CylancePROTECT® Cloud

How Technology Ensures the Security of our Products, the Cloud, and our Software Development Process

Benefits

- Highly available, scalable, and secure
- Less cumbersome than legacy security products
- Reduced operational costs
- Ease of maintenance
- Encryption, authentication, audit logging, and penetration testing
- Flexible scaling
- 24x7 data center and software support

CylancePROTECT's console and back-end services are hosted on Amazon Web Services (AWS). It is a highly available, scalable, and secure service that makes deploying CylancePROTECT less cumbersome than legacy security products. Our cloud service provides customers:

- Lower operational costs by procuring hardware/resources to run the service/console
- High availability and performance monitoring of the service
- Ease of maintenance by applying updates to our service
- Safeguards such as encryption, authentication, audit logging, penetration testing, etc.
- Flexible scaling of service as needed on demand
- 24x7 data center and software support operations

How We Use The Cloud

Cylance uses the cloud for data processing and hosting our cloud-based management. CylanceINFINITY ENGINE, at its heart, is a massively scalable data processing system in the cloud capable of generating highly efficient mathematical models to solve the malware problem. It works by collecting data, training and learning from the data, and calculating likely outcomes based on what it sees. It's constantly getting smarter from environmental feedback and a continual stream of new data from all around the world.

Cylance uses the cloud to host its cloud-based management console, allowing customers to manage all of their CylancePROTECT agents in one location.

Below is an overview of the architecture of CylancePROTECT and its interactions with the cloud.

The CylancePROTECT agent is lightweight when installed on endpoint devices and communicates with the cloud service to:

- Pull down policy
- Send information about threats and hosts
- Receive commands sent out through the console
- Upload threat samples (optional)
- Download agent updates

The agent uses secure communications by using Transport Layer Security (TLS) for privacy and data integrity. In addition, the agent and cloud connection also uses digitally signed certificates to authenticate the agent to the cloud. The agent also authenticates against the shard as agents are locked to shards cryptographically. Cylance also supports strong authentication via external identity providers, such as OneLogin & OKTA, Active Directory Federation Services, Azure Active Directory, and PingOne. These SAML integrations allow for multi-factor authentication and the ability to restrict portal usage to defined source IP ranges and other admin-defined protections.

