VMware
Vnitřní bezpečnost

Mikulov 2020

Ondřej Číž
Lead Solution Engineer NSX
ociz@vmware.com

Bezpečnost je pro transformaci nezbytná

Sjednocené

Sila

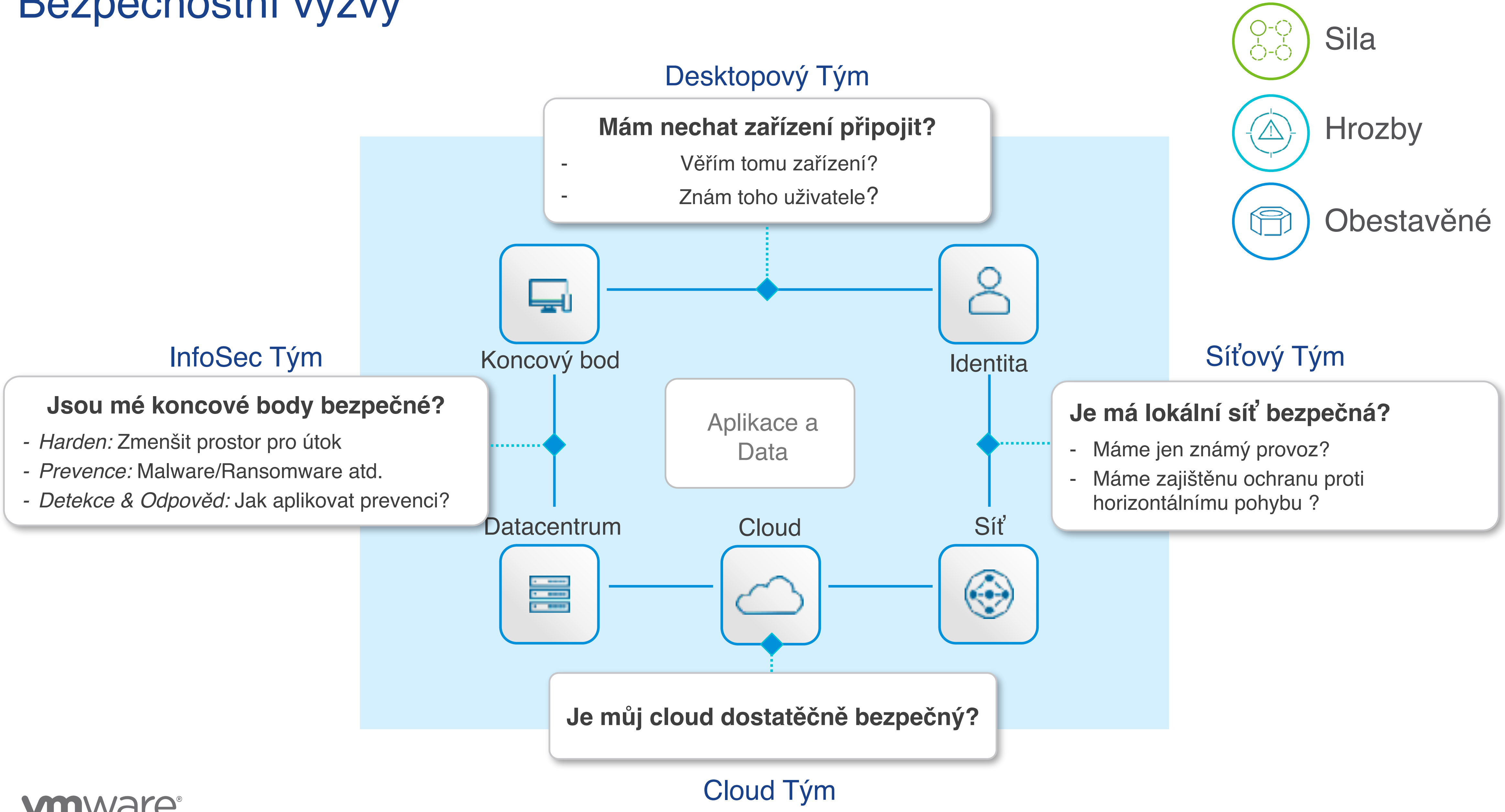
Zaměřeno na aplikace

Zaměřeno na obecné hrozby

Vestavěné

Obestavěné

Bezpečnostní výzvy



Sila

Hrozby

Obestavěné

Desktopový Tým

Mám nechat zařízení připojit?
- Věřím tomu zařízení?
- Znám toho uživatele?

InfoSec Tým

Jsou mé koncové body bezpečné?
- *Harden:* Zmenšit prostor pro útok
- *Prevence:* Malware/Ransomware atd.
- *Detekce & Odpověď:* Jak aplikovat prevenci?

Síťový Tým

Je má lokální síť bezpečná?
- Máme jen známý provoz?
- Máme zajištěnu ochranu proti horizontálnímu pohybu ?

Koncový bod

Identita

Aplikace a Data

Datacentrum

Cloud

Síť

Je můj cloud dostatěčně bezpečný?

Cloud Tým

vmware®

Digital Risk Management

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

Mobile Security

appdome BETTER BlackBerry blue cedar Fyde
Check Point cellrox COMMUNITAKE Cyber adAPT
INPEDIO KAYMERA KOOLSPAN Lookout mobileiron
prodeo Pradeo SaltDNA SOTI
Symantec TeleSign tigertext TRUSTLOOK
WULTO wandera vkey ZIMPERIUM

Endpoint Security

AhnLab avast Avecto Avira Barkly Bitdefender
BINARY DEFENSE BLUERIDGE 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
SentinelOne SOPHOS sparkcognition STORMSHIELD
Symantec TEHTRIS WEBROOT ZIO

Data Security

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

Block Chain

Chain guardtime IDEE NuID remme
vchain ShoCard xage

Threat Intelligence

4iQ Bluelive ANOMALI Malware MUCLEUS
Bluvector Centripetal CISCO Recorded Future RISKIQ
digital shadows_ DOMAINTOOLS ThreatQ Siegill SURFWATCH

Security Operations & Incident Response

BlackStratus CORRELOG CYGILANT DEVO
exabeam FORTINET HanSight Huntsman IBM RSA
IGLOO JASK logentries logpoint LogRhythm
logz.io McAfee MICRO FOCUS Palantir SECURONIX
solarwinds splunk> sumologic TIBCO Trustwave
atarlabs ayehu CYBERSPONSE CYBERBIT
DEMISTO D3 FIREEYE
Microsoft paloalto radar RAPID7
Raytheon resilient SIEMPLIFY
servicenow Siemplify
SWIMLANE ThreatConnect UPLEVEL VERINT
AWAKE
Darktrace Fluency haystax IronNet
mistnet observe it patternex Reservoir Labs
RSA SECURONIX THETARAY
TripleCyber VECTRA Verodin

Koncový bod

Risk and Compliance

AXONIUS Balbix cavirin cyber OBSERVER
GRX DELVE FIREEYE KENNA
NOPSEC OPAQ Outpost24
panaseer PRIVAFENT REDSEAL riskrecon
RedSeal tenable UpGuard VENAFI
zeguro BITSIGHT corax FICO RiskLens
SecurityScorecard ATTACKIQ Cobalt
CYBERRAT CYBERGRX CYMULATE DEPTH
MAZEBOLT PCYSYS PICUS
RAPID7 SafeBreach VERODIN
algosec secure Lockpath MetricStream
netwrix Onspring RESOLVER RSA
SAI GLOBAL
Barracuda
proofpoint
RANGEFORCE

Aplikace a Data

Identity & Access Management

Acceptto Auth0 aveion BehavioSec BIOCATCH Callsign Centrify
CLEF CORE DUO EXOSTAR FORGEROCK FUDO Google HYPR
IDEE imprivata INTRINSIC ID nok nok pindrop pirID SAASPASS
transmit SECUREPUSH SILVERFORT tascent ThreatMetrix
TransUnion TRUSONA UNBOUND LINKEN V-KEY VERIDIUM
Centrify IBM idaptive Microsoft okta RSA
onelogin ORACLE THALES BeyondTrust MICRO FOCUS
CYBERARK HITACHI ManageEngine ONE IDENTITY
Remediant SECURELINK thycotic AXIOMATICS
helpsystems SailPoint simeio Akamai IDExperts ID.me
lognradius Trusteer vchain verato VERIFF

Identita

Network & Infrastructure Security

Barracuda BLUEHEXAGON BLUVECTOR CISCO CORSA lastline
FIREEYE FORTINET HUAWEI HYSOLATE JOESecurity JUNIPER McAfee
mimecast OPSWAT paloalto RESEC SOTI SCANNER SONICWALL SOPHOS
Symantec Versa WatchGuard aruba ARUBA NET AXONIUS Cymmetria Cynet
ForeScout NANOSEC SKYPORT portnox
Trustwave zentera Genians TEMPERED VERSA zscaler Akamai
Check Point imperva neustar NEWSGUARD NSFOCUS ORACLE
STACKPATH BULLCAT neustar ThreatSTOP Qualys
Infoblox algosec CATO
endian FORCEPOINT SAFESHIELD OPAQ SANGFOR
lecudcloud SONICWALL STORMSHIELD tufin Fidelis
Attivo Illusive Counter Craft VIPER CyberTrap
Cymmetria TRAPX APERIO BAYSHORE BELDEN
CYBERBIT FIRMITAS Indegy dimension NOZOMI
Claroty CyberX DRAGOS PFP radiflow Rheo SCADAfence VERVE
sentryo AWAKE BRICATA CCS CloudShark corelight CORE Corvil
DARKTRACE ExtraHop GREYCORTEX IronNet NixMode NETSCOUT
PERCH Plixer SECI SS8 utimaco VECTRA

Síť

Cloud Security

anchore aqua deepfence
NeuVector Polyverse portshift
Qualys StackRox Sysdig
Twistlock
cavirin Check Point
CloudPassage
Illumio Lacework SHIELDX threat stack AVANAN
bitglass CISCO Microsoft netskope

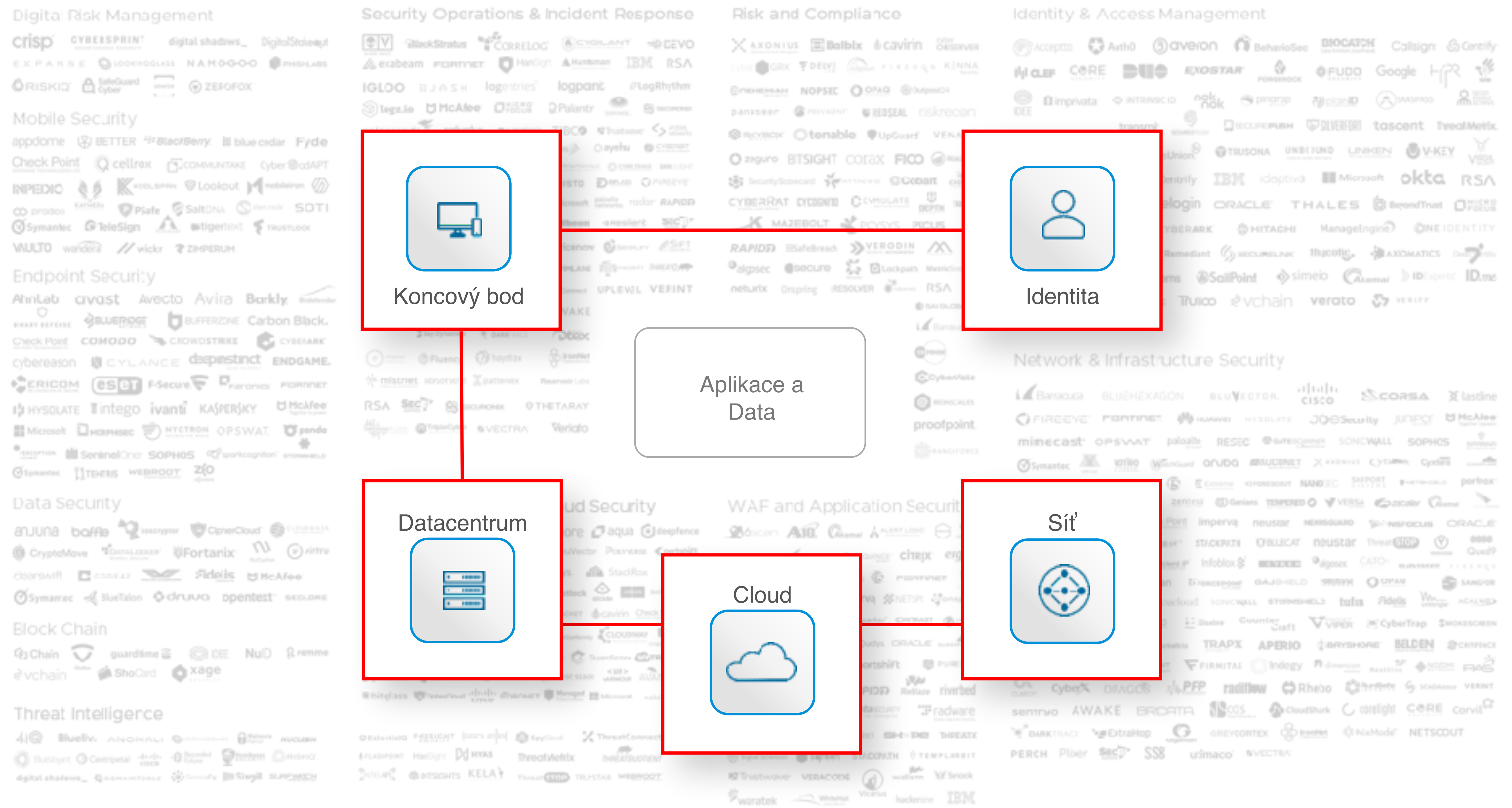
Datacentrum

WAF and Application Security

Akamai ALERT LOGIC
Barracuda CHECKMARX citrix ergon
CyKickLabs FORTINET
imperva NETSPI
ORACLE
portshift PURESEC
RAPID7 Reblaze riverbed
radware
riverbed SUCURI SHAPE THREATX
Signal Sciences sqreen STACKPATH TEMPLARBIT
Trustwave VERACODE wallarm Snyk
waratek WhiteHat hackerone IBM

