THE SITUATION

The platforms and features that enable omnichannel customer experiences have created security and compliance vulnerabilities. Today, regulations require retailers to be more and more accountable by proving that effective controls are in place to ensure the critical systems inside and outside the Card Data Environment (CDE) are protected. Additionally, attackers' techniques are getting more sophisticated, causing retail CIOs to increase security headcount, budgets and, in some cases, implement threat hunting teams.

73% of retail organizations said they’ve seen an increase in cyberattack sophistication over the past year

66% of organizations have encountered ransomware over the last year while 33% have experienced an island-hopping attack

40% of retail organizations said they lost revenue in 2019 as a result of a cyberattack

1 VMware Carbon Black, Holiday Season Cyber Heists Report
The VMware Carbon Black Cloud is a cloud-native endpoint protection platform (EPP) that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay. It delivers a line of products spanning the detection and response workflow through a single platform and one lightweight agent, offering retail organizations a single solution for reducing endpoint and workload risk and disrupting cyberattacks as they occur. With the VMware Carbon Black cloud you can:

Deploy Endpoint Detection and Response (EDR)

Traditional antivirus solutions provide organizations with preventive protection on known bad filenames—which can’t protect from the full spectrum of attacks. Specifically, traditional AV is architected to look for indicators of compromise (IOC) associated only with malware. Fileless and living-off-the-land (LotL) attacks are a blindspot for such solutions. VMware Carbon Black provides a more comprehensive solution that includes behavioral intelligence, which is compulsory to detect living-off-the-land and fileless attacks. With this in place, security teams can continually collect, analyze, and store endpoint activity, providing them with surveillance-like visibility to proactively hunt for threats or investigate a past incident.

Lock Down Critical Systems

In retail, it is imperative to protect corporate-issued devices, critical servers, and point of sale systems from malware and non-malware attacks. VMware Carbon Black lets you lockdown these systems to stop malware, ransomware, zero-day, and non-malware attacks. Built-in file-integrity monitoring and memory protection block unauthorized change, keeping your systems running safely and smoothly.

Prove Compliance

With the risk of attack ever present, it's important to audit systems regularly and establish remediation steps across all your security infrastructure. VMware Carbon Black allows you to assess the risk of your endpoints, in real time, and at scale. This eases the burden of managing complexity for teams by making it simple to find vulnerabilities and to achieve (and prove) compliance—streamlining security operations and saving teams time.

See: carbonblack.com/epp-cloud

To learn more about how the VMware Carbon Black Cloud can help secure your organization, contact us.