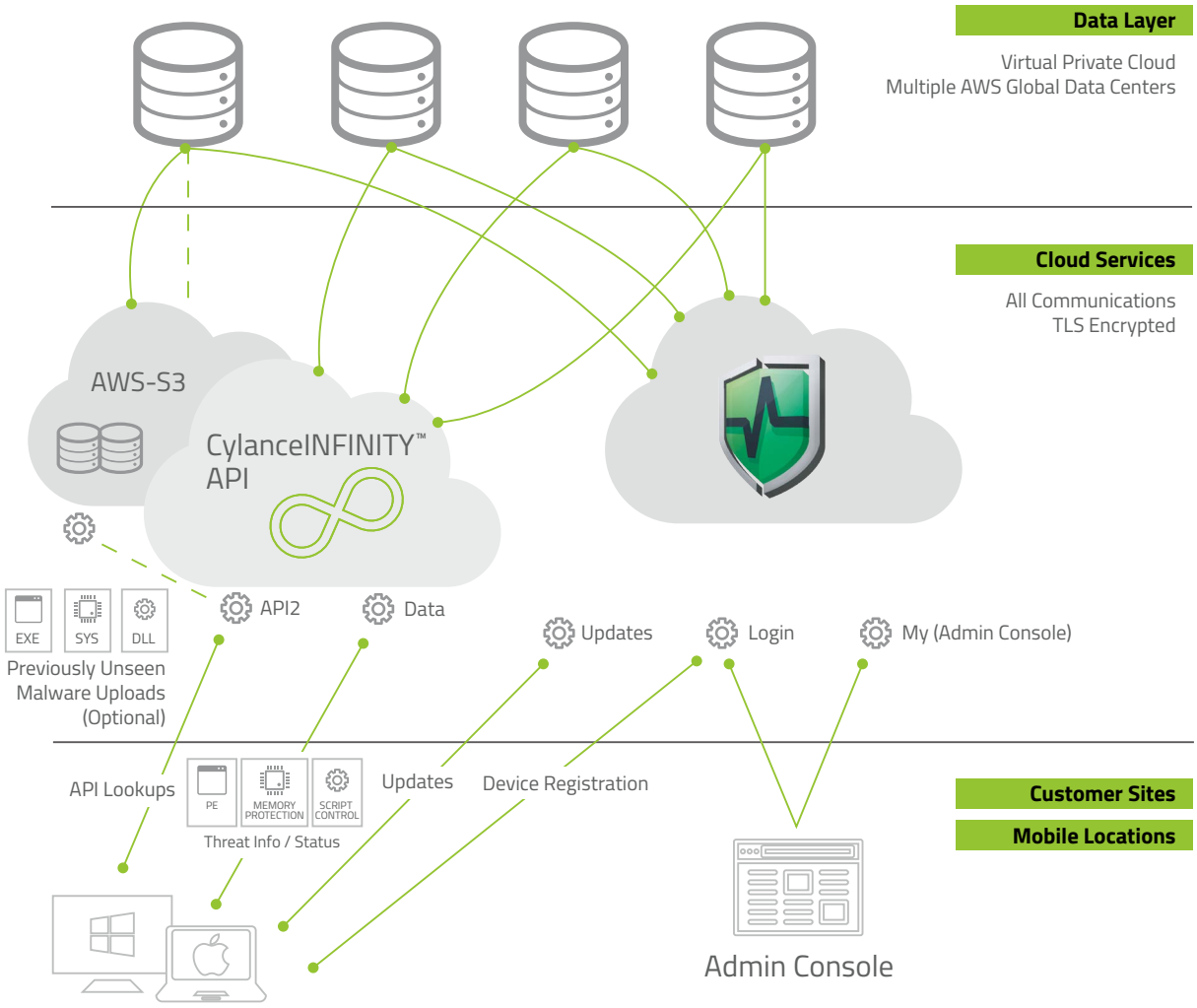

Figure 1 - Architecture diagram illustrating Cylance technology

We outline the steps taken to ensure the data integrity, security, availability, and scalability of CylancePROTECT in the following sections.

Data Control, Privacy, and Portability

Multi-tenancy — Databases are run within Amazon's Relational Database Service (RDS). Amazon RDS automatically patches and backs up the database, enabling point-in-time recovery. Critical and private data is isolated with, and protected using the encryption on RDS with both key management and rotation to ensure customer data is never exposed. Using the multi-zone deployment option for mission-critical workloads ensures high availability and provides a built-in automated failover from the primary database to a synchronously replicated secondary database in case of a failure. We support deployments in AWS GovCloud and can also provide dedicated databases for customers at an additional cost. Cylance uses a multi-tier architecture and never exposes RDS instances to the Internet.

Data Security — Cylance only collects and holds minimal customer data. No data is shared among customers. We utilize OAuth for administrator authentication to limit exposure to sensitive customer login details, which means that no login credentials can be retrieved, even if someone accessed our entire database.

Data Privacy — Samples are immediately anonymized when they are submitted to Cylance and we do not track which customers submitted a particular file. We anonymize all inputs from the API perspective. We do aggregate some data to calculate metrics and use individualized API keys for accounting and abuse prevention, but cannot link individual submissions to API keys. As an example, we can tell if a customer is using the service, and at what rate, but it is impossible to generate a report detailing information they have retrieved.

Customers have the option of uploading portable executable files to CylancePROTECT, which generates additional evidence such as threat indicators by analyzing uploaded

files. The uploaded files are stripped of any origination elements and simply referenced by cryptographic hashes. This prevents identifying who submitted any particular file.

CylancePROTECT collects a set of data from each device on which it is installed. Below is the data that CylancePROTECT generates and transfers to our cloud servers.

User account information for each CylancePROTECT administrator login	
Email address	
Device details for each device running a CylancePROTECT Agent	
Operating system, version and service pack	Windows Security settings enabled/disabled Antivirus Anti-malware Firewall UAC Windows Update Network Access Protection
Hostname and FQDN	Last logged in user account name
IP address(es)	CylancePROTECT agent version
MAC address(es)	Distinguished name, Group membership from Active Directory
Unknown executables	Hash and file uploaded to cloud (if enabled in policy)
Threat details for every threat reported by a CylancePROTECT Agent	
Location on disk and Drive type (USB|Internal|Network, etc.)	File owner
SHA256, MD5 and SHA1	File path
Cylance score	Created/Access/Modified date time
Certificate information	Publisher information
User name, Group membership from Active Directory	File sample (optional - uploaded to CylanceINFINITY ENGINE)
Operational metrics about the CylancePROTECT service running on each endpoint	
CPU user %	Paged memory size 64 (K)
CPU priv %	Peak paged memory size 64 (K)
CPU total %	Paged system memory Size 64 (K)
Thread count	Nonpaged system memory size 64 (K)
Handle count	Working set private memory (K)
Working set 64 (K)	Elapsed time
Peak working set 64 (K)	Io data bytes per second
Private memory size 64 (K)	Page faults per second
Virtual memory size 64 (K)	Bandwidth usage
Peak virtual memory size 64 (K)	Agent logs (optional)

Data Portability — We allow exports of many pieces of information in CylancePROTECT's console. Users can extract their threat and device data and take it with them, or back it up locally. CylancePROTECT's APIs let customers extract this information programmatically.