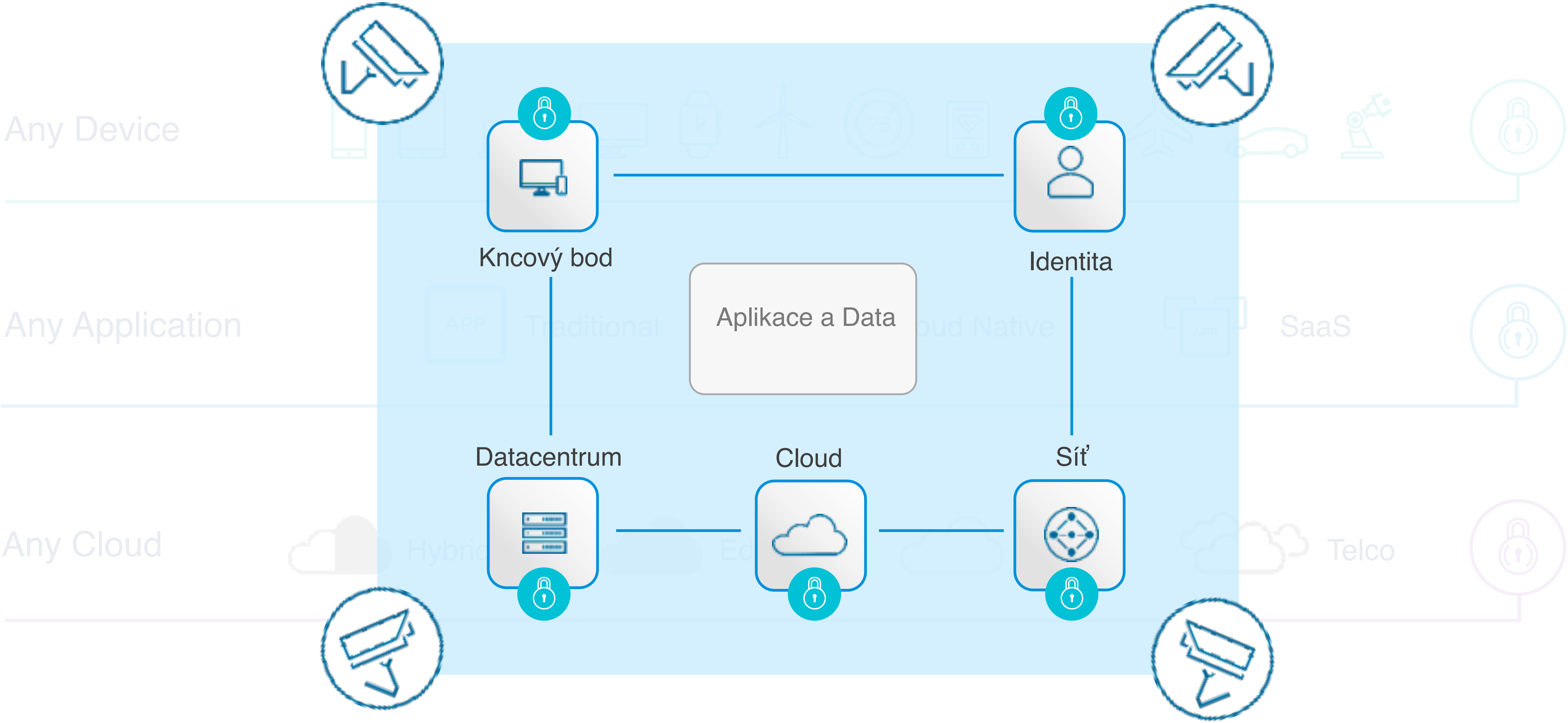
Cloud

CyberSponse EclecticIQ FireEye InSight KELA HYAS
ThreatMetrix THREATQUOTIENT INTSIGHTS TRUSTAR WEBROOT



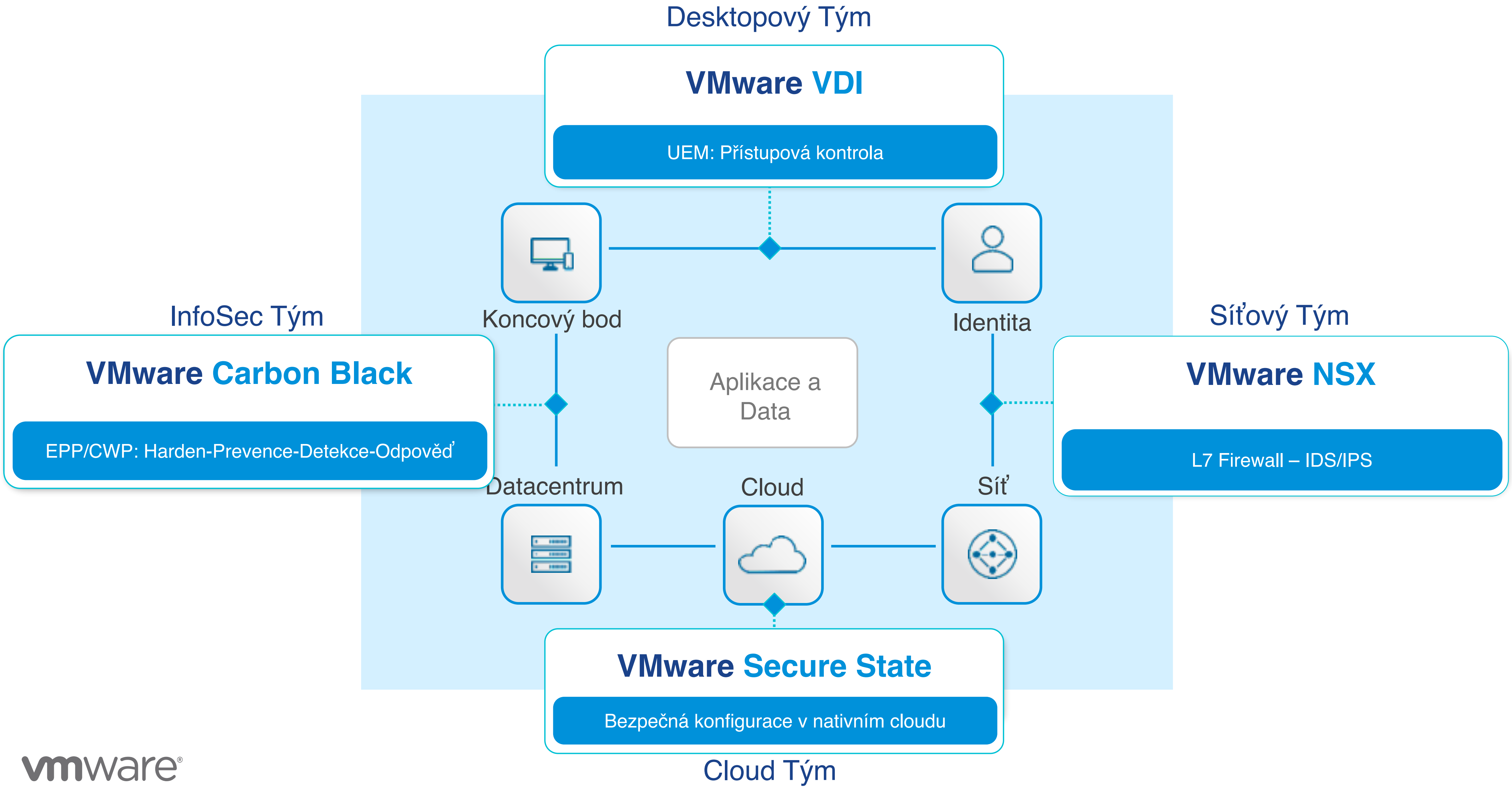
Digital Risk Management
Security Operations & Incident Response
Risk and Compliance
Identity & Access Management
Mobile Security
Endpoint Security
Network & Infrastructure Security
Data Security
Cloud Security
WAF and Application Security
Block Chain
Threat Intelligence
Koncový bod
Identita
Aplikace a Data
Datacentrum
Cloud
Síť

