Netskope and Carbon Black

Threats propagating in the cloud

With more than 900 cloud apps in the average enterprise and one-third of business data now in the cloud, organizations are largely unprotected from cloud-based malware. The cloud malware attack "fan-out" effect exacerbates this, with cloud-interconnected endpoints creating an opportunity for exponential malware propagation. The increasing complexity of the threat landscape and frequency of attacks has also led to an unprecedented shortage of skills and cognitive overload for IT security professionals.

For organizations to combat cloud-based threats, they require:

- Malware detection, in and en route to or from cloud apps
- Communication with endpoint devices to block, remove, or remediate malware
- Correlated and continuous threat intelligence between cloud and endpoint devices to increase detection confidence
- Endpoint watchlists updated with the latest indictors of compromise learned from the cloud

The Netskope-Carbon Black solution

Carbon Black Enterprise Response is the industry's most complete endpoint detection and response solution available. It provides security teams a single platform for detecting malicious behavior, hunting threats, disrupting attacks. Only Carbon Black Enterprise Response continuously records all endpoint activity, centralizes and correlates that data with unified intelligence sources, and reveals a complete kill chain that pinpoints attack root cause to power live threat containment, banning and remediation activities.

Netskope is the leading cloud access security broker (CASB). Netskope gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organizations to direct usage, protect sensitive data, and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.

Together, Carbon Black and Netskope help organizations:

- Expand their kill chain view and response to include cloud-propagated malware
- Make endpoint threat protection smarter by incorporating intelligence from the cloud
- Close the cloud threat remediation loop by alerting and coordinating with endpoints

Value for Joint Netskope-Carbon Black Customers

- Get more value out of Carbon Black investment by incorporating cloud-based files, threats, anomalies, and IOCs
- Gain visibility into potential threats hidden in cloud-bound SSL-encrypted traffic
- Protect against and remediate threats propagating in the cloud

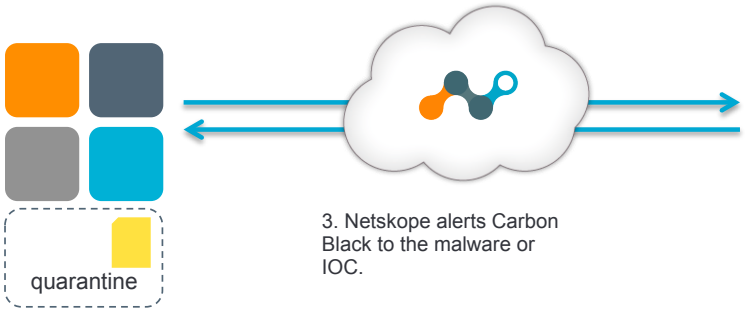
How the integration works

- **Malware.** Netskope detects malware in or en route to cloud apps and alerts Carbon Black on the endpoint. If the malware has not yet reached the endpoint, Carbon Black is able to watch for and block it. If the malware has reached the endpoint but not yet detonated, Carbon Black can delete it. If the malware has reached the endpoint and has detonated, Carbon Black is prepared to kill its processes and isolate the endpoint. Netskope can also serve as a second verification for suspicious files found on the endpoint.
- **Threats.** Netskope identifies endpoints that are visiting risky or malicious websites or IP addresses and alerts Carbon Black on the endpoint. Carbon Black provides intelligence about the threat, and both Carbon Black and Netskope can increase their confidence that the endpoint is compromised and take action.
- **User Behavior.** Netskope identifies anomalous cloud behavior (e.g., excessive uploads or activity at an unusual hour) and alerts Carbon Black on the endpoint. Carbon Black provides intelligence about the processes or files on the endpoint associated with the activity, and both Carbon Black and Netskope can increase their confidence that the behavior is malware-related and take action.
- **IOC Detection.** Netskope identifies potential indicators of compromise in user cloud activity or files found in cloud apps and checks in with Carbon Black Enterprise Response. If there is a match to those IOCs on the endpoint, Carbon Black takes appropriate action, such as killing processes and isolating the endpoint.

Netskope-Carbon Black (Malware or IOCs)

1. Netskope identifies malware or related IOCs in or en route from cloud app.

2. Netskope quarantines malicious file, notifies user, and blocks all future versions of malware seen across our cloud.



3. Netskope alerts Carbon Black to the malware or IOC.

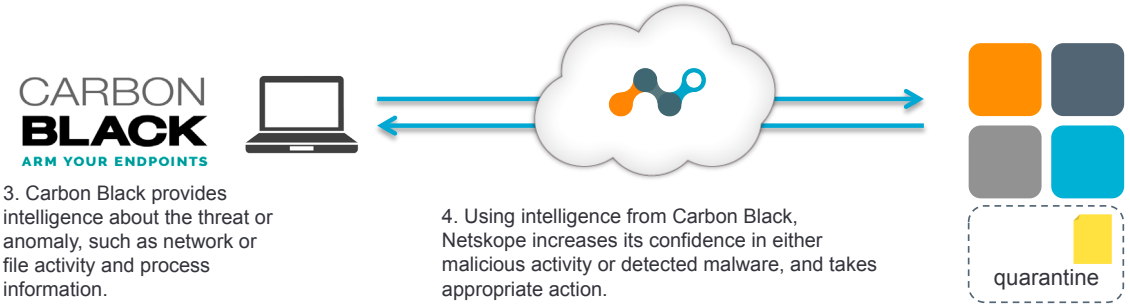
4. Carbon Black takes action. If the malware has not yet reached the endpoint, it can watch for and block the malware. If the malware has reached the endpoint but not yet detonated, it can delete it. If the malware has reached the endpoint and has detonated, it can kill its processes and isolate the endpoint. If it is an IOC, Carbon Black can take appropriate action.

5. (optional) Carbon Black can send suspicious files found on endpoint to Netskope for evaluation. If malicious, Netskope blocks all future versions of malware seen across our cloud.

Netskope-Carbon Black (Threats, Anomalies)

1. Netskope identifies poor reputation users or anomalous activity in cloud apps.

2. Netskope alerts Carbon Black.



3. Carbon Black provides intelligence about the threat or anomaly, such as network or file activity and process information.

4. Using intelligence from Carbon Black, Netskope increases its confidence in either malicious activity or detected malware, and takes appropriate action.

5. If Netskope-determined malicious activity involves an identified malicious file, it will quarantine the file and notify the user. Netskope blocks all future versions of malware seen across our cloud.