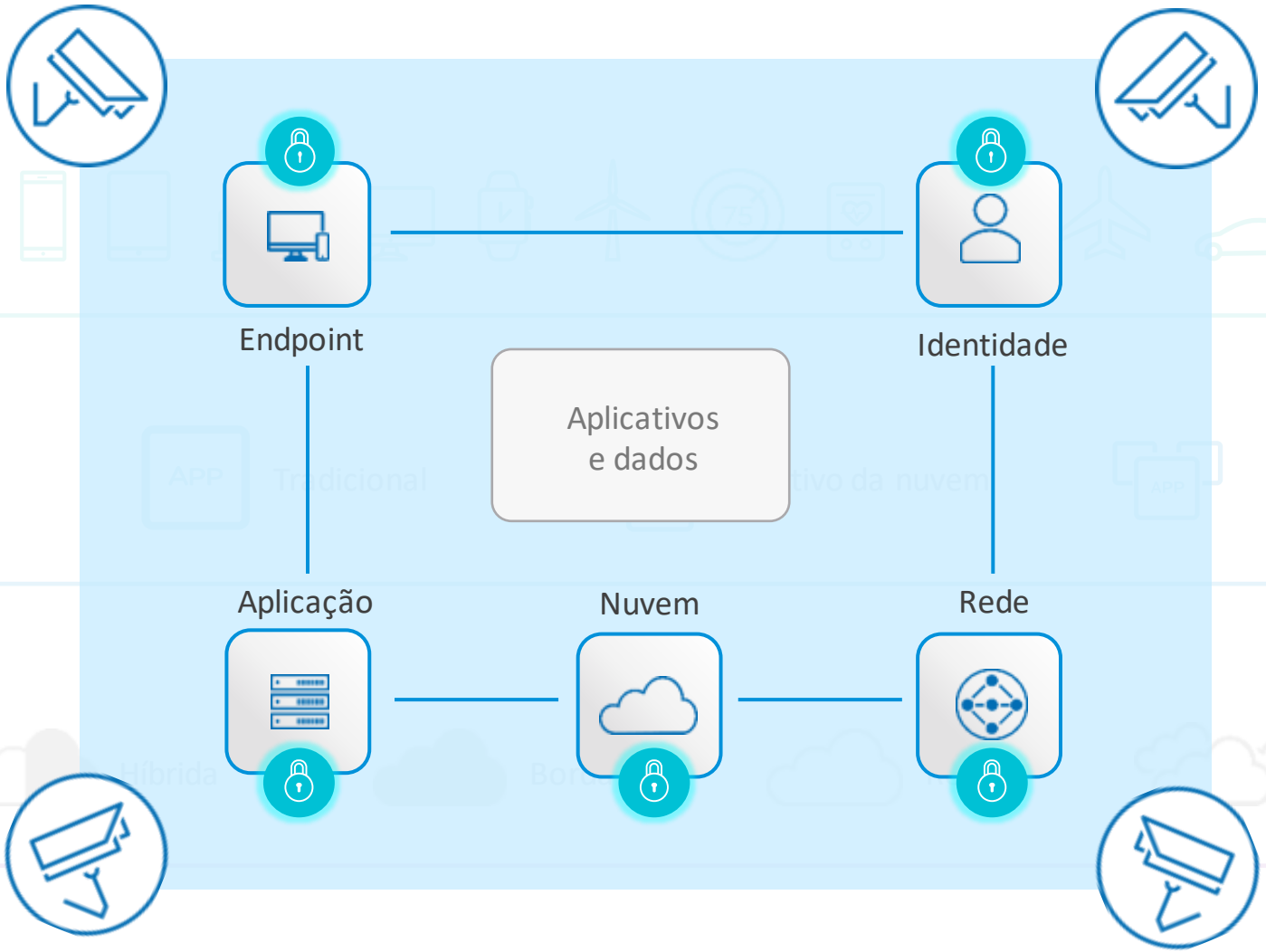
Visão da VMware

Qualquer dispositivo

Qualquer aplicação

Qualquer nuvem

Controle e visibilidade integrados



Transformando a Segurança

Unificada

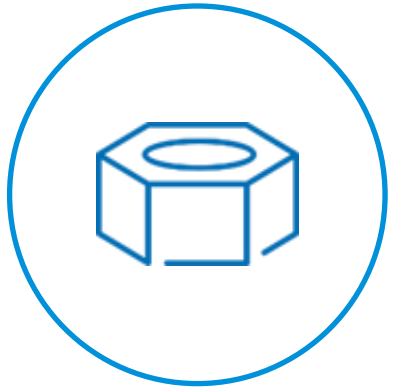
Fragmentação

Centrada no contexto

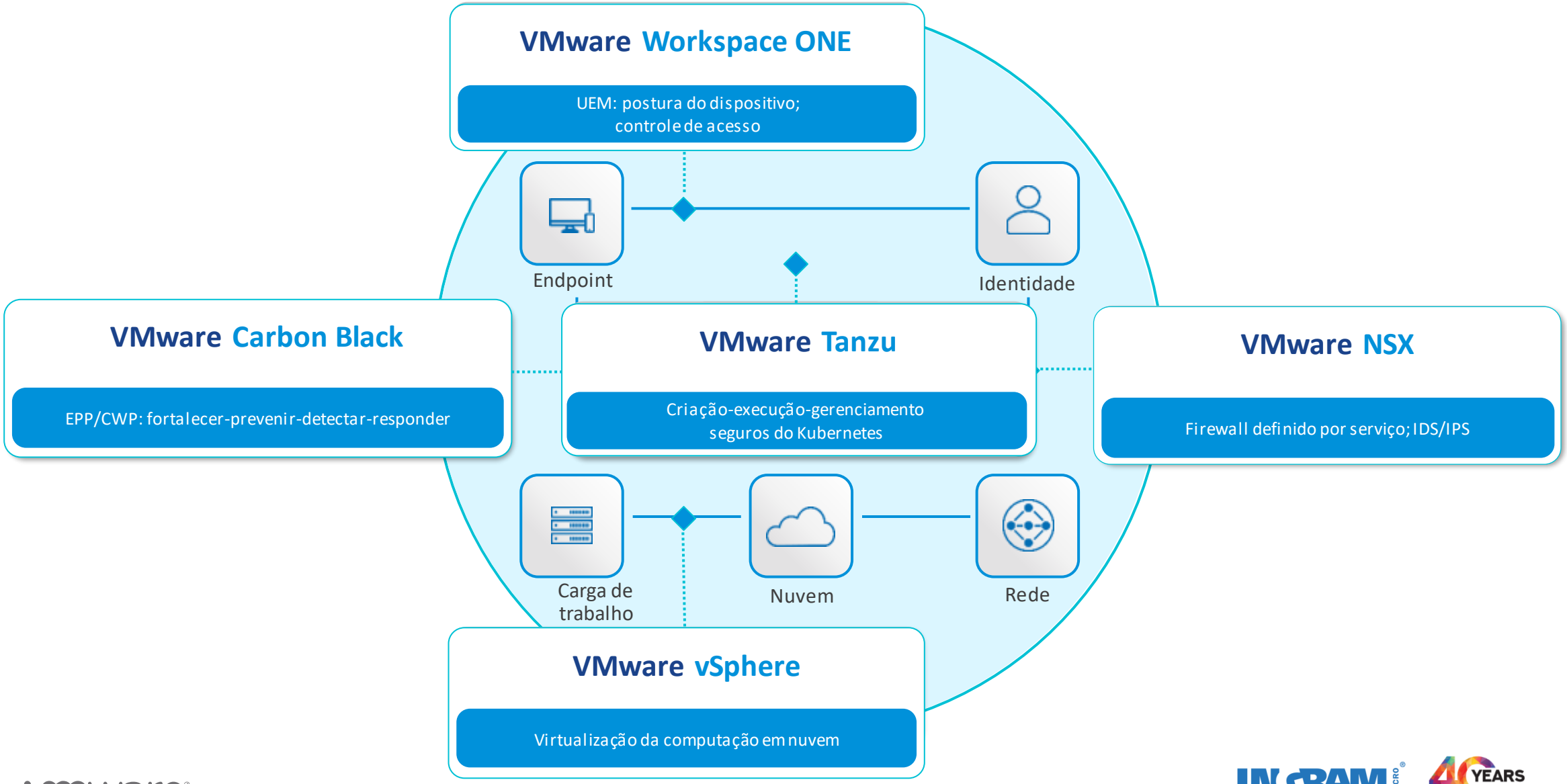