Jednotný bezpečnostní kontrolní bod



vmware

VMware bezpečnostní řešení



Desktopový Tým

VMware VDI

UEM: Přístupová kontrola

InfoSec Tým

VMware Carbon Black

EPP/CWP: Harden-Prevence-Detekce-Odpověď

Síťový Tým

VMware NSX

L7 Firewall – IDS/IPS

VMware Secure State

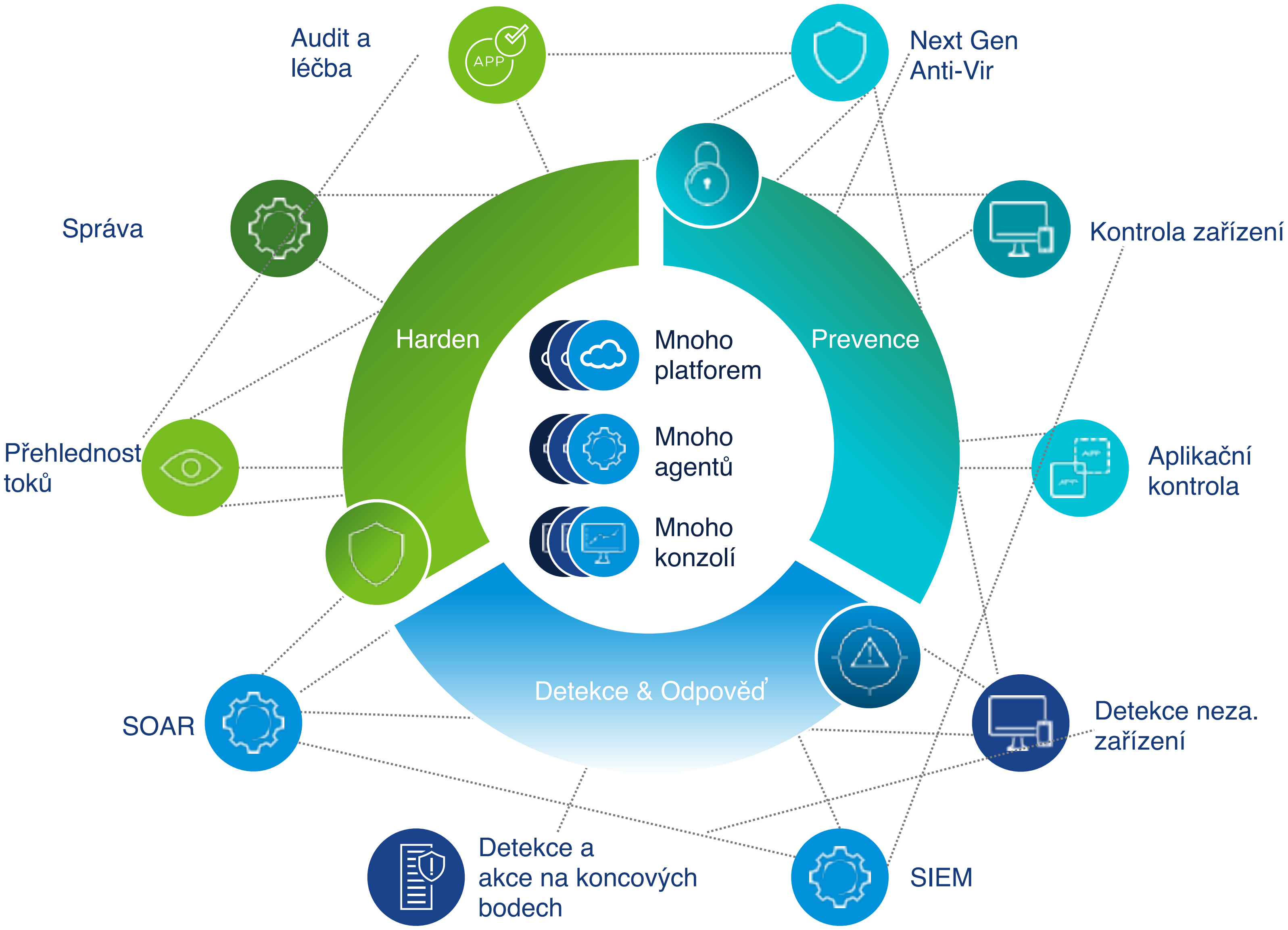
Bezpečná konfigurace v nativním cloudu

Cloud Tým

Zabezpečení koncových bodů & aplikací

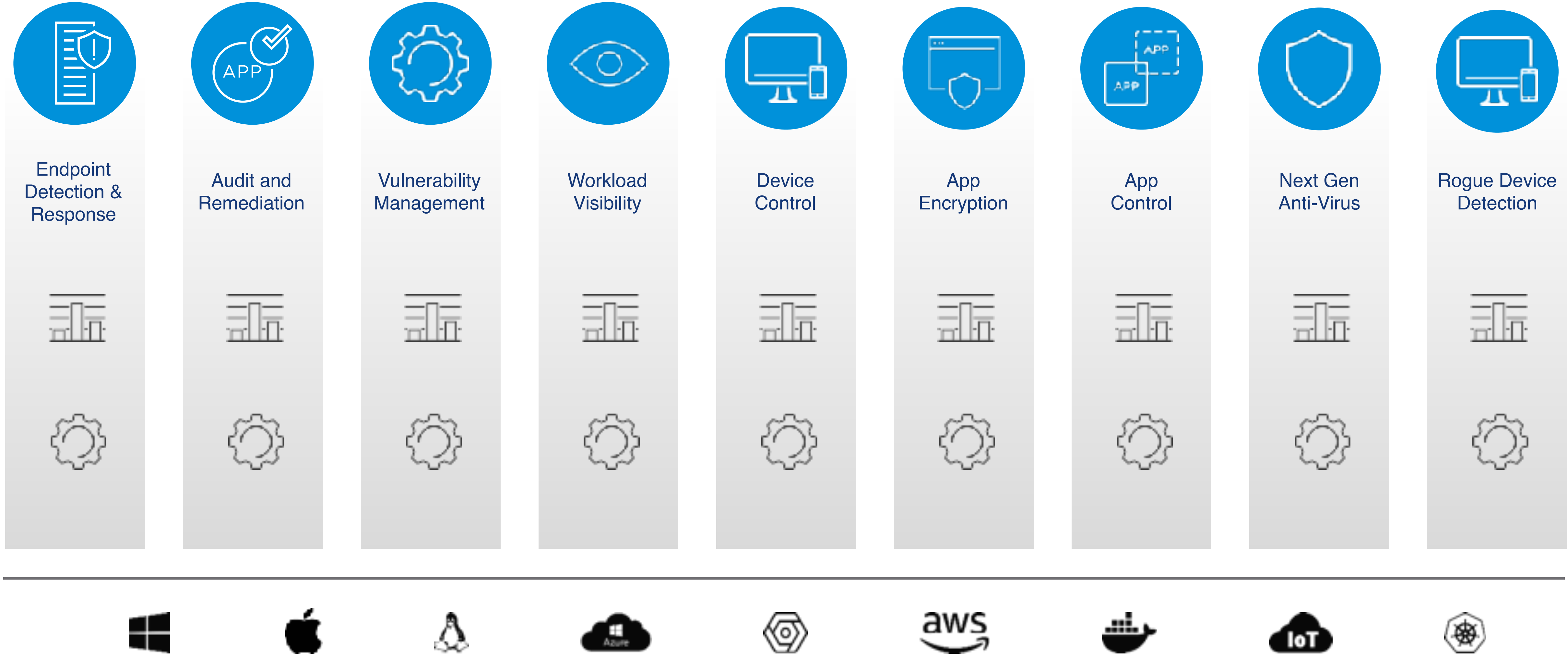
Výzvy

- Informační sila
- Různé komunikační jazyky
- Rozdílné procesy
- Rozdílná pravda
- Nulový obsah



Od inforačních sil…

Fragmentovaných, V silech s mnoha konzolemi, Sety rozdílných pravidel, Agenty…



Endpoint Detection & Response

Audit and Remediation

Vulnerability Management

Workload Visibility

Device Control

App Encryption

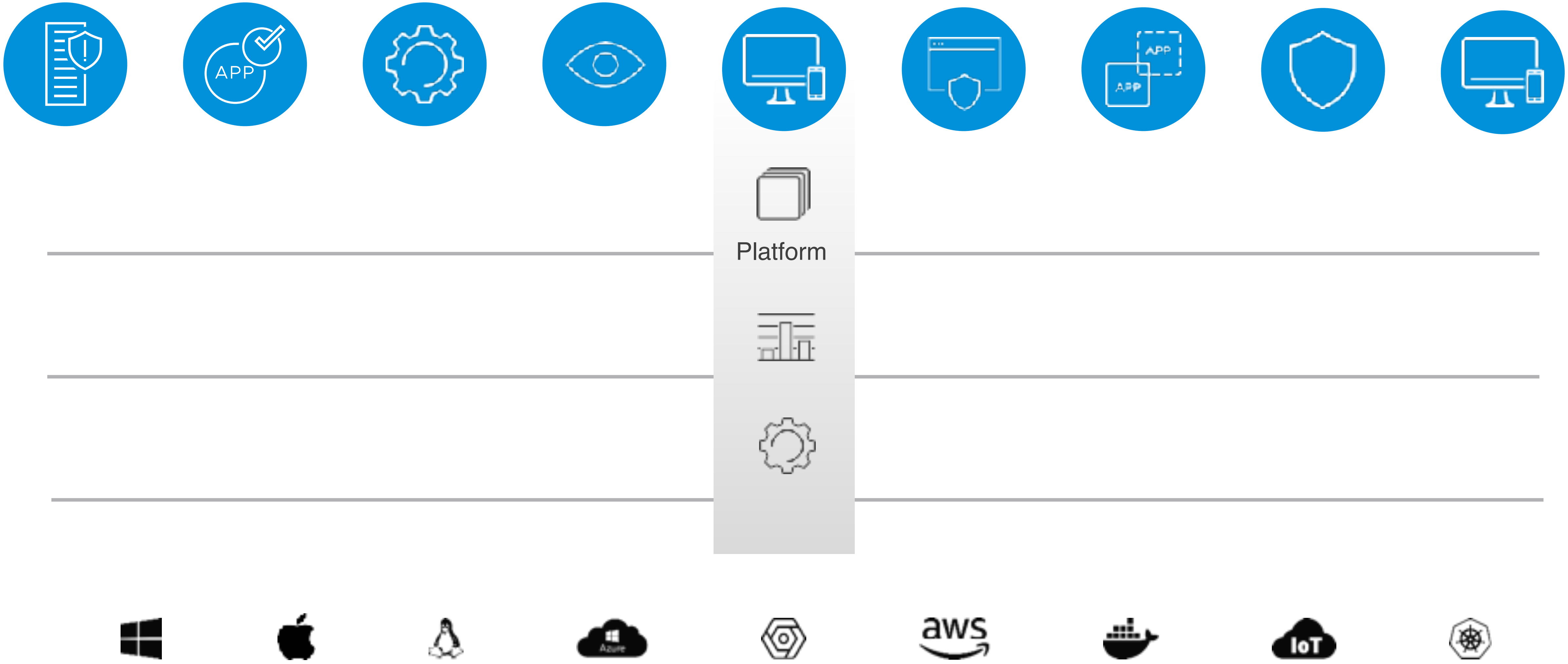
App Control

Next Gen Anti-Virus

Rogue Device Detection

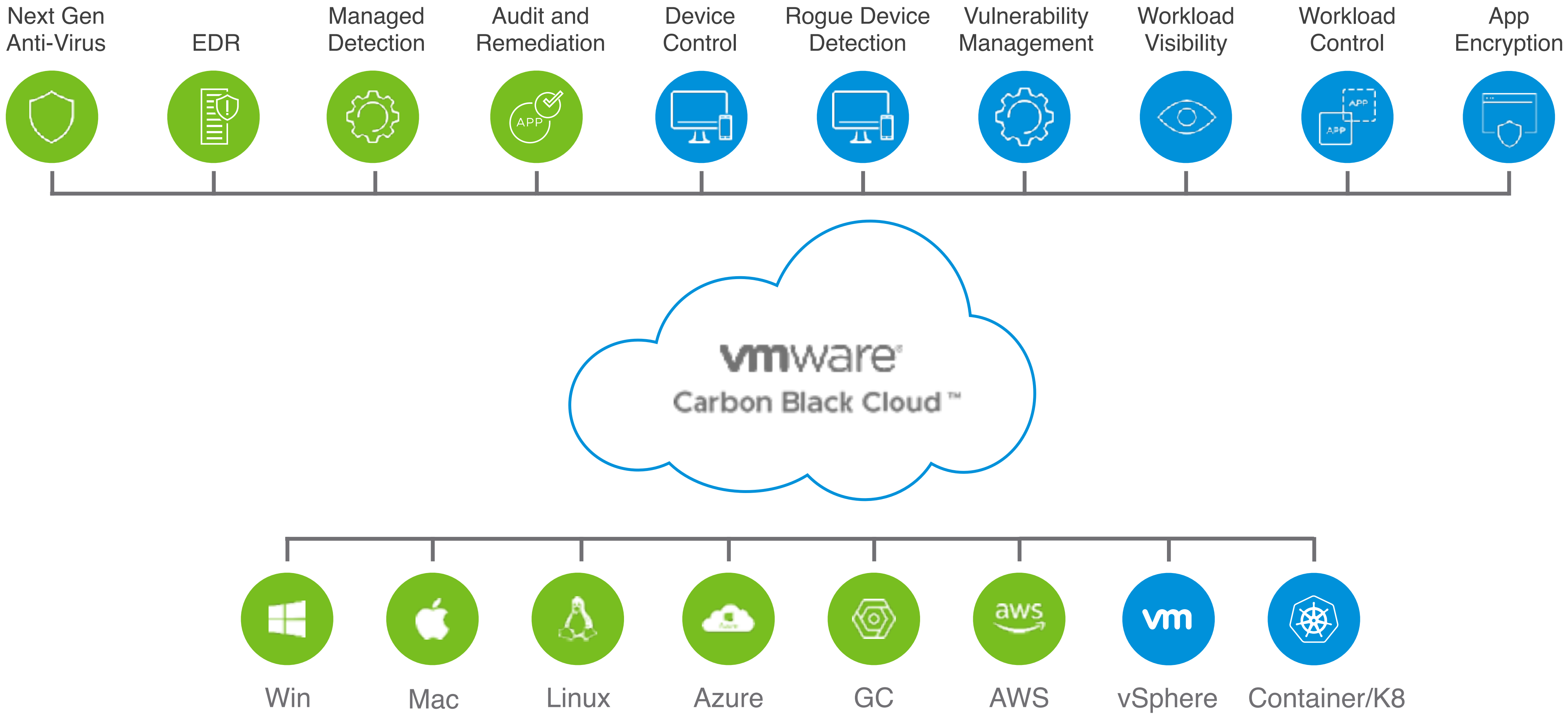
K jednotné platformě

Jednotná kontrola, Podpora prostředí a platforem a Jednomu agentu



VMware Carbon Black Cloud

Funkce



Next Gen Anti-Virus

EDR

Managed Detection

Audit and Remediation

Device Control

Rogue Device Detection

Vulnerability Management

Workload Visibility

Workload Control

App Encryption

Win

Mac

Linux

Azure

GC

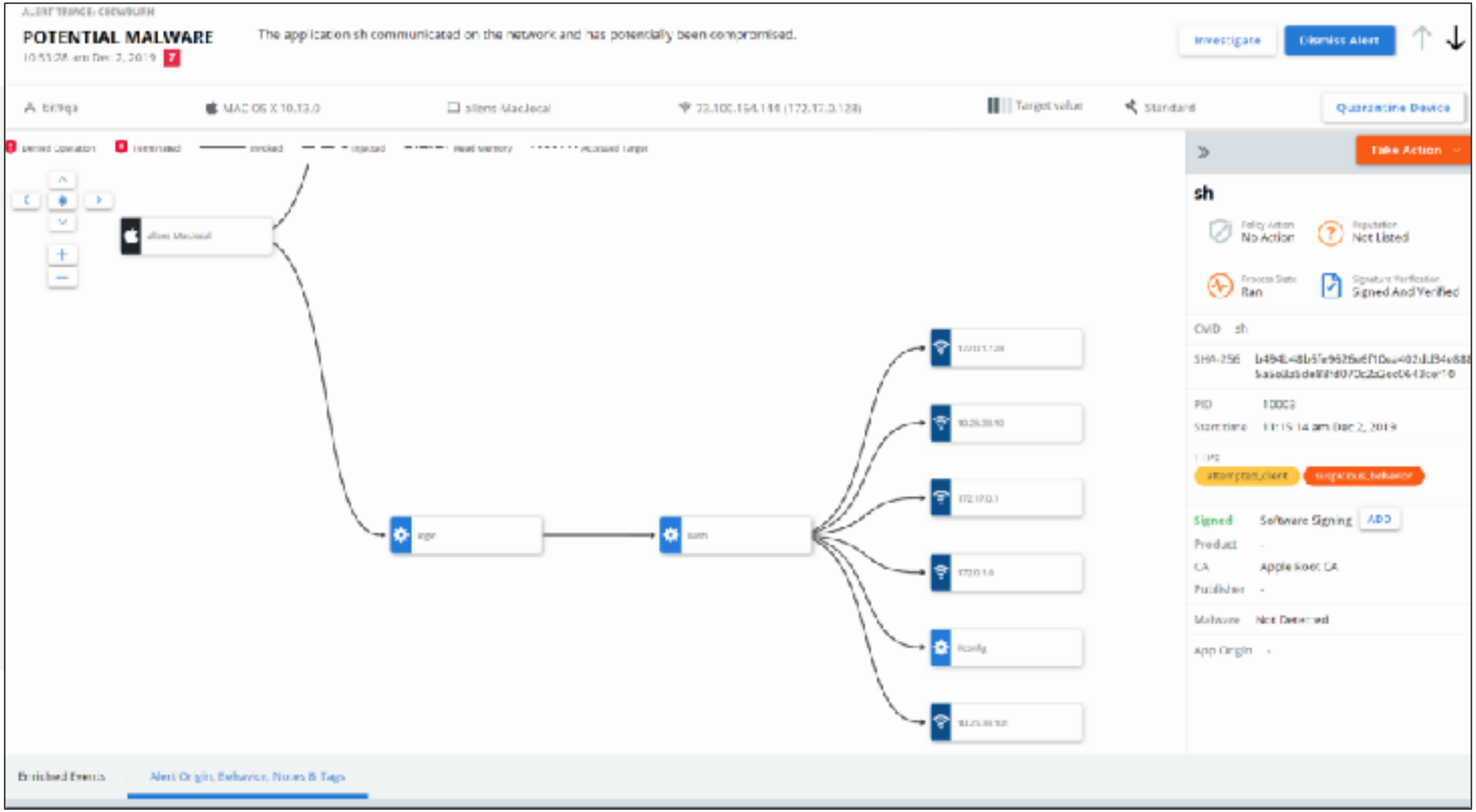
AWS

vSphere

Container/K8

Rychlé porozumění hrozby a vygenerované události

- Odpověď na důležité otázky
- Porovnání s globálními daty
- Informace co je podezřelé a proč



POTENTIAL MALWARE

10:53:28 am Dec 2, 2019 7

The application sh communicated on the network and has potentially been compromised.

