VMware Carbon Black

Company Overview

Fernando León
Presales Engineer

Discussion

PEOPLE

TECHNOLOGY

ENVIRONMENT

The Situation

INEFFECTIVE PREVENTION

Traditional endpoint security doesn’t stop modern attacks

ESCALATING COMPLEXITY

Adding capabilities leads to too many agents and tools to manage

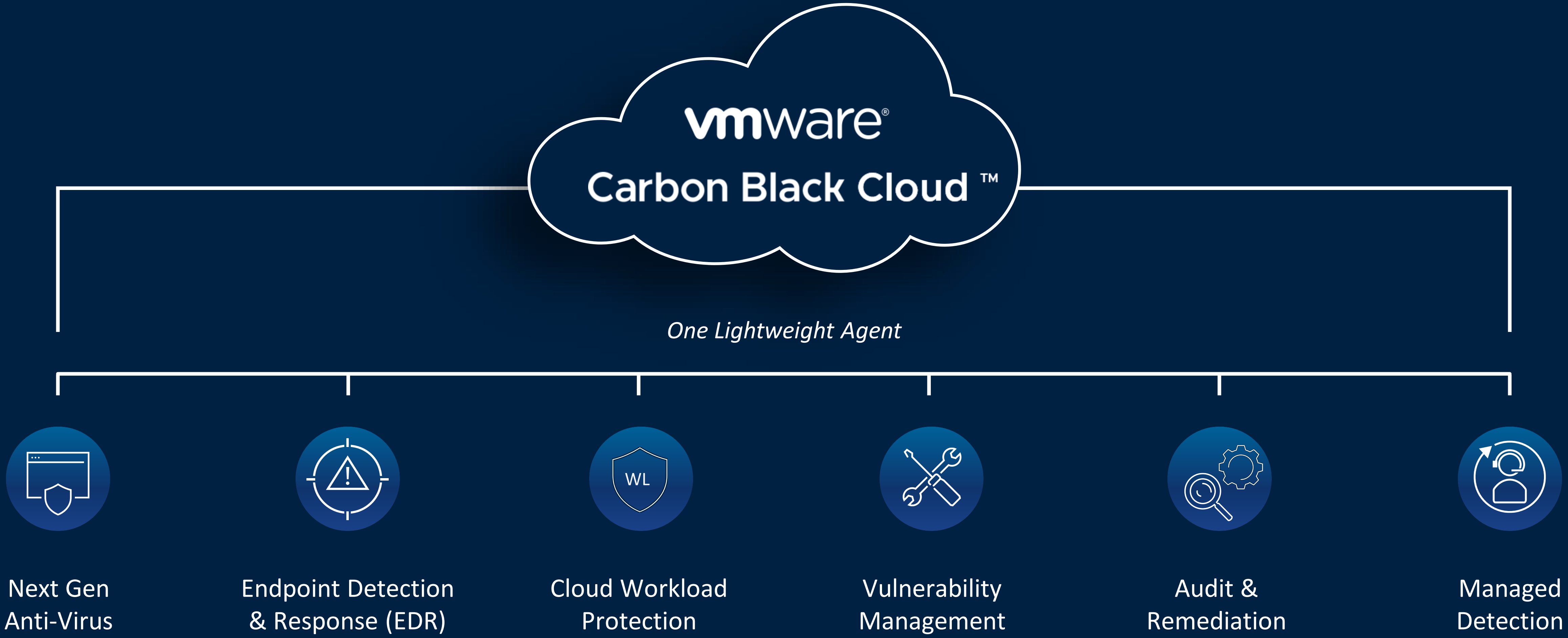
DROWNING IN ALERTS

Security lacks clear data to prioritize and make confident decisions

LACK OF QUALIFIED STAFF

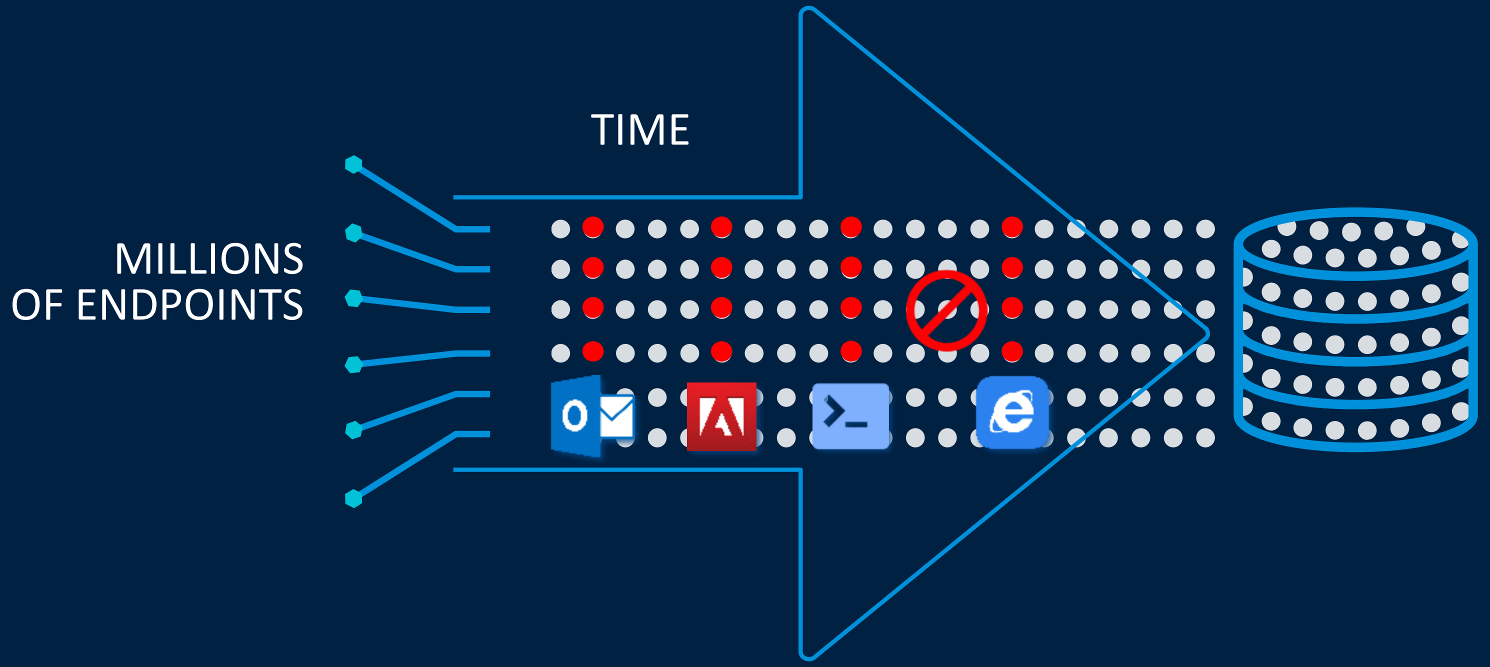
Skills shortage results in security staff being stretched thin

Cloud-Native Endpoint Protection Platform



Carbon Black's Unique Approach

Analyzing Endpoint Behavior



STOP NEVER SEEN BEFORE ATTACKS

STAY AHEAD OF EMERGING ATTACKS

More than 500TB of endpoint data and over
1 TRILLION events per day

What the Carbon Black Cloud Delivers

Reduce cost and complexity by consolidating multiple security solutions

SUPERIOR PROTECTION

Prevent known and new threats as they evolve

ACTIONABLE INSIGHTS

Real-time investigation and remediation

SIMPLIFIED OPERATIONS

Operate faster and more effectively

6,000+

Customers

1/3

Fortune 100

DocuSign®

Adobe®

indeed™
one search. all jobs.

Evernote

DraftKings

kordia®

EPSON®

Pinterest

Valvoline®

Core-Mark®

ASRC FEDERAL

FREEPORT LNG

vmware® Carbon Black

Appendix

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

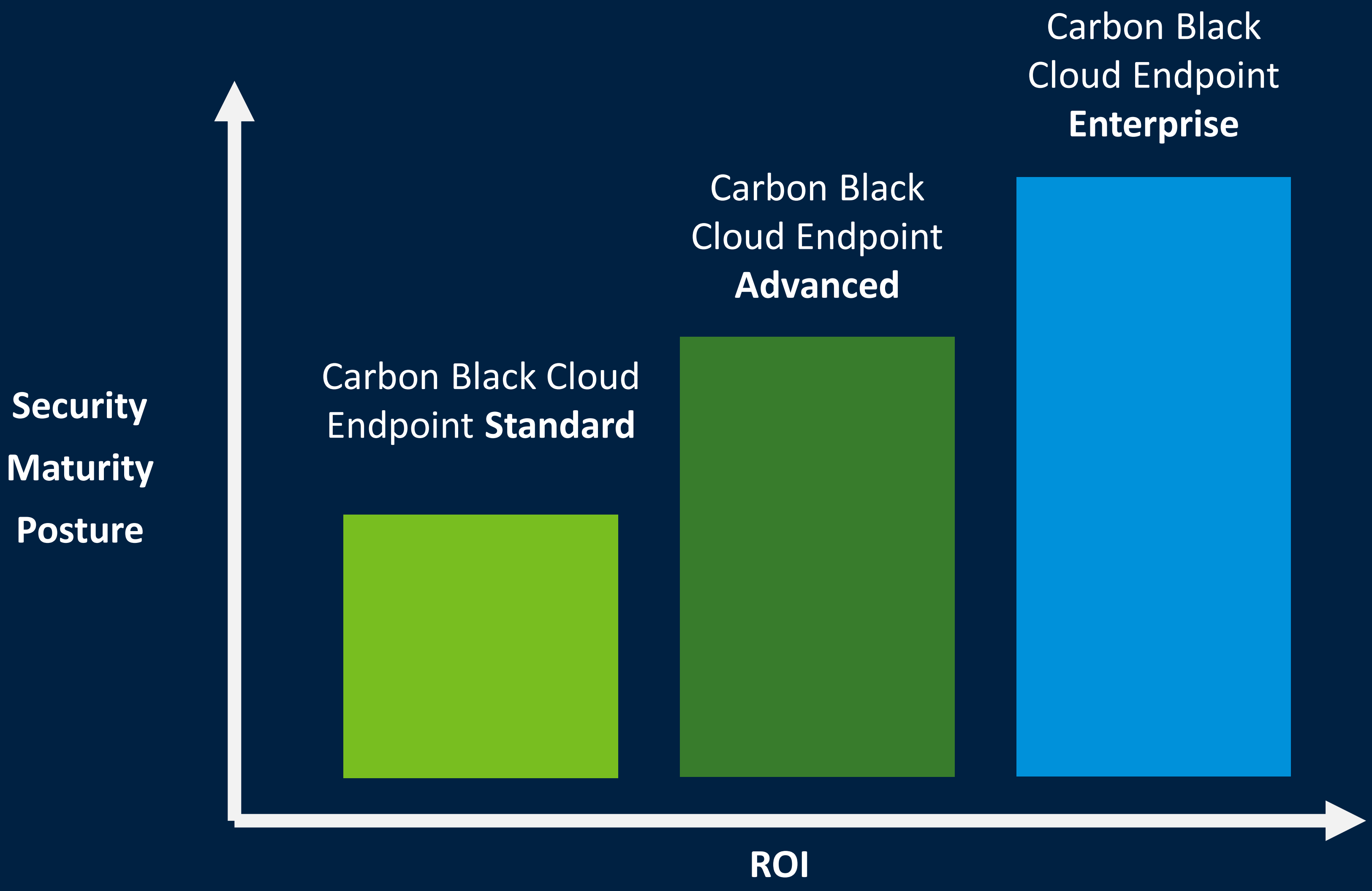
- Stop advanced threats
- Automate the hunt
- Reduce the attack surface
- Integrate defenses
- Leverage community experts