Foco em ameaças

Integrada

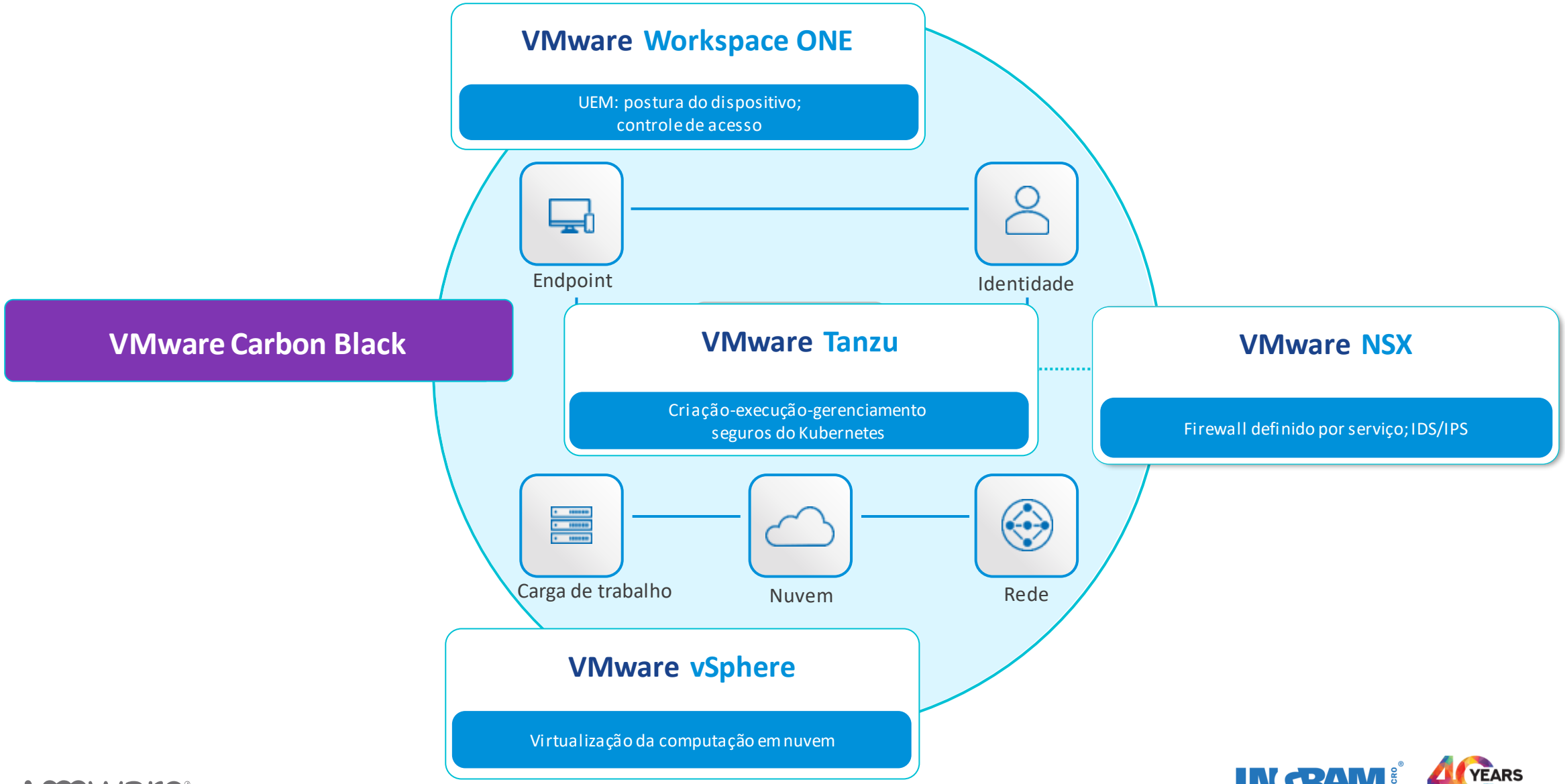
Agregação



Soluções VMware



Segurança na base



Proteção de Endpoints e Workloads

Identificar riscos

- Linha de base/visibilidade/ validação
- Acompanhe vulnerabilidade, mudança de estado/configuração
- Aproveitamento para reforço e contexto

