CylancePROTECT®

Administrator Guide

CYLANCE™

Product: CylancePROTECT

Document: CylancePROTECT Administrator Guide. This guide is a succinct resource for analysts, administrators, and customers who are reviewing or evaluating the product.

Document Release Date: v1.8.4, March 2017

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 math and machine learning with a unique understanding of an attacker's mentality, Cylance provides the technology and services to be truly predictive and preventive against advanced threats. For more information, visit cylance.com.

Global Headquarters

18201 Von Karman Avenue, Irvine, CA 92612

Professional Services Hotline

+1-877-97DEFEND ▪ +1-877-973-3336

Corporate Contact

+1-914-CYLANCE ▪ +1-914-295-2623

Email

sales@cylance.com

Website

https://www.cylance.com

To Open a Support Ticket

https://support.cylance.com — Click on **Submit a Ticket**

To View Knowledge Base and Announcements

Login to https://support.cylance.com

To Request a Callback from Cylance Support

+1-844-295-2623

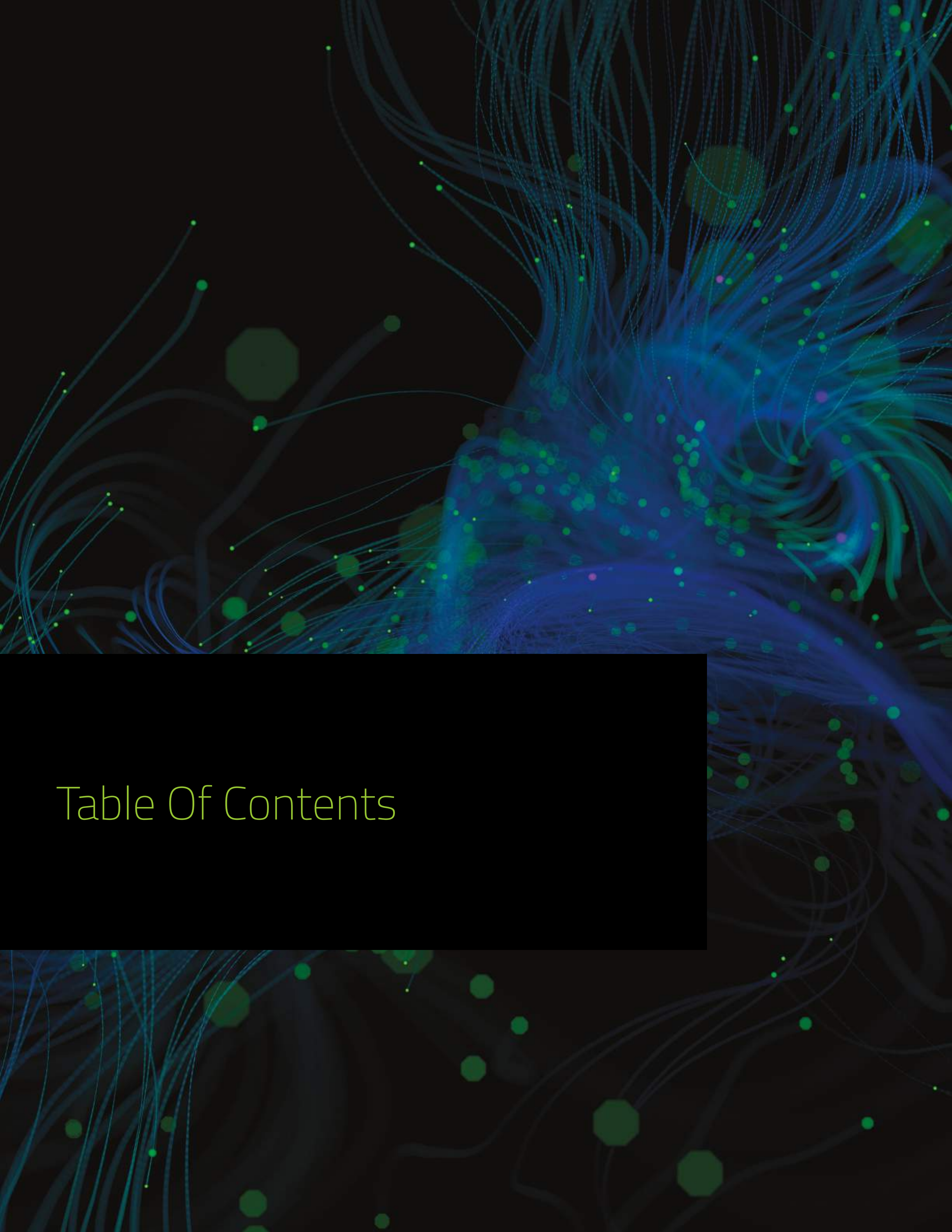
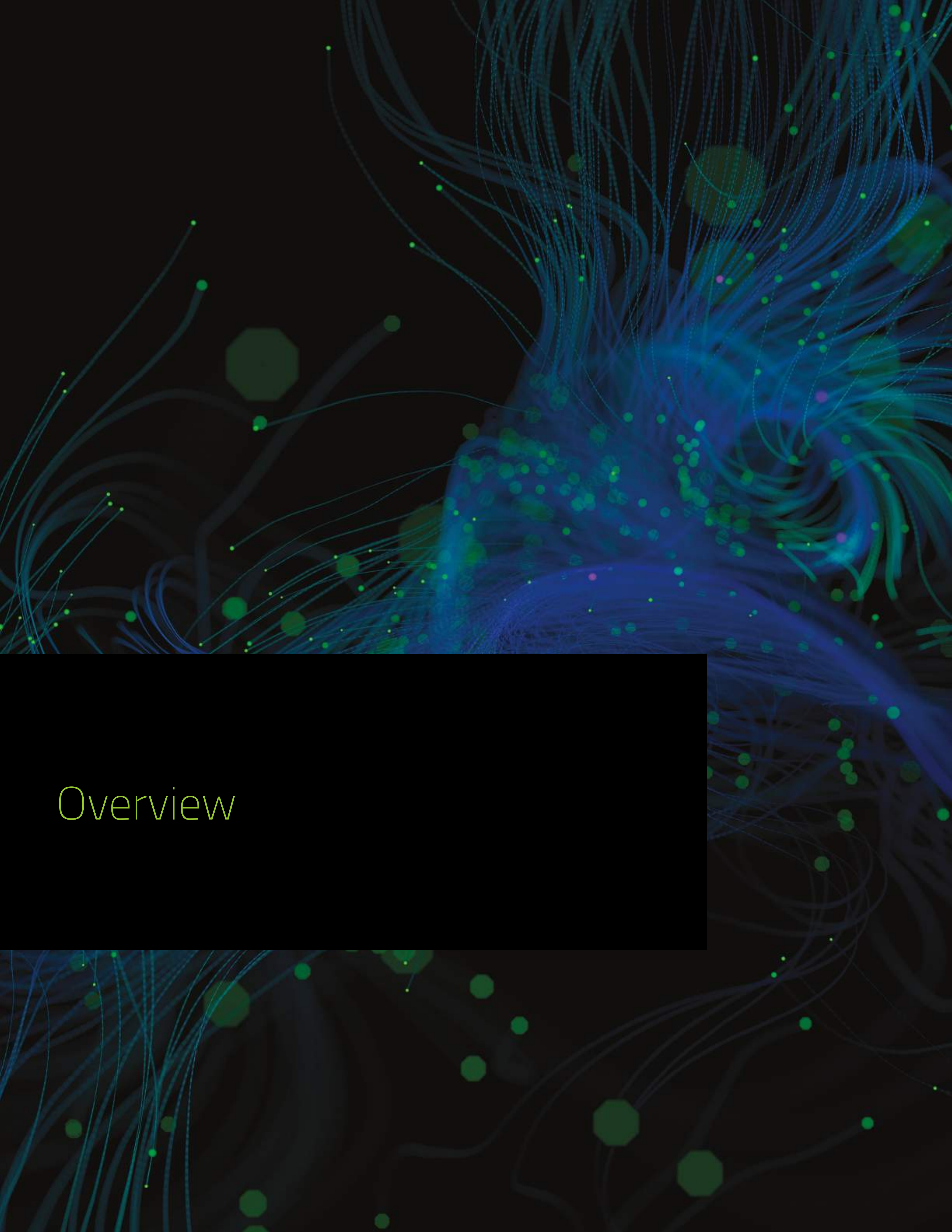


Table Of Contents

Contents



Overview

CylancePROTECT detects and blocks malware before it can affect your computer. Cylance uses a mathematical approach to malware identification, using machine learning techniques instead of reactive signatures, trust-based systems, or sandboxes. Cylance's approach renders new malware, viruses, bots, and future variants useless. **CylancePROTECT** analyzes potential file executions for malware in the operating system (OS) and memory layers to prevent the delivery of malicious payloads.

This guide covers using the Cylance Console, installing the **CylancePROTECT** Agent, and how to configure both products. Best practices are included, where applicable.

How It Works

CylancePROTECT consists of a small Agent, installed on each host, which communicates with Cylance's Console (cloud-based user-interface). The Agent detects and prevents malware on the host by using tested mathematical models, doesn't require continuous cloud connectivity or continual signature updates, and works in both open and isolated networks. As the threat landscape evolves, so does **CylancePROTECT**. By constantly training on enormous, real-world data sets, **CylancePROTECT** stays one step ahead of the attackers.