MAC OS X 10.13.0

73.100.154.144 (172.17.0.128)

sh

Policy Action: No Action

Reputation: Not Listed

Process State: Ran

Signature Verification: Signed And Verified

CMD: sh

SHA-256: [illegible]

PID: 10003

Start time: 11:15:14 am Dec 2, 2019

TTPs: attempted_client, suspicious_behavior

Signed: Software Signing

Product: -

CA: Apple Root CA

Publisher: -

Malware: Not Detected

App Origin: -

Lídr segmentu NGAV

Gartner peerinsights™

MOST 5-STAR RATINGS

A Gartner Peer Insights
Customers' Choice for EDR Solutions
January 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 Evaluation
November 2018

Gartner®

A VISIONARY

Gartner Magic Quadrant for
Endpoint Protection Platforms
2019

CYBER SECURITY
EXCELLENCE AWARDS
★ FINALIST ★
2019

BEST CYBERSECURITY COMPANY & BEST ENDPOINT SECURITY SOLUTION

2019 Cybersecurity Excellence Awards

FORRESTER®

STRONG PERFORMER

The Forrester Wave™
Endpoint Security Suites
2019

Blue Cross Blue Shield of Florida

Endpoint Standard & EDR

26,000 Endpoints

Too Many Tools

Detection Gaps

Siloed Teams

INDUSTRY – Healthcare
USE CASE – Replace AV

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

vmware®

Mercy Medical Center

Endpoint Standard

4,500 Endpoints

Visibility Gaps

Detection Gaps

Siloed Teams

INDUSTRY – Healthcare
USE CASE – Next-Gen AV

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

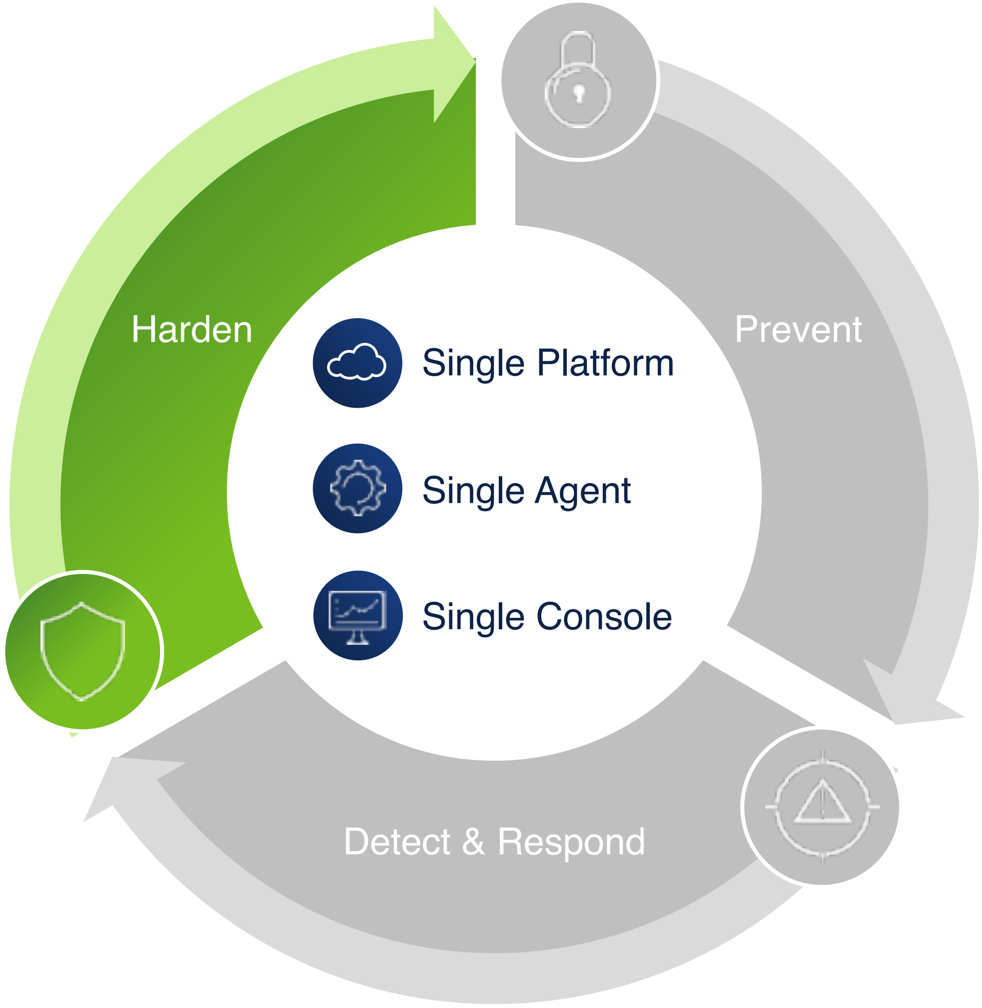
vmware®

Děkuji za pozornost

Ondřej Číž
ociz@vmware.com

Current Capabilities

Real-time Device Assessment and Remediation

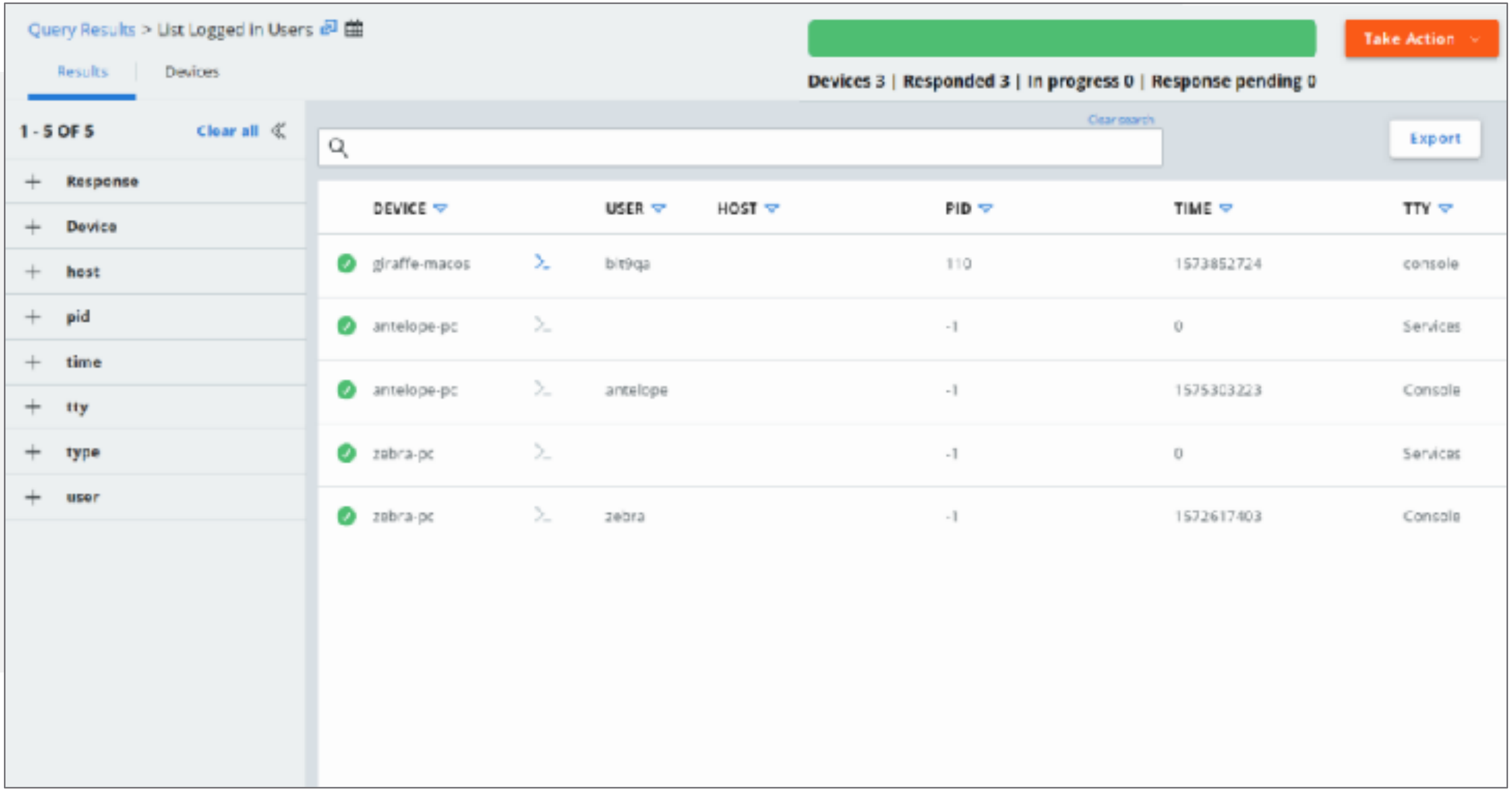


- ✓ **Understand current state** of over 1,500 artifacts on any endpoint
- ✓ **Run ongoing assessments** to track IT hygiene
- ✓ **Take immediate action** with live, remote access

Context-centric system hardening

Understand what is normal in your environment

- Demonstrate baseline configurations
- Know which internal systems are unique
- Compare with global peers



Query Results > List Logged In Users

Results | Devices

Take Action

Devices 3 | Responded 3 | In progress 0 | Response pending 0

1 - 5 OF 5 Clear all

Clear search

Export

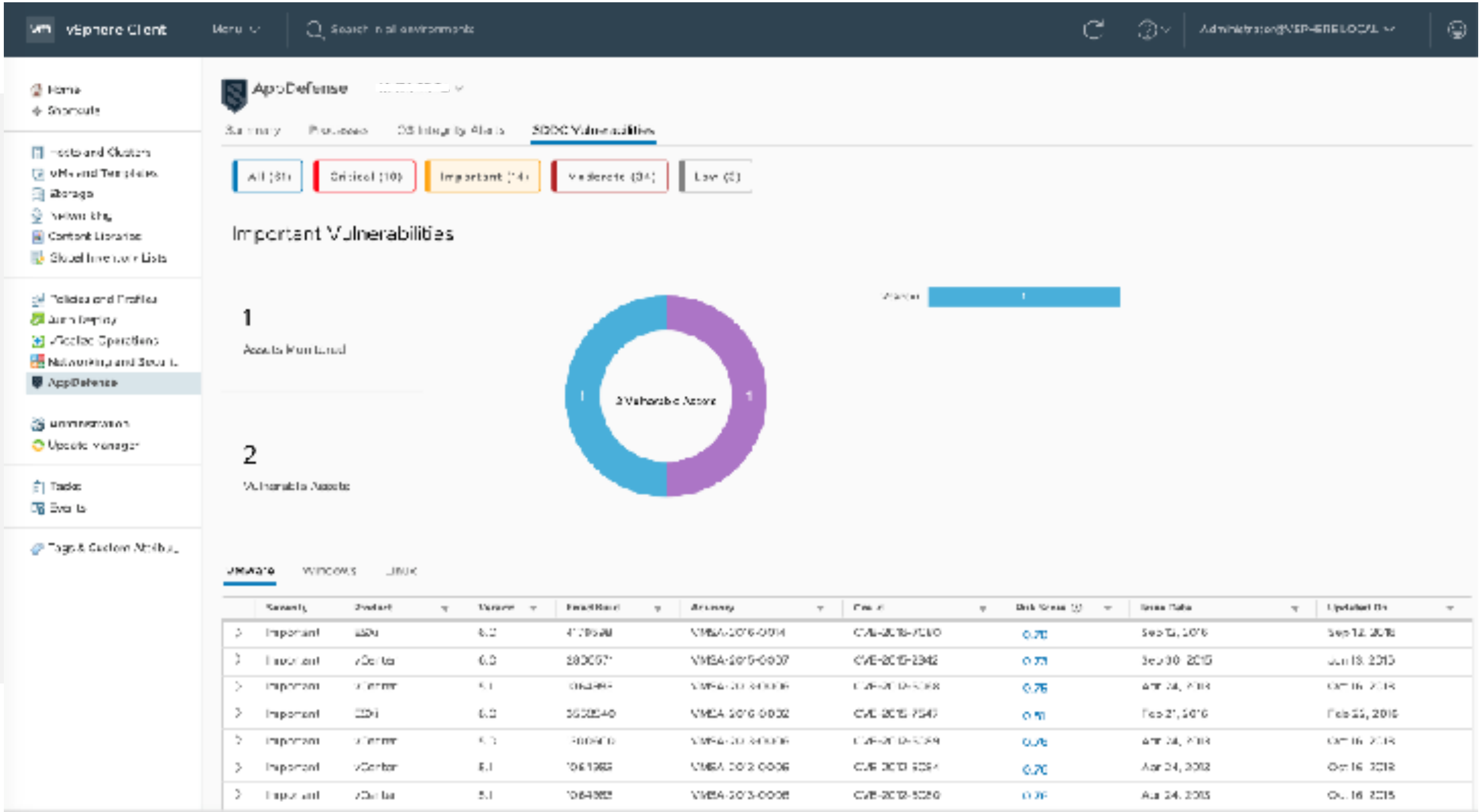
- Response
- Device
- host
- pid
- time
- tty
- type
- user

DEVICE	USER	HOST	PID	TIME	TTY
giraffe-macos	bit9qa		110	1573852724	console
antelope-pc			-1	0	Services
antelope-pc	antelope		-1	1575303223	Console
zebra-pc			-1	0	Services
zebra-pc	zebra		-1	1572617403	Console

Prioritized remediation

Get the context you need to make the most impact

- Reveal the riskiest systems
- Identify vulnerability prevalence
- Focus remediation efforts