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 Workspace Security

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

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

VMware Carbon Black Cloud Managed Detection

Prevent breaches with expert threat hunters at your side

Managed Alert Triage

Expert Threat Validation

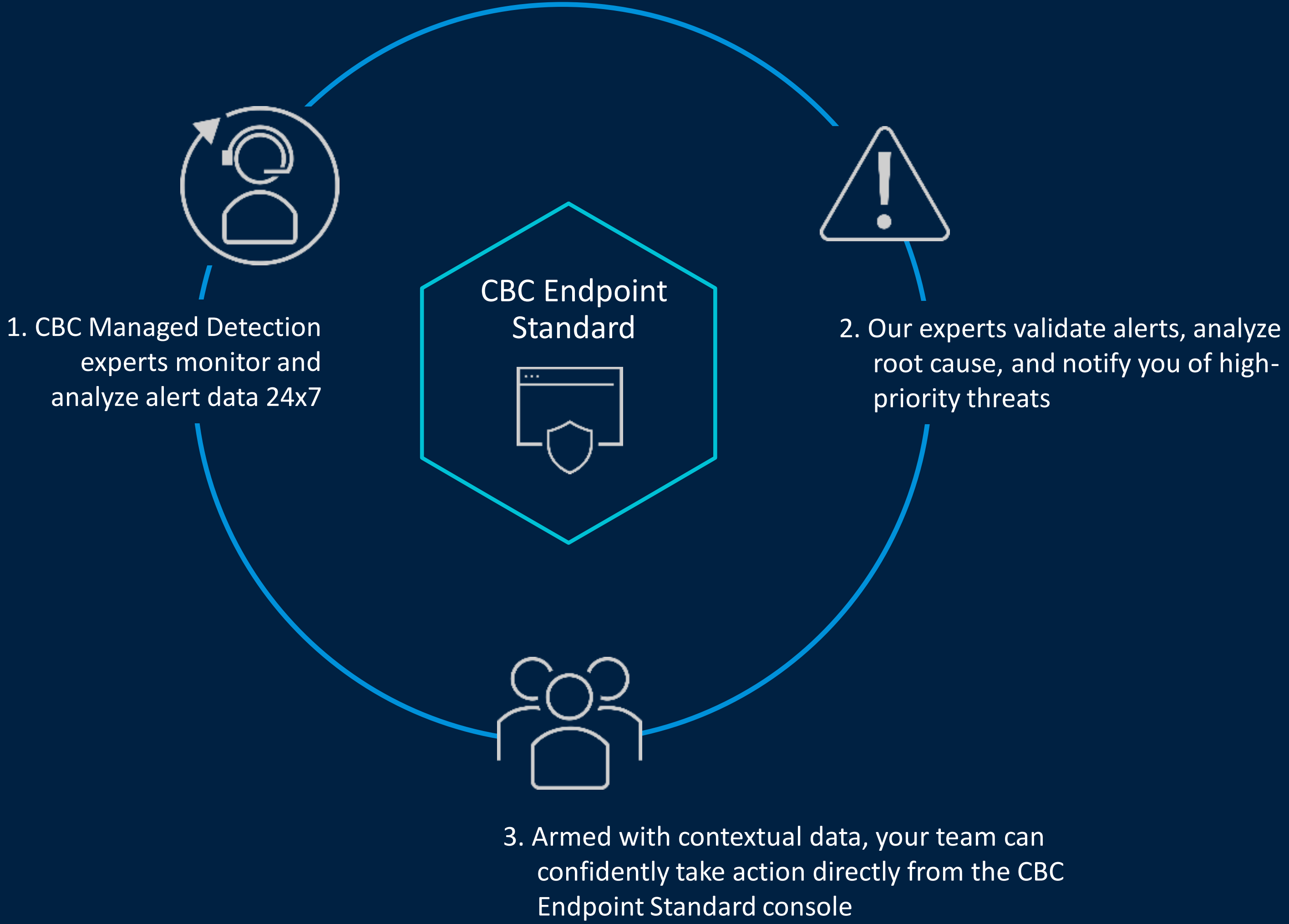
Analyzes, validates, and prioritizes alerts so that nothing is missed

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



CBC Endpoint Standard

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

VMware Carbon Black Vision:

Transform the industry with a modern security platform built for any application, running on any cloud, on any device.

vmware® Carbon Black

Our View: Security Must Be Transformed

Built-in

Proactive

Aligned

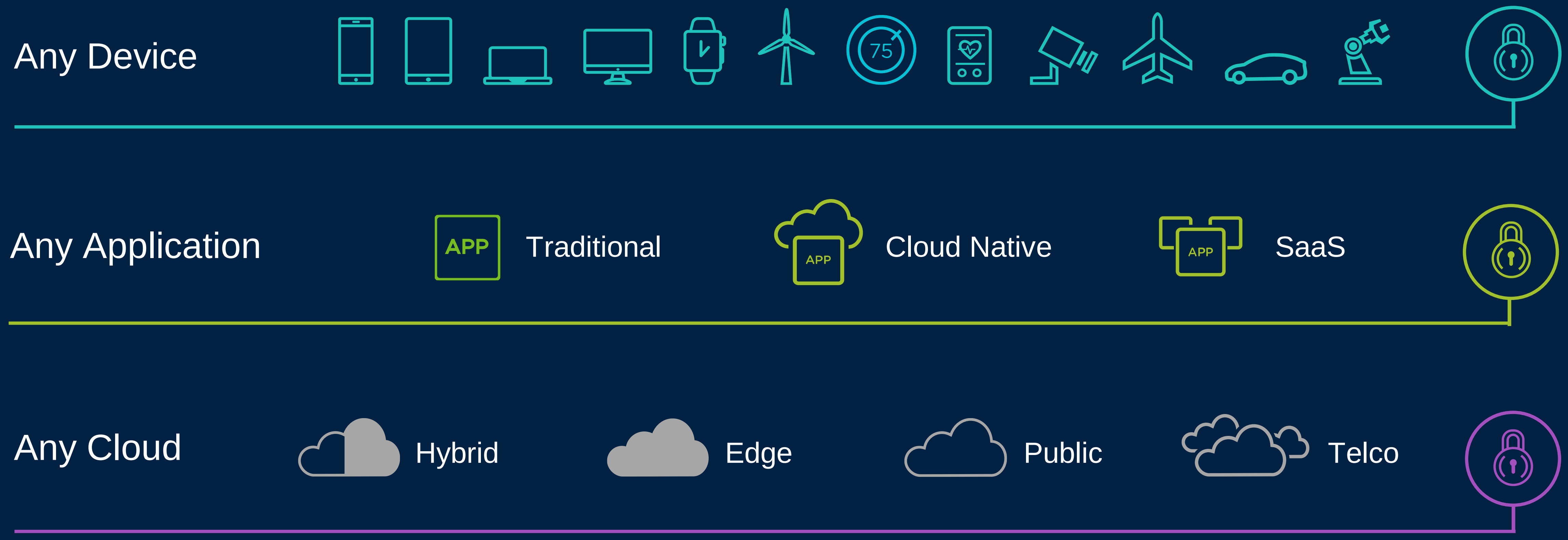
Bolted-on

Reactive

Siloed

Our Vision:

The essential, ubiquitous digital foundation



Any Device

Any Application

Traditional

Cloud Native

SaaS

Any Cloud

Hybrid

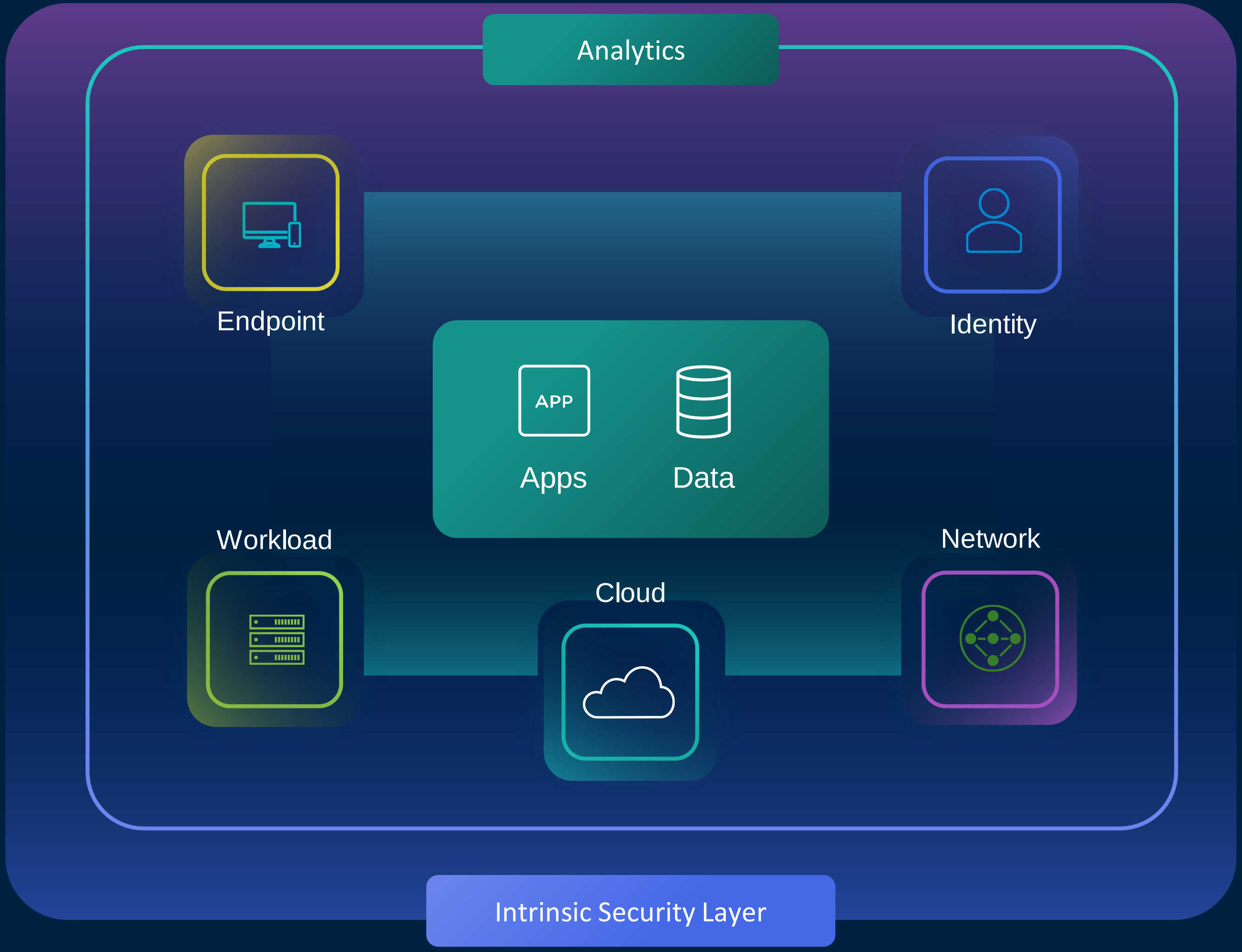
Edge

Public

Telco

The Intrinsic Security Layer

Building security into key control points



Major Breaches Have Made Security **#1 BOD Priority**

EQUIFAX

JULY 2017

143M RECORDS

verizon

JULY 2017

14M RECORDS

ORBITZ

MARCH 2018

880K RECORDS

U.S. DEPT. OF HHS

APRIL 2016

5M RECORDS

DEC-JUNE 2018

$1.1B CRYPTO

LinkedIn

MAY 2016

117M RECORDS

ORACLE micros

AUG 2016

333K SITES

Panera BREAD

APR 2018

37M RECORDS

DEEP ROOT

JUNE 2017

198M RECORDS

myspace

MAY 2016

360M RECORDS

Critical Business Data is at Risk

15x

Increase in damages from ransomware since 2015

Cybersecurity Ventures research

68%

Of breaches took months or longer to discover

Verizon Data Breach Incident Report 2018

27%

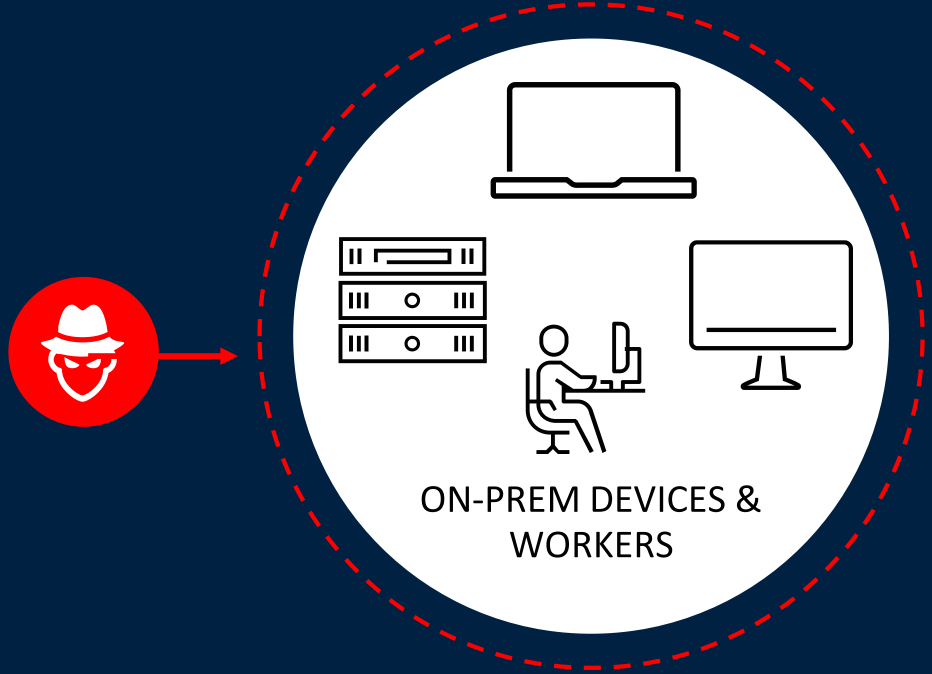
Are confident that AV will protect them from ransomware

Ponemon Rise of Ransomware report

Mobility & Cloud Are Transforming Security

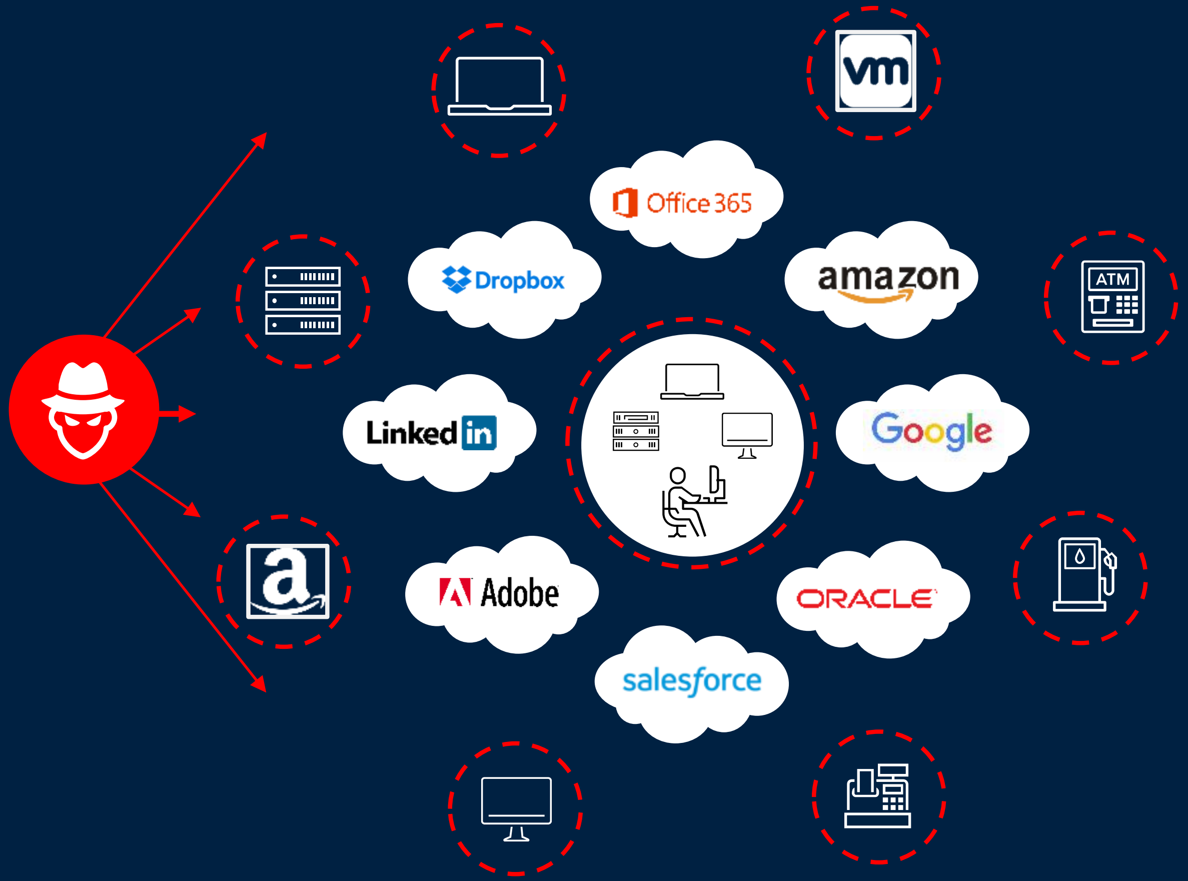
Before

The Network Was the Perimeter



Today

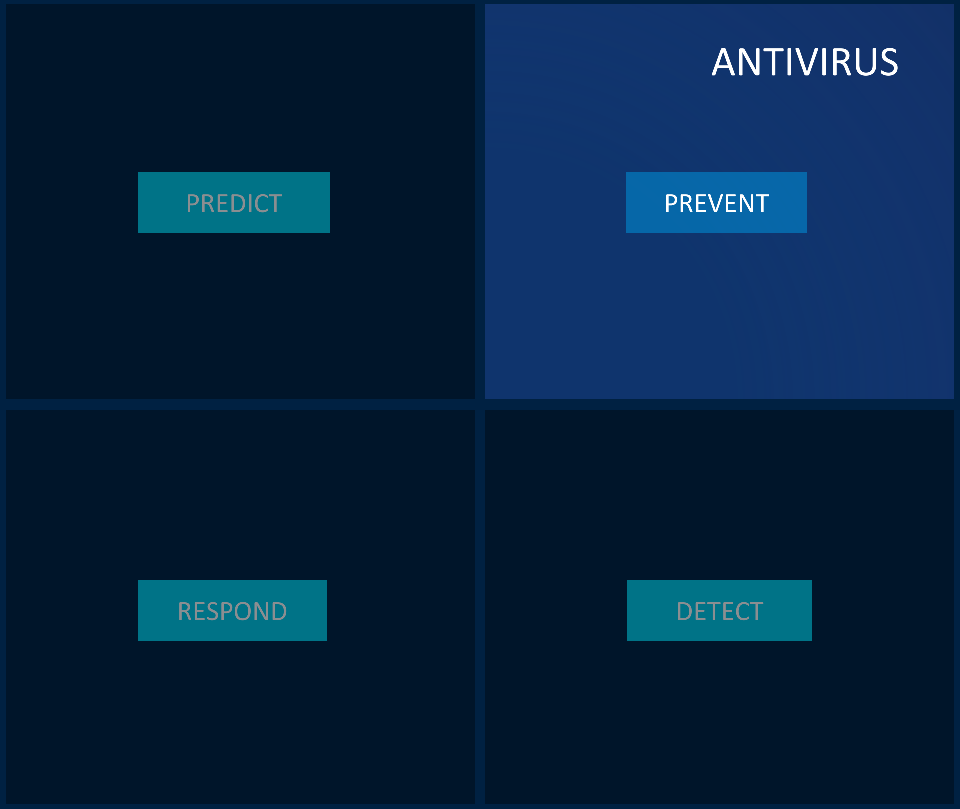
The Endpoint Is the NEW Perimeter



Solving the Full Security Lifecycle with Data

Traditional Antivirus

Focuses on Prevention Only



ANTIVIRUS

PREDICT

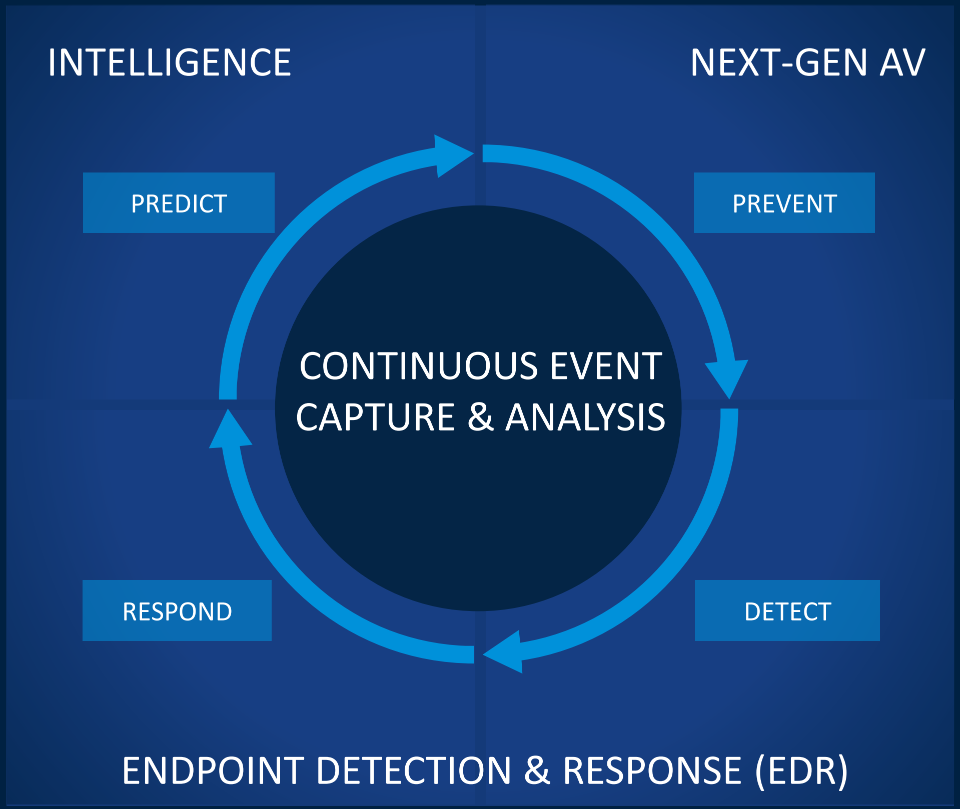
PREVENT

RESPOND

DETECT

Carbon Black

Provides Full Security Lifecycle



INTELLIGENCE

NEXT-GEN AV

PREDICT

PREVENT

CONTINUOUS EVENT CAPTURE & ANALYSIS

RESPOND

DETECT

ENDPOINT DETECTION & RESPONSE (EDR)