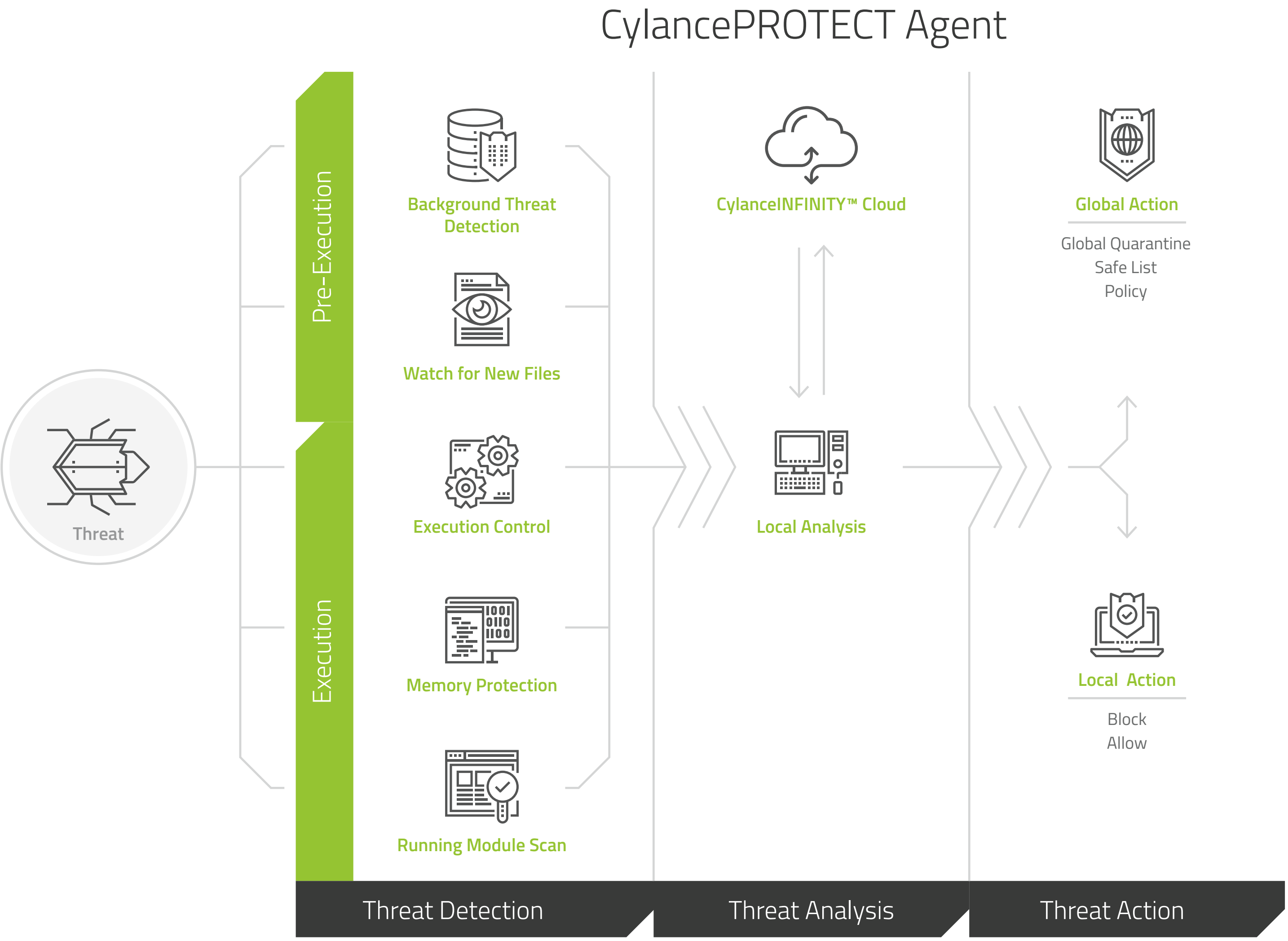


Figure 1: **CylancePROTECT** *Threat Analysis Flowchart*

- **Threat:** When a threat is downloaded to the system or there is an exploit attempt (something running in memory that attempts to execute an attack).
- **Threat Detection:** How the Agent identifies threats.
    - **Background Threat Detection:** Scans files on the system, runs in the background, and is designed to consume a small amount of system resources. It is recommended to enable Background Threat Detection and Watch For New Files. If Watch For New Files is enabled, it is recommended to configure Background Threat Detection to Run Once. You need to check existing files one time only if you are also watching for new and updated files.
    - **Watch For New Files:** Scans new and updated files for threats. Because this feature only looks for new and updated files, it is recommended to use Background Threat Detection set to Run Once. Background Threat Detection scans all files on the device.
    - **Running Module Scan:** Scans processes running on the device. This is collected after the initial installation of **CylancePROTECT** and when the Cylance Service starts (example: system boot).
    - **Execution Control:** Analyzes processes upon execution only. This includes all files that run at system startup, that are set to auto-run, and that are manually executed by the user.
    - **Script Control:** Protects users from malicious scripts running on their devices. This includes PowerShell, Active Script, and Microsoft Office Macros.
- **Analysis:** How files are identified as malicious or safe.
    - **Cylance OEM Engine:** The **CylancePROTECT** Mathematical Model in the cloud that is used to score files.
    - **Local:** The **CylancePROTECT** Mathematical Model included with the Agent. This allows analysis when the device is not connected to the Internet.
- **Action:** What the Agent does when a file is identified as a threat.
    - **Global:** Checks policy settings, including the Global Quarantine and Safe Lists.
    - **Local:** Checks for files manually Quarantined or Waived.

About This Guide

It is recommended that users become familiar with the Console before installing the Agent on their endpoints. Understanding how endpoints are managed should make protecting and maintaining endpoints easier. This workflow is just a recommendation. Users can approach deploying to their environment in a way that makes sense for them.

> **EXAMPLE:** *Zones help group devices in your organization. You can create a Zone Rule to automatically add new devices to a zone based on your selected criteria (like operating system, device name, or domain name). This requires some planning before you install any Agents.*

> **NOTE:** *Instructions for installing the Agent comes after learning about the Console in this guide. Users can start with installing the Agent if they prefer to do so.*

Communications

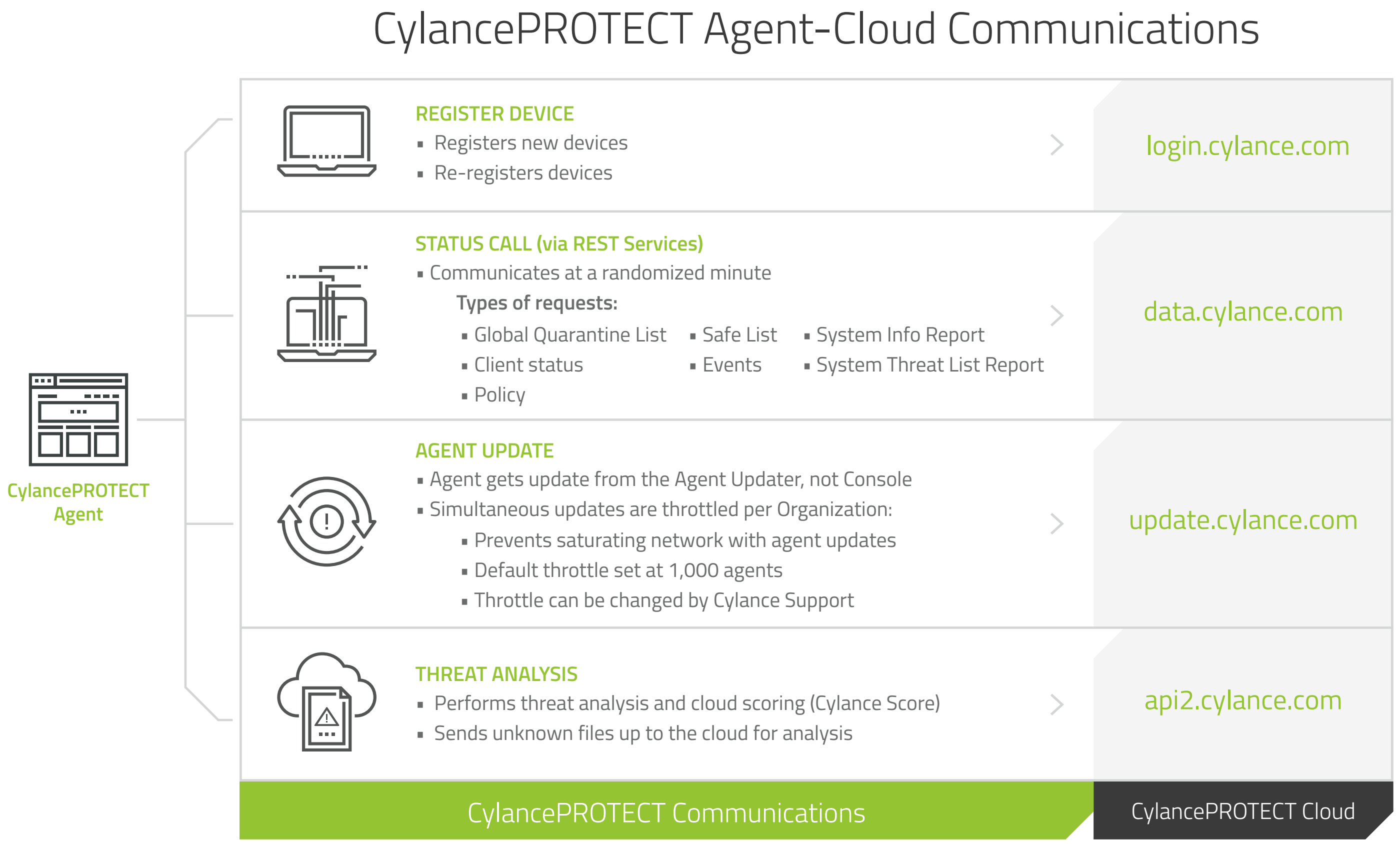
The Agent reports to and is managed by the Console. Networks with a proxy server or firewall should allow communication with the following sites (over port 443). For a list of Cylance hosts to allow, based on the region your organization belongs to, see Cylance Host URLs.

> **NOTE:** *The* **CylancePROTECT** *Agent-Cloud Communications image displays the Cylance Host URLs for North America. For other regions, the Agents would use the Cylance Host URLs for your region.*

> **EXAMPLE:** *login.cylance.com, login-au.cylance.com, login-euc1.cylance.com, and login-apne1.cylance.com are hosts that perform the same function in different regions.*

What's New in CylancePROTECT

To view new updates and releases, log in to the Cylance Support Portal at https://support.cylance.com and go the **CylancePROTECT** Release Notes (requires login).



CylancePROTECT Agent-Cloud Communications

CylancePROTECT Agent

REGISTER DEVICE
- Registers new devices
- Re-registers devices

login.cylance.com

STATUS CALL (via REST Services)
- Communicates at a randomized minute

Types of requests:
- Global Quarantine List
- Client status
- Policy
- Safe List
- Events
- System Info Report
- System Threat List Report

data.cylance.com

AGENT UPDATE
- Agent gets update from the Agent Updater, not Console
- Simultaneous updates are throttled per Organization:
  - Prevents saturating network with agent updates
  - Default throttle set at 1,000 agents
  - Throttle can be changed by Cylance Support

