skyhigh

CYPHORT

SOLUTION BRIEF

## Benefits

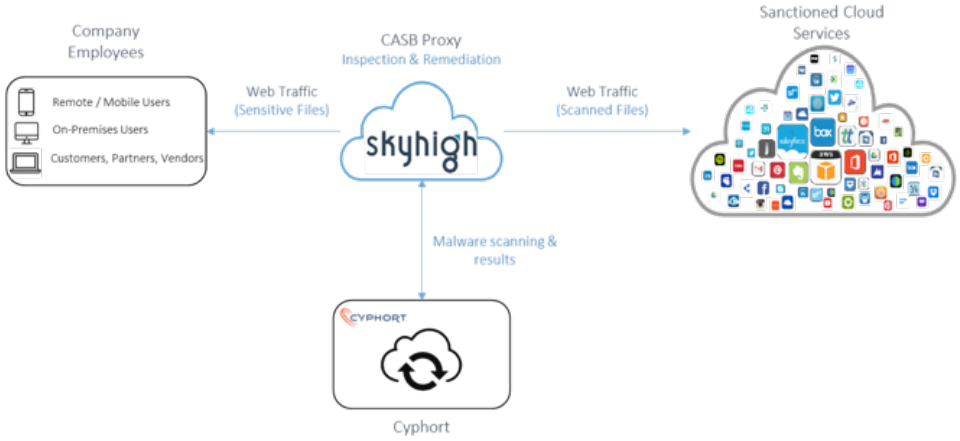
- **Collaborate effectively** with teams and third parties without losing control of sensitive company data
- **Seamless deployment** of the combined solution that does not disrupt end-user workflows or require any endpoint agents
- **Protect company assets** from malware infections, including protection from zero day threats
- **Pervasive cloud control** that enables policy enforcement for BYOD, off-network, and third party users

# Skyhigh & Cyphort

### Protecting Enterprise Cloud Services from Malware-Driven Threats and Data Loss

As business users are increasingly adopting cloud services, companies are concerned about the growing impact and frequency of malware attacks. The use of file sync and share services has amplified the impact of these attacks as a malware infected file is automatically downloaded to the desktops and mobile devices of several collaborators. Enterprises are seeing massive productivity benefits from cloud services and are looking for ways to allow employees to use these services while securing their data and systems.

Skyhigh and Cyphort have partnered to enable companies to leverage the benefits of cloud services without compromising the security of their data. The combined solution allows customers to inspect files being uploaded to cloud services for malware and enforce policies accordingly. Skyhigh uses the API integration with Cyphort to send the file for malware inspection. Cyphort inspects this file using its Dynamic Detection method, which combines machine Learning with behavioral inspection analytics, and returns the results. Skyhigh accordingly applies remediation to either allow, block or quarantine the file.




## Capabilities

### Dynamic Malware Detection

Scan files for malware using a machine learning engine combined with behavioral inspection analytics to adapt to evolving malware and new threat techniques, including evasion tactics

### Malware Lifecycle Coverage

Detect threats across the threat lifecycle and correlates the information as threat changes state across Exploit, Download, Command & Control, Lateral Spread and Internal Threat Activity

### Broad Malware Coverage

See all threats irrespective of which vectors (web, email or file share) they utilize to spread and the platforms (Windows, Mac, Android, Linux) they are targeting

### Minimize False Positives

Accurate malware detection combined with the knowledge of intent, target value, cyber kill-chain stage and security posture of the target

### On-Demand Data Scan

Examines existing content in all or specific folders to identify sensitive data subject to compliance requirements or security policies

### Cloud Data Loss Prevention

Enforces DLP policies based on data identifiers, keywords, and expressions and supports alerting, blocking, encrypting, tombstoning, and quarantining actions

### Enterprise-Class Remediation

Provides multiple remediation options including block, encrypt, quarantine, and delete and enables tiered response based on the severity of the violation

### Policy Violation Management

Offers a unified interface to both review and remediate all DLP, access control, or collaboration policy violations

## Use Cases

### Malware Detection – On-demand

Using Skyhigh and Cyphort, companies can examine data in existing cloud deployments for malware and other policy violations. For example, if a company wants to examine data in its existing Box deployment for policy violations and malware, it can use Skyhigh and Cyphort to run an on-demand scan of the existing Box deployment. As Skyhigh inspects the files the compliance and security policy violations, it sends the files to Cyphort for malware inspection. Based on the scan results, Skyhigh can block or quarantine the files.

### Malware Detection – Inline

The Skyhigh-Cyphort solution can be used to inspect files uploaded and downloaded by employees from sanctioned cloud services such as Box and Office 365 to identify malware. For instance, as an employee uploads a file into OneDrive, Skyhigh inspects the file for compliance violations an send the file to Cyphort for malware inspection. If the result is positive for malware, then Skyhigh can block the upload and quarantine the file.

## About Skyhigh

Skyhigh Networks, the world's leading Cloud Access Security Broker (CASB), enables enterprises to safely adopt SaaS, PaaS and IaaS cloud services, while meeting their security, compliance and governance requirements. With more than 600 enterprise customers globally, Skyhigh provides organizations the visibility and management for all their cloud services, including enforcement of data loss prevention policies; detecting and preventing internal and external threats; encrypting data with customer-controlled keys; and implementing access-control policies. Headquartered in Campbell, Calif., Skyhigh Networks is backed by Gridlock Partners, Sequoia Capital, Thomvest Ventures, Tenaya Capital and other strategic investors. For more information, visit www.skyhighnetworks.com.

## About Cyphort

Cyphort, Inc., provides the Adaptive Detection Fabric, a distributed Security Analytics solution that delivers advanced threat defense and improves operational efficiency for SOC and IR teams within mid- and large-size organizations. Based in Santa Clara, California, the company was founded in 2011 and distributes its software through direct sales and channel partners across North America and international markets. Learn more at www.cyphort.com.

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com

Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com