Fraud Detection and Prevention was Transformed

By Leveraging the Cloud and Big Data Behavioral Analytics

From

To

Manual point-in-time analytics focused on fraud techniques

Automated real-time analytics focused on behavior of users/apps

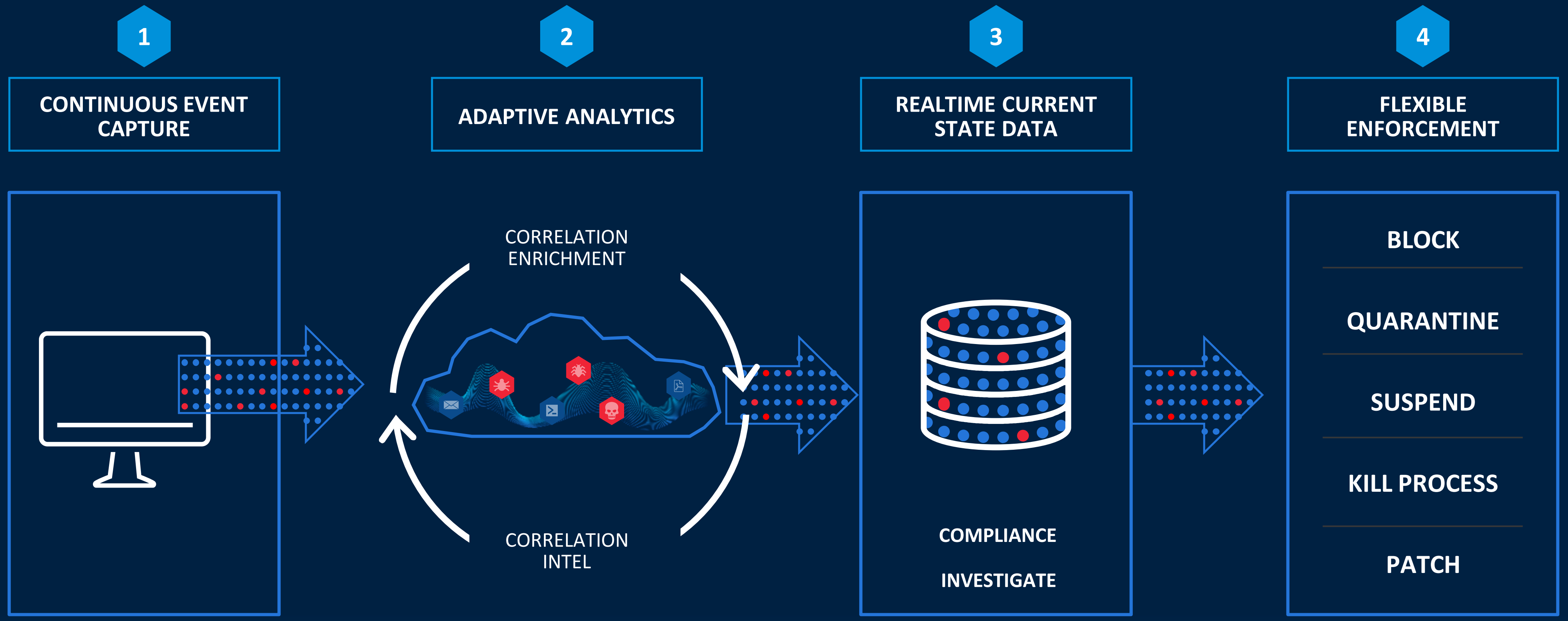
Fraud Loss Dropped

$4B (20%) over 4 years

Stolen Credit Card Value Plummets

$300 to $5 per credit card number

The Best Data Provides the Best Security



1

CONTINUOUS EVENT CAPTURE

2

ADAPTIVE ANALYTICS

CORRELATION ENRICHMENT

CORRELATION INTEL

3

REALTIME CURRENT STATE DATA

COMPLIANCE

INVESTIGATE

4

FLEXIBLE ENFORCEMENT

BLOCK

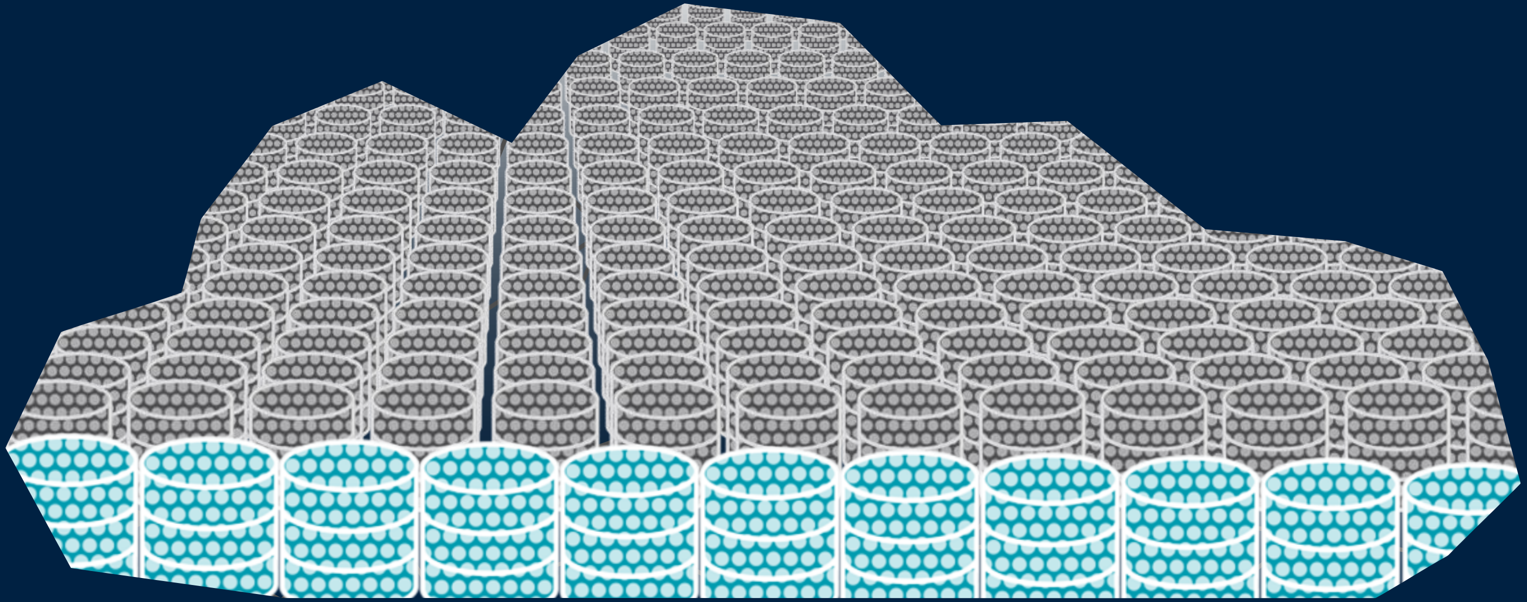
QUARANTINE

SUSPEND

KILL PROCESS

PATCH

OPEN & EXTENSIBLE PLATFORM ARCHITECTURE



>500TB

Endpoint Data
Analyzed Per Day

1 Trillion

Security Events Per Day

The Scope and Scale of Our Analytics

By comparison, the number of events and quantity of data we analyze every day is….

WhatsApp

~20X

events

65B messages / day*

Google

~230X

events

5.6B searches / day**

twitter

~2,500X

events

500M tweets / day***

virustotal

~700X

data

1.8 TB / day****

*Business Insider May 9, 2018

**SearchEngineLand- 2019

***David Sayce – 10/2019

****VirusTotal – 2019

Linux is Different

A lot of malware	Not much malware
Variety of assets with many different purposes	Highly controlled; uptime & performance are essential
Standard, predictable release cycles	New versions daily, compiled on custom kernels

How to Solve Unique Linux Challenges

Our Linux Design Principles

Do No Harm

Speed of Delivery Cadence

Breadth of Coverage Over Depth

Provide value to **both** the Security Operations Team and the Linux System Admin

Security Controls

Digital Risk Management

- crisp
- CYBERSPRINT BREAKTHROUGH SECURITY
- digital shadows_
- DigitalStakeout
- EXPANSE
- LOOKINGGLASS
- NAMOGOO
- PHISHLABS
- RISKIQ
- SafeGuard Cyber
- source defense
- ZEROFOX

Mobile Security

- appdome
- BETTER
- BlackBerry
- blue cedar
- Fyde
- Check Point SOFTWARE TECHNOLOGIES LTD
- cellrox
- COMMUNITAKE
- Cyber adAPT
- INPEDIO
- KAYMERA
- KOOLSPAN
- Lookout
- mobileiron
- pradeo
- PSafe
- SaltDNA
- silent circle
- SOTI
- Symantec
- TeleSign
- TESKALABS
- tigertext
- TRUSTLOOK
- VAULTO
- wandera
- wickr
- ZIMPERIUM

Endpoint Security

- AhnLab
- avast
- Avecto
- Avira
- Barkly
- Bitdefender
- BINARY DEFENSE
- BLUERIDGE NETWORKS
- BUFFERZONE
- Carbon Black.
- Check Point SOFTWARE TECHNOLOGIES LTD
- COMODO
- CROWDSTRIKE
- CYBERARK
- cybereason
- CYLANCE
- deepinstinct BEFORE YOU KNOW IT
- ENDGAME.
- ERICOM Be Connected, Be Secure
- eset
- F-Secure
- Faronics
- FORTINET
- HYSOLATE
- intego
- ivanti
- KASPERSKY
- McAfee Together is power.
- Microsoft
- MORPHISEC
- NYOTRON SECURING THE WORLD
- OPSWAT.
- panda
- PERCEPTION POINT
- SentinelOne
- SOPHOS
- sparkcognition
- STORMSHIELD
- Symantec
- TEHTRIS
- WEBROOT Smarter Cybersecurity
- ZEO ADVANCE

Data Security

- anjuna
- baffle
- boxcryptor
- CipherCloud
- CLOUDMASK
- CryptoMove
- DATALOCKER SIMPLY SECURE
- Fortanix
- NuCypher
- virtru
- clearswift
- CODE42
- DIGITAL GUARDIAN
- Fidelis Cybersecurity
- McAfee
- Symantec
- BlueTalon
- druva
- opentext
- SECLORE

Block Chain

- Chain
- Gladius
- guardtime
- IDEE
- NuID
- remme
- vchain
- ShoCard
- xage SECURITY

Security Operations & Incident Response

- ALIEN VAULT
- BlackStratus
- CORRELOG
- CYGILANT SECURITY AS A SERVICE
- DEVO
- exabeam
- FORTINET
- HanSight
- Huntsman
- IBM
- RSA
- IGLOO
- JASK
- logentries
- logpoint
- LogRhythm
- logz.io
- McAfee
- MICRO FOCUS
- Palantir
- SAWMILL
- SECURONIX
- solarwinds
- splunk>
- sumologic
- TIBCO
- Trustwave
- arctos networks
- atarlabs
- ayehu
- CYBERBIT
- Bay Dynamics
- DARKTRACE
- AWAKE
- CYBERSPONSE
- CYBER TRIAGE
- DARK|LIGHT
- empow
- Fluency
- Dtex
- DEMISTO
- DFLABS
- FIREEYE
- mistnet
- observe it
- IronNet Cybersecurity
- Microsoft
- paloalto networks.
- radar
- RAPID7
- RSA
- FORTINET
- Reservoir Labs
- Raytheon
- resilient
- SECBI
- servicenow
- SIEMPLIFY
- SIFT SECURITY
- THRESHING FLOOR
- TripleCyber
- THETARAY
- SWIMLANE
- SYNCURITY
- THREATQ
- patternex
- haystax
- Veriato
- ThreatConnect
- UPLEVEL
- VERINT
- VECTRA
- SECURONIX

Threat Intelligence

- 4iQ
- Blueliv.
- ANOMALI
- LOOKINGGLASS
- Malware Patrol
- NUCLEON
- BlueVoyant
- Centripetal
- CISCO
- Recorded Future
- RiskBased SECURITY
- RISKIQ
- digital shadows_
- DOMAINTOOLS
- SenseCy
- Sixgill
- SURFWATCH NEWS & ANALYSIS
- EclecticIQ
- FARSIGHT SECURITY
- GROUP-IB
- SpyCloud
- ThreatConnect
- FLASHPOINT
- HanSight
- HYAS
- ThreatMetrix
- THREATQUOTIENT
- INTEL471
- INTSIGHTS
- KELA
- ThreatSTOP
- TRU*STAR
- WEBROOT Smarter Cybersecurity