update.cylance.com

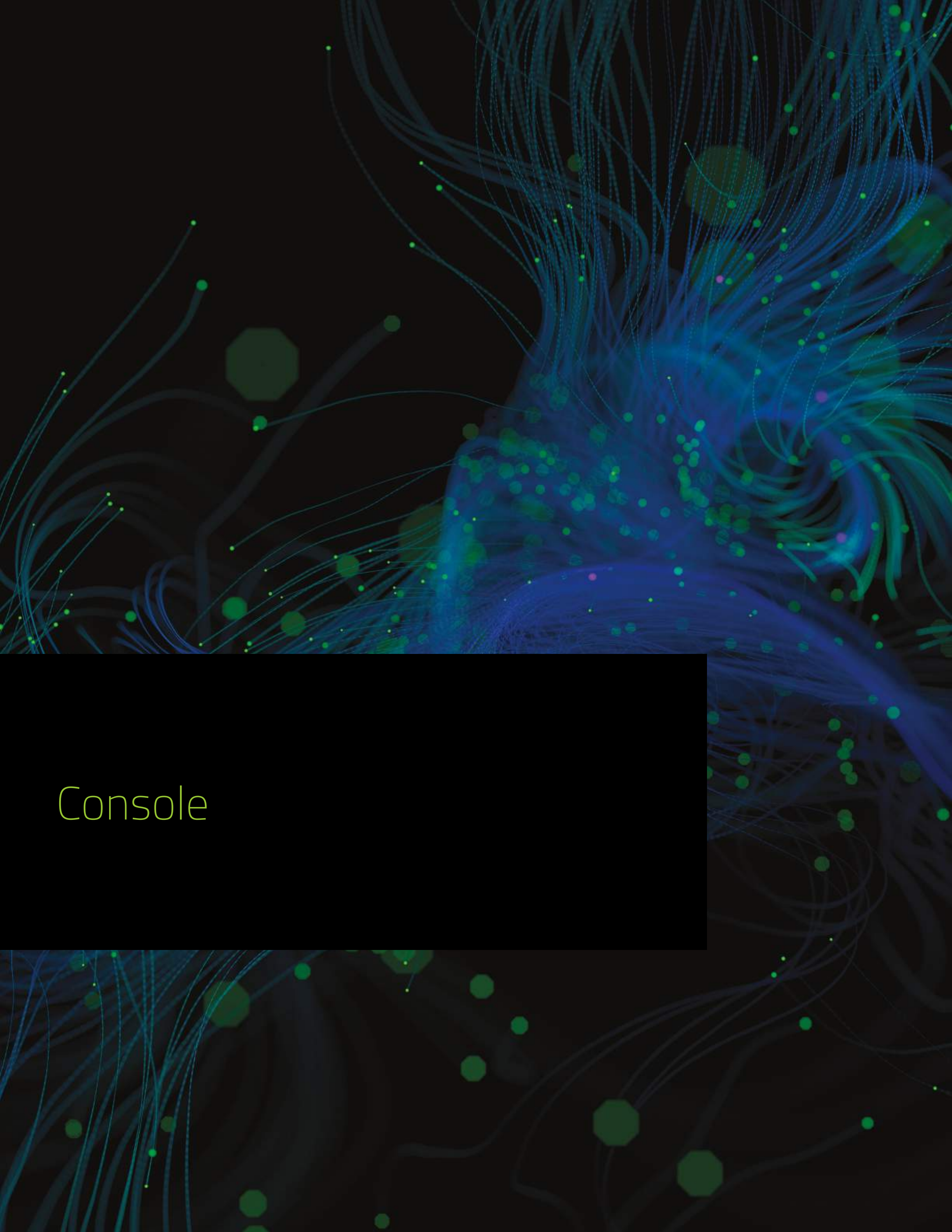
THREAT ANALYSIS
- Performs threat analysis and cloud scoring (Cylance Score)
- Sends unknown files up to the cloud for analysis

api2.cylance.com

CylancePROTECT Communications

CylancePROTECT Cloud

Figure 2: **CylancePROTECT** *Agent-Cloud Communications*

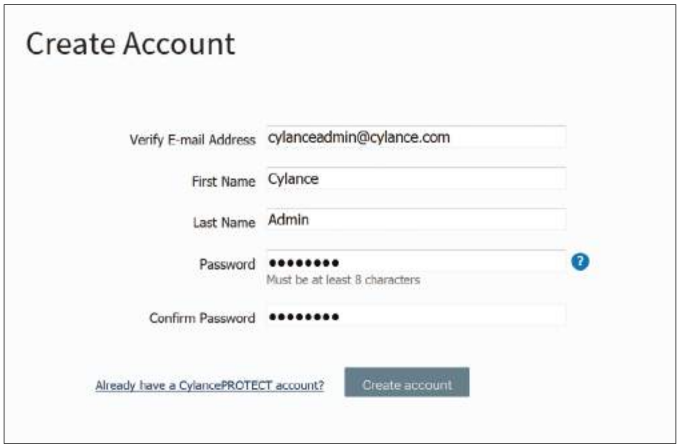


Console

The Console is a website you log in to and view threat information for your organization. You can organize your devices into groups (Zones), configure what to do with a threat when it is discovered on a device (Policy), and download the installation files (Agent).

Login

Upon activation of your account, you will receive an email requesting that you create a password to the Console. Click on the link in the email and you will be prompted to create a password.



Create Account

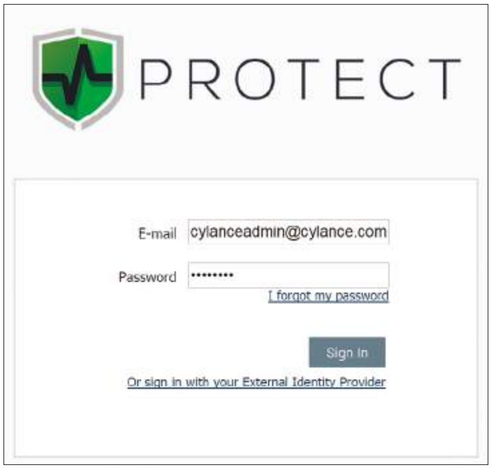
Verify E-mail Address: cylanceadmin@cylance.com
First Name: Cylance
Last Name: Admin
Password: ••••••••
Must be at least 8 characters
Confirm Password: ••••••••

Figure 3: Account Setup

The email address will serve as your account login. Once you have established your password, you will be able to proceed to the Console.

Your login URL depends on the region your organization belongs to:

- **Asia-Pacific North East:** https://login-apne1.cylance.com
- **Asia-Pacific South East:** https://login-au.cylance.com
- **Europe Central:** https://login-euc1.cylance.com
- **North America:** https://login.cylance.com



E-mail: cylanceadmin@cylance.com
Password: ••••••••

Figure 4: Console Login

Language Preferences

The Console is localized into the following languages: English, French, German, Italian, Japanese, Korean, Portuguese (Brazil), Portuguese (Portugal), and Spanish. The Console will use the language preferences or settings in your web browser to determine which localized content to display.

In Google Chrome:

1. Click **Customize and Control Google Chrome** (upper-right), then click Settings.
2. Scroll down and click **Show advanced settings**.
3. Click **Language** and **input settings**.
4. Click **Add**, select the language you want to add, then click OK. You can change the order of the languages by dragging a language to the preferred location.
5. Click **Done**.

In Mozilla Firefox:

1. Click **Open Menu** (upper-right), then click Options.
2. In the left-pane, click **Content**.
3. Under Languages, click **Choose**.
4. Select the language you want to display from the **Select a language to add list**, then click **Add**.
5. Click **OK**.

Device Policy

A policy defines how the Agent handles threats (malware) it encounters — automatically quarantine, ignore if in a specified folder, watch for new files, etc. Every device must be in a policy. If no policy is assigned, the device is placed in the Default policy.

To Add a Policy

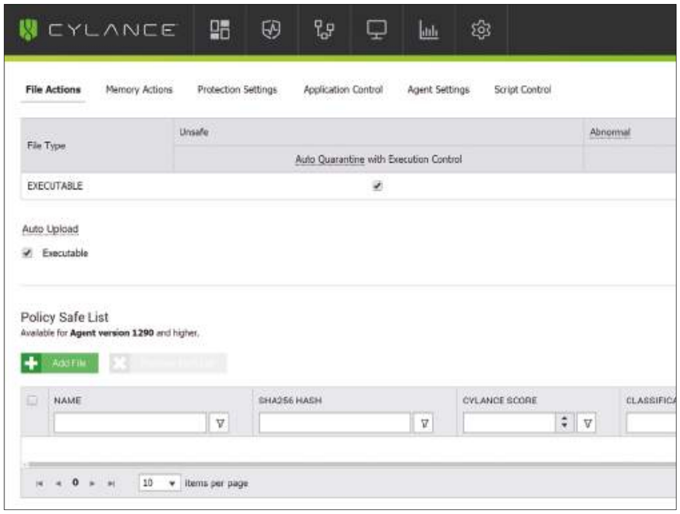
1. Log in to the Console as an Administrator. Only Administrators can create Policies.
2. Select **Settings > Device Policy**, then click Add **New Policy**.
3. Type a Policy Name and select policy options. Descriptions for each policy option are listed below, including Policy Best Practices.
4. Click **Save**.

File Actions

Settings > Device Policy > [select a policy] > File Actions

File Actions provide different options for handling files detected by the Agent. Threats are classified as either Unsafe or Abnormal.

> **TIP:** *To learn more about Cylance's classification method of Unsafe or Abnormal files, refer to the Protection section.*



File Type	Unsafe	Abnormal
	Auto Quarantine with Execution Control	
EXECUTABLE	☑	

Auto Upload

☑ Executable

Policy Safe List

Available for **Agent version 1290** and higher.

□	NAME	SHA256 HASH	CYLANCE SCORE	CLASSIFICA

10 items per page

Figure 5: Policy Details > File Actions

Auto Quarantine with Execution Control

The Agent will quarantine or block an Unsafe or Abnormal file to prevent it from executing. On a device, quarantining a file will move the file from its original location to the Cylance Quarantine directory.

- **For Windows:** C:\ProgramData\Cylance\Desktop\q.
- **For OS X:** /Library/Application Support/Cylance/Desktop/q.

Some malware is designed to drop other files in certain directories. This malware will continue to do so until the file is successfully dropped. To stop the malware from continually dropping the removed file, the Agent will modify the dropped file so it won't execute and leave it in the folder.

> **TIP:** *If you plan on using the Auto Quarantine feature, test this feature on a small number of devices before applying it to your production environment. This is so you can observe the test results and ensure that no business-critical applications are blocked at execution.*

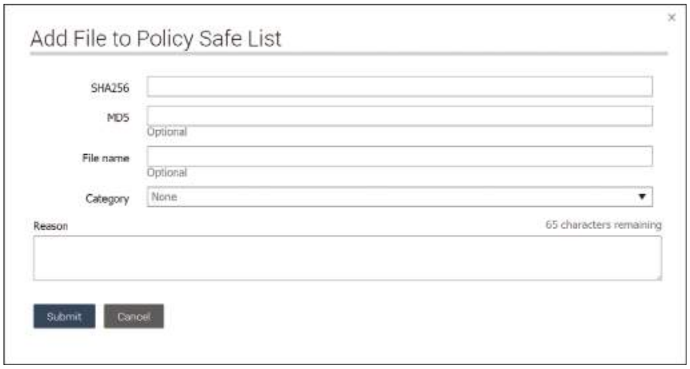
Auto Upload

It is recommended that users enable Auto Upload for both Unsafe and Abnormal files. If the Agent finds an Unsafe or Abnormal file that the CylanceINFINITY Cloud has never analyzed before, the Agent will upload the file for analysis and provide details when analysis is complete. If the same unknown file is discovered on multiple devices in your organization, the Agent should only upload one file for analysis, not one file per device.

Policy Safe List

You can add files that you consider safe to a Policy. Using the Policy Safe List means all Agents in that policy will treat the file as Safe, even if the Cylance Score ranks it as Unsafe or Abnormal. This is a good option if you need to allow a file for a group of devices, but you do not want to allow it for your entire organization.

1. Log in to the Console as an Administrator. Only Administrators can create Policies.
2. Select **Settings > Device Policy**, then either add a new policy or edit an existing policy.
3. Under Policy Safe List, click **Add File**.
4. Enter the **SHA256** information. Optionally, you can include the MD5 and File Name.
5. Select a **Category** to help you identify what this file does.
6. Type a reason for adding this file to the Policy Safe List, then click **Submit**.