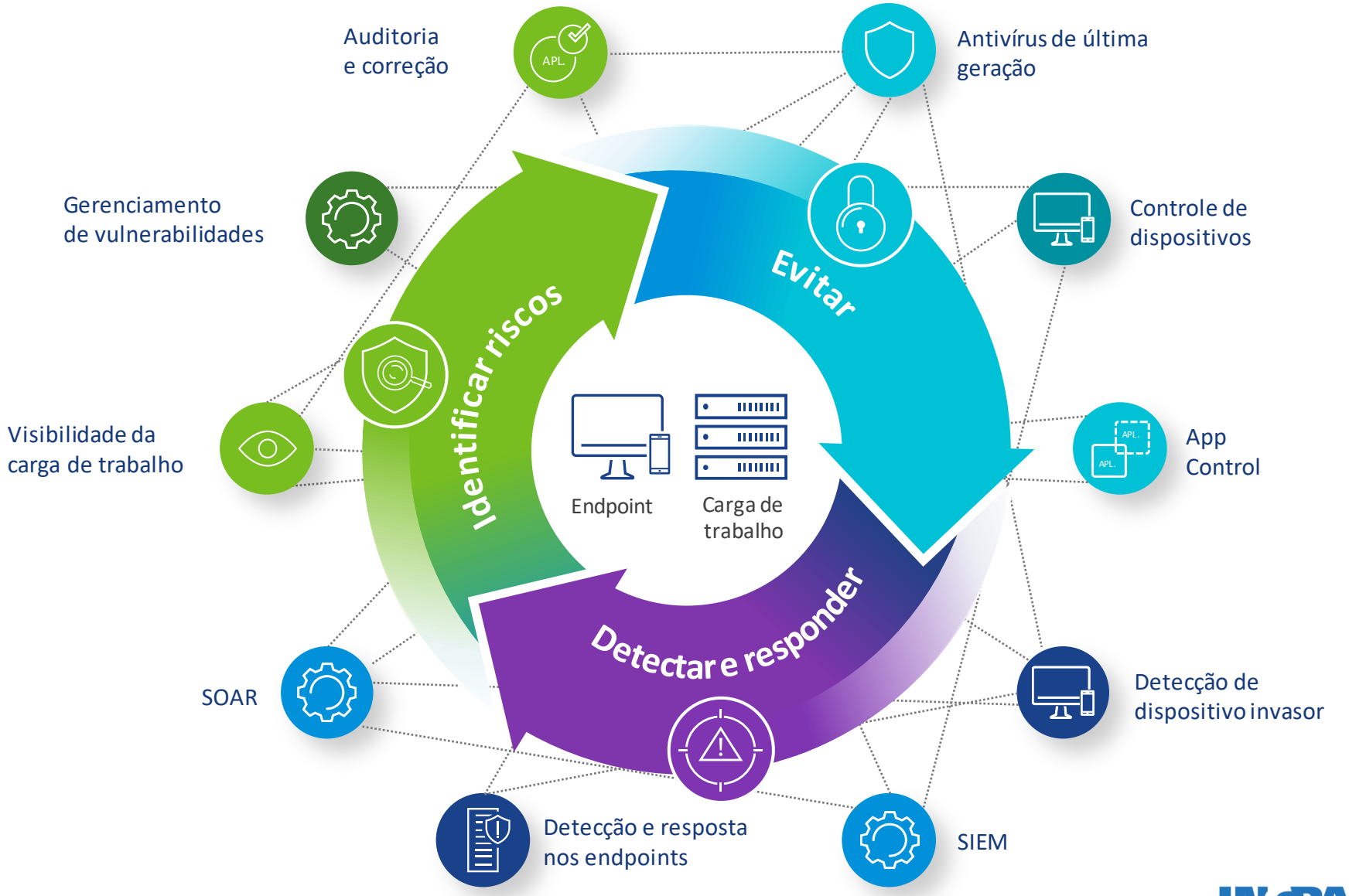
Evitar

- Fortaleça ativos
- Evite malwares e softwares e processos indesejados
- Impeça ataques sem programa malicioso e os que aproveitam os programas já instalados

Detectar e responder

- Visão detalhada: detecção (precoce/precisa)
- Visão global: veja a “campanha”
- Responda: correção e prevenção

Proteção de Endpoints e Workloads



379%
ROI over 3 years

7.5
hours saved per security incident

94%
of respondents saw significant improvement in security efficacy

75%
less frequent reimaging

Proteção de Endpoints e Workloads

Detecção e resposta nos endpoints

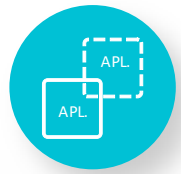
Auditoria e correção

Gerenciamento de vulnerabi-lidades

Visibilidade da carga de trabalho

Controle de dispositivos

Criptografia de apps



App Control

Antivírus de última geração

Detecção de dispositivo invasor

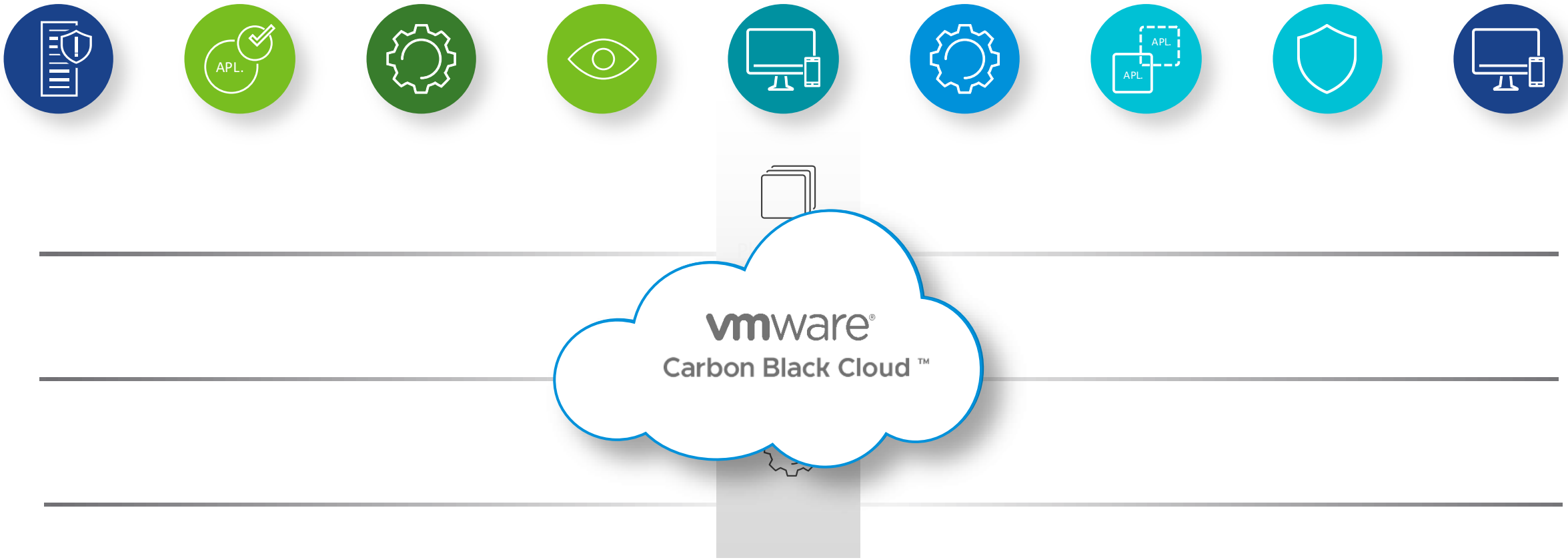
vmware

INGRAM MICRO

40 YEARS

Proteção de Endpoints e Workloads

Um único console, plataforma e agente



vmware

INGRAM MICRO 40 YEARS

O Carbon Black se integra ao seu stack de segurança

Como preparar sua estratégia de segurança de longo prazo

Aprimore os fluxos de trabalho

Adapta-se aos fluxos de trabalho existentes nas ferramentas de segurança e TI e os aprimora