Important Vulnerabilities

1

Assets Monitored

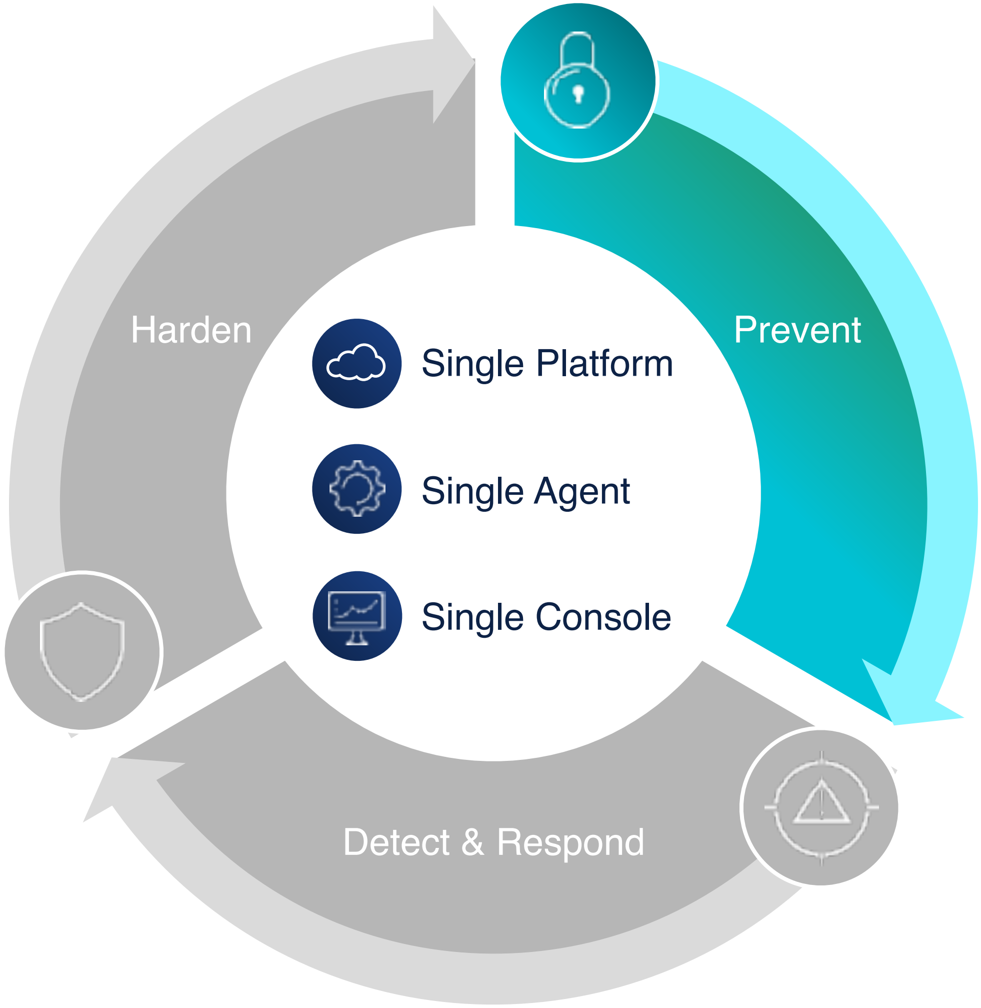
2

Vulnerable Assets

	Severity	Product	Version	Fixed Build	Advisory	Cve #	Risk Score	Issue Date	Updated On
>	Important	ESXi	6.0	4179598	VMSA-2016-0014	CVE-2016-7080	0.70	Sep 13, 2016	Sep 13, 2016
>	Important	vCenter	6.0	2800571	VMSA-2015-0007	CVE-2015-2342	0.71	Sep 30, 2015	Jun 13, 2016
>	Important	vCenter	5.1	[illegible]	[illegible]	[illegible]	0.76	Apr 24, 2013	Oct 16, 2013
>	Important	ESXi	6.0	3620240	VMSA-2016-0002	CVE-2015-7547	0.91	Feb 21, 2016	Feb 22, 2016
>	Important	vCenter	5.1	[illegible]	[illegible]	[illegible]	0.76	Apr 24, 2013	Oct 16, 2013
>	Important	vCenter	5.1	1064983	VMSA-2013-0006	CVE-2013-3034	0.70	Apr 24, 2013	Oct 16, 2013
>	Important	vCenter	5.1	1064983	VMSA-2013-0006	CVE-2012-5050	0.76	Aug 24, 2013	Oct 16, 2013

Current Capabilities

Adaptive Prevention for Malware and Fileless Attacks

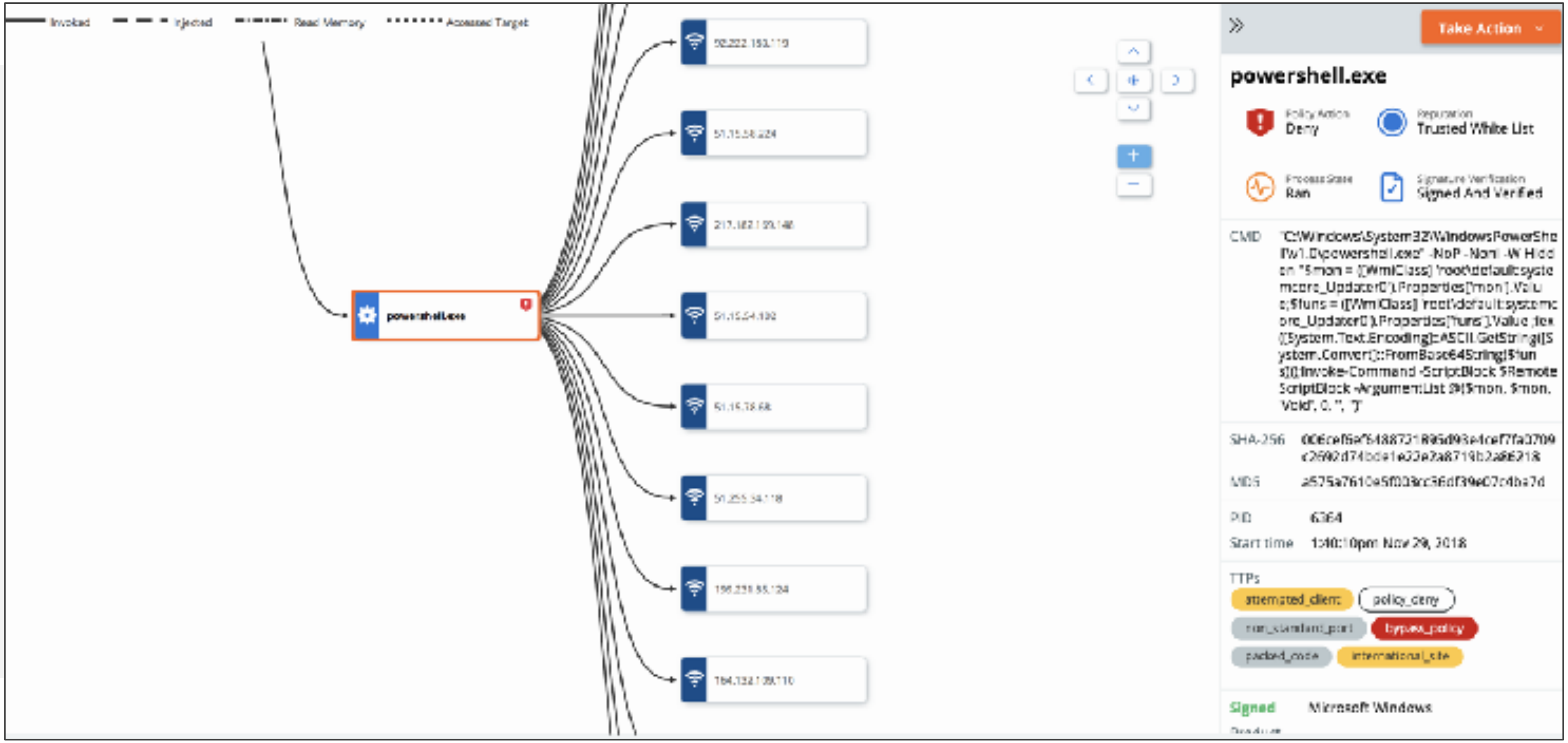


- ✓ **Stop more malware** by combining exploit prevention, machine learning, and file reputation
- ✓ **Shut down unknown attacks** with behavioral analytics and ransomware decoys
- ✓ **Easily adapt prevention** to detected behavior in your environment

Prevent malware and non-malware attacks

Layer prevention techniques to stop each attack type

- Reputation and ML for known and unknown malware
- Behavioral prevention for fileless and LOL attacks
- Deception for ransomware



powershell.exe

Policy Action: Deny

Reputation: Trusted White List

Process State: Ran

Signature Verification: Signed And Verified

CMD "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden "$mon = ([WmiClass] 'root\default:systemcore_Updater0').Properties['mon'].Value;$funs = ([WmiClass] 'root\default:systemcore_Updater0').Properties['funs'].Value ;iex ([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String($funs)));Invoke-Command -ScriptBlock $RemoteScriptBlock -ArgumentList @($mon, $mon, 'Void', 0, '', '')"

SHA-256 006cef6ef5488731895d93e4cef7fa0709c2692d74bde1e03e2a8719b2a6E218

MD5 a575a7610e5f003cc36df39e07c4ba7d

PID 6364

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

TTPs

attempted_client

policy_deny

non_standard_port

bypass_policy

packed_code

international_site

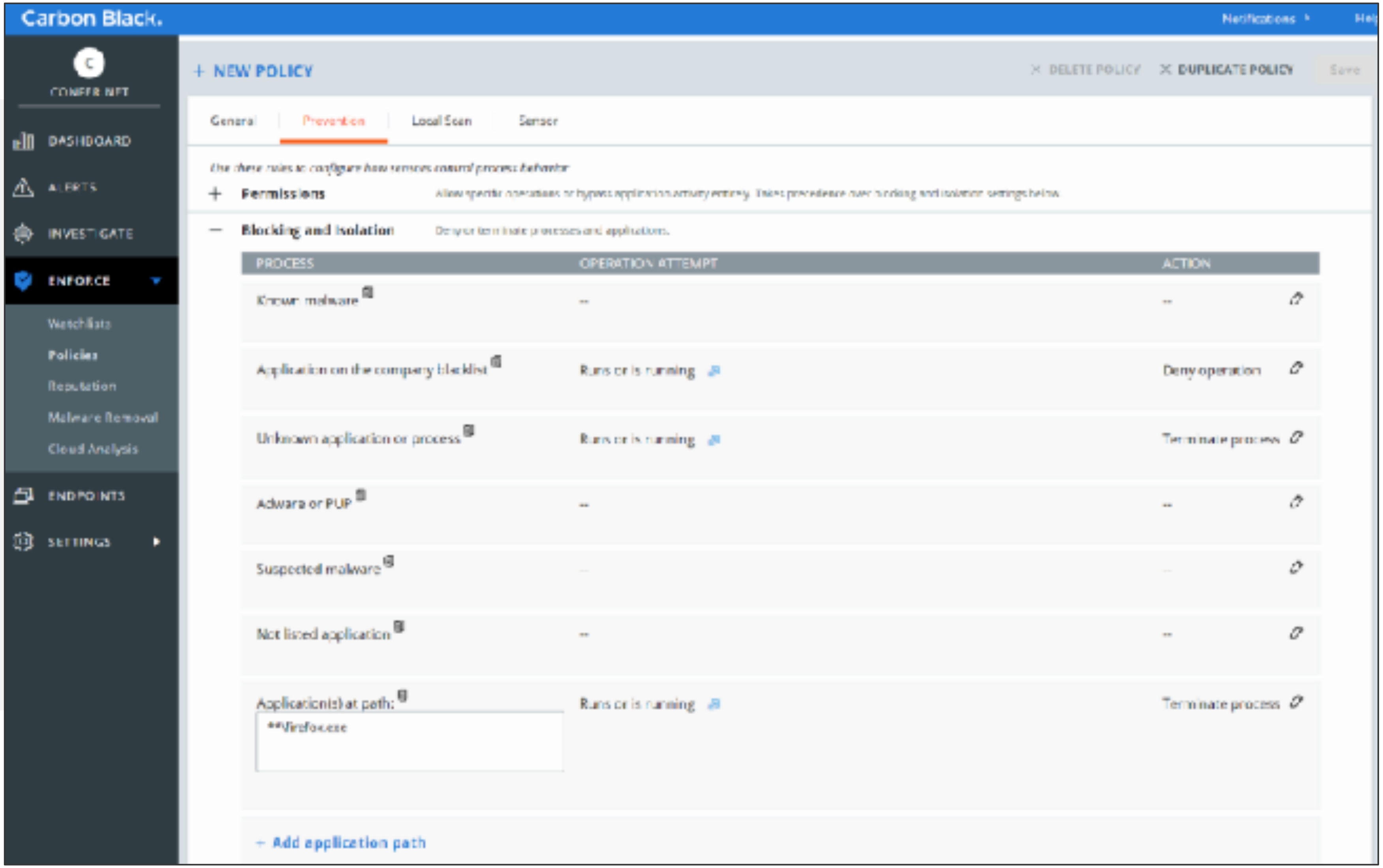
Signed Microsoft Windows

Product

Adapt to your unique business

Easily translate prevention from behavior in your environment

- Implement flexible prevention policy
- Whitelist expected behavior
- Minimize user disruption



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.