Add File to Policy Safe List

SHA256

MD5 Optional

File name Optional

Category None

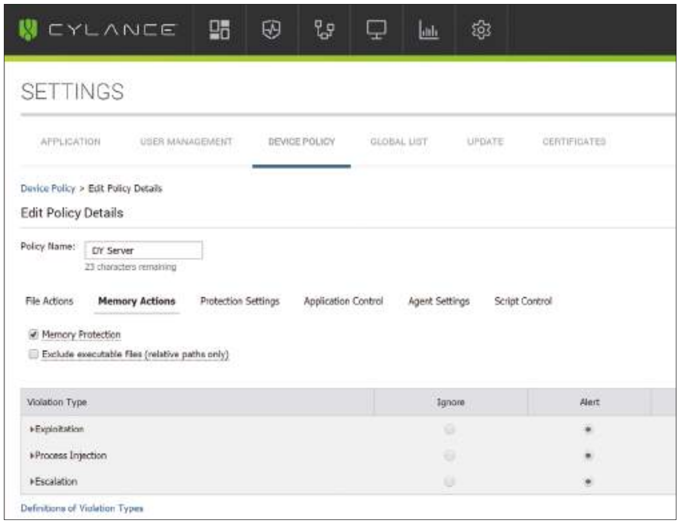
Reason 65 characters remaining

Figure 6: Policy Details > Memory Actions

Memory Actions

Settings > Device Policy > [select a policy] > Memory Actions

Memory Actions provide different options for handling memory exploits, including process injections and escalations. You can also add executable files to an exclusion list, allowing these files to run when this policy is applied.



Edit Policy Details

Policy Name: DY Server
23 characters remaining

☑ Memory Protection
☐ Exclude executable Files (relative paths only)

Violation Type	Ignore	Alert
▸Exploitation	○	●
▸Process Injection	○	●
▸Escalation	○	●

Figure 7: Policy Details > Memory Actions

Memory Protection

The Agent will scan and monitor running processes to protect devices from malware that attempts to take advantage of software vulnerabilities that exploit running processes or executes from within memory space. It is recommended that you Block all types of memory violations.

For descriptions of the different Violation, Process, and Escalation Types, see Memory Protection Violation Types.

> **WARNING:** *Enabling Memory Protection may cause errors if there is another application that also monitors running processes. It is recommended to disable the other application's memory protection before enabling Cylance's. If that is not possible, then leave Cylance's Memory Protection disabled in your policies.*

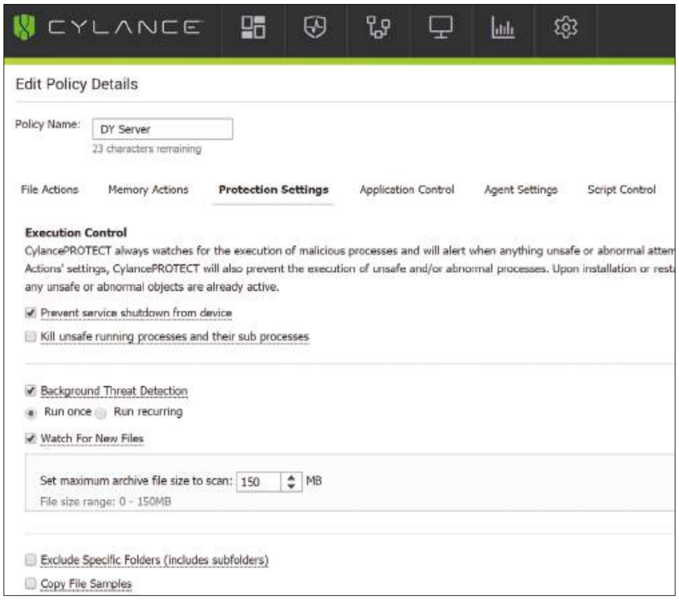
- **Ignore:** The Agent will not take any action against identified memory violations.
- **Alert:** The Agent will record the violation and report the incident to the Console.

Devices > [select a device] > Exploit Attempts (under Threats & Activities).

- **Block:** If an application attempts to call a memory violation process, the Agent will block the process call. The application that made the call is allowed to continue to run.
- **Terminate:** If an application attempts to call a memory violation process, the Agent will block the process call and will also terminate the application that made the call.
- **Exclude Executable Files:** Users are able to exclude executable files from Memory Protection by specifying the relative path of the file. This will allow the specified files to run or be installed on any device within that policy.
    - **Example — Windows:** \Application\Subfolder\application.exe
    - **Example — OS X:** /Mac\ HD/Users/application.app/executable

Protection Settings

Settings > Device Policy > [select a policy] > Protection Settings



Edit Policy Details

Policy Name: DY Server
23 characters remaining

Execution Control

CylancePROTECT always watches for the execution of malicious processes and will alert when anything unsafe or abnormal attem
Actions' settings, CylancePROTECT will also prevent the execution of unsafe and/or abnormal processes. Upon installation or resta
any unsafe or abnormal objects are already active.

☑ Prevent service shutdown from device
☐ Kill unsafe running processes and their sub processes

☑ Background Threat Detection
● Run once ○ Run recurring
☑ Watch For New Files

Set maximum archive file size to scan: 150 MB
File size range: 0 - 150MB

☐ Exclude Specific Folders (includes subfolders)
☐ Copy File Samples

Figure 8: Policy Details > Protection Settings

Execution Control

The Agent always watches for the execution of malicious processes and will alert when anything unsafe or abnormal attempts to run.

Prevent Service Shutdown from Device

If checked, the Cylance service is protected from being shutdown either manually or by another process.

Kill Unsafe Running Processes and Their Sub Processes

Terminates processes, and child processes, regardless of state when a threat is detected (EXE or DLL). This offers a high level of control over malicious processes that might be running on a device. The file must be auto-quarantined, manually quarantined, or quarantined using the Global Quarantine list. This feature must be enabled before the file is quarantined.

> **NOTE:** *If this feature is enabled but the file is not quarantined or auto-quarantined, the processes will continue to run.*

> **EXAMPLE:** *A file is allowed to run, then you decide to quarantine the file. With this feature enabled, the file is quarantined and the process is terminated. Without this feature enabled, the file would be quarantined, but because the file was allowed to run, any processes started by the file could continue to run.*

Background Threat Detection

Background Threat Detection will perform a full disk scan to detect and analyze any dormant threats on the disk. The full disk scan is designed to minimize impact to the end-user by using a low amount of system resources.

The user can choose to run the scan once (upon installation only) or run recurring (which performs a scan every 9 days). A significant upgrade to the Cylance model, like adding new operating systems, will also trigger a full disk scan. Each time a new scan is performed, all files will be rescanned.

It is recommended that users set Background Threat Detection to Run Once. Due to the predictive nature of the **CylancePROTECT** technology, periodic scans of the entire disk are not necessary but can be implemented for compliance purposes.

Watch for New Files

The Agent will detect and analyze any new or modified files for dormant threats. It is recommended that users enable Watch for New Files. However, if Auto Quarantine is enabled for all Unsafe or Abnormal files, all malicious files will be blocked at execution. Hence, it is not necessary to enable Watch For New Files with Auto Quarantine mode unless the user prefers to quarantine a file as it is added to a disk (Watch For New Files) but before execution (Auto-Quarantine).

Set Maximum Archive File Size To Scan

Set the maximum archive file size the Agent will scan. This setting applies to Background Threat Detection and Watch for New Files. Setting the file size to 0MB means no archive files will be scanned.

Exclude Specific Folders

Users are able to exclude specific folders, including subfolders, from Background Threat Detection and/or Watch For New Files (when these features are enabled) by specifying the path of the folder location. For Windows, use an absolute path (including the drive letter). For OS X, use a relative path and remember to escape any spaces in the path.

Example — Windows: C:\Test

Example — OS X: /Mac\ HD/Users/Application\ Support/Cylance

Copy Malware Samples

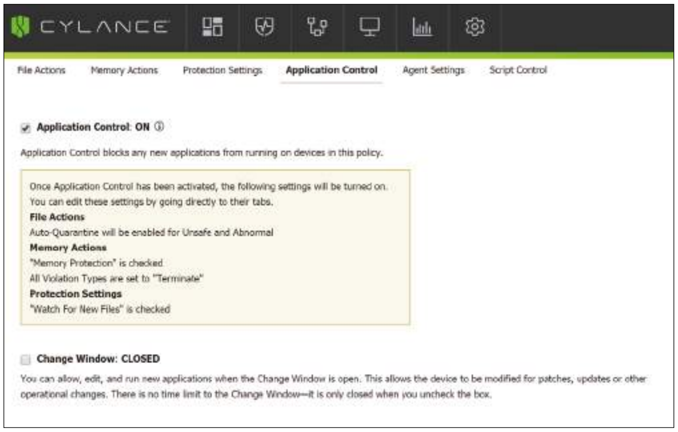
Allows you to specify a network share to which malware samples can be copied. This allows users to do their own analysis of files the Agent considers Unsafe or Abnormal.

- Supports CIFS/SMB network shares.
- Specify one network share location. You should use a fully qualified path. Example: \\server_name\shard_folder.
- All files meeting the criteria will be copied to the network share, including duplicates. No uniqueness test will be performed.
- Files are compressed (requires Agent version 1390 and higher).
- Files are password protected (requires Agent version 1390 and higher). The password is infected.

Application Control

Application Control is an optional setting available for licensed users only. If enabled, this feature allows users to lockdown specified systems and restrict any changes on the devices after being locked down. Only the applications that exist on a device before the lockdown occurs are allowed to execute on that device. Any new applications, as well as changes to the executables of existing applications, will be denied. The Agent Updater will also be disabled when Application Control is enabled.

When you activate Application Control, the following recommended settings will take place (see image below). With Application Control enabled, you can edit these policy settings by going directly to their tasks.



☑ **Application Control: ON** ⓘ

Application Control blocks any new applications from running on devices in this policy.

Once Application Control has been activated, the following settings will be turned on.
You can edit these settings by going directly to their tabs.
File Actions
Auto-Quarantine will be enabled for Unsafe and Abnormal
Memory Actions
"Memory Protection" is checked
All Violation Types are set to "Terminate"
Protection Settings
"Watch For New Files" is checked

☐ **Change Window: CLOSED**

You can allow, edit, and run new applications when the Change Window is open. This allows the device to be modified for patches, updates or other operational changes. There is no time limit to the Change Window—it is only closed when you uncheck the box.

Figure 9: Policy Details > Application Control

To view Application Control activity, users can sign in to the Console and click on any device that is in a device policy with Application Control enabled. The Device Details page will list out all actions relevant to Application Control under the Threats & Activities section.

Change Window

Use the Change Window option to temporarily disable Application Control to allow, edit, and run new applications or perform updates. This includes updating the Agent. After performing the necessary changes, turn Change Window off (Closed).

> **NOTE:** *Using the Change Window retains any changes made to the Application Control settings. Turning Application Control OFF and then back ON resets the Application Control settings back to default.*

Folder Exclusions (Including Subfolders)

Specify an absolute path to allow application changes and additions to the specified folders while Application Control is enabled. Requires Agent 1410 and higher.