Cloud Security

- anchore
- aqua
- deepfence
- EDGEWISE NETWORKS
- Guardicore
- HYTRUST
- NeuVector
- POLYVERSE
- portshift
- threat stack
- <VA> VARMOUR
- AVANAN
- Qualys.
- StackRox
- Sysdig
- Managed Methods
- Microsoft
- netskope
- Twistlock
- alcide
- ARMOR
- BetterCloud
- illumio
- Lacework
- SHIELDX
- BRACKET COMPUTING
- cavirin
- Check Point SOFTWARE TECHNOLOGIES LTD
- bitglass
- CipherCloud
- CISCO
- CORONET
- Cloud Conformity
- CLOUDIWAY
- CYBERARK

Risk and Compliance

- AXONIUS Cybersecurity Asset Management
- Balbix
- cavirin
- cyber OBSERVER
- cyberGRX
- DELVE LABS
- eclypsium
- FIREMON
- KENNA Security
- NEHEMIAH SECURITY
- NOPSEC
- OPAQ
- Outpost24
- panaseer
- PREVALENT
- REDSEAL
- riskrecon
- SKYBOX SECURITY
- tenable
- UpGuard
- VENAFI
- zeguro
- BITSIGHT
- corax
- FICO
- RiskLens
- SecurityScorecard
- ATTACKIQ
- Cobalt
- CRONUS
- CYBERHAT proactive cyber defense
- CYCOGNITO
- CYMULATE
- DEPTH SECURITY
- tufin
- MAZEBOLT
- PCYSYS
- PICUS
- RAPID7
- SafeBreach
- VERODIN SECURITY, INSTRUMENTED.
- algosec
- secure
- Galvanize
- Lockpath
- MetricStream
- netwrix
- Onspring
- :RESOLVER
- riskonnect
- RSA
- Barracuda
- COFENSE
- CyberVista
- SAI GLOBAL
- IRONSCALES
- proofpoint.
- RANGEFORCE

WAF and Application Security

- 6scan
- A10
- Akamai
- ALERT LOGIC
- ARXAN
- Barracuda
- CEQUENCE SECURITY
- CITRIX
- ergon
- THREATX
- CyKickLabs
- F5
- FORTINET
- L7 DEFENSE
- SHAPE
- imperva
- NETSPI
- onapsis
- TEMPLARBIT
- netsparker
- CONTRAST SECURITY
- TREND MICRO
- Synack
- STACKPATH
- Qualys.
- ORACLE
- CLOUDFLARE
- wallarm
- Vicarius
- IBM
- portshift
- PURESEC
- hackerone
- Real Geeks SEWORKS
- RAPID7
- Reblaze
- riverbed
- riverbed
- sucuri
- PentaSECURITY cloud - iot - enterprise
- radware Every second counts
- Signal Sciences
- sqreen
- waratek
- WhiteHat SECURITY
- Trustwave
- VERACODE
- sentryo
- AWAKE
- BRICATA
- CGS Tower Networks
- DARKTRACE
- ExtraHop
- Gigamon
- PERCH
- Plixer
- SECBI
- SS8

Identity & Access Management

- Acceptto
- Auth0
- averon
- BehavioSec
- BIOCATCH Less Friction. Less Fraud.
- Callsign
- CLEF
- CORE SECURITY
- DUO
- EXOSTAR
- FORGEROCK
- FUDO SECURITY
- Google
- IDEE
- imprivata
- INTRINSIC ID
- nok nok
- pindrop
- plainID
- SAASPASS
- transmit SECURITY
- SECUREDTOUCH
- SECUREPUSH
- SILVERFORT
- tascent
- ThreatMetrix
- TransUnion
- TRUSONA
- UNBOUND
- UNIKEN
- V-KEY
- VIRGIL SECURITY
- Centrify
- Centrify
- IBM
- idaptive
- Microsoft
- okta
- RSA
- HYPR
- onelogin
- ORACLE
- THALES
- BeyondTrust
- MICRO FOCUS
- SECRET DOUBLE OCTOPUS
- CYBERARK
- HITACHI
- ManageEngine
- ONE IDENTITY
- Remediant
- SECURELINK
- thycotic
- AXIOMATICS
- Deep Identity
- helpsystems
- SailPoint
- simeio
- Akamai
- IDExperts
- loginradius
- Trulioo
- vchain
- verato
- VERIFF
- ID.me

Network & Infrastructure Security

- Barracuda
- BLUEHEXAGON
- BLUVECTOR.
- CISCO
- CORSA
- FIREEYE
- FORTINET
- HUAWEI
- HYSOLATE
- JOESecurity
- JUNIPER NETWORKS
- mimecast
- OPSWAT
- paloalto NETWORKS
- RESEC
- GATESCANNER by Sasa Software
- SONICWALL
- SOPHOS
- Symantec
- VMRAY
- VOTIRO
- WatchGuard
- aruba
- AUCONET
- AXONIUS
- Cyberbit
- Cyxtera
- DOS arrest
- F5
- Extreme
- FORESCOUT
- NANOSEC
- SKYPORT SYSTEMS
- NETSHIELD
- portnox
- NextNine
- Trustwave
- zentera
- Genians
- TEMPERED NETWORKS
- VERSA NETWORKS
- Zscaler
- Akamai
- CROWDSTRIKE
- RunSafe SECURITY
- Check Point SOFTWARE TECHNOLOGIES LTD
- imperva
- neustar
- NEXUSGUARD
- NSFOCUS
- ORACLE
- corelight
- SECURE64
- STACKPATH
- BLUECAT
- neustar
- ThreatSTOP
- VERISIGN
- Quad9
- MixMode
- efficient iP
- Infoblox
- CYREN
- algosec
- CATO NETWORKS
- clavister
- FIREMON
- lastline
- endian
- FORCEPOINT
- GAJSHIELD
- Hillstone NETWORKS
- OPAQ
- SANGFOR
- McAfee Together is power.
- secucloud.
- SONICWALL
- STORMSHIELD
- tufin
- Fidelis
- untangle
- ACALVIO
- SPAMINA
- PAS
- Attivo NETWORKS
- illusive
- CounterCraft
- PACKET VIPER
- CyberTrap
- SMOKESCREEN
- CLOUDFLARE
- VERINT
- Cymmetria
- TRAPX SECURITY
- APERIO
- BAYSHORE
- BELDEN
- CRITIFENCE
- NOZOMI NETWORKS
- CYBERBIT
- FIRMITAS
- Indegy
- n-dimension solutions
- SCADAfence
- Corvil
- NETSCOUT
- CLAROTY
- CyberX
- DRAGOS
- PFP Cybersecurity
- radiflow
- Rhebo
- CORE SECURITY
- IronNet Cybersecurity
- CloudShark
- utimaco
- GREYCORTEX

vmware®

Security Controls

Digital Risk Management

crisp CYBERSPRINT digital shadows_ DigitalStakeout
EXPANSE LOOKINGGLASS NAMOGOO PHISHLABS
RISKIQ SafeGuard Cyber source defense ZEROFOX

Mobile Security

appdome BETTER BlackBerry blue cedar Fyde
Check Point cellrox COMMUNITAKE Cyber adAPT
INPEDIO KOOLSPAN Lookout mobileiron
pradeo KAYMERA PSafe SaltDNA silent circle SOTI
Symantec TeleSign TESLABS tigertext TRUSTLOOK
VAULTO wandera wickr ZIMPERIUM

Endpoint Security

AhnLab avast Avecto Avira Barkly Bitdefender
BINARY DEFENSE BLUERIDGE NETWORKS BUFFERZONE Carbon Black.
Check Point COMODO CROWDSTRIKE CYBERARK
cybereason CYLANCE deepinstinct ENDGAME.
ERICOM eset F-Secure Faronics FORTINET
HYSOLATE intego ivanti KASPERSKY McAfee
Microsoft MORPHISEC NYOTRON OPSWAT panda
PERCEPTION POINT SentinelOne SOPHOS sparkcognition STORMSHIELD
Symantec TEHTRIS WEBROOT ZIO ADVANCE

Data Security

anjuna baffle boxcryptor CipherCloud CLOUDMASK
CryptoMove DATALOCKER Fortanix NuCypher virtru
clearswift CODE42 DIGITALGUARDIAN Fidelis McAfee
Symantec BlueTalon druva opentext SECLORE

Block Chain

Chain Gladius guardtime IDEE NuID remme
vchain ShoCard xage SECURITY

Security Operations & Incident Response

ALIEN VAULT BlackStratus CORRELOG CYGILANT DEVO
exabeam FORTINET HanSight Huntsman IBM RSA
IGLOO JASK logentries logpoint LogRhythm
logz.io McAfee MICRO FOCUS Palantir SAWMILL SECURONIX
solarwinds splunk> sumologic TIBCO Trustwave arctos networks
atarlabs ayehu CYBERBIT Bay Dynamics DARKTRACE AWAKE
CYBERSPONSE CYBER TRIAGE DARK LIGHT empow Fluency Dtex
DEMISTO DFLABS FIREEYE mistnet observe it IronNet
Microsoft paloalto networks radar RAPID7
Raytheon Resilient SECBI RSA FORTINET Reservoir Labs
servicenow SIEMPLIFY SIFT SECURITY THRESHING FLOOR TripleCyber THETARAY
SWIMLANE SYNCURITY THREATQ patternex haystax Veriato
ThreatConnect UPLEVEL VERINT VECTRA SECURONIX

Threat Intelligence

4iQ Blueliv. ANOMALI LOOKINGGLASS Malware Patrol NUCLEON
BlueVoyant Centripetal CISCO Recorded Future RiskBased Security RISKIQ
digital shadows_ DOMAINTOOLS SenseCy Sixgill SURFWATCH
EclecticIQ FARSIGHT SECURITY GROUP-IB SpyCloud ThreatConnect
FLASHPOINT HanSight HYAS ThreatMetrix THREATQUOTIENT
INTEL471 INTSIGHTS KELA ThreatSTOP TRUSTAR WEBROOT

Cloud Security

anchore aqua deepfence EDGEWISE Guardicore HYTRUST
NeuVector POLYVERSE portshift threat stack ARMOUR AVANAN
Qualys. StackRox Sysdig Managed Methods Microsoft netskope
Twistlock alcide ARMOR BetterCloud illumio Lacework SHIELDX
BRACKET cavirin Check Point bitglass CipherCloud CISCO CORONET
Cloud Conformity CLOUDWAY CYBERARK

Risk and Compliance

AXONIUS Balbix cavirin cyber observer
cyberGRX DELVE eclypsium FIREMON KENNA Security
NEHEMIAH SECURITY NOPSEC OPAQ Outpost24
panaseer PREVALENT REDSEAL riskrecon
SKYBOX tenable UpGuard VENAFI
zeguro BITSIGHT corax FICO RiskLens
SecurityScorecard ATTACKIQ Cobalt CRONUS
CYBERHAT CYCOGNITO CYMULATE DEPTH tufin
MAZEBOLT PCYSYS PICUS
RAPID7 SafeBreach VERODIN
algosec secure Lockpath MetricStream
netwrix Onspring RESOLVER riskonnect RSA
Barracuda COFENSE CyberVista SAI GLOBAL
IRONSCALES proofpoint RANGEFORCE

WAF and Application Security

6scan A10 Akamai ALERT LOGIC ARXAN
Barracuda CEQUENCE CITRIX ergon THREATX
CyKickLabs FORTINET L7 DEFENSE SHAPE
imperva NETSPI onapsis TEMPLARBIT
netsparker CONTRAST SECURITY TREND MICRO Synack STACKPATH
Qualys. ORACLE CLOUDFLARE wallarm Vicarius IBM
portshift PURESEC hackerone SEWORKS
RAPID7 Reblaze riverbed riverbed sucuri
PentaSECURITY radware Signal Sciences sqreen
waratek WhiteHat SECURITY Trustwave VERACODE
sentryo AWAKE BRICATA CGS
DARKTRACE ExtraHop Gigamon
PERCH Plixer SECBI SS8

