SolarWinds Breach

Tactical recommendations and VMware Carbon Black product updates

Summary

In December 2020, FireEye revealed that it had been breached. Subsequently, it was disclosed that the FireEye breach was part of a larger SolarWinds breach, where SolarWinds' software was leveraged for a supply chain attack, impacting a broad set of organizations. According to U.S. law enforcement officials, this attack was likely carried out by state-sponsored threat actors. In response to these series of events, VMware has taken several actions to inform and protect our customers.

Core principles to endpoint and workload security

At VMware, we believe there are three core principles to securing endpoints and workloads. We have built our solutions on these very principles. We align our capabilities to these core principles and have updated our solutions using findings from our leading threat research team.

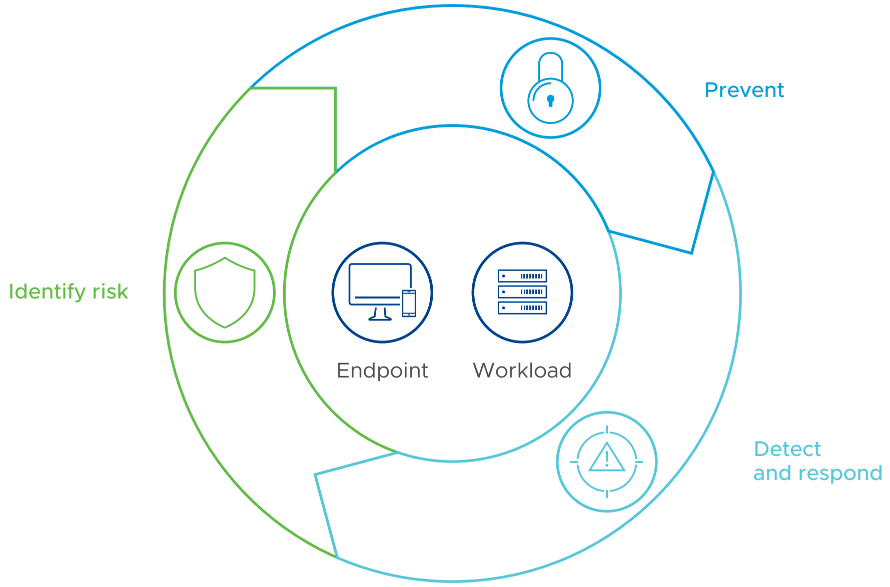

FIGURE 1: VMware's core principles for securing endpoints and workloads.

Identify risk – You must reduce the attack surface by ensuring you can identify risk and harden your environments. Risk can be identified on initial install or during the lifecycle of the endpoint and workload utilizing tools such as VMware Carbon Black® Cloud Audit and Remediation™ and vulnerability management.

Prevent – You must expand the prevention net. It's important to have a tiered approach to prevention that goes beyond traditional point-in-time indicators. That's why, in VMware Carbon Black Cloud Endpoint™ Standard, we have implemented techniques such as dynamic analysis, cloud-based reputation, ransomware decoys, and machine learning, all combined to provide ongoing analysis that prevents a much broader range of unwanted files, both pre- and mid-execution.

Detect and respond – You need to be able to zoom in and zoom out when a breach happens. To zoom in, you need automated detection intelligence, so you know when and where to start an investigation. This requires the right data and analysis tools. To zoom out, you need to rewind the tape, so you can go from initial detection to understanding the entire campaign.

Tactical recommendations

Protecting endpoints and workloads requires a different approach—an approach that reduces risk, shrinks the attack surface, and understands behavior. By using VMware Carbon Black products, you are able to reduce the amount of dwell time an attacker remains silent within an enterprise, and quickly detect and mitigate lateral movement to contain the attack.

NGAV and behavioral EDR

Next-generation antivirus (NGAV) and behavioral endpoint detection and response (EDR) decrease risk and minimize the attacker's ability to utilize different techniques following a breach. Our solutions have tamper prevention that mitigates the preventative capabilities from being turned off.

VMware Carbon Black Cloud Audit and Remediation

We also have the capability to query more than 1,500 IT and security configurations, as well as create our own custom queries with our live query capability. During an investigation, you are able to create customer queries specifically targeting the critical assets that have been identified as being at risk in your environment.