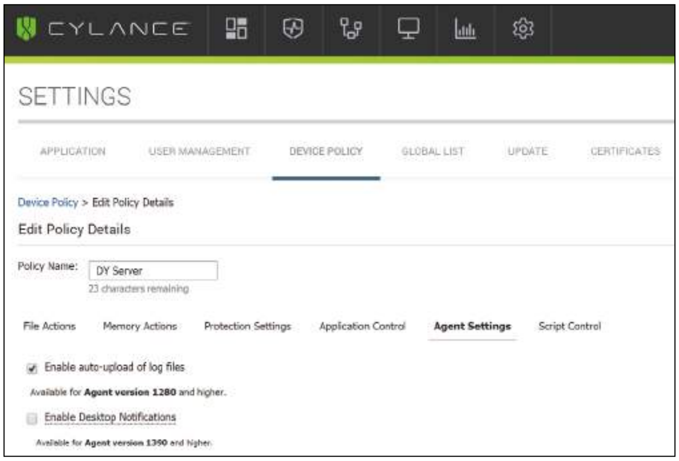
Agent Settings

Settings > Device Policy > [select a policy] > Agent Settings

Enable Auto-upload of Log Files

Enabling Agent Logs in the Console uploads log files and allows you to view them in the Console.

1. Log in to the Console.
2. Select **Settings > Device Policy**.
3. Click on a policy, then click **Agent Logs**. Make sure the device you want log files for is assigned to this policy.
4. Select **Enable auto-upload of log files**, then click **Save**.
5. Click the **Devices tab**, then **click on a device**.
6. Click **Agent Logs**, then click on a **log file**. The log file name is the date of the log.



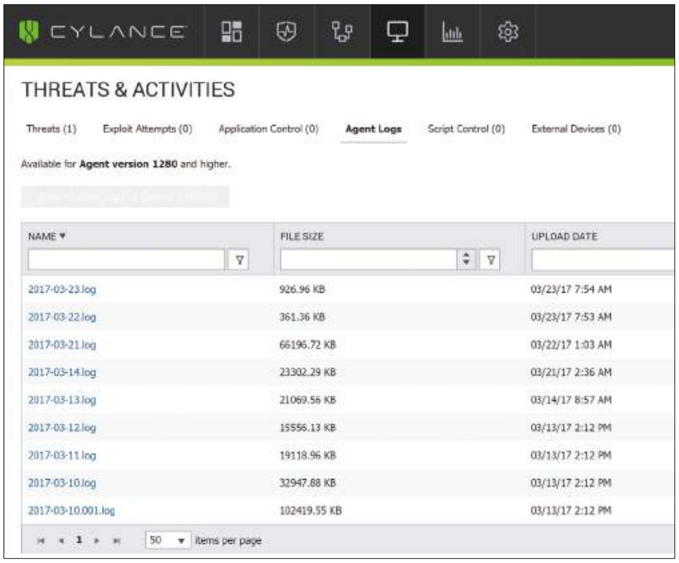
Edit Policy Details

Policy Name: DY Server
23 characters remaining

☑ Enable auto-upload of log files
Available for **Agent version 1280** and higher.

☐ Enable Desktop Notifications
Available for **Agent version 1390** and higher.

Figure 10: Policy Details > Agent Logs



Available for **Agent version 1280** and higher.

NAME ▾	FILE SIZE	UPLOAD DATE
2017-03-23.log	926.96 KB	03/23/17 7:54 AM
2017-03-22.log	361.36 KB	03/23/17 7:53 AM
2017-03-21.log	66196.72 KB	03/22/17 1:03 AM
2017-03-14.log	23302.29 KB	03/21/17 2:36 AM
2017-03-13.log	21069.56 KB	03/14/17 8:57 AM
2017-03-12.log	15556.13 KB	03/13/17 2:12 PM
2017-03-11.log	19118.96 KB	03/13/17 2:12 PM
2017-03-10.log	32947.88 KB	03/13/17 2:12 PM
2017-03-10.001.log	102419.55 KB	03/13/17 2:12 PM

Figure 11: Devices > [select a device] > Agent Logs

Enable Desktop Notifications

Agent Notification popups can be configured on each device or set at the policy-level in the Console. Enabling or disabling the Agent Notification popups at the device-level takes precedence over the Console settings.

This feature requires Agent version 1390 or higher.

To Enable Desktop Notifications from the Console

1. Log in to the Console as an Administrator. Only Administrators can change policy settings.
2. Select **Settings > Device Policy**.
3. Click on a policy, then click **Agent Logs**. Make sure the device you want log files for is assigned to this policy.
4. Select **Enable Desktop Notifications**, then click **Save**.

To Clear Agent Notifications on a Device

When Agent notifications are enabled or disabled on a device, that setting is saved to a file on the device. This setting overrides the setting in the Console. To allow the Console to control Agent notifications, this saved file must be deleted from the device (if this file exists).

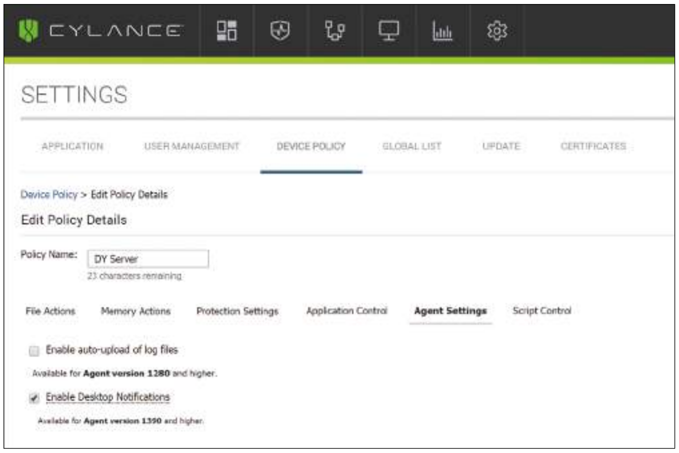
1. On the device, right-click the **Agent icon**, then select **Exit**.

2. Delete the configuration file

   a. **Windows:** \Users\<username>\AppData\Local\Cylance\Desktop, delete **CylanceUI.cfg**

   b. **OS X:** Run defaults delete com.cylance.CylanceUI from the Terminal. :

3. Restart the Agent UI.



Policy Name: DY Server
23 characters remaining

☐ Enable auto-upload of log files
Available for **Agent version 1280** and higher.

☑ Enable Desktop Notifications
Available for **Agent version 1390** and higher.

Figure 12: Policy Details > Desktop Notifications

Script Control

Script Control protects devices by blocking malicious Active Script and PowerShell scripts from running. With Agent versions 1380 and higher, you can alert or block malicious Microsoft Office macros.

Script Control monitors and protects against scripts running in your environment. The Agent is able to detect the script and script path before the script is executed. Depending on the policy set for Script Control (Alert or Block), the Agent will allow or block the execution of the script.

Microsoft Office macros use Visual Basic for Applications (VBA) that allows embedding code inside an Office document (typically Word, Excel, and PowerPoint). The main purpose for macros is to simplify routine actions, like manipulating data in a spreadsheet or formatting text in a document. However, malware creators can use macros to run commands and attack the system. It is assumed that a Microsoft Office macro trying to manipulate the system is a malicious action. The Agent looks for malicious actions originating from a macro that affects things outside the Microsoft Office products.

> **TIP:** *Starting with Microsoft Office 2013, macros are disabled by default. Most of the time, you do not need to enable macros to view the content of an Office document. You should only enable macros for documents you receive from users you trust, and you have a good reason to enable it. Otherwise, macros should always be disabled.*

1. Log in to the Console.
2. Select **Settings > Device Policy**.
3. Click on a policy, then click Protection Settings.
4. Enable **Script Control** by selecting the checkbox.

   a. **Alert:** Monitors scripts running in your environment. Recommended for initial deployment.

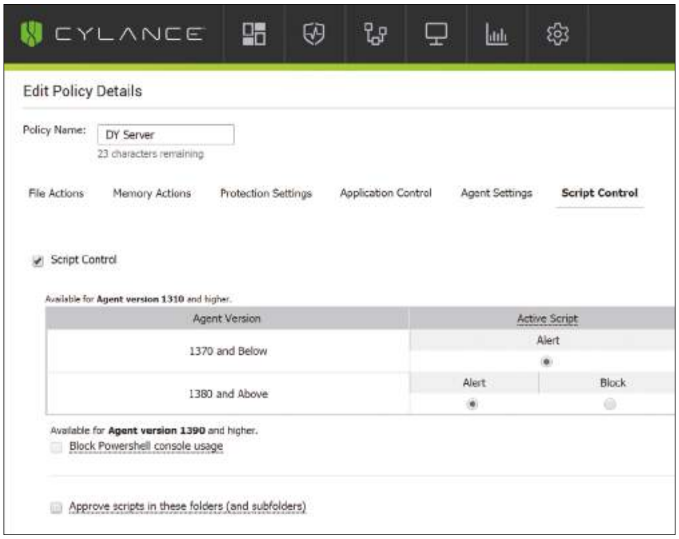
   b. **Block:** Only allow scripts to run from specific folders. Use after testing in Alert mode.

   c. **Approve scripts in these folders (and subfolders):** Script folder exclusions must specify the relative path of the folder.

   d. **Block PowerShell Console usage:** Blocks the PowerShell console from launching. This provides additional security by protecting against the use of PowerShell one-liners.

   > **NOTE:** *If the script launches the PowerShell console, and Script Control is set to block the PowerShell console, the script will fail. It is recommended that users change their scripts to invoke the PowerShell scripts, not the PowerShell console.*

5. Click Save.



Edit Policy Details

Policy Name: DY Server

23 characters remaining

File Actions | Memory Actions | Protection Settings | Application Control | Agent Settings | **Script Control**

☑ Script Control

Available for **Agent version 1310** and higher.

Agent Version	Active Script	
1370 and Below	Alert ●	
1380 and Above	Alert ●	Block ○

Available for **Agent version 1390** and higher.

□ Block Powershell console usage

□ Approve scripts in these folders (and subfolders)

Figure 13: Policy Details > Script Control

Device Control

Device Control protects devices by controlling USB mass storage devices connecting to devices in your organization. With Agent version 1410 and higher, you can allow or block things identified as USB mass storage devices, including USB flash drives, external hard drives, and smartphones. Device Control is available for the Windows platform only.