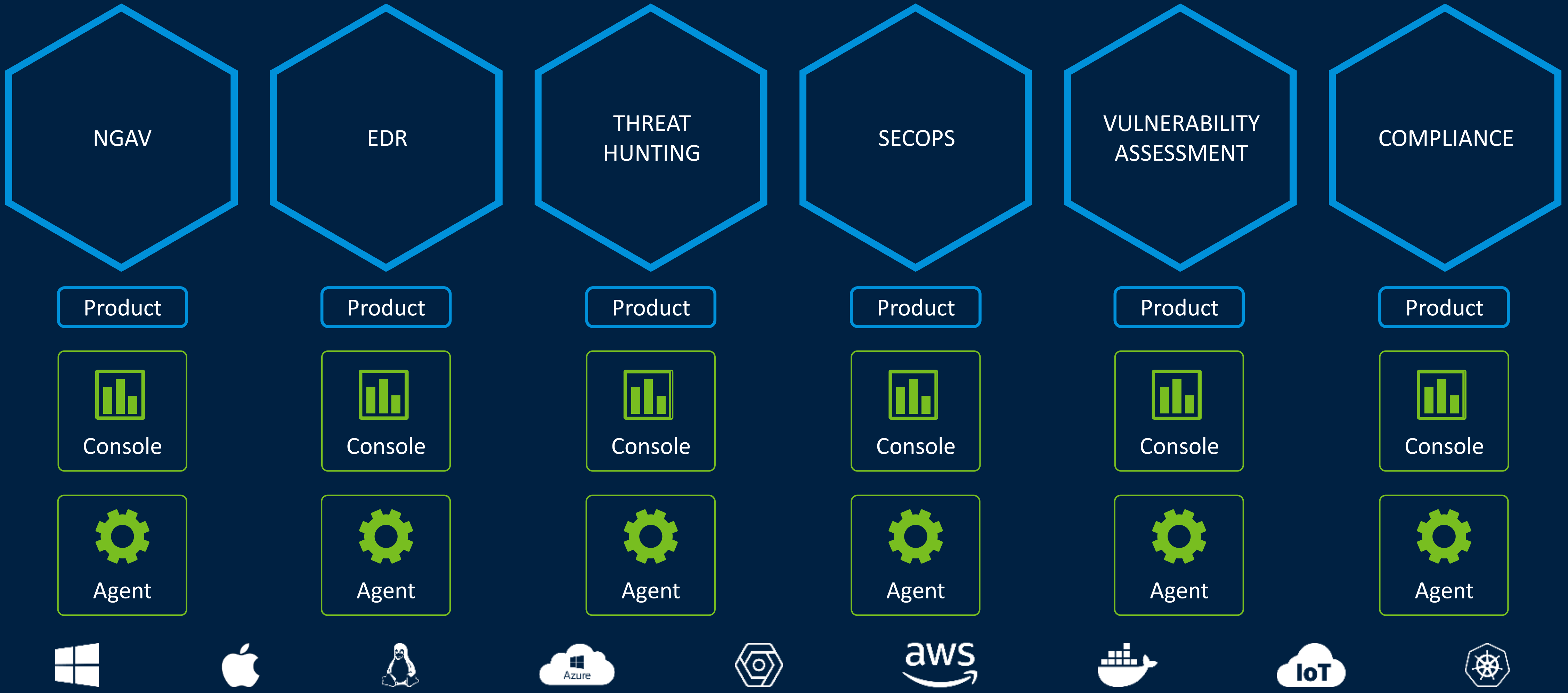
Identity & Access Management

Acceptto Auth0 averon BehavioSec BIOCATCH Callsign
CLEF CORE SECURITY DUO EXOSTAR FORGEROCK FUDO SECURITY Google
IDEE imprivata INTRINSIC ID nok nok pindrop plainID SAASPASS
transmit security SECUREDTOUCH SECUREPUSH SILVERFORT tascent ThreatMetrix.
TransUnion TRUSONA UNBOUND UNIKEN V-KEY VIRGIL SECURITY Centrify
Centrify IBM idaptive Microsoft okta RSA HYPR
onelogin ORACLE THALES BeyondTrust MICRO FOCUS
SECRET DOUBLE OCTOPUS CYBERARK HITACHI ManageEngine ONE IDENTITY
Remediant SECURELINK thycotic AXIOMATICS Deep Identity
helpsystems SailPoint simeio Akamai IDExperts
loginradius Trulioo vchain verato VERIFF ID.me

Network & Infrastructure Security

Barracuda BLUEHEXAGON BLUVECTOR CISCO CORSA
FIREEYE FORTINET HUAWEI HYSOLATE JOESecurity JUNIPER
mimecast OPSWAT paloalto RESEC GATESCANNER SONICWALL SOPHOS
Symantec VMRAY VOTIRO WatchGuard aruba AUCONET AXONIUS Cyberbit Cyxtera
botsarrest Extreme FORESCOUT NANOSEC SKYPORT SYSTEMS NETSHIELD portnox NextNine
Trustwave zentera Genians TEMPERED VERSA zscaler Akamai RunSafe
Check Point imperva neustar NEXUSGUARD NSFOCUS ORACLE corelight
SECURE64 STACKPATH BLUECAT neustar ThreatSTOP VERISIGN Quad9 MixMode
efficient iP Infoblox CYREN algosec CATO NETWORKS CLAVISTER FIREMON lastline
endian FORCEPOINT GAJSHIELD Hillstone OPAQ SANGFOR McAfee
secucloud. SONICWALL STORMSHIELD tufin Fidelis untangle ACALVIO SPAMINA PAS
Attivo illusive CounterCraft PACKET VIPER CyberTrap SMOKESCREEN CLOUDFLARE VERINT
Cymmetria TRAPX APERIO BAYSHORE BELDEN CRITIFENCE NOZOMI
CYBERBIT FIRMITAS Indegy dimension SCADAfence Corvil NETSCOUT
CLAROTY CyberX DRAGOS PFP radiflow Rhebo CORE IronNet
CloudShark utimaco GREYCORTEX