Aumente a visibilidade

Estende a visibilidade e a correção entre endpoints, redes, cargas de trabalho e contêineres

Amplifique os investimentos

Ajuda você a aumentar a produtividade do Carbon Black e de seus outros investimentos em segurança e TI

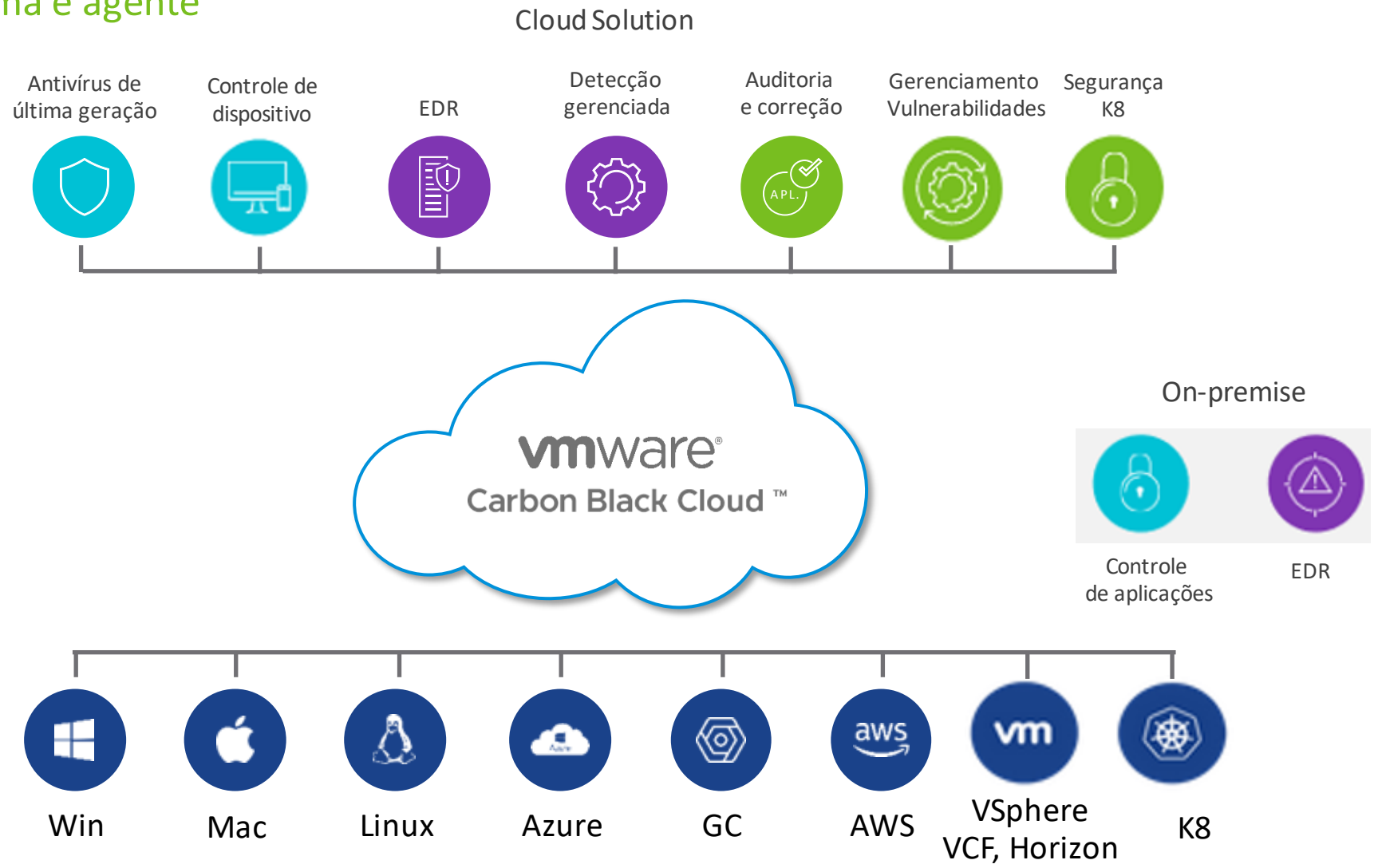
Proteção de Endpoints e Workloads

Um único console, plataforma e agente

Evitar

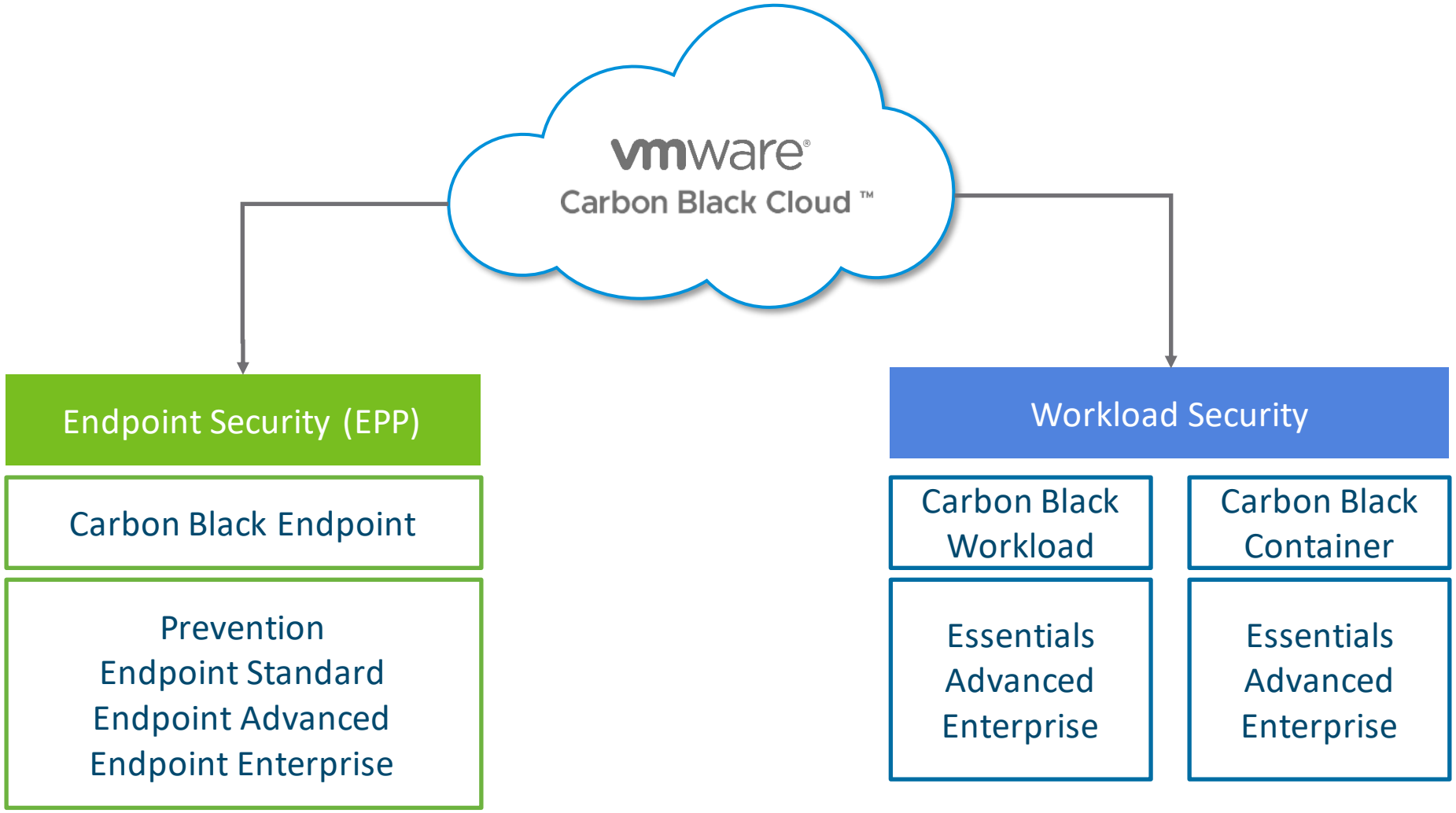
Detectar e responder

Identificar riscos



Proteção de Endpoints e Workloads

Carbon Black Cloud Framework



Carbon Black Endpoint

Prevention Prevent	Endpoint Standard Prevent, Detect & Reponse	Endpoint Advanced Prevent, Detect & Response, Identify Risk	Endpoint Enterprise Prevent, Detect & Response, Identify Risk
Next-Gen Antivirus	• Next-Gen Antivirus • Device Control • Behavior EDR	• Next-Gen Antivirus • Device Control • Behavior EDR • Audit & Remediation • Vulnerability Management	• Next-Gen Antivirus • Device Control • EDR • Audit & Remediation • Vulnerability Management
➢ Block malware, fileless, and living off the land attacks	➢ Add ability to investigate unusual behavior, block external devices, and respond in real-time to threats	➢ Add device audit and risk remediation for system hardening and risk-prioritized visibility into vulnerabilities	➢ Add continuos event capture, threat hunting, and threat intelligence with customizable detections

Carbon Black Endpoint Standard

Certified to replace and extend traditional antivirus

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

Carbon Black Endpoint Audit & Remediation

Ask questions and take action in real time

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

Carbon Black Endpoint Vulnerability Management

Risk-prioritized vulnerability assessment

INCREASE VISIBILITY

- Leverage existing endpoint agent for inventory data

TRACK AND REPORT VULNERABILITIES

- Buit-in vulnerability context and links to resources
- Filterable and export results
- Two-way APIs

PRIORITIZED BY RISK

- Prioritized and scored based on risk of exploit
- Built-in risk scoring leveraging Kenna Security's data science approach