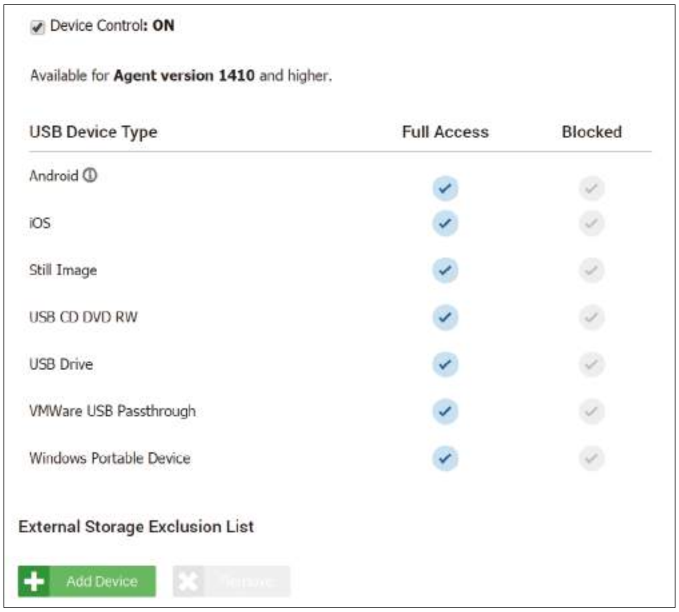
Administrators can enable Device Control using a Device Policy, and can choose to allow or block access to USB mass storage devices. This only applies to USB devices that are classified as Mass Storage. USB peripherals, such as a keyboard, are not affected. For example, if an administrator creates a policy to block USB mass storage devices, an end-user can still use a USB mouse, but a USB flash drive would be blocked.

As part of a Device Control policy, administrators can also define exceptions to the policy. This is done by using the Vendor ID, Product ID, and Serial Number to specify the exception. Minimally, the Vendor ID must be entered, but the Product ID and Serial Number can also be used for a more specific exception.

When enabled, Device Control will log all USB mass storage devices that are inserted, along with the policy that was applied (Allow or Block). If Desktop Notifications are enabled, end-users will see a pop-up notification only if the policy is set to Block. Device Control events can be found on the Protection page, under the External Devices tab.

Enable Device Control

1. In the Console, select **Settings > Device Policy**.
2. Create a new policy or edit an existing policy.
3. Click the **Device Control tab**.
4. Select **Device Control** to enable it.



☑ Device Control: **ON**

Available for **Agent version 1410** and higher.

USB Device Type	Full Access	Blocked
Android ⓘ	✓	
iOS	✓	
Still Image	✓	
USB CD DVD RW	✓	
USB Drive	✓	
VMWare USB Passthrough	✓	
Windows Portable Device	✓	

External Storage Exclusion List

Figure 14: Device Policy > Device Control

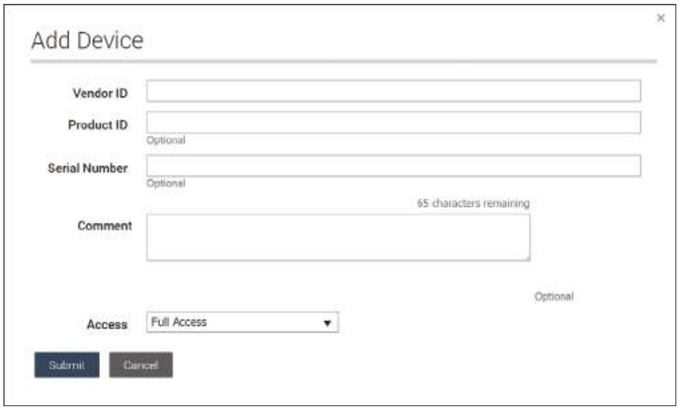
5. Block the USB Device Types you do not want connecting to devices.

> **NOTE:** *An Android device could connect and be identified as Android, Still Image, or Windows Portable Device. If you want to block Android devices, consider blocking Still Image and Windows Portable Device as well.*

6. Click **Save**.

Add External Storage Exclusion

1. In the Console, select **Settings > Device Policy**.
2. Create a new policy or edit an existing policy.
3. Click the **Device Control** tab and make sure Device Control is enabled.
4. Under External Storage Exclusion List, click **Add Device**.



Add Device

Vendor ID

Product ID
Optional

Serial Number
Optional

65 characters remaining

Comment
Optional

Access: Full Access

Figure 15: Add device to External Storage Exception List

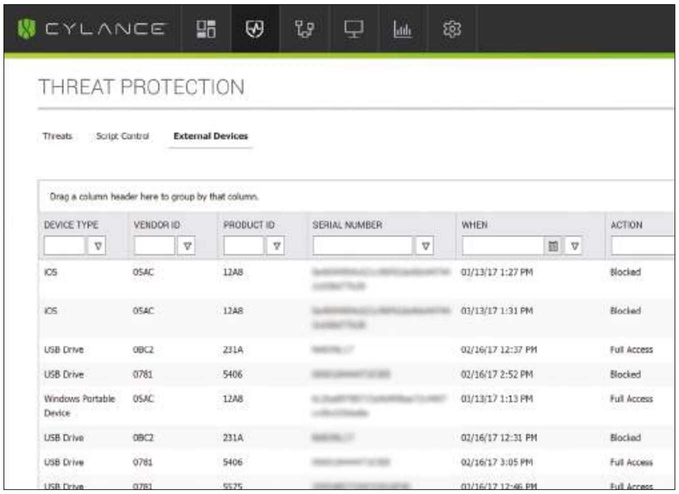
5. Type in the Vendor ID (required). Include the Product ID and Serial Number to refine the exclusion. You can also add a Comment to describe the exclusion.
6. For Access, select **Full Access** or **Block**.
7. Click **Submit**.

View External Device Log

You can view External Device logs on the Protection tab or on the Device Details page (External Devices tab).

Using the Protection Tab

1. In the Console, click the **Protection tab**.
2. Click **External Devices**.



THREAT PROTECTION

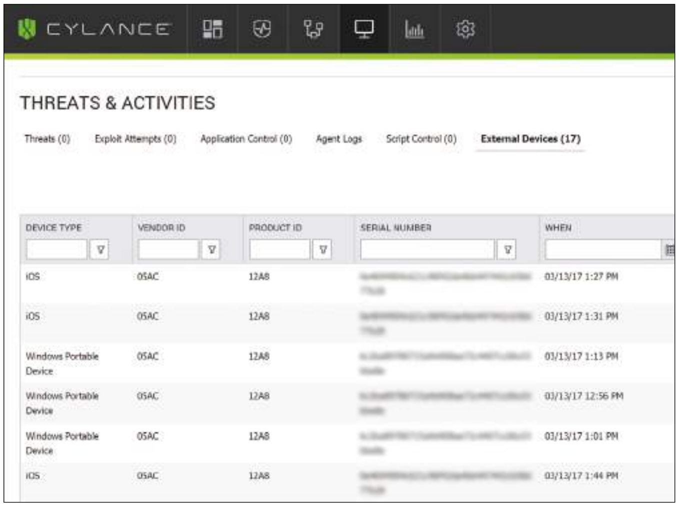
Drag a column header here to group by that column.

DEVICE TYPE	VENDOR ID	PRODUCT ID	SERIAL NUMBER	WHEN	ACTION
iOS	05AC	12A8	[redacted]	03/13/17 1:27 PM	Blocked
iOS	05AC	12A8	[redacted]	03/13/17 1:31 PM	Blocked
USB Drive	0BC2	231A	[redacted]	02/16/17 12:37 PM	Full Access
USB Drive	0781	5406	[redacted]	02/16/17 2:52 PM	Blocked
Windows Portable Device	05AC	12A8	[redacted]	03/13/17 1:13 PM	Full Access
USB Drive	0BC2	231A	[redacted]	02/16/17 12:31 PM	Blocked
USB Drive	0781	5406	[redacted]	02/16/17 3:05 PM	Full Access
USB Drive	0781	5575	[redacted]	01/16/17 12:46 PM	Full Access

Figure 16: Protection Tab > External Devices

Using the Device Details Page

1. In the Console, click the **Devices tab**.
2. Click on the **device**.
3. Under Threats & Activities, click the **External Devices tab**.



THREATS & ACTIVITIES

DEVICE TYPE	VENDOR ID	PRODUCT ID	SERIAL NUMBER	WHEN
iOS	05AC	12A8	[redacted]	03/13/17 1:27 PM
iOS	05AC	12A8	[redacted]	03/13/17 1:31 PM
Windows Portable Device	05AC	12A8	[redacted]	03/13/17 1:13 PM
Windows Portable Device	05AC	12A8	[redacted]	03/13/17 12:56 PM
Windows Portable Device	05AC	12A8	[redacted]	03/13/17 1:01 PM
iOS	05AC	12A8	[redacted]	03/13/17 1:44 PM

Figure 17: Device Details > Threats & Activities > External Devices

Policy Best Practices

When you first create policies, it is recommended to implement policy features in a phased approach to ensure performance and operations are not impacted. As you understand how Cylance functions in your environment, you can create new policies with more features enabled.

1. When creating your initial policies, enable **Auto-Upload** only.
   a. The Agent will use Execution Control and Process Monitor to analyze running processes only. This includes all files that run at system startup, that are set to auto-run, and that are manually executed by the user. The Agent will only send alerts to the Console, and nothing will be blocked or quarantined.
   b. Check the Console for any threat alerts. The goal is to find any applications or processes that are required to run on the system that Cylance considers a threat (Abnormal or Unsafe). If this happens, you can configure policy or console settings to allow these things to run (examples: exclude folders in a policy, waive the files for that system, or add the files to the Safe List).
   c. You should use this initial policy for a day to allow applications and processes that are typically used on the system to run and be analyzed by **CylancePROTECT**.

   > **NOTE:** *There may be applications and processes that run periodically on a system (example: once a month) that Cylance might consider a threat. It is up to you to decide if you want to run that during this initial policy or remember to monitor the system when it runs as scheduled.*

2. After Execution Control and Process Monitor are complete, enable **Background Threat Detection — Run Once** and **Watch For New Files**.
   a. The Background Threat Detection scan can take up to one week, depending on how busy the system is and the number of files on the system that require analysis.
   b. It is recommended to set Background Threat Detection to Run Once. Due to the predictive nature of Cylance's technology, periodic scans of the entire disk are not necessary. You can implement periodic scanning for compliance purposes (example: PCI compliance).
   c. Watch For New Files might impact performance. Check if disk or message processing performance has changed.
   d. Excluding folders might improve performance and ensure that certain folders and files do not get scanned or analyzed by the Agent.
   e. If identified threats include any legitimate applications necessary for business operations, make sure to Waive or Safe list these files. You can also exclude the folder containing the file.

3. Next, turn on **Auto-Quarantine** and **Memory Protection**, with Violation Type set to **Alert**.
   a. Auto-Quarantine moves any malicious files to the quarantine folder.
   b. Memory Protection set to Alert will send information to the Console but will not block or terminate any processes running in memory.
   c. If Memory Protection identifies any legitimate processes necessary for business operations, exclude the executable file. In the policy, include the relative path to the file.

4. After testing Memory Protection set to Alert, change the Violation Type to **Block**.
   a. Memory Protection set to Block will send information to the Console and will stop any malicious processes running in memory. It will not terminate the file initiating the malicious process.

5. For Device Control, before setting the policy and creating exceptions, administrators should:
   a. Create or edit a policy used for testing. Make sure a test device is assigned to this policy.
   b. Enable Device Control and set it to Full Access.
   c. On the test device, insert a USB device and examine the logs to ensure the right Vendor ID, Product ID, and Serial Number are used in the exception.