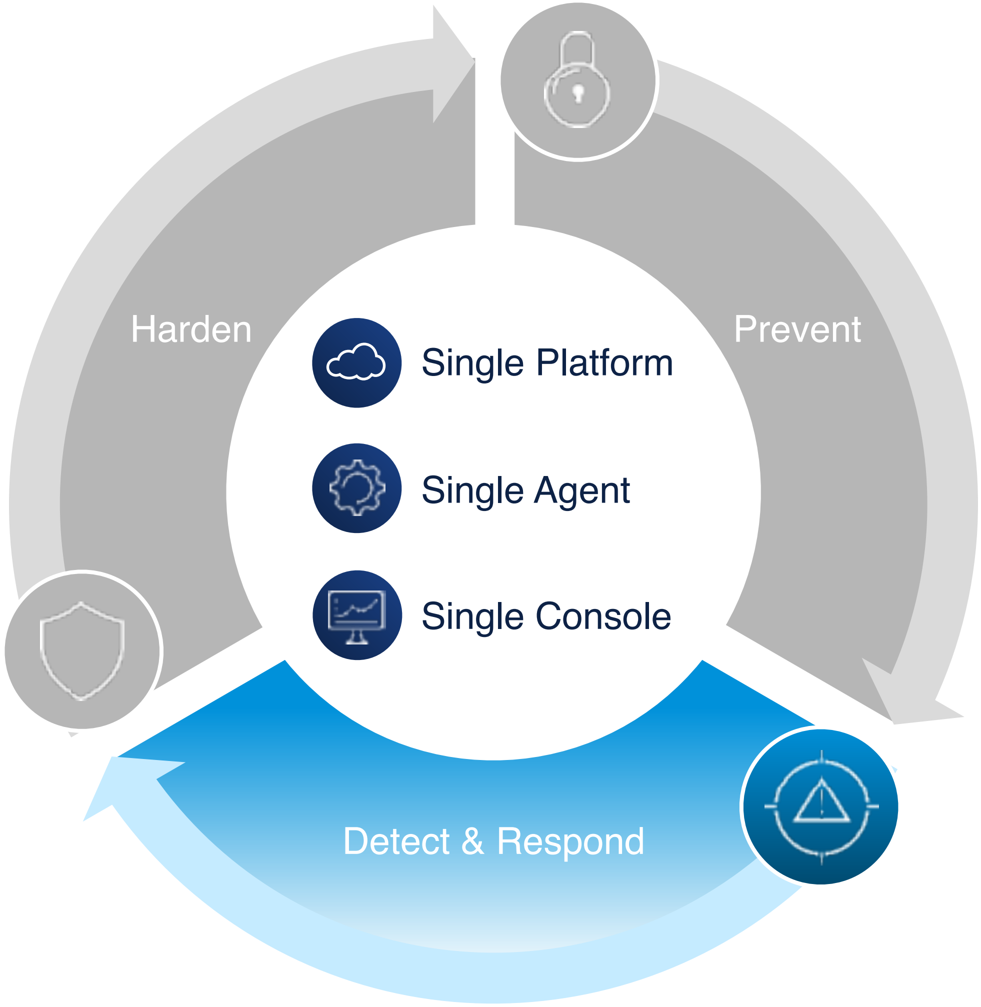
− **Blocking and Isolation** Deny or terminate processes and applications.

PROCESS	OPERATION ATTEMPT	ACTION
Known malware	--	--
Application on the company blacklist	Runs or is running	Deny operation
Unknown application or process	Runs or is running	Terminate process
Adware or PUP	--	--
Suspected malware	--	--
Not listed application	--	--
Application(s) at path: **\firefox.exe	Runs or is running	Terminate process

+ Add application path

Current Capabilities

Endpoint Detection and Response

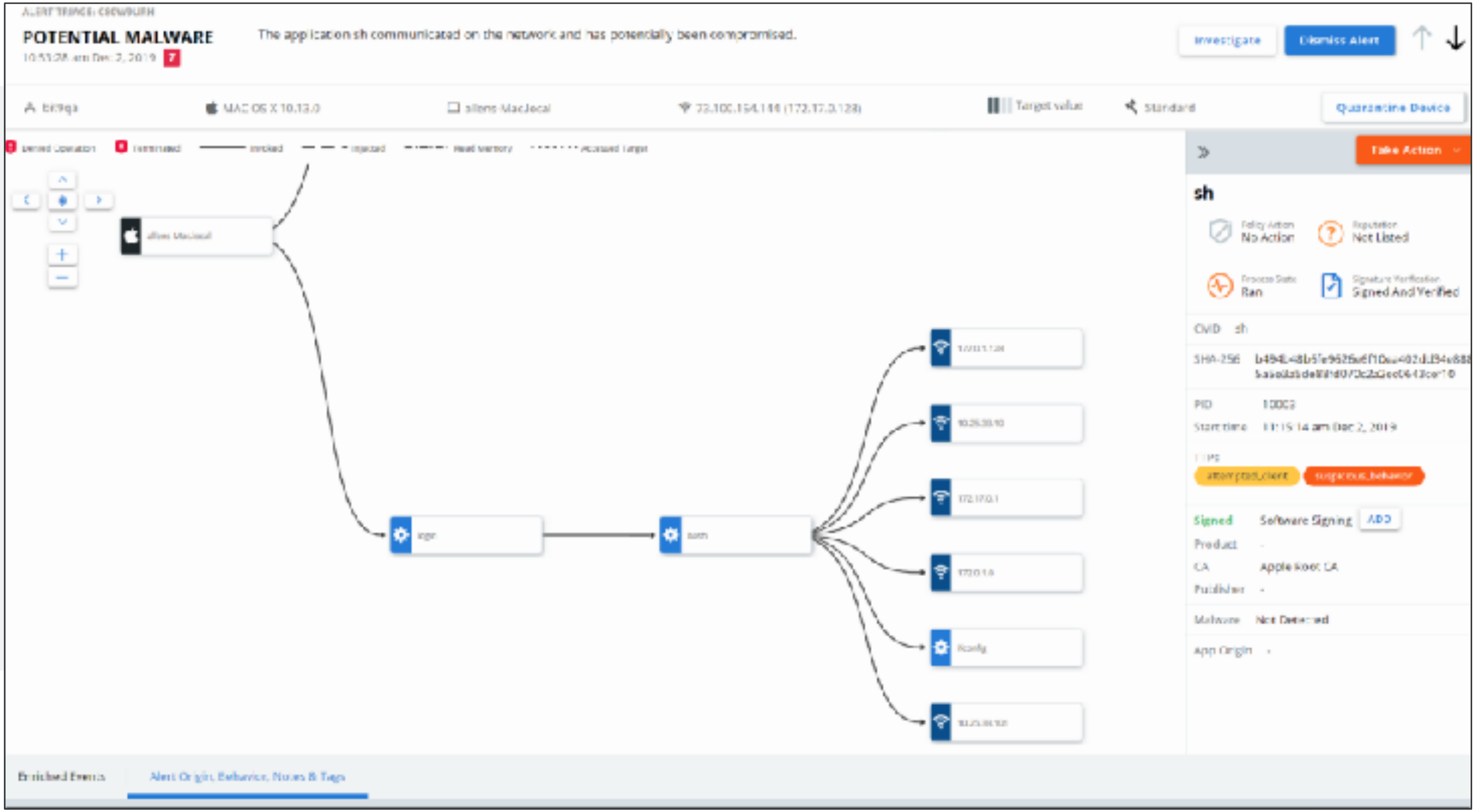


- ✓ **Hunt for threats** with recordings of all endpoint activity
- ✓ **Detect anomalous activity** with threat intelligence and frequency analysis
- ✓ **Feed response actions** directly back into hardening and prevention

Rapidly understand the risk of an event

Combine commonality of events with MITRE ATT&CK TIDs

- Answer the important questions
- Compare with global data
- Know what was suspicious and why



ALERT TRIAGE: [illegible]

POTENTIAL MALWARE

10:53:28 am Dec 2, 2019 7

The application sh communicated on the network and has potentially been compromised.

MAC OS X 10.13.0

Take Action

sh

Policy Action: No Action

Reputation: Not Listed

Process State: Ran

Signature Verification: Signed And Verified

CMD sh

SHA-256 [illegible]

PID 10003

Start time 11:15:14 am Dec 2, 2019

Signed Software Signing

Product -

CA Apple Root CA

Publisher -

Malware Not Detected

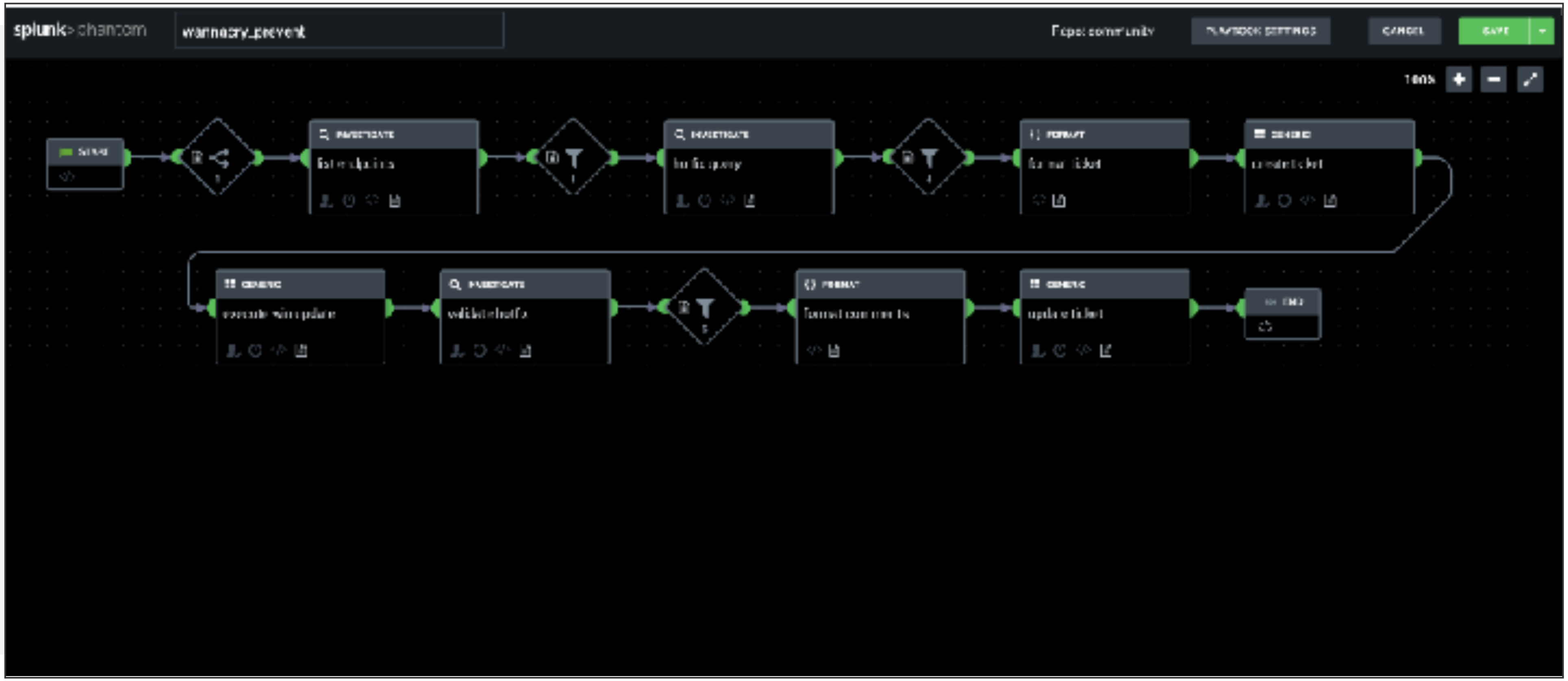
App Origin -

vmware®

Automate Endpoint Protection into your workflow

Integrate directly with the rest of the ecosystem

- Use bi-directional APIs
- Send contextualized events to other tools
- Leverage robust SIEM/SOAR integrations



vmware®

Module Slides

vmware®

Endpoint Standard (NGAV + Behavioral EDR)

Certified to Replace and Extend Traditional Antivirus

Benefits

- Prevent Modern Attacks
- Cut Incident Response Times
- Boost Productivity

Key Features & Capabilities

- Stops malware, fileless, ransomware and living-off-the-land attacks
- Out-of-the-box prevention policies and ability to customize to environment
- Visibility into the entire attack chain for easy investigation
- Remote shell into endpoints for immediate action
- Cloud-native platform with single agent & console
- Automation via integrations & open APIs

Audit and Remediation

Ask Questions and Take Action in Real Time

Benefits

- Increase Visibility
- Track & Report IT Drift
- Speed Up Audits

Key Features & Capabilities

- Pull over 1,500 artifacts across all endpoints
- Secure shell for remote remediation
- Flexible query scheduler
- Filterable & exportable results
- Automated email notifications
- Two-way API

Managed Detection

Prevent Breaches with Expert Threat Hunters at Your Side

Benefits

Increase Visibility

Reduce Staffing Pressures

Uncover Root Cause

Key Features & Capabilities

- Analyze every stage of an attack
- Analysts monitoring 24/7 to protect you always
- Expert alert triage to reduce your investigation
- More efficient and proactive security operations
- Notifications provide critical threat intel
- View of threat and security trends help guide policy

Enterprise Endpoint Detection and Response (EDR)

Detect and Respond to Advanced Attacks

Benefits

Increase Visibility

Reduce Dwell Time

Uncover Root Cause

Key Features & Capabilities

- Continuous and centralized recording of endpoint activity
- Out-of-the-box and customizable threat intelligence
- Attack chain visualization and enterprise-wide search
- Live Response for remote remediation
- Automation via integrations & open APIs

Endpoint Detection and Response (EDR) – On Prem

Detect and Respond to Advanced Attacks

Benefits

- Increase Visibility
- Reduce Dwell Time
- Uncover Root Cause

Key Features & Capabilities

- Supports on-premises requirements for hybrid deployments
- Continuous and centralized recording of endpoint activity
- Out-of-the-box and customizable threat intelligence
- Attack chain visualization and enterprise-wide search
- Live Response for remote remediation
- Automation via integrations & open APIs

App Control – On Prem

Market-Leading Application Control Solution

Benefits	Key Features & Capabilities
Meet Regulatory Mandates Protect Legacy Systems Boost Productivity	• Stops malware, ransomware and next-gen attacks • Eliminate unplanned downtime for critical systems • Prevent unwanted changes to system configurations • Protect unsupported OS • Single agent for application whitelisting, FiM & device control • Memory/tamper protection • Direct control for PCI DSS 5.0

VMware Carbon Black Cloud Solution Bundles

The Endpoint Bundles

Easy to Right-size for Each Organization’s Maturity

Endpoint Standard	Endpoint Advanced	Endpoint Enterprise
✓ Next-gen Antivirus ✓ Behavioral EDR	✓ Next-gen Antivirus ✓ Behavioral EDR ✓ Audit and Remediation	✓ Next-gen Antivirus ✓ Enterprise EDR ✓ Audit and Remediation
➢ Block malware, fileless, and Living-off-the-land attacks, and detect behavior unusual to *your* organization.	➢ Add device audit and risk remediation for system hardening across your environment.	➢ Add continuous event capture, threat hunting, and threat intelligence with customizable detections.

