CYLANCE

CylanceHYBRID™

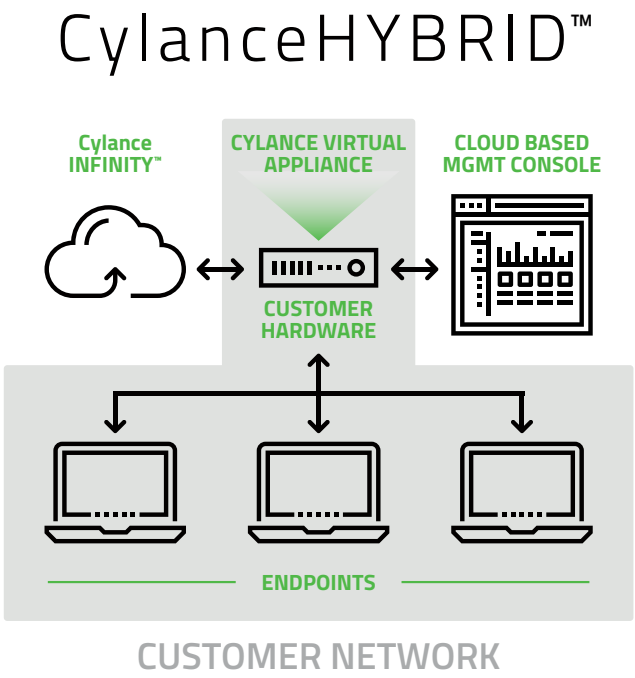
Security Through a Single Connection

The Limited Connectivity Dilemma

Some companies operate with limited Internet connectivity due to design or operational circumstances. Such businesses use restricted/guarded networks, a private cloud, or operate in remote areas with limited connectivity. CylanceHYBRID ensures these businesses remain secure by directing all Cylance communication through a single connection.

Single-Point Connectivity Solution

CylanceHYBRID facilitates security-related communication between the cloud and local infrastructure without exposing the local network to the Internet. The standard configuration of the Cylance® agent requires endpoints to individually communicate with the cloud for updates, but CylanceHYBRID requires only a single connection to the cloud. It downloads the endpoint updates once, then distributes them over the internal network.



By routing all Cylance communication through CylanceHYBRID, the connectivity requirements for maintaining a secure environment are greatly reduced. Overhead is also reduced as CylanceHYBRID stores centroids (mathematical threat detection models) locally rather than requiring each endpoint to download their own copy.

This model is especially useful for organizations with heavily restricted networks, for example:

- Federal and Defense
- Financial
- Industrial Control Systems
- Healthcare
- Manufacturing
- Retail
- Aviation
- Oil and Gas

Industries that operate in remote or technologically under-served areas may also benefit from the single-point connection capability of CylanceHYBRID. Examples include cruise lines, emergency relief organizations, and resource extraction companies such as mining, oil, and lumber, which all rely on 3G/4G connectivity.

About Cylance

Cylance uses artificial intelligence to deliver prevention-first, predictive security products and specialized security services that change how organizations approach endpoint security. Cylance's security solutions provide full spectrum predictive threat prevention and visibility across the enterprise, combatting threats such as malware, ransomware, fileless malware, malicious scripts, weaponized docs, and other attack vectors. With AI based malware prevention, application and script control, memory protection, device policy enforcement, root cause analysis, threat hunting, automated threat detection and response, coupled with expert security services, Cylance can protect endpoints without increasing staff workload or costs.

CylanceHYBRID Details

Data Handling

Data Type	Details
Centroid Updates	Centroids are mathematical models that analyze files to determine if they are threats. CylanceHYBRID creates a local repository of the latest centroids.
Agent Update Binaries	CylanceHYBRID downloads and distributes copies of the latest Cylance agent updates.
Environment Updates	Changes to security policies, permissions, and other management changes initiated by the Cylance Cloud Console are relayed to the environment through CylanceHYBRID.

Hardware Requirements

CylanceHYBRID deploys as a virtual appliance. It requires the following resources, which may change with further testing:

RAM: 4GB minimum, 8GB recommended

CPU: 3.0 GHz 2 core minimum, 3.0 GHz 4 core recommended

Disk: 100 GB minimum, 1TB recommended

+1-844-CYLANCE
sales@cylance.com
www.cylance.com

CYLANCE

20180928-0238