CylanceAPI™

Scalable, Repeatable, and Automated Workflow Integration

The Case for Integration

To improve the operating efficiency of any security team, it is imperative that the security tools it uses to protect the organization easily integrate and share critical security-related information in a scalable, repeatable, and automated fashion.

CylanceAPI is a series of RESTful APIs that deliver easy access to CylancePROTECT® data, administration, and investigation tasks to enable full integration of CylancePROTECT into an existing security framework and workflows. Unlike other security product integration frameworks that require extensive coding expertise, CylanceAPI allows anyone to use CylancePROTECT data without being an expert programmer. With straightforward data structures and the ability to test integrations easily, CylanceAPI sets the standard for smooth product integration.

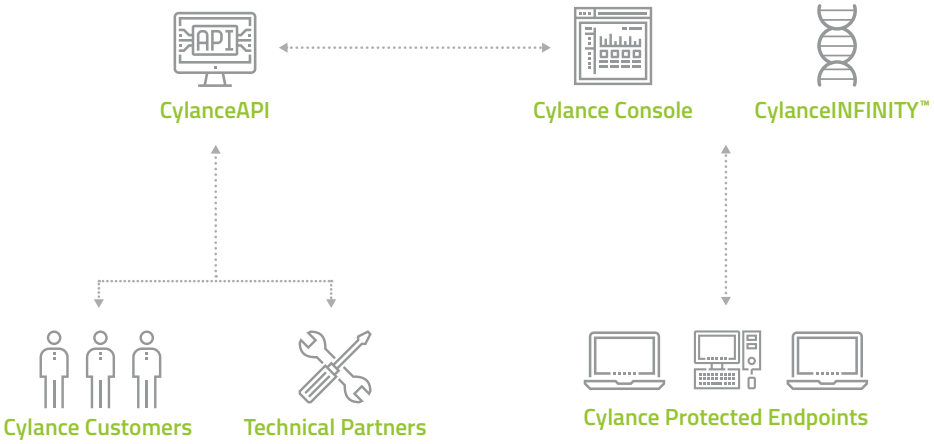
For CylancePROTECT customers, CylanceAPI allows security teams to easily automate recurring tasks such as adding new devices to the environment and performing routine security operations.

Cylance technical partners can make use of the CylanceAPI framework to integrate CylancePROTECT into other third-party tools such as orchestration and case management products.

The following APIs are available within CylanceAPI:

- **Tenant User:** Reporting, creation, and management of tenant uses (user, zone manager, and admin)
- **Device:** Reporting and management of devices belonging to a tenant
- **Zone:** Creation and management of zones belonging to a tenant
- **Policy:** Creation and management of device policies belonging to a tenant
- **Threat:** Reporting and management of threat events detected by CylancePROTECT
- **Global List:** Management of the Global Safe List and the Global Quarantine List within a tenant

CylanceAPI Workflow



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.

Common Use Cases

The following uses cases are supported by CylanceAPI:

- Bulk Actions
  - Move devices from one zone to another
  - Update policy for multiple devices
  - Add policy-level exclusions
- Reporting
  - Device health and summary
  - Threat overview
- Device Grouping and Management
  - Zone creation
  - Auto device-zone assignment
- Activity Response
  - Add new files to global safelist and quarantine lists
  - Waive and quarantine incoming threats
- Event Correlation
  - Integrate CylancePROTECT data with other security tool data
  - Improve the ability to identify advanced threats

CylanceAPI Benefits

For Cylance Customers	For Cylance Technical Partners
Use the rich CylancePROTECT data to improve security posture ▪ Use CylancePROTECT threat data in other security tools in the environment ▪ Correlate threat data to further understand the attack surface ▪ Improve situational awareness across the security team	**Automate common tasks to improve IT and security team efficiency** ▪ Reduce the time and potential errors associated with common IT tasks such as adding devices to the environment ▪ Drive consistency across the IT and security team ▪ React quickly and apply changes quickly across the environment

For more information on how to make use of these APIs, visit www.cylance.com.

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
18201 Von Karman Avenue, Suite 700, Irvine, CA 92612

20180215-0201