Endpoint Standard Bundle

Protect and Contain Today’s Advanced Cyber Attacks From One Console and Agent

Endpoint Standard

Next-Gen Antivirus

Behavioral EDR

➢ Industry-leading detection and response capabilities reveal threat activity in real time.

Key Capabilities

- ✓ **Block** malware, fileless, and living-off-the-land attacks
- ✓ **Detect** behavior unusual to *your* organization
- ✓ **Gain** comprehensive on-and-offline prevention
- ✓ **Visualize** every stage of an attack to uncover root cause
- ✓ **Secure shell** into any endpoint on or off your network

Endpoint Advanced Bundle

Stop Advanced Attacks and Harden Systems in Real-time From One Console and Agent

Endpoint Advanced	Key Capabilities
Next-Gen Antivirus Behavioral EDR Audit and Remediation	Endpoint Standard capabilities, plus: ✓ **Easily access** artifacts from all endpoints and workloads ✓ **Gain visibility** into precise details about current state of all devices ✓ **Make quick, confident decisions** to improve IT hygiene and harden systems against attacks ✓ **Schedule queries** to run on a daily, weekly, or monthly basis to automate operational reporting

Endpoint Enterprise Bundle

Protect, Secure, and Hunt Across Your Entire Enterprise From One Console and Agent

Endpoint Enterprise

- Next-Gen Antivirus
- Enterprise EDR
- Audit and Remediation

Key Capabilities

Endpoint Advanced capabilities, plus:

- ✓ **Access** the complete activity record of every endpoint
- ✓ **See** what happened at every stage of an attack
- ✓ **Automatically collect** and store detailed forensic data for investigation
- ✓ **Consolidate** threat intelligence for your environment to automatically detect suspicious behavior
- ✓ **Isolate** infected systems and remove malicious files to prevent lateral movement

Workspace Security Bundle

Combat Threats and Protect Enterprise Data Across Your Modern Digital Workspace

Workspace Security

- Next-Gen Antivirus
- Behavioral EDR
- Audit and Remediation

Workspace ONE Intelligence

Key Capabilities

Endpoint Advanced capabilities, plus:

✓ **Gain endpoint visibility** and actionable insights through a single dashboard

✓ **Improve** user experience through powerful automation

✓ **Correlate** deep endpoint telemetry and alerts with native and 3rd-party data

✓ **Enable** data-driven decisions across your environment

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

Over 500 Product and Service Partners

Powerful Security Community

Connect With Thousands Of Security Experts

20,000+
Community Members

Global Footprint

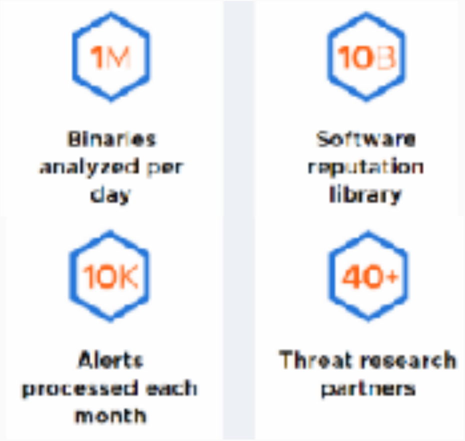
Gather Real-time Threat Intelligence

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

Actionable Threat Intel

IOCs, Watchlists and More

Direct Access to VMware Carbon Black's Threat Analysis Unit



1M
Binaries analyzed per day

10B
Software reputation library

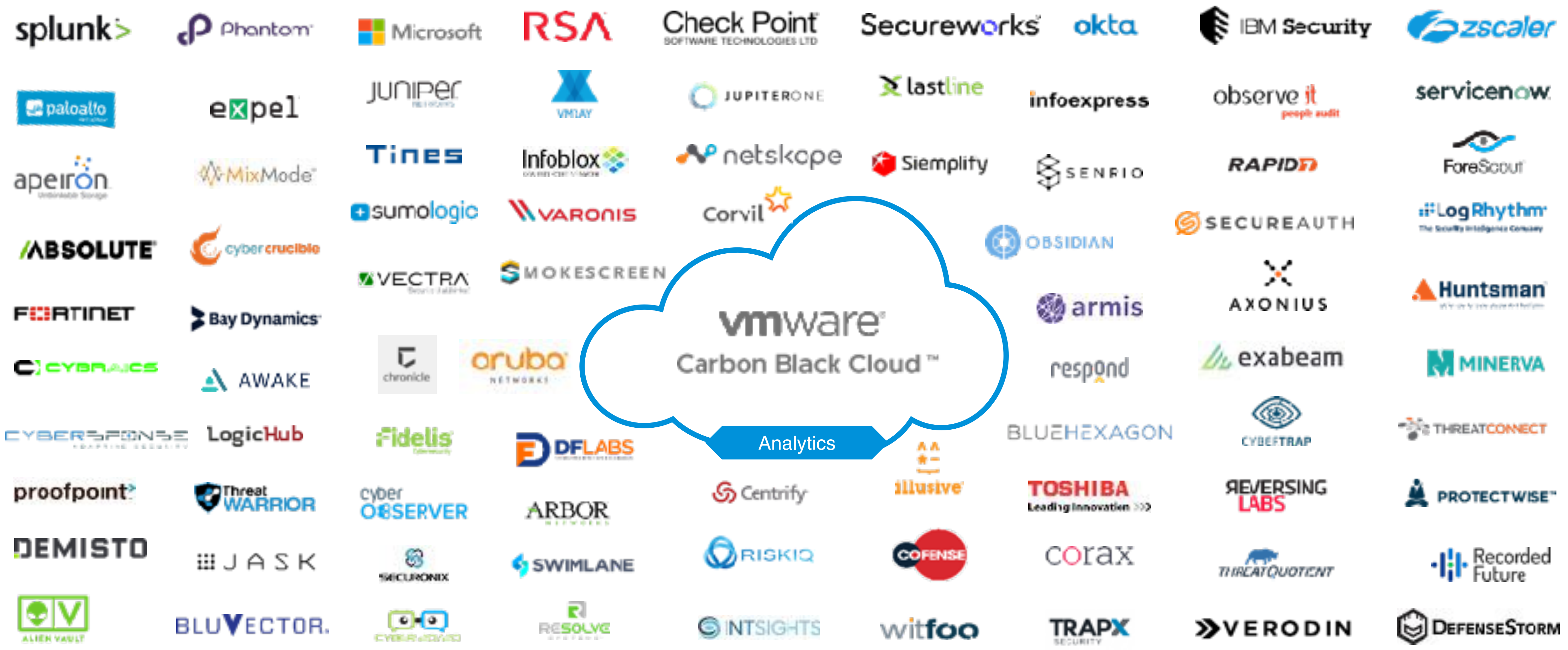
10K
Alerts processed each month

40+
Threat research partners

Analysis of Advanced Threats and Threat Advisory Alerts

Integrating Into Your Existing Security Solutions

Open APIs and over 100 Product Integrations with Leading Security Vendors



6,300+

Customers

1/3

Fortune 100

DocuSign

Adobe

indeed one search. all jobs.

Johnson Controls

Valvoline.

kordia

EPSON

Pinterest

OFS

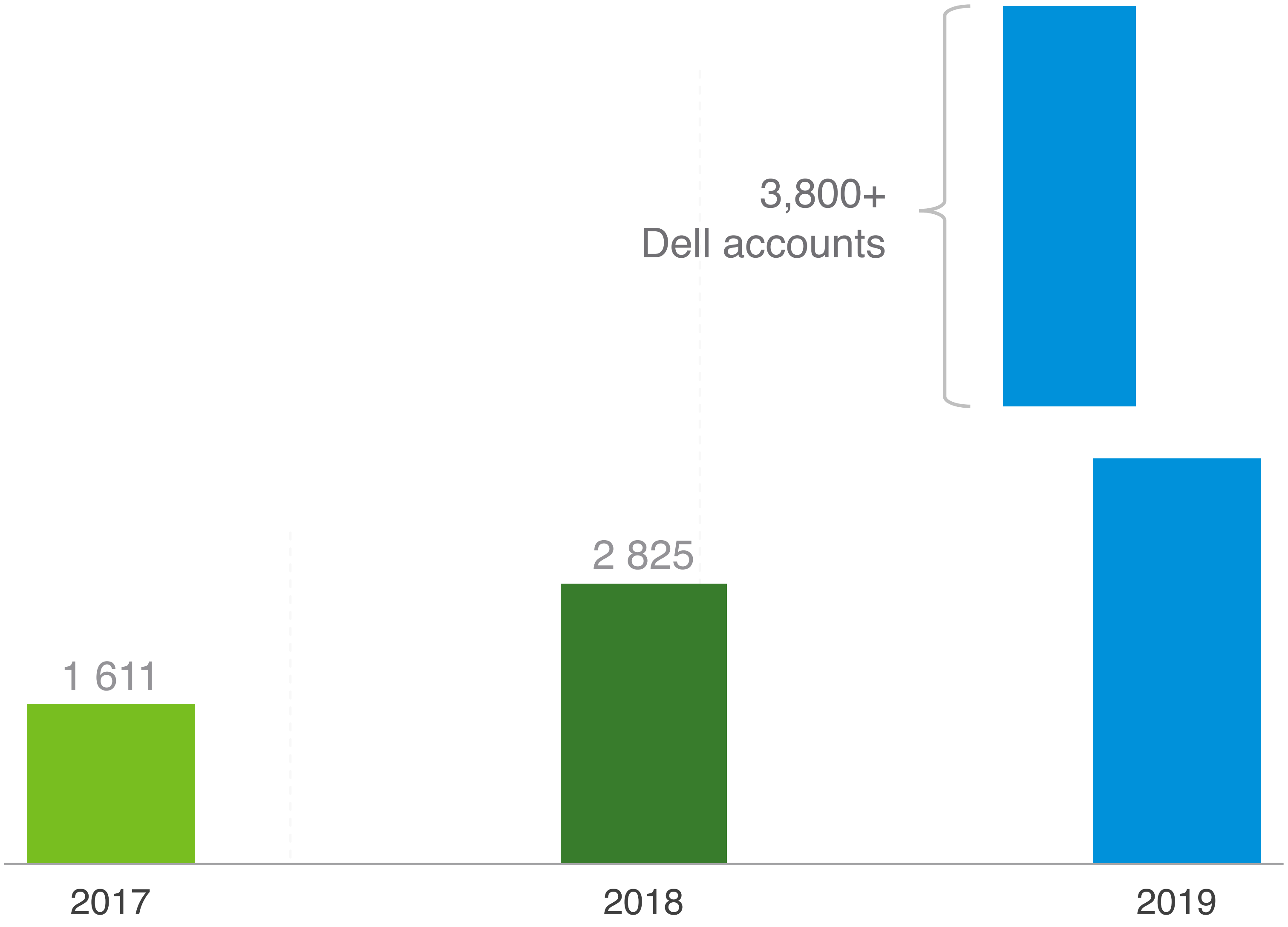
Core-Mark

ASRC FEDERAL

FREEPORT LNG

Rapid Customer Adoption of the Carbon Black Cloud

66% of customers use our cloud products



4,000+ customers

75+ IR & MSSP partners

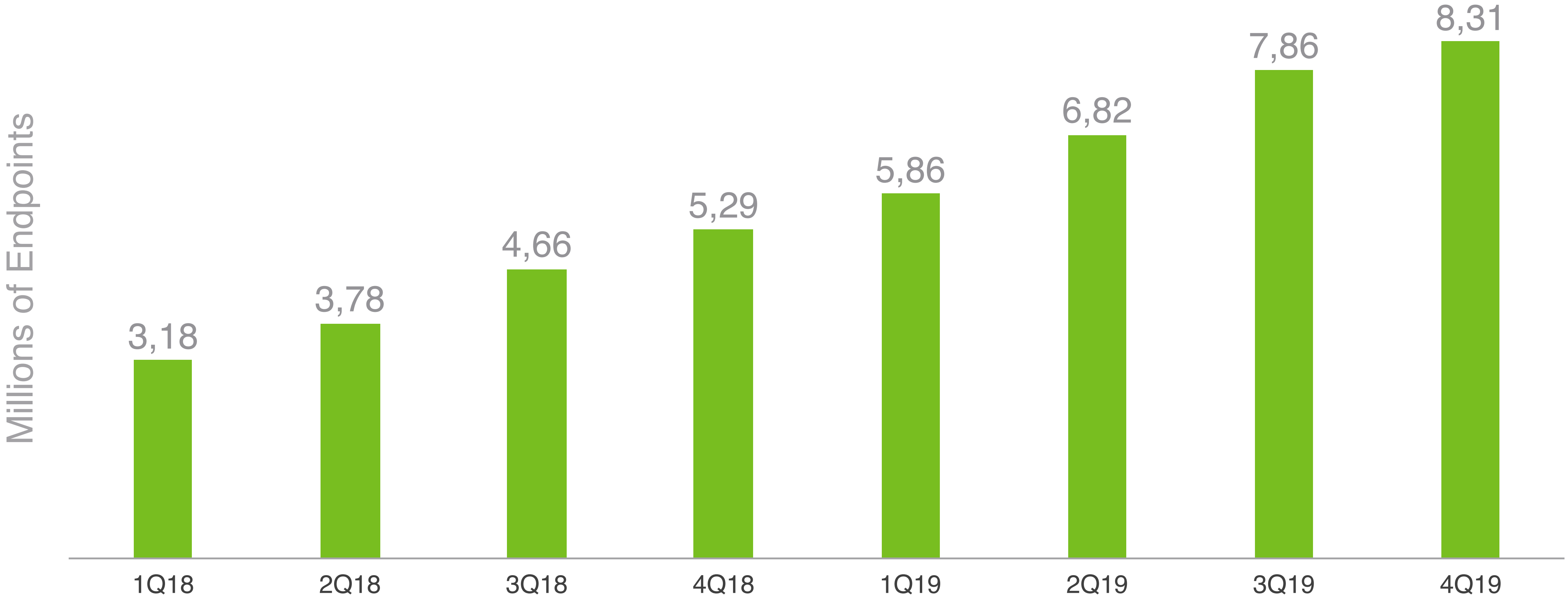
Largest deployment to date:
350K+ endpoints