Carbon Black Endpoint Enterprise EDR

Detect and respond to advanced attacks

COMPLETE VISIBILITY

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

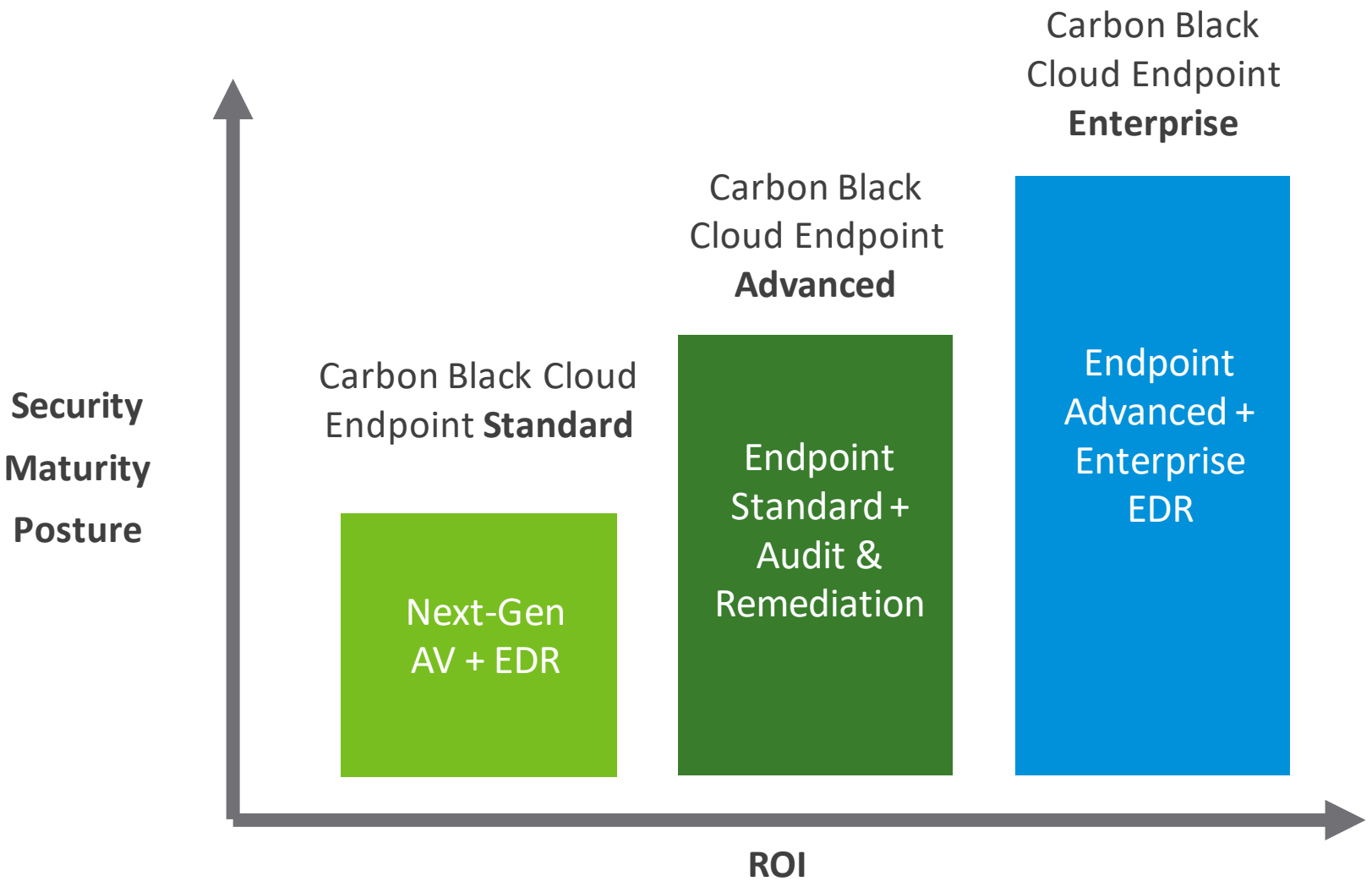
SCALE THE HUNT

- 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 Endpoint Bundles



Endpoint Standard provides Next-Gen AV + EDR

Endpoint Advanced comes with Endpoint Standard + Audit & Remediation

Endpoint Enterprise comes with Endpoint Advanced + Enterprise EDR

Carbon Black Endpoint Managed Detection

Prevent breaches with expert threat hunters at your side

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

vmware

Carbon Black Workload Security

Industry Leading Workload Protection purpose-built for vSphere

Vulnerability Management

Workload Inventory & Lifecycle Management

vSphere Integration

Audit/Remediation

NGAV

EDR for Workloads

Reduce Attack Surface

Identify risk and harden workloads against attack.

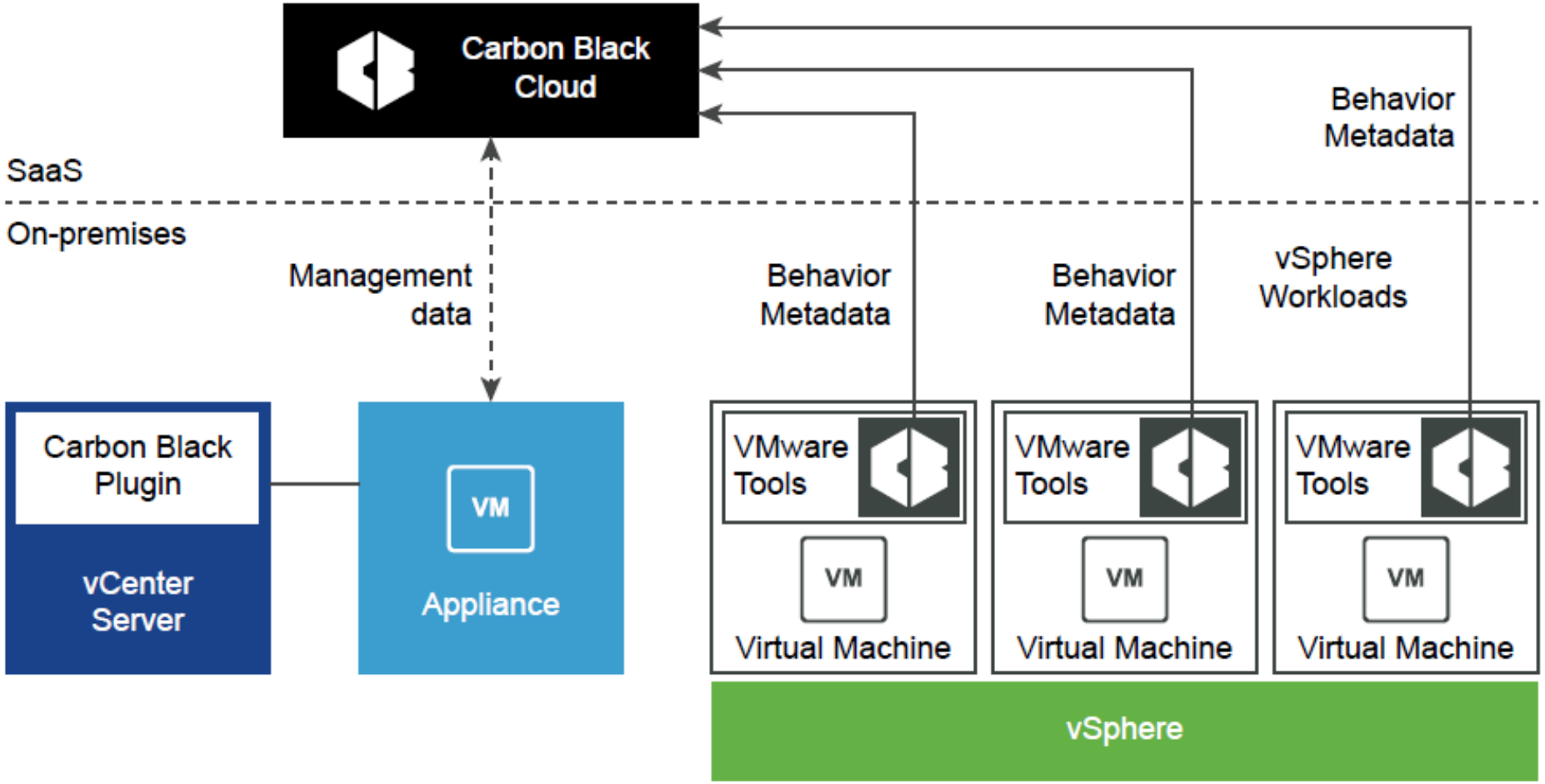
Increase Visibility

Easy to understand current state of workloads and vulnerabilities.

Simplify Operations

Better collaboration and shared intelligence for IT and Security teams.