   > **NOTE:** *Not all manufacturers use a serial number with their products. Some manufacturers use the same serial number for multiple products.*

   d. Once testing is complete, set Device Control to Full Access or Block, and add any exceptions needed.

Zones

A zone is a way to organize and manage your devices. For example, you may want to split your devices up based on geography or function. If you have a group of mission critical systems, you can group those systems together and assign a high priority to the zone. Additionally, policies are applied at the zone level, so you can group devices together in a zone based on the policy that will be applied to those devices.

An organization has a default zone (Unzoned) that only Administrators can access. New devices are assigned to Unzoned, unless there are Zone Rules that automatically assign devices to zones.

Zone Managers and Users can be assigned to Zones, allowing them to view devices in those Zones. If a Zone Manager or User is responsible for a device with **CylancePROTECT**, make sure that device is in a zone to which they have access. At least one Zone must be created to allow anyone with a Zone Manager or User role to view Zones.

A device can belong to multiple zones, but only one policy can be applied to a device. Devices existing in multiple zones could occur because: the device is manually added to multiple zones, the device complies with the rules of more than one zone, or the device already resides in one zone and then complies with rules of another zone.

For recommended ways to use Zones, see Zone Management Best Practices.

To Add a Zone

1. Log in to the Console as an Administrator. Only Administrators can create Zones.
2. Click **Zones**, then click **Add New Zone**.
3. Type a Zone Name, select a Policy, then select a Value. A Zone must have an associated Policy. The Value is the Priority for the zone.
4. Click **Save**.

To Add Devices To a Zone

1. Log in to the Console as an Administrator. Only Administrators can add devices to a zone. Zone Managers and Users can install the Agent on a device, but do not have access to the Default zone (Unzoned), and therefore cannot assign the new device to zones.
2. Click **Zones**, then click on a zone from the Zones List. The current devices in that zone display in the Zones Device List, at the bottom of the page.
3. Click **Add Devices to Zone**. A list of devices displays.
4. Check each device to add to the zone, then click **Save**. Optionally, select **Apply zone policy to selected devices**. Adding a device to a zone doesn't automatically apply the Zone Policy because you might be using a zone to organize your devices, not manage the policy for those devices.

To Remove a Zone

1. Log in to the Console as an Administrator. Only Administrators can remove Zones.
2. Click **Zones**, then select the checkboxes for the zones you want to remove.
3. Click **Remove**. A message displays, asking you to confirm removing the selected zones.
4. Click **Yes**.

Zone Properties

You can edit the zone properties, as needed.

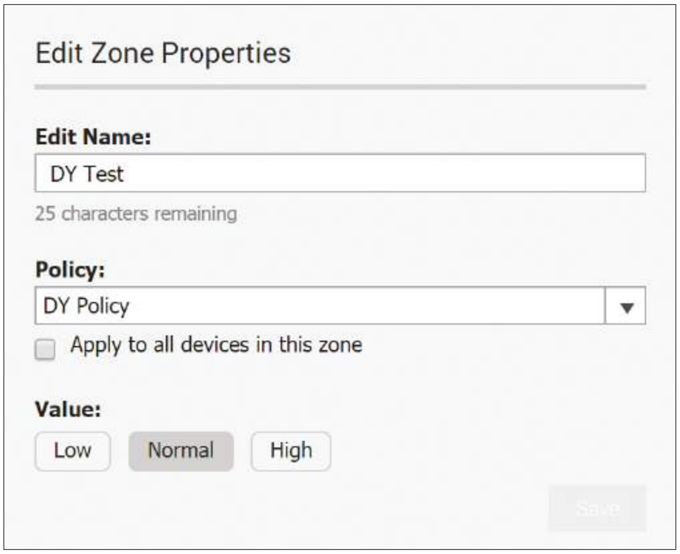
About Zone Priority

Zones can be assigned different priority levels (Low, Normal, or High) that serve to classify the significance or criticality of the machines in that zone. In several areas of the dashboard, devices are displayed by priority to help identify which machines need to be addressed immediately.

The priority can be set when a zone is created or the zone's properties can be edited to change the priority value.

To Edit Zone Properties

1. Log in to the Console as an Administrator or Zone Manager.
2. Click **Zones**, then click on a zone from the Zones List.
3. To change the zone name, type a new name in the **Edit Name** field.
4. To change the policy, select a different policy from the **Policy** list.
5. Under Value, select **Low**, **Normal** or **High**.
6. Click **Save**.



Edit Zone Properties

Edit Name: DY Test

25 characters remaining

Policy: DY Policy

□ Apply to all devices in this zone

Value: Low [✓ Normal] High

Figure 18: Change Zone Properties

Zone Rule

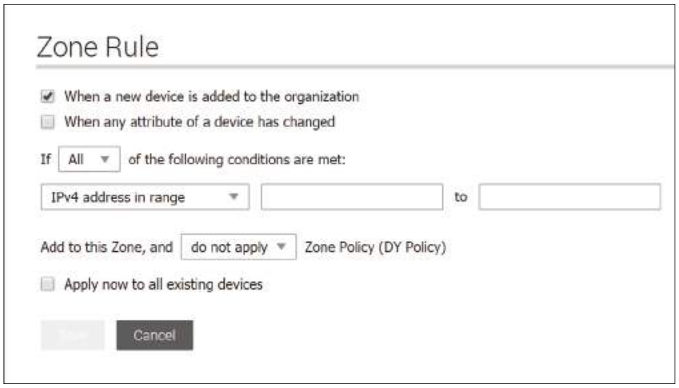
Devices can be automatically assigned to a zone based on certain criteria. This automation is beneficial when adding numerous devices to zones. When new devices are added that match a Zone Rule, those devices are automatically assigned to that zone. If **Apply now to all existing devices** is selected, all existing devices in your organization that match the rule will be added to that zone.

> **NOTE:** *Zone Rules automatically add devices to a zone but cannot remove devices. Changing the device's IP address or hostname will not remove that device from a zone. Devices must be removed manually from a zone.*

There is an option to apply the Zone Policy to devices that are added to the zone as a result of matching the Zone Rule. This means the device's existing policy will be replaced by the specified zone policy. To view which policy is applied to a device, view the Device Details page in the Console.

To Add a Zone Rule

1. Log in to the Console as an Administrator. Only Administrators can create a Zone Rule.
2. Click **Zones**, then click on a zone from the Zones List.
3. Under Zone Rule, click **Create Rule**.
4. Specify the criteria for the selected zone. Click the **plus sign** to add more conditions. Click the **minus sign** to remove a condition.
5. Click **Save**.



Zone Rule

☑ When a new device is added to the organization

□ When any attribute of a device has changed

If All of the following conditions are met:

IPv4 address in range to

Add to this Zone, and do not apply Zone Policy (DY Policy)

□ Apply now to all existing devices

Figure 19: Zone Rule

Zone Rule Criteria

- **When a new device is added to the organization:** When selected, any new device added to the organization that matches the zone rule will be added to the zone.
- **When any attribute of a device has changed:** When selected, when attributes on an existing device change and then match the zone rule, that existing device will be added to the zone.
- **If All/Any of the following conditions are met:**
  - **All:** A device must meet all of the conditions listed in the Zone Rule to be added to the zone.
  - **Any:** A device must meet at least one of the conditions listed in the Zone Rule to be added to the zone.
- **IPv4 Address in Range:** Type in an IPv4 address range.
- **Device Name:**
  - **Starts With:** Device names must start with this.
  - **Contains:** Device names must contain this string, but it can be anywhere within the name.
  - **Ends With:** Device names must end with this.
- **Distinguished Name:**
  - **Starts With:** Distinguished name must start with this.
  - **Contains:** Distinguished name must contain this string, but it can be anywhere within the name.
  - **Ends With:** Distinguished name must end with this.
- **Member Of (LDAP):**
  - **Is:** Member Of information must match this string.
  - **Contains:** Member Of information must contain this string.
- **Domain Name:**
  - **Starts With:** Domain name must start with this.
  - **Contains:** Domain name must contain this string, but it can be anywhere within the name.
  - **Ends With:** Domain name must end with this.
- **Operating System:**
  - **Is:** Operating system must be the selected system.
  - **Is Not:** Operating system must not be the selected system. Example: If the only Zone Rule states that the operating system must not be Windows XP, then all operating systems, including non-Windows systems, are added to this zone.
- **Add to this Zone, and do not apply/apply Zone Policy (policy_name):**
  - **Do not apply:** As devices are added to the zone, do not apply the Zone Policy.
  - **Apply:** As devices are added to the zone, apply the Zone Policy.

> **WARNING:** *Automatically applying a Zone Policy might negatively impact some of the devices on your network. You should only automatically apply the Zone Policy if you are certain that the Zone Rule will only find devices that must have this particular Zone Policy.*

- **Apply Now to All Existing Devices:** Applies the Zone Rule to all devices in your organization. This does not apply the Zone Policy.

About Distinguished Names (DN)

Some things to know about Distinguished Names (DN) when using them in Zone Rules:

- Wildcards are not allowed, but you can use the Contains condition to accomplish similar results.
- DN errors and exceptions related to the Agent are captured in the log files.
- If the Agent finds DN information on the device, that information is automatically sent to the Console.
- When adding DN information, it must be properly formatted.
  - **Example:** CN=JDoe,OU=Sales,DC=cylance,DC=COM
  - **Example:** OU=Demo,OU=SEngineering,OU=Sales

Zones Device List

The Zones Device List displays all devices assigned to this zone. Devices can belong to multiple zones. Use the Export button to download a CSV file with information for all devices on the Zone Device List.

> **NOTE:** *If you do not have permission to view a zone and you click the zone link in the Zones column, you will see a Resource Not Found page.*

Zone Management Best Practices

Zones are best thought of as tags, where any device can belong to multiple zones (or have multiple tags). While there are no restrictions on the number of zones you can create, best practices identifies three different zone memberships between testing, policy, and role granularity within your organization.

These three zones consist of:

- Update Management
- Policy Management
- Role Based Access Management

Zone Organization for Update Management

One common usage of zones is to help manage Agent Updates. **CylancePROTECT** supports the latest Agent version and the previous version. This enables the enterprise to support change freeze windows, and do thorough testing of new Agent versions.