Multiple Products, Multiple Consoles, Multiple Agents



NGAV

Product

Console

Agent

EDR

Product

Console

Agent

THREAT HUNTING

Product

Console

Agent

SECOPS

Product

Console

Agent

VULNERABILITY ASSESSMENT

Product

Console

Agent

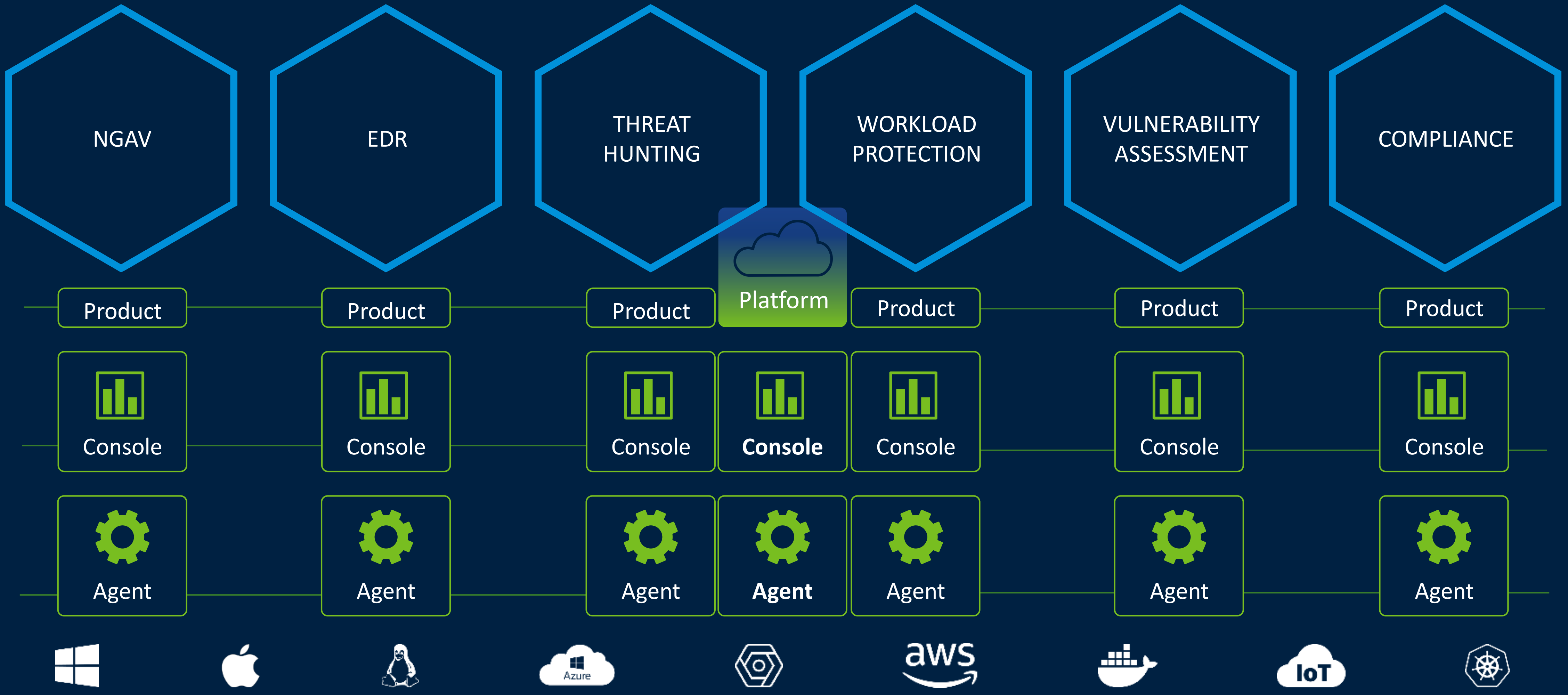
COMPLIANCE

Product

Console

Agent

We Need a New Approach

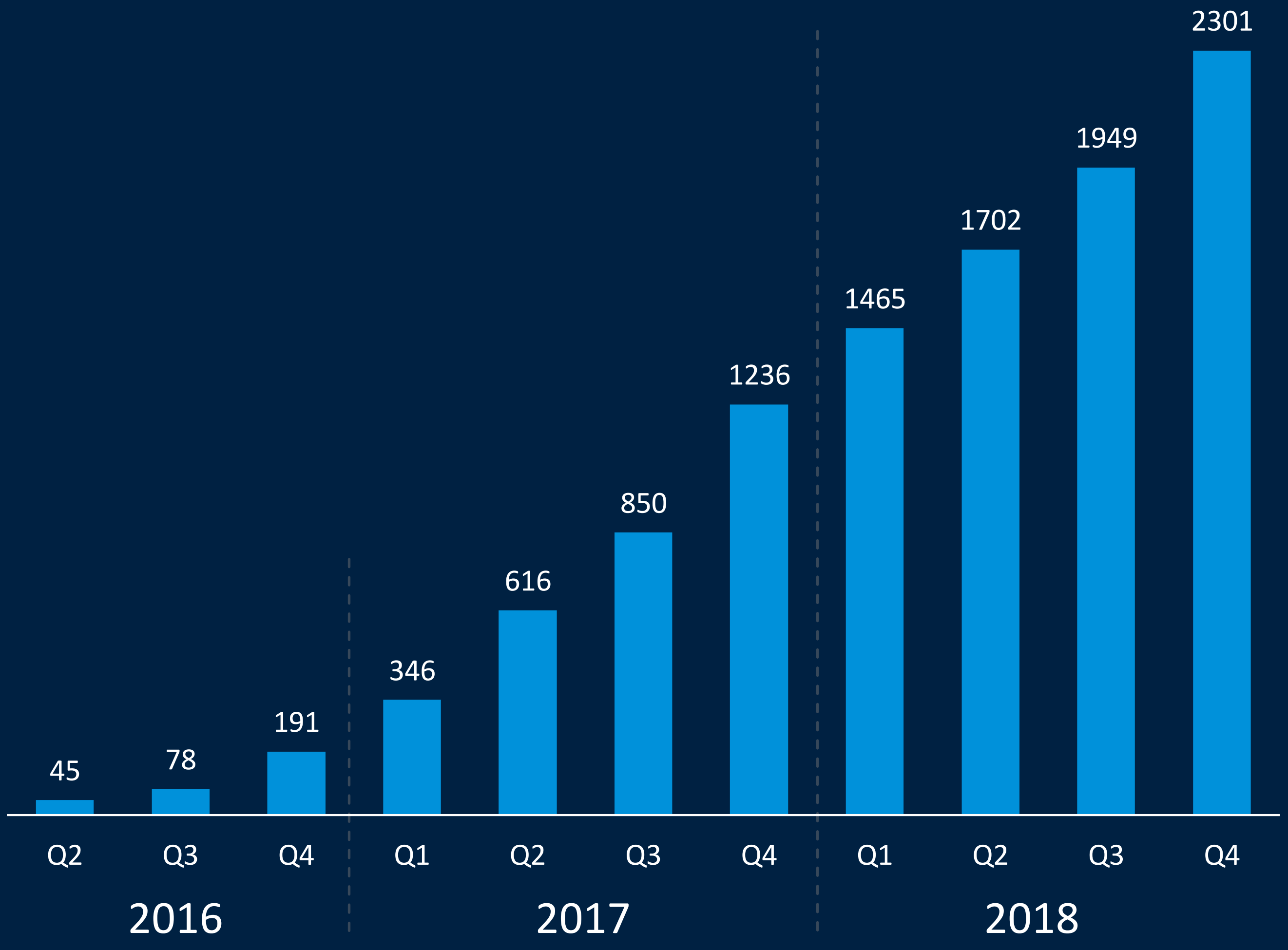


vmware® Carbon Black

VISION

A World Safe from Cyber Attacks

Rapid Customer Adoption of the PSC



2,300+ PSC customers

68 PSC IR & MSSP partners

Largest PSC deployment to date: **350K+** endpoints

Multiple global PSC deployments exceeding **100K+** endpoints

Community of **20K+** security professionals sharing intel

Protecting Brand Leaders Across Industries

OIL & GAS	HEALTHCARE	RETAIL	TECHNOLOGY	MANUFACTURING
3	**2**	**6**	**7**	**5**
OF THE	OF THE	OF THE	OF THE	OF THE
TOP 5	**TOP 11**	**TOP 11**	**TOP 10**	**TOP 10**

Based on 2019 Fortune 100 ranking

Proven Leadership Team

Patrick Morley
President and CEO

Michael Viscuso
Co-founder and Chief Strategy Officer

Ryan Polk
Chief Product Officer

Thomas Hansen
Chief Operating Officer

Sandra O’Sullivan
Chief People Officer

Scott Lundgren
Chief Technology Officer

Brad Rinklin
Chief Marketing Officer

Steve Webber
Chief Financial Officer

Tom Barsi
SVP, Corporate
& Business Development

Eric Pyenson
SVP, General Counsel

Carbon Black on the World Stage

Recognized By Leading Analysts & Publications

IDC

Leader

Worldwide Endpoint Specialized Threat Analysis and Protection, 2017

FORRESTER

A Leader

The Forrester Wave^{TM}: Endpoint Detection And Response, Q3 2018

EMA

Leader

2017 Next-Generation Endpoint Security Vendor Landscape and Five-Year Market Forecast, Q3 2017

MITRE ATT&CK

Highest Marks for Detecting Threats

MITRE ATT&CK Evaluation, November 2018

NSS LABS RECOMMENDED

Recommended

Highest “Recommended” ranking in Advanced Endpoint Protection (AEP) Test, 2018

SC Awards 2017 Europe

Best Solution

SC Magazine Awards Europe, 2017

FROST & SULLIVAN

Vendor of the Year 2017

Asia-Pacific Emerging Cybersecurity Vendor of
the Year, 2017

*as of 21 February 2019 out of 114 total five-star ratings in the EDR category.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved. https://www.gartner.com/reviews/customers-choice/endpoint-detection-and-response-solutions.

Best in Class Protection

100%

Prevention Rate Against Known and Unknown Ransomware Samples

Product of Choice for IR Professionals

SANS

The Race to Detection:
A Look at Rapidly Changing IR Practices

68%

IR professionals **prefer Carbon Black** for incident response and forensics

Commitment To Excellence

Carbon Black works with reputable organizations to put the PSC through extensive reviews and testing

AV-TEST
The Independent IT-Security Institute

99.27% in real world attack blocking, 100% on commodity malware

NSS LABS

“Recommended” status with perfect scores for HTTP malware, email malware, doc & script attacks with 0.58% false positive rate

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

100% efficacy against 42 different ransomware families

ICSA labs
CERTIFIED ADVANCED THREAT DEFENSE

99.79% efficacy
0 false positives

SANS

“High degree of intelligence and analytics”

COALFIRE

“Enables customers to not only meet PCI-DSS requirement 5, but to go beyond compliance”

SC MEDIA
THE CYBERSECURITY SOURCE

“One of the most efficient user interfaces we’ve seen”

Ovum

“A compelling option for any EPP project”

Extensive Channel Partnerships

We work with the industry’s most trusted advisors globally

VARs & DISTRIBUTORS

(100s)

ARROW

OPTIV

CDW

dimension data

MSSPs & IRs

(150+)

Kroll

SecureWorks

red canary

EY Building a better working world

STRATEGIC PARTNERS

IBM

DELL

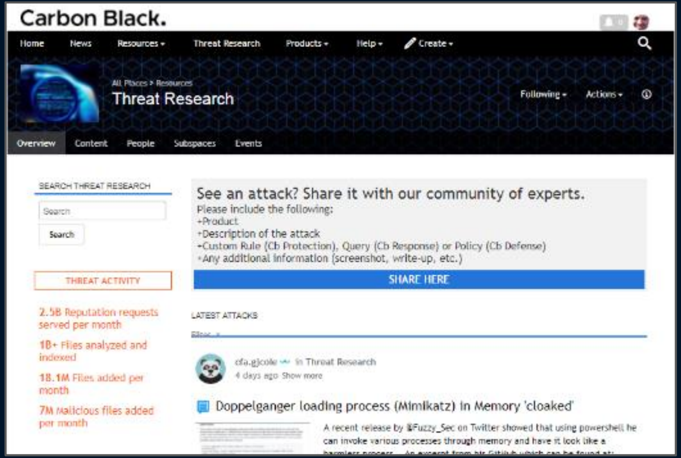
Powerful Security Community

CONNECT WITH THOUSANDS OF SECURITY EXPERTS

20,000+ COMMUNITY MEMBERS

GLOBAL FOOTPRINT

GATHER REAL-TIME THREAT INTELLIGENCE



2.5B Reputation requests served per month

1B+ Files analyzed and indexed

18.1M Files added per month

7M Malicious files added per month

See an attack? Share it with our community of experts.

Please include the following:
+Product
+Description of the attack
+Custom Rule (Cb Protection), Query (Cb Response) or Policy (Cb Defense)
+Any additional information (screenshot, write-up, etc.)

cfa.gjcole in Threat Research
4 days ago Show more

Doppelganger loading process (Mimikatz) in Memory 'cloaked'

A recent release by @Fuzzy_Sec on Twitter showed that using powershell he can invoke various processes through memory and have it look like a

ACTIONABLE THREAT INTEL

IOCs, WATCHLISTS & MORE

DIRECT ACCESS TO CB'S THREAT ANALYSIS UNIT

1M Binaries analyzed per day

10B Software reputation library

10K Alerts processed each month

40+ Threat research partners

ANALYSIS OF ADVANCED THREATS

THREAT ADVISORY ALERTS

What the Carbon Black Cloud Means for CB Response

1

WE ARE EXTENDING OUR OFFERINGS TO THE PSC

Best place for analytics, operational excellence & rapid innovation

2

WE ARE COMMITTED TO CB RESPONSE ON-PREM

Thousands of customers and dozens of partners

3

WHEN YOU ARE READY, YOU WILL BE ABLE TO MOVE TO PSC

Migration is optional, can be done at a time of your choosing, and will be eased by us

4

CB RESPONSE ON-PREM WILL BENEFIT FROM PSC

Threat analysis in cloud will power PSC & CB Response threat feeds

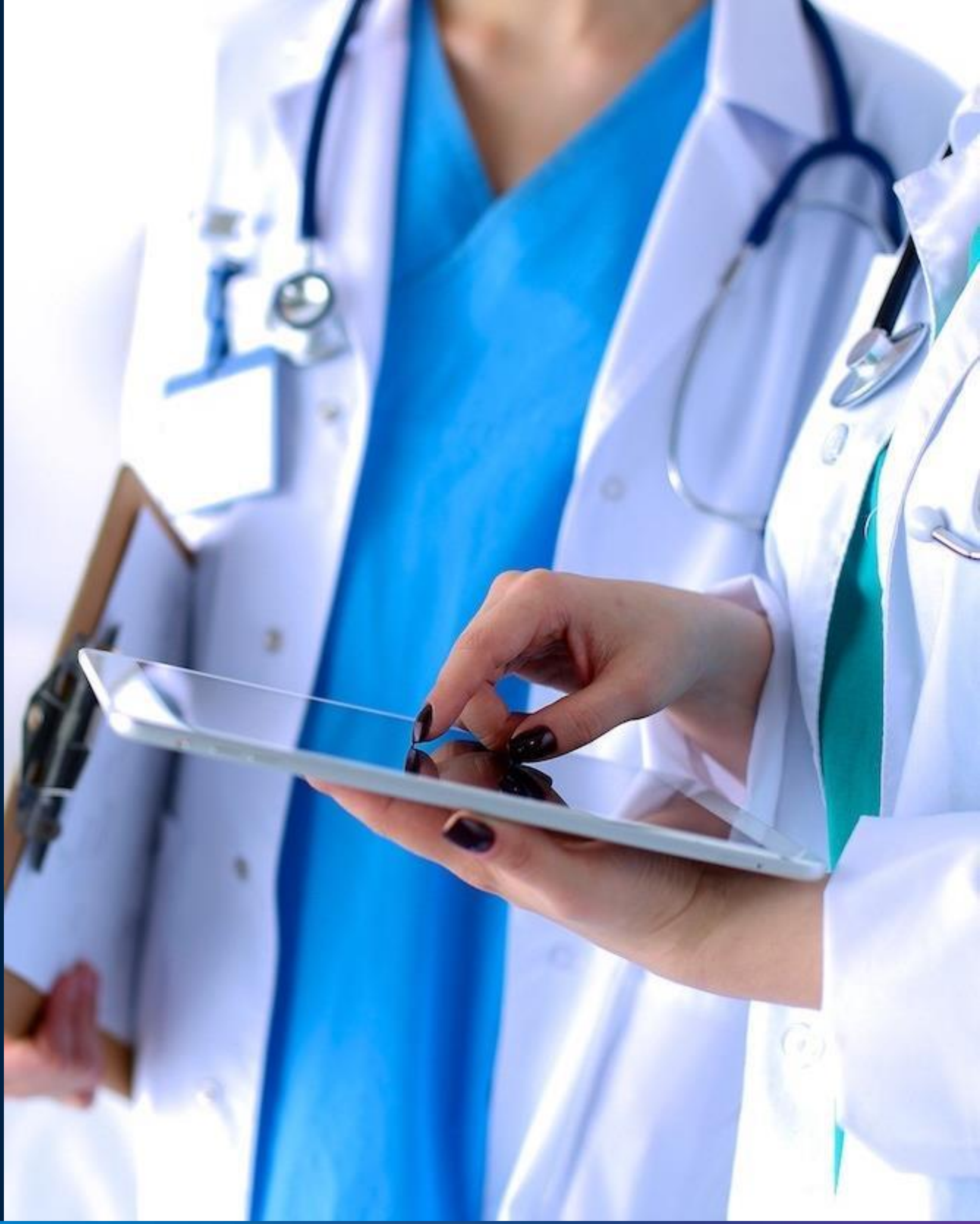
Blue Cross Blue Shield of Florida

VMware Carbon Black Cloud Endpoint Standard

13,000 Endpoints

INDUSTRY – Healthcare
USE CASE – Replace AV

- Needed endpoint protection from advanced threats
- Dramatically reduced overhead by replacing AV with CBC Endpoint Standard
- CB integration with SIEM via Splunk allows team to move faster & stay organized