Carbon Black Workload Security



Carbon Black Workload Security

VMware Carbon Black Cloud

Workload Essentials

IDENTIFY RISK / HARDEN

- Asset Inventory
- Audit and Remediation
- Vulnerability
- vCenter Plug-in
- Agentless
- Lifecycle Management

LIST PRICE:

$/CPU/YR/US Hosted

VMware Carbon Black Cloud

Workload Advanced

+ PREVENTION

- **NGAV**
- **Behavioral EDR**
- Workload Essentials Functionality

LIST PRICE:

$/CPU/YR/US Hosted

VMware Carbon Black Cloud

Workload Enterprise

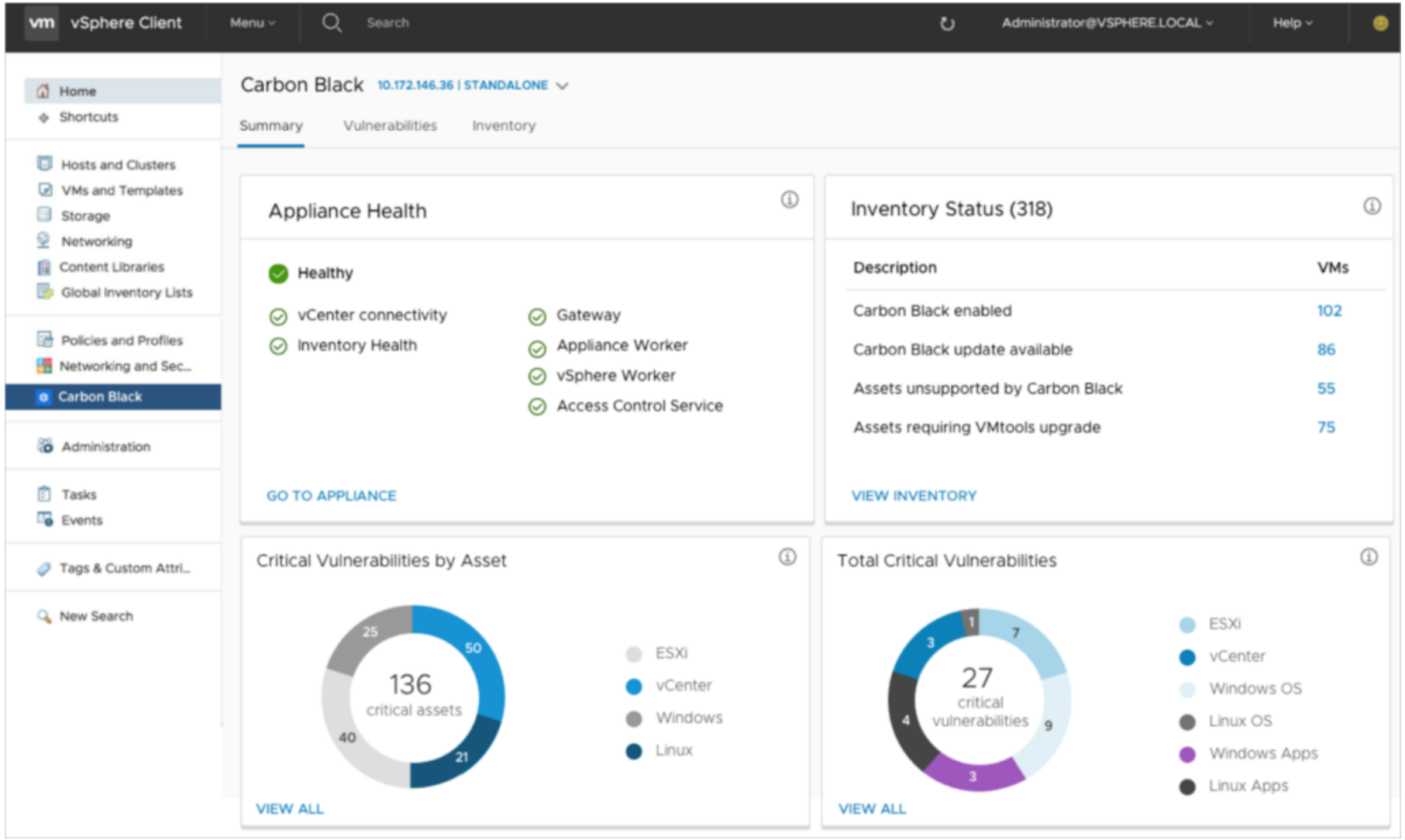
+ THREATHUNTING

- **Enterprise EDR**
- Workload Advanced Functionality

LIST PRICE:

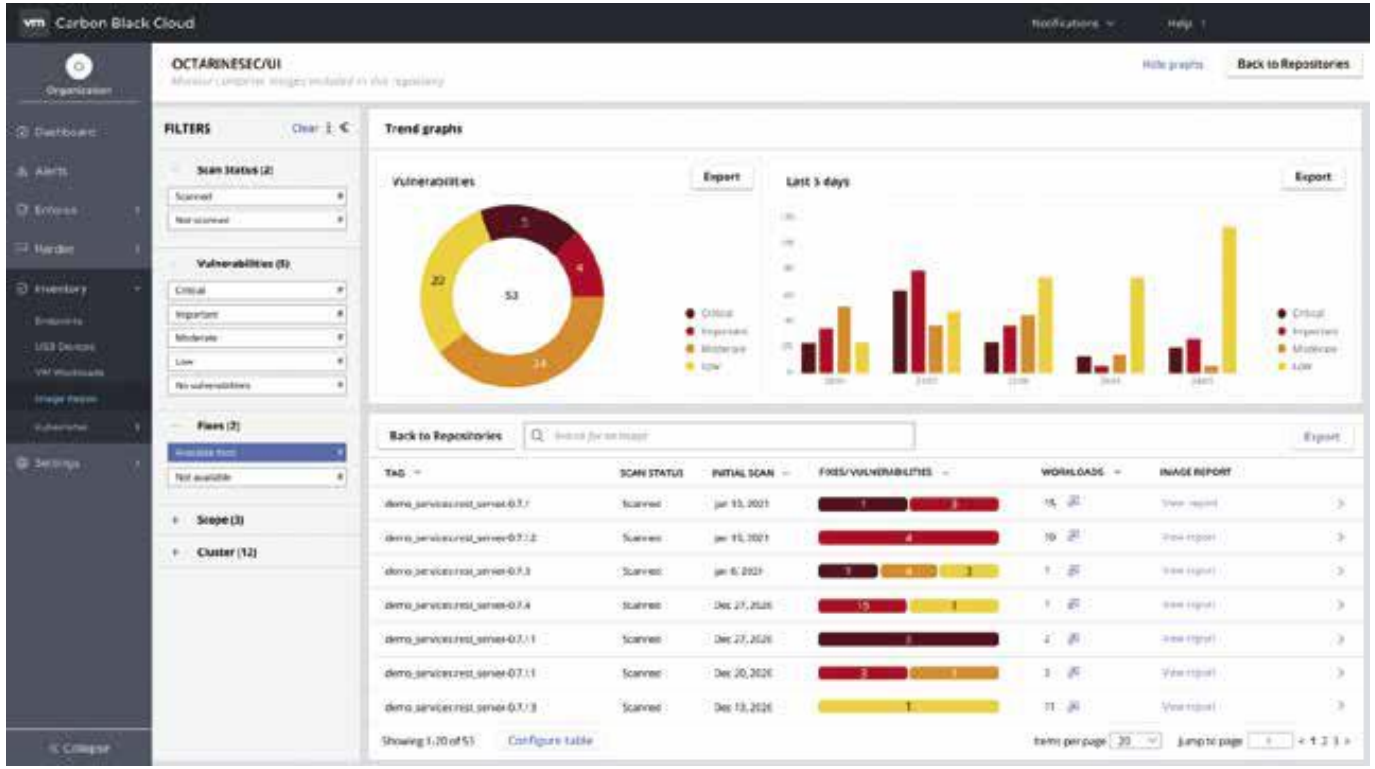
$/CPU/YR/US Hosted

Carbon Black Workload Security



Carbon Black Container Security

- ✓ Security posture dashboard
- ✓ Container image scanning
- ✓ Compliance policy automation
- ✓ Prioritized risk assessment
- ✓ Governance and enforcement
- ✓ CI/CD integration
- ✓ Integration with Harbor registry