Security

AWS is a secure cloud services platform, offering compute power, database storage, and content delivery that utilizes broad security certification and accreditation, data encryption at rest and in-transit, hardware security modules, and strong physical security that provides a highly secure environment. All cloud resources are hosted in a virtual private cloud (VPC) environment. This means that by default, the CylancePROTECT network is completely isolated – both from the outside world and all other AWS customers. Additionally, all resources inside the VPCs are protected using NACLs and AWS Security Groups as additional layers of defense.

We host all externally facing resources in an isolated demilitarized zone (DMZ). A DMZ is a network segment that is behind an externally facing firewall, with another internally facing firewall that blocks direct access to the rest of our systems. We further reduce this attack surface by utilizing AWS-controlled load balancers that do not give direct Internet access to any of our resources, only permitting controlled access from and to very small number of selected hosts. This means a greatly reduced attack surface where approximately 95% of our hosts do not expose any resources at all to the Internet. All other hosts that have a need to expose services such as the web management console has filtering applied at least at the host (SG) and network layer (NACL) layer. All data in transit is encrypted using TLS version 1.2. In cases where TLS isn't available on legacy devices, we use the highest level of security provided by the endpoint running the CylancePROTECT agent.

The host data in the database shards are separate for each customer and is not shared between shards. The only back hauled data from shards is anonymized portable executables (PE) files from customer tenants to the cloud where it processes/moves the anonymized PE data to be stored, secured and classified, and finally added to the sample corpus for future versions of the model.

All access for operations within our VPCs is controlled by an VPN configured to only use strong cryptography. It uses usernames, passwords, individualized certificates and a secondary two-factor authentication token.

We utilize Amazon Identity and Access Management to prescribe security policies for access everywhere. We have no default open resources within our AWS infrastructure. Each role within the organization has security policies that constrain the level of access. All access to any AWS resource by any actor is logged and frequently reviewed using CloudWatch (logs) and CloudTrail (API), which are independently audited and certified to create a very trustworthy logging infrastructure.

All hosts have additional detective security controls (e.g., host IDS) in place. To ensure no temporary files or swap space data is ever exposed, EC2 instance volumes are encrypted.

Availability and Scalability

Amazon runs one of the best connected networks. AWS datacenters are massively cross-connected to every major backbone provider. Details on the AWS global infrastructure can be found on Amazon's website. Additionally, AWS offers large interconnect points at nine global centers, with more than 100 edge connections, ensuring high likelihood of continued availability. We could mirror our external presence to any of the nine major centers with very little effort.

The Cylance DevOps team is responsible for uptime and currently tracks to 99.95% availability. Customers are notified about all planned maintenance. Unplanned outages trigger email notifications and are posted on the Cylance Customer Support Portal. Even in the event of an unexpected outage of the cloud service, all devices are fully protected. The CylancePROTECT agent can analyze and quarantine threats autonomously without a cloud connection. There is no loss of protected devices' logging data.

AWS is one of the most scalable cloud-based web services available today. A recent report found that a third of Internet users access at least one site hosted on AWS on an average day. AWS receives around 1% of all Internet traffic. Many of the most popular sites use AWS exclusively, while many more use it in some capacity. AWS clients include the FDA, NASA/JPL, Centers for Disease Control and Prevention, Comcast, Unilever, Siemens, Novartis, Instagram, Netflix, Pinterest, and Salesforce.com.

Product Certifications

Cylance is also pursuing product certifications to demonstrate leadership in product security and to ensure we follow a standardized approach to security assessments, data handling, and continuous monitoring.

We are currently in the process of achieving FedRAMP certification to ensure the cloud components of our solutions follow a standardized approach to security assessment, authorization, and continuous monitoring. This certification will provide and demonstrate consistent application of existing security practices, increase confidence in security assessments, and ensure we are continuously monitoring our cloud solution for security.

Additionally, we have other third-party validation for PCI and HIPAA/HITECH. CylancePROTECT has been certified 100% compliant with HIPAA/HITECH malicious software protection, detection, and reporting requirements. The certification is made by DirectDefense, a leading provider of HIPAA/HITECH security assessment services to industries, such as healthcare and insurance, that process, store or transmit electronic protected health information (EPHI). CylancePROTECT also achieved 100% PCI-DSS Requirement 5 compliance certification, which states that all organizations must run anti-malware solutions to protect payment card data.

CylancePROTECT is not under any US export control restrictions. CylancePROTECT has an EAR99 designation.

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