Vulnerability management

By utilizing vulnerability management, we are able to collect and display vulnerabilities that exist in your infrastructure in a prioritized way. This means that security and IT will have visibility into, be able to communicate clearly about, and understand which workloads are the most critical to update. This allows IT and security to prioritize and harden the environment. Common vulnerabilities and exposures (CVEs) from the FireEye tool set that exist in your environment are automatically detected and displayed in your environment. These CVEs are prioritized based on contextual information.

VMware Carbon Black Cloud Enterprise EDR

Investigations that typically take days or weeks can be completed in just minutes. VMware Carbon Black® Cloud Enterprise EDR™ collects and visualizes comprehensive information about endpoint events, giving security professionals unparalleled visibility into their environments. Carbon Black Cloud Enterprise EDR customers can scale their investigations quicker by understanding tactics, techniques and procedures utilizing hundreds of detections available in the platform. Customers can subscribe to the feed in the VMware Carbon Black Cloud™ console by selecting Enforce from the left-hand menu bar > Watchlists > Add watchlists (upper-right corner). Then select the AMSI Threat Intelligence feed and click Subscribe. The antimalware scan interface (AMSI) support will hook and provide visibility into PowerShell, Windows Script Host, User Account Control, Windows Management Instrumentation (WMI) events, JavaScript, and VBScript.

Enhancements post SolarWinds breach

<table>
<tr><th>PRODUCT</th><th colspan="3">ENHANCEMENTS</th></tr>
<tr><td rowspan="4">VMware Carbon Black Cloud Endpoint Standard</td><td colspan="3">The VMware Threat Analysis Unit™ deployed targeted behavioral prevention rules focused on the SolarWinds breach and moved immediately to prevent execution of all known compromised files. To take full advantage of out-of-the-box prevention, customers should ensure they are running the latest 3.6 sensor and confirm on the Policies page that they are blocking all types of malware from executing (known, suspect, and potentially unwanted program [PUP]). Deploy rules to a small subset of sensors, assess, and then define permissions to reduce false positives. If you don't find false positives, deploy across additional groups.</td></tr>
<tr><td>PROCESS</td><td>OPERATION</td><td>ACTION</td></tr>
<tr><td>Known malware</td><td>Runs or is running</td><td>Terminate process</td></tr>
<tr><td>Suspect malware</td><td>Runs or is running</td><td>Terminate process</td></tr>
<tr><td>VMware Carbon Black Cloud Audit and Remediation</td><td colspan="3">Use to search for vulnerable SolarWinds versions.
Use to apply Yara signatures associated with either SUNBURST or FireEye tooling.</td></tr>
<tr><td>Vulnerability management</td><td colspan="3">Automatically identify and prioritize vulnerabilities associated with FireEye and SUNBURST.</td></tr>
<tr><td>VMware Carbon Black Cloud Enterprise EDR</td><td colspan="3">In addition to the hundreds of detections already available to our customers, the VMware Threat Analysis Unit vetted and published more than 20 new detections related to the FireEye and SolarWinds disclosed intelligence. Each of these detections is run against new data being collected as well as historical data previously collected by the product. These detections were deployed as part of the VMware Threat Analysis Unit feeds for advanced threats, suspicious indicators, and AMSI threat intelligence. Full details on the updates can be found on the VMware Carbon Black User Exchange.</td></tr>
<tr><td>VMware Carbon Black® EDR™</td><td colspan="3">In addition to the hundreds of detections already available to our customers, the VMware Threat Analysis Unit vetted and published more than 20 new detections related to the FireEye and SolarWinds disclosed intelligence. Each of these detections is run against new data being collected as well as historical data previously collected by the product. These detections were deployed as part of the VMware Threat Analysis Unit feeds for advanced threats and suspicious indicators. Full details on the updates can be found on the VMware Carbon Black User Exchange.</td></tr>
<tr><td>VMware Carbon Black® App Control™</td><td colspan="3">We recommend that all endpoints be set to High Enforcement, default-deny, with Suspicious Command Line Protection and Suspicious Application Protection Rapid Configs enabled. If you do not use SolarWinds in your environment, and you are in High Enforcement, installs of the impacted SolarWinds versions will be blocked.</td></tr>
</table>

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com