CHEAT SHEET

VMware Carbon Black Cloud – Securing Remote Workers

OBJECTIVE/GTM MOTION

Displace legacy on-premises antivirus tools by emphasizing the strategic advantages of VMware Carbon Black Cloud for securing remote devices that are not on the corporate network.

TARGETS

Who are we targeting?

- Cross-sell to existing accounts (Workspace ONE and Horizon)
- New accounts (using traditional antivirus)
- Any organization with a sudden influx of remote workers

Buyers/Influencers

- **Director of IT Security** – Interested in improving their team's productivity, ability to triage alerts and close out tickets as quickly as possible
- **Chief Information Security Officer** – Interested in investing in improved visibility and control for preventing threats on remote workstations
- **Chief Information Officer** – Interested in saving on upfront infrastructure and gaining efficiencies across the entire IT stack

CHALLENGES

Time-consuming Deployment & Maintenance
IT and security teams are slowed down by the need to stand up additional hardware and configure policies for multiple siloed tools.

Inconsistent Prevention
Reliance on signatures and signature updates to stop attacks leaves organizations with remote machines at increased risk of attack.

Visibility & Detection Gaps
Dispersed workers, including IT and security teams, makes it difficult to identify threats and investigate alerts coming from the machines that they are responsible for securing. Delays in these investigations lead to a higher risk of monetary damages from a breach.

Inability to Track IT Configuration Drift
With workers being remote for weeks or months at a time, it's difficult for IT and security teams to audit, report, and remediate changes to configuration settings such as Bitlocker status, auto-update, and patches.

DISCOVERY QUESTIONS

- Who is your **incumbent endpoint security vendor** and when are you due to renew?
- Are you looking to **consolidate** security tools and **reduce the number of agents** on your endpoints?
- Are you reviewing your **work-from-home security program** for the rest of 2020?
- What challenges is your team dealing with as far as securing **the influx of remote machines**?
- What **visibility or context are you currently lacking** on those machines that is vital to the success of your security program?

TRIGGERS/USE CASES

- Slow deployment and time-consuming maintenance of on-prem security tools
- Inconsistent prevention of malware, ransomware and non-malware attacks
- Visibility & detection gaps for remote endpoints
- Inability to audit configuration drift across the enterprise at scale

CARBON BLACK BUNDLES

ENDPOINT STANDARD
- Next-gen Antivirus
- Behavioral EDR

RECOMMENDED

ENDPOINT ADVANCED
- Next-gen Antivirus
- Behavioral EDR
- + **Audit & Remediation**

ENDPOINT ENTERPRISE
- Next-gen Antivirus
- Behavioral EDR
- Audit & Remediation
- + **Enterprise EDR**

Note: *Next generation Antivirus and behavioral EDR features are available for Windows and Mac only. Linux features are included in the Audit and Remediation and Enterprise EDR functionality.*

WHY CARBON BLACK

- Simplifies and accelerates deployments from a cloud-based platform
- Eliminates the need to monitor and maintain on-premises infrastructure
- Consolidates endpoint security into a single console
- Flexible, behavior-based prevention policies that adjust to your environment's needs
- Gives prioritized alerts with full context via attack visualization
- Provides a platform to deploy any new application in days not months
- Combines multiple tiers of prevention, including malware signatures, machine learning, and behavioral prevention to provides protection against ransomware, never-before-seen attacks, and non-malware attacks

VMWARE CARBON BLACK RESOURCES

Access Sales Play Resources on the VMware Carbon Black Partner Connect page, including:

- Market and analyst reports
- Case Studies
- Sales script
- Customer email
- And more

OBJECTION HANDLING

"A lot of my users are remotely accessing data with mobile devices, but your platform doesn't cover mobile."
AV and EDR solutions are not nearly as effective on mobile devices, especially given the challenges of deploying them on personal mobile devices. However, the zero-trust approach taken by Workspace ONE provides a productivity- and privacy-focused strategy that is both effective and palatable for your employees.

"Your solution doesn't provide device control, so I won't be able to replace my traditional AV."
Device control is a top priority on our roadmap for 2020, but even without that functionality in the near term, the increased off-network visibility and prevention capabilities you'll gain from our platform will dramatically improve security for your remote workforce.

"Carbon Black doesn't support non-persistent VDI and instant copy."
Carbon Black currently prioritizes the protection of persistent VDI environments because they are most at risk of a compromise, lasting more than a few hours and most likely to contain sensitive information.

WHAT YOU NEED TO DO

- **Leverage** the VMware Carbon Black resources (left and on Partner Connect)
- **Register** your opportunities through the VMware Partner Connect Portal
- **Contact** your Carbon Black SE/Partner Specialist to arrange a demo for your customer