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

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

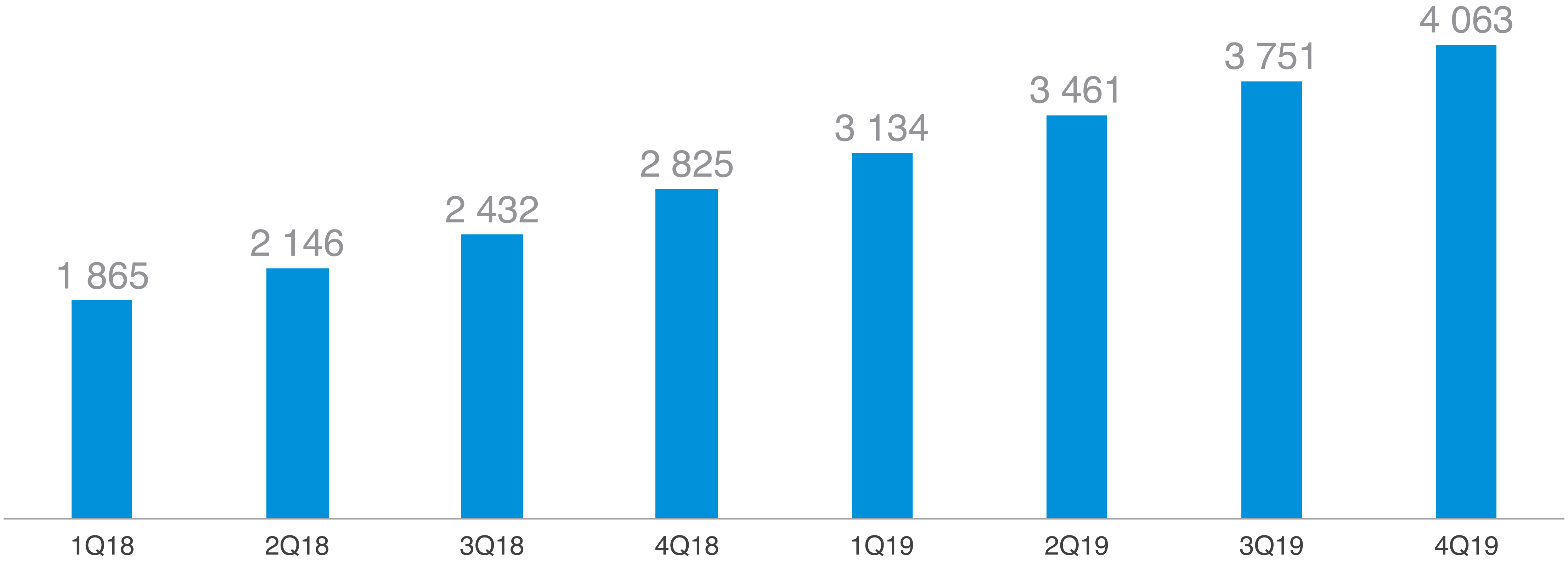
Cloud Endpoint Growth

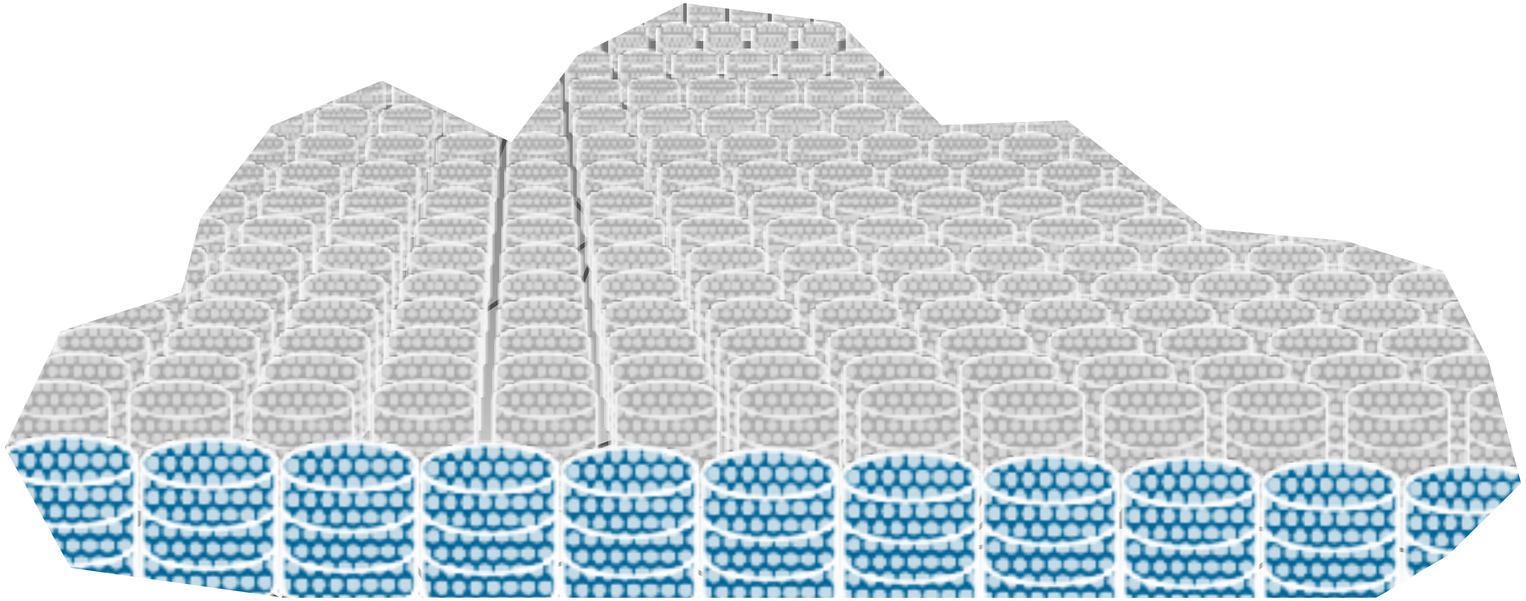
57% increase in cloud endpoints YoY



Cloud Customer Growth

66% of customers use our cloud products





>500TB

Endpoint Data Analyzed Per Day

1 Trillion

Security Events Per Day

Customer Stories

NASDAQ

Endpoint Standard, Enterprise EDR & App Control

17,000 Endpoints

Too Many Tools

Detection Gaps

Siloed Teams

INDUSTRY – Finance
USE CASE – Incident Response, Threat Hunting

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

vmware®

PeoplesBank

Endpoint Standard

400 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

INDUSTRY – Finance
USE CASE – Replace AV, Replace McAfee

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

vmware

Johnson Controls

Endpoint Standard

51,000 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

INDUSTRY – Manufacturing
USE CASE – Prevention, Consolidation

- Lacking prevention and needed visibility into expanding environment
- Looking to a cloud environment while consolidating agents
- Overall coverage and response times greatly improved compared to previously

vmware®

OFS

Endpoint Standard

800 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

INDUSTRY – Retail
USE CASE – Replace AV

- Traditional AV bogged down the network
- Carbon Black performed top tier when tested for deployment, time to value, interface and ease of use
- Spending less time on false positives and more on triaging and acting on real threats

BraunAbility

Endpoint Standard & App Control

1,000 Endpoints

Visibility Gaps

Detection Gaps

Siloed Teams

INDUSTRY – Manufacturing
USE CASE – Visibility

- Wanted to partner with Carbon Black to be more proactive and have agility in security
- Allowed team to have global reach and visibility
- Flexibility in granting access across IT and security teams

Kaas Tailored

Endpoint Standard

100 Endpoints

Visibility Gaps

Detection Gaps

Siloed Teams

INDUSTRY – Manufacturing
USE CASE – Replace AV, Visibility

- Legacy AV was not fulfilling needs and a waste of time and resources
- Interface and UI make it easy to use and understand
- Endpoint Standard prevents team from chasing after unnecessary reports or logs

Medibank

Endpoint Enterprise, App Control & EDR

14,500 Endpoints

○ Siloed Teams

Detection Gaps

Visibility Gaps

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

Motors Management Corp.

Endpoint Standard

3,000 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

INDUSTRY – Automotive
USE CASE – Next-Gen AV

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

Other Brands We Protect:

NISSAN

UBER

vmware®

Royal Philips NV

EDR

90,000 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

INDUSTRY – Manufacturing
USE CASE – Incident Response

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

Adobe

Endpoint Standard & EDR

69,000 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

INDUSTRY – Technology
USE CASE – Next-Gen AV

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

Cox Communications

Endpoint Standard, EDR & App Control

41,000 Endpoints

Too Many Tools

Detection Gaps

Siloed Teams

INDUSTRY – Technology
USE CASE – Prevention, Open APIs

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

vmware®

Motorola

App Control & Enterprise EDR

26,000 Endpoints

Too Many Tools

Detection Gaps

Siloed Teams

INDUSTRY – Telecommunications
USE CASE – Incident Response, Threat Hunting

- Needed to streamline detection & response processes
- Carbon Black was only solution that provided complete visibility into every endpoint across the enterprise
- Impressed with the speed, functionality, scalability and modularity of Enterprise EDR

Kordia

App Control

850 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

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, App Control has them covered

Stonewall Kitchen

Endpoint Standard & App Control

750 Endpoints

Too Many Tools

Detection Gaps

Visibility Gaps

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
- Endpoint Standard consolidated multiple systems into one – eliminated 3+ servers

vmware®

Why Are We Here?

The challenges that drive VMware Carbon Black

Localized Analysis and Detection

- Employees are remote
- Context is limited
- Threat analysis isolated to one environment

Security Tools are One-size-fits-all

- Every org is different
- Patches have exceptions
- System usage not considered

Majority of Attacks Abuse Legitimate Tools

- Software not all black/white
- Activity hidden in memory
- Lateral movement is prevalent

Dozens of Agents, Dozens of Consoles, Dozens of Truths

What is Needed to Solve These Challenges?

Requirements for success

Localized Analysis and Detection

Security Tools are One-size-fits-all

Majority of Attacks Abuse Legitimate Tools

- Visibility from outside user space
- Centralized, global asset analysis
- Flexible, automated prevention
- Continuous intel on threats and legitimate application behavior
- Open APIs and automation

Single Agent, Single Console, Single Truth

Intrinsic Security

Stop Sacrificing

Production Compute

Device Performance

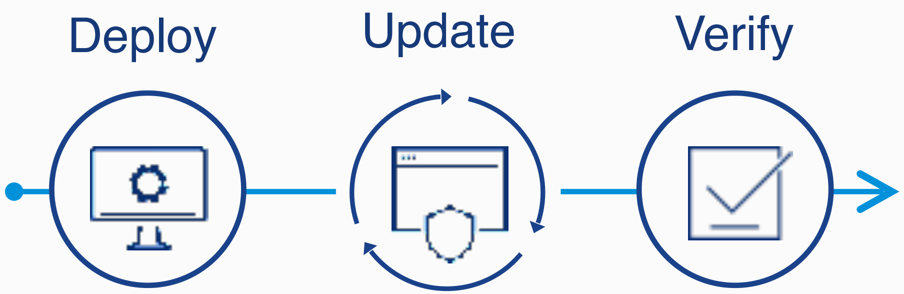
User Experience

Intrinsic Security Plan: Two Top Investments

Endpoints and Workloads

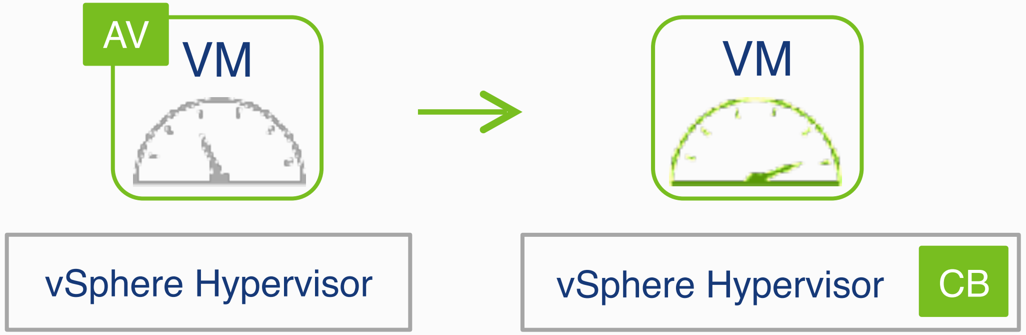
Endpoint Protection

- From the management plane
- Replace SCCM & AV
- Streamline process for endpoint protection and management



Workload Protection

- From the hypervisor
- Replace Server AV
- Eliminate performance impact and footprint


AV
VM
vSphere Hypervisor
VM
vSphere Hypervisor
CB