Platform Support

Upstream Kubernetes
VMware Tanzu™ Kubernetes Grid™

Red Hat OpenShift
Amazon Elastic Kubernetes Service (EKS)

Google Kubernetes Engine (GKE)
Azure Kubernetes Service (AKS)

Carbon Black Workspace Security

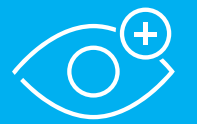
Combines best-in-class behavior threat detection, NGAV, and digital workspace analytics & remediation

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

Carbon Black Workspace Security

- Context/Compliance
- Threat Detection
- Consolidation

Carbon Black App Control

Market-leading application control solution

On-premise

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)

Carbon Black Hosted EDR

Detect and respond to advanced attacks

On-premise

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

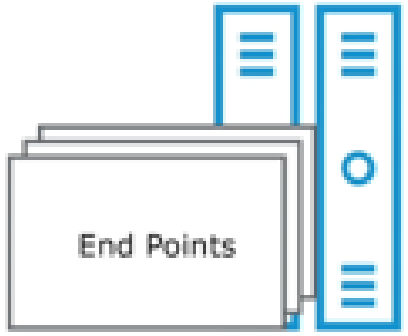
vmware

INGRAM MICRO 40 YEARS

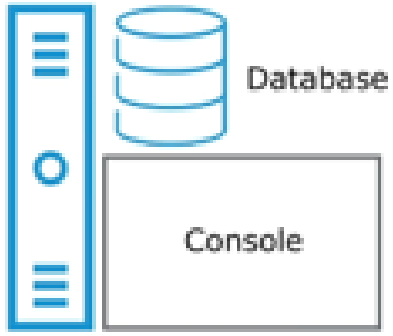
Realize the Promise of Technology

Carbon Black AppControl

Architecture



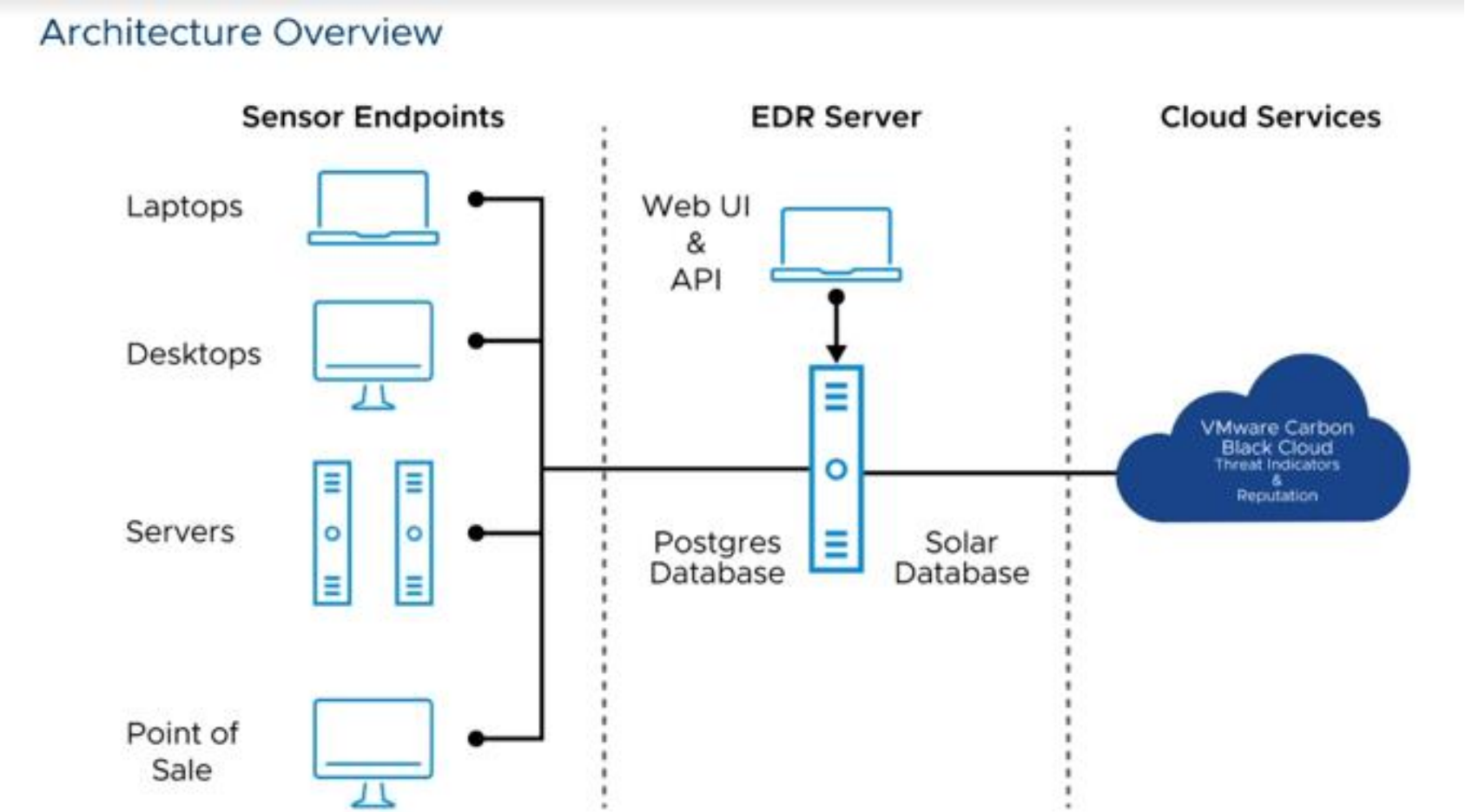
The Endpoint:
The Carbon Black App Control Agent maintains an active inventory of the system endpoints and enforces policies supplied by the Server.



The Server:
It contains the product console and interfaces with a Microsoft SQL Server database.

The Carbon Black File Reputation Service:
This combines software reputation, threat indicators, and attack classification capabilities.

Carbon Black EDR



Carbon Black Hosted EDR