CylancePROTECT® Cloud

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 traditional security products. Our cloud service saves clients the trouble of:

1. Procuring hardware/resources to run the service/console
2. Monitoring availability and performance of the service
3. Applying updates to our service
4. Securing the service through audit logging, pen testing, fixing vulnerabilities, etc.
5. Scaling the service as needed on demand

How We Use The Cloud

CylancePROTECT Console – A web application that provides group and device management, reporting, dashboard and workflow

CylancePROTECT Agent - A lightweight agent installed on endpoint devices, which communicates with the cloud service to:

1. Pull down policy
2. Send information about threats and hosts
3. Receive commands sent out through Console
4. Upload threat samples (optional)
5. Download agent updates

We outline the steps taken to ensure 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. Data can be shared by tenant for physical isolation or by size for logical isolation and scaling optimization. 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 charge.

Data Security - Cylance® only collects and holds minimal customer data. No data is shared among customers. We utilize OAUTH type authentication to limit exposure to sensitive customer login details, which means that no login credentials could be retrieved if somebody 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 never 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 us from identifying who submitted any particular file.

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 essentially datacenter space, posing the same security risks as any datacenter, including ones owned by clients who choose internal hosting. 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. No packets can be transmitted to our systems without our knowledge.

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 to a very small number of selected hosts. This means that about 95% of our hosts do not have any open ports connected to the Internet. All data in transit is encrypted using TLS. In cases were TLS isn't available on legacy devices, we use the highest level of security provided by the endpoint running the CylancePROTECT agent.

All access for operations within our VPC is controlled by an SSL 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.

Availability

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 here 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.

Scalability

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 one percent 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.

About Cylance:

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cybersecurity and improve the way companies, governments and end-users proactively solve the world's most difficult security problems. Using a breakthrough predictive analysis process, Cylance quickly and accurately identifies what is safe and what is a threat, not just what is in a blacklist or whitelist. By coupling sophisticated machine learning and artificial intelligence with a unique understanding of a hacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com

+1 (877) 973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700, Irvine, CA 92612

CYLANCE