Netskope and Cyphort

Threats propagating in the cloud

With 4.1% of enterprises' sanctioned cloud apps laced with malware and total cloud app usage totaling more than 20x that of sanctioned apps, organizations are largely unprotected from cloud-based threats. The cloud malware attack "fan-out" effect exacerbates this, with the cloud's tapestry of cloud-connecting 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 malware, they require:

- Detection of suspected malware in and en route to or from cloud apps
- Detonation of suspected malware in a sandbox environment
- Remediation in the cloud and on user endpoints

The Netskope-Cyphort solution

Cyphort is the next generation APT defense solution for enterprise organizations. Cyphort provides a single pane of glass across perimeter and laterally moving threats, correlates threat signals before and after an incident, while eliminating noise from false alerts and red herrings. Cyphort has leveraged the power of machine learning and data science to build a next generation threat detection engine that evolves ahead of the threats. A virtualized deployment model combined with open API based integration allows customers to address APT security gaps across global locations while leveraging their existing investments in perimeter and endpoint security for threat defense.

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, Cyphort and Netskope help organizations:

- Extend Cyphort's next-generation APT defense to cloud apps
- Gain visibility into SSL-encrypted cloud traffic for threat monitoring
- Close the remediation loop by alerting endpoint systems

Value for Joint Netskope-Cyphort Customers

- Get more out of Cyphort investment by incorporating cloud-based threats
- 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

- Netskope makes suspicious files available to Cyphort by inspecting files in a cloud app or within traffic en route to or from, a cloud app
- Traffic can include on-premises, remote, or even that originating from a mobile device
- Suspicious files are routed to Cyphort Core for analysis via Cyphort's REST API
- Netskope takes action based on Cyphort result (e.g., quarantine or block and notify)
- The result may be shared with endpoint threat protection solutions via integration (e.g., with Carbon Black) to take further action if malware is seen on the endpoint

Netskope-Cyphort Integration