Mercy Medical Center

VMware Carbon Black Cloud Endpoint Standard

4,000 Endpoints

INDUSTRY – Healthcare
USE CASE – Next-Gen AV

- Needed to upgrade traditional AV with a proactive security solution
- CBC Endpoint Standard allowed team to reclaim some of their resources for other security work
- Behavior monitoring capabilities provided increased visibility that prior solution did not

NASDAQ

Carbon Black EDR & Carbon Black App Control

15,000 Endpoints

INDUSTRY – Finance
USE CASE – Incident Response, Threat Hunting

- Experiencing lack of visibility, needed prevention across wide range of endpoints
- CB EDR gave visibility across Nasdaq's entire environment
- Considers CB App Control the "gold standard" for prevention

D.A. Davidson

VMware Carbon Black Cloud Endpoint Standard

1,750 Endpoints

INDUSTRY – Finance
USE CASE – Next-Gen AV, Replace AV, Prevention

- Looking for solution with ability to block ransomware attacks that traditional AV couldn't
- CBC Endpoint Standard was able to prevent malicious activity vs. signature-based activity
- Deployed CBC Endpoint Standard within minutes from cloud & found product invisible to end users

vmware®

Confidential |

Peoples Bank

VMware Carbon Black Cloud Endpoint Standard

400 Endpoints

INDUSTRY – Finance
USE CASE – Replace AV, Replace McAfee

- Traditional AV was not preventing all types of attacks
- CBC Endpoint Standard chosen after intensive testing due to robust preventative capabilities
- Team is able to conduct further analysis & investigate attacks

Medibank

Carbon Black EDR & Carbon Black App Control

5,500 Endpoints

INDUSTRY – Insurance
USE CASE – Prevention, Visibility, Incident Response

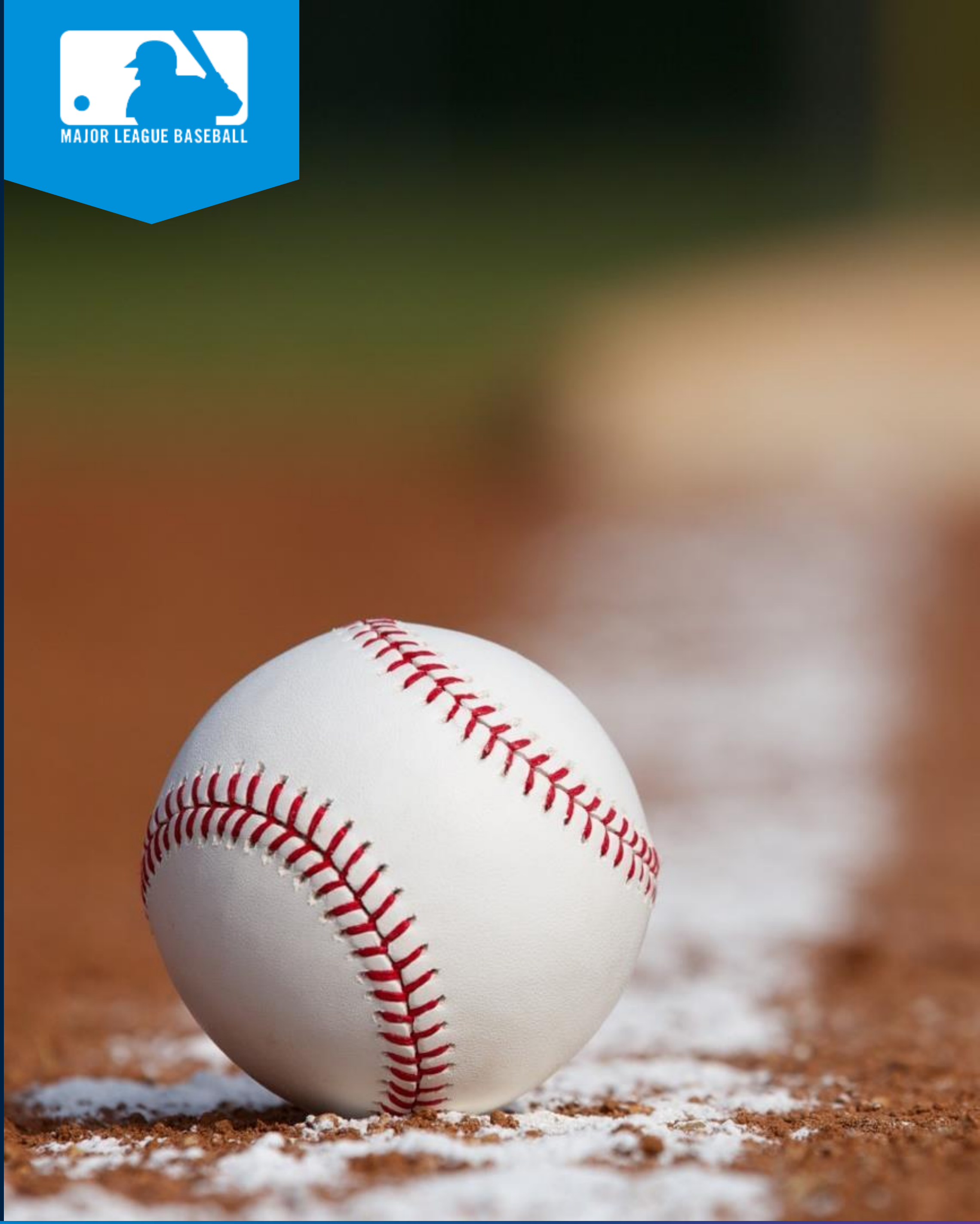
- Targeted by 2-3 ransomware attacks/quarter
- Carbon Black helped prevent 100% ransomware attack attempts
- Additional visibility creates better understanding of how desktop is being used

MLB

VMware Carbon Black Cloud Endpoint Standard & Carbon Black EDR

24,000 Endpoints

- Legacy AV not effective against new threat types, including ransomware
- Chose Carbon Black due to better effectiveness, ease of management, and efficient use of endpoint resources
- Efficacy against ransomware dramatically improved



Motors Management Corp.

VMware Carbon Black Cloud Endpoint Standard

INDUSTRY – Automotive
USE CASE – Next-Gen AV

- Needed to replace AV with better prevention
- Evaluated a number of endpoint solution
- Chose CBC Endpoint Standard for efficacy

Other Brands We Protect:

NISSAN

UBER

vmware®

Philips Lighting

Carbon Black EDR

Cloud 74,000 Endpoints

- Enable high-speed security operations center (SOC) team
- CB EDR only cloud solution able to support increasingly mobile user base
- Reduced response times to “a fraction” of what they were

Adobe

VMware Carbon Black Cloud Endpoint Standard 20,000 Endpoints

INDUSTRY – Technology
USE CASE – Next-Gen AV

- Needed next-gen antivirus & EDR
- Looking to replace current AV solution
- Chose CBC Endpoint Standard for single agent vision

Evernote

VMware Carbon Black Cloud Endpoint Standard

1,000 Endpoints

INDUSTRY – Technology
USE CASE – Replace AV

- Needed a solution that would allow both flexibility & prevention
- CBC Endpoint Standard provided endpoint detection, prevention & IR
- Eliminated constant care that AV products require – now able to discard false positives

DocuSign

Carbon Black Hosted EDR

2,500 Endpoints

INDUSTRY – Business Services
USE CASE – Incident Response, Threat Hunting

- Needed a tool that would allow visibility across multiple machines
- Chose CB EDR Cloud for improved visibility & ability to immediately respond when necessary
- Carbon Black is an essential part in their security strategy

Cox Communications

Carbon Black App Control

35,000 Endpoints

INDUSTRY – Technology
USE CASE – Prevention, Open APIs

- Experiencing lack of visibility into files & needed better insight into their endpoints
- CB App Control improved security posture dramatically with a simple rule set
- Integration with Palo Alto provides added visibility into files

Lithium

VMware Carbon Black Cloud Endpoint Standard

600 Endpoints

INDUSTRY – Technology
USE CASE – Replace AV

- Legacy AV was bogging down endpoints
- Chose CBC Endpoint Standard because it reports on everything & not just on detected malware
- Team can focus on protecting endpoints instead of resolving agent issues

AUTODESK COMMUNITY
FORUMS | ARTICLES | IDEAS
AUTODESK COMMUNITY
Find answers, share expertise, and connect with your peers

Find Answers

Recently Solved

✓ Efficient way of copying a sketch for making male and female solids?
Posted to: Inventor General Discussion on 09/26/2015 by: cookk

✓ MTEXT to ALL CAPS
Posted to: AutoCAD LT General Discussion on 09/25/2015 by: ethridgechad

✓ Can't install AutoCad Mechanical 2015
Posted to: AutoCAD Mechanical General Discussion on 09/27/2015 by: mate31032000

More Solutions in: All GO

Common Issues

Posted to: Community F

Give Solutions

Unanswered Posts

add a fix contrain for a line will create a new line?
Posted to: AutoCAD 2013/2014/2015/2016 on 09/28/2015 by: huanggs

3ds max 2016 doesn't import ellipse shapes
Posted to: 3ds Max / 3ds Max Design General on 09/28/2015 by: simarikan

Autodesk IdeaStatio

Pattern Feature
Posted to: Inventor Idea

Making Scripting timeou
Posted to: PLM 360 Idea

Daily Reports - Overtime Tracking

DraftKings

VMware Carbon Black Cloud Endpoint Standard

600 Endpoints

INDUSTRY – Technology
USE CASE – Replace AV, Cloud-based Console

- Current solution was taking up valuable system resources
- Vetted dozens of different products over 6-8 months
- CBC Endpoint Standard was clear winner providing increased visibility & prevention

Motorola

Carbon Black EDR & Carbon Black App Control

25,000 Endpoints each

INDUSTRY – Telecommunications

USE CASE – Incident Response, Threat Hunting

- Needed solution that would allow team to streamline detection & response processes
- Carbon Black was only solution that provided complete visibility into every endpoint across enterprise
- Monitoring & alert capabilities have saved significant time during investigations

vmware®

Samsung RA

VMware Carbon Black Cloud Endpoint Standard

2,500 Endpoints

INDUSTRY – Telecommunications
USE CASE – Replace AV

- Looking to replace AV, performed extensive evaluation of endpoint vendors
- Tested products against real-world attacks, CBC Endpoint Standard was the only vendor to stop all of them
- CBC Endpoint Standard has been integral to security strategy & protection against ransomware

Kordia

Carbon Black App Control

850 Endpoints

INDUSTRY – Telecommunications
USE CASE – Visibility

- Desktop lockdown was not working
- CB was only solution able to keep environment secure while giving users flexibility
- Minimal effort required, CB App Control has them covered

Stonewall Kitchen

VMware Carbon Black Cloud Endpoint Standard & Carbon Black App Control

750 Endpoints

INDUSTRY – Retail
USE CASE – Next-Gen AV, Prevention, Visibility

- Symantec AV was producing more false positives than blocking anything malicious
- Chose CB due to its ability to keep up with latest threats
- CBC Endpoint Standard consolidated multiple systems into one – eliminated 3+ servers

Thank You