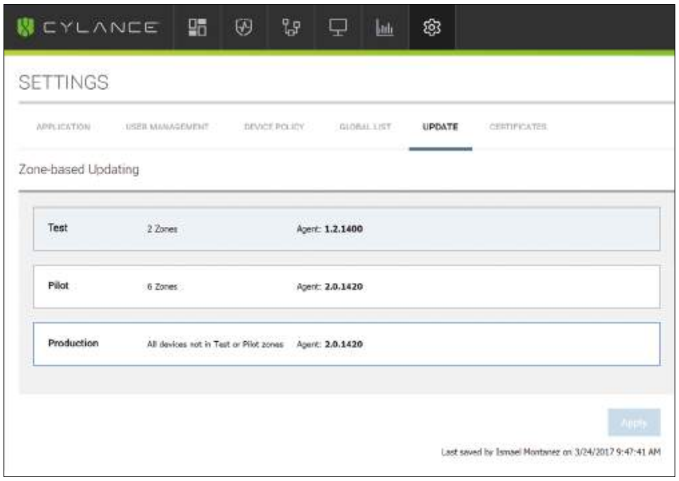
There are three suggested zone types used to direct and specify the agent testing and production phases:

- Update Zone — Test Group
- Update Zone — Pilot Group
- Update Zone — Production

Add a Test or Pilot Zone

1. Log in to the Console as an Administrator. Only Administrators can change the Agent Update settings.
2. Select **Settings > Update**.
3. For Test or Pilot zones, click **Select Test Zones** or **Select Pilot Zones**, then click on a **zone** to add it. If the Production Zone is set to **Auto-Update**, the Test and Pilot Zones are not available. Change Auto-Update in the Production Zone to something else to enable the Test and Pilot Zones.
4. Click **Please Select Version**, then select an Agent version to apply to the Test or Pilot zone.
5. Click **Apply**.

> **NOTE:** *For updating the Agent to the Production Zone, see Agent Update.*



SETTINGS

Zone-based Updating

Test	2 Zones	Agent: **1.2.1400**
Pilot	6 Zones	Agent: **2.0.1420**
Production	All devices not in Test or Pilot zones	Agent: **2.0.1420**

Last saved by Ismael Montanez on 3/24/2017 9:47:41 AM

Figure 20: Zone-based Updating

Zone Organization for Policy Management

Another set of zones to create should help apply different policies to different types of systems. Consider the following examples:

- Policy Zone — Windows Workstations
- Policy Zone — OS X Workstations
- Policy Zone — Servers
- Policy Zone — Servers — Exclusions
- Policy Zone — Executives — High Protection

In each one of these zones, it's suggested you apply a policy by default to all devices in this policy zone. Be careful not to put one device in multiple policy zones, as this can create a conflict over which policy is applied. Also remember that the Zone Rule engine can help automatically organize these hosts based on IP, Hostname, OS, and Domain.

Zone Organization for Role-Based Access Management

Role-based access is used to limit a console user's access to a group of systems the user is responsible for managing. This might include separation by IP range, host names, operating system, or domain.

Administrators can view everything in your organization's console. Zone Managers and Users can only view data from the zones to which they are assigned. This allows access based on the role (Administrator, Zone Manager, or User) assigned to the user.

Consider groupings by geographical location, type, or both.

- RBAC Zone — Desktops — Europe
- RBAC Zone — Servers — Asia
- RBAC Zone — Red Carpet (Executives)

In the example above, you could assign a Zone Manager to RBAC Zone — Desktops — Europe to give access to that zone only. The Zone Manager for RBAC Zone — Desktops — Europe would not be able to see RBAC Zone — Servers — Asia or RBAC Zone — Red Carpet (Executives), including any devices or threats that are unique to the other zones.

User Management

Administrators have global permissions and can add or remove users, assign users to zones (either as a Zone Manager or User), add or remove devices, create policies, and create zones. Administrators can also delete users, devices, policies, and zones permanently from the console.

Zone Managers and Users only have access and privileges pertaining to the Zone to which they are assigned.

A comprehensive list of user permissions allowed for each user can be accessed on the Console in the How-To Guide **(Profile > How-To Guide > User Permissions).**

To Add Users

1. Log in to the Console as an Administrator.
   Only Administrators can create Users.
2. Select **Settings > User Management**.
3. Under Add Users, type the user's email address, then select a Role.
   - **Administrator:** Has global permissions, can create users, policies, and zones.
   - **Zone Manager:** Assigned to one or more zones, can assign other Zone Manager and Users to their zone, and can quarantine or waive threats.
   - **User:** Assigned to one or more zones and can quarantine or waive threats.
4. Click **Add**. An email is sent to the user, with a link to create a password.

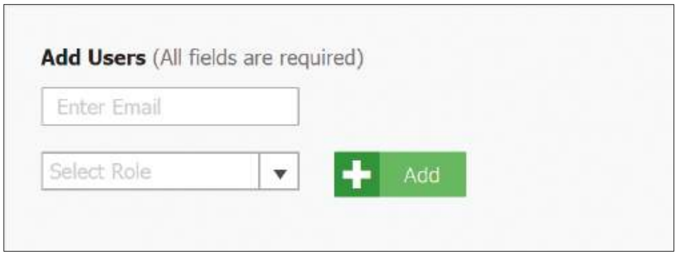


Figure 21: Add Users

To Change User Roles

1. Log in to the Console as an Administrator.
   Only Administrators can create Users.
2. **Select Settings > User Management**.
3. Click on a user. The User Details page displays.
4. Select a role, then click **Save**.

To Remove Users

1. Log in to the Console as an Administrator.
   Only Administrators can create Users.
2. Select **Settings > User Management**.
3. Select the checkbox for the user or users you want to remove, then click **Remove**. A message displays asking you to confirm the action.
4. Click **Yes**.

Network Related

You should configure your network to allow the Agent to communicate with the Console over the Internet. This section covers firewall settings and proxy configurations.

> **TIP: CylancePROTECT** *supports a Disconnected Mode for Agents disconnected from the network and cannot access the Console.*

Firewall

No on-premise software is required to manage endpoints. Agents are managed by and report to the Console. Port 443 (HTTPS) is used for communication and must be open on the firewall in order for the Agents to communicate with the Console. The Console is hosted by Amazon Web Services (AWS) and doesn't have any fixed IP addresses.

For a list of Cylance hosts to allow, based on the region to which your organization belongs, see Cylance Host URLs. Alternatively, you can allow HTTPS traffic to *.cylance.com.

Proxy

Proxy support for **CylancePROTECT** is configured through a registry entry. When a proxy is configured, the Agent will use the IP address and port in the registry entry for all outbound communications to Cylance servers.

1. Access the registry.

   > **NOTE:** *Depending on how the Agent was installed (Protected Mode enabled or not), you may need to elevate your privileges or take ownership of the registry.*

2. In Registry Editor, navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
3. Create a new String Value (REG_SZ):
   - Value Name = ProxyServer
   - Value Data = proxy settings (Example: http://123.45.67.89:8080)

In authenticated environments, the Agent attempts to use the credentials of the currently logged in user to communicate out to the Internet. If an authenticated proxy server is configured and a user is not logged onto the device, the Agent cannot authenticate to the proxy and cannot communicate with the Console. In this instance, either:

- Configure the proxy and add a rule to allow all traffic to *.cylance.com.
- Use a different proxy policy, allowing for unauthorized proxy access to Cylance hosts (*.cylance.com).

By doing this, if no user is logged onto the device, the agent will not need to authenticate and should be able to connect to the cloud and communicate with the Console.

Devices

Once an Agent is installed on a system, it becomes available as a device in the Console. You can now manage your devices by assigning policies (to handle identified threats), group your devices (using zones), and manually take actions on each device (Quarantine and Waive).

Device Management

Devices are systems with an Agent. You can manage your devices from the Console.

1. Log in to the Console as an Administrator. Only Administrators can manage Devices.
2. Click **Devices**.
3. Selecting a device checkbox allows the following actions:
   - **Export:** Creates and downloads a CSV file. The file contains device information (Name, State, Policy, etc.) for all devices in your organization.
   - **Remove:** Removes selected devices from the Device List. This does not uninstall the Agent from the device.
   - **Assign Policy:** Allows you to assign the selected devices to a policy.
   - **Add to Zones:** Allows you to add the selected devices to a zone or zones.
4. Clicking on a device displays the Device Details page.
   - **Device information:** Displays information like Hostname, Agent Version, OS Version, etc.
   - **Device Properties:** Allows changing the Device Name, Policy, Zones, and Logging Level.
   - **Threats & Activities:** Displays threat information and other activities related to the device.
5. Clicking **Add new device** displays a dialog box with your Installation Token and links to download the agent installer.
6. In the Zones column, clicking on a zone name displays the Zone Details page.

Threats & Activities

Displays threat information and other activities related to the selected device.

Threats

Displays all threats found on the device. By default, the threats are grouped by status (Unsafe, Abnormal, Quarantined, Waived, etc.).

- **Export:** Creates and downloads a CSV file that contains information for all threats found on the selected device. Threat information includes: Name, File Path, Cylance Score, Status, etc.).
- **Quarantine:** Quarantines the selected threats. This is a Local Quarantine, meaning this threat is only quarantined on this device. To quarantine a threat for all devices in your organization, make sure the Also, quarantine this threat any time it is found on any device checkbox is selected (Global Quarantine) when you quarantine a file.
- **Waive:** Changes the status of the selected threats to Waived. A waived file is allowed to run. This is a Local Waive, meaning this file is only allowed on this device. To allow this file on all devices in your organization, select the Also, mark as safe on all devices checkbox (Safe List) when you waive a file.

Exploit Attempts

Displays all exploit attempts on the device. This includes information about the Process Name, ID, Type, and Action taken.

Application Control

Displays all activities relevant to Application Control, like denied file changes. Application Control activities are also displayed in the Agent user interface, on the Events tab.

Agent Logs

Displays log files uploaded by the Agent on the device. The log file name is the date of the log. There are three ways to view agent log files:

- Upload the Current Log File for a single device. **Devices > Agent Logs**, then click **Upload Current Log File**. This could take a few minutes, depending on the size of the log file.
- Policy settings: **Settings > Device Policy > [select a policy] > Agent Logs**, then click **Enable auto-upload of log files** and click **Save**.

To view verbose logs, change the Agent Logging Level before you upload any log files.

- In the Console: **Devices > [click on a device]**, select **Verbose** from the Agent Logging Level drop-down menu, then click **Save**. After the verbose log files are uploaded, it is recommended to change the Agent Logging Level back to Information.
- On the Device, close the Cylance UI (right-click the Cylance icon in the system tray, then click Exit). Open the Command Line as an Administrator. Type cd C:\Program Files\Cylance\Desktop, then press **Enter**. Type CylanceUI.exe –a, then press Enter. The Cylance icon appears in the system tray. Right-click, select **Logging**, then click **All** (same as Verbose in the Console).

Script Control

Displays all activities relevant to Script Control, like denied scripts. This list includes the date/time of the event, the file path, and the action taken.

Duplicate Devices

When the Agent is first installed on a device, a unique identifier is created which is used by the Console to identify and reference that device. However, certain events, such as using a virtual machine image to create multiple systems, may cause a second identifier to be generated for the same device. If a duplicate entry appears on the Devices page in the Console, simply select the device and click the Remove button.

To aid in identifying such devices, use the column sorting feature on the Devices page to sort and compare the devices, typically by device name. Alternately, the Devices list can be exported as a .CSV file and then viewed in Microsoft Excel or something similar which has powerful sorting/ organizing features.

Example Using Microsoft Excel

1. Open the device CSV file In Microsoft Excel.
2. Select the device name column.
3. Select **Conditional Formatting > Highlight Cell Rules > Duplicate Values**. You can find this on the Home tab.
4. Make sure **Duplicate** is selected, then select a highlight option.
5. Click **OK**. Duplicate items are highlighted.

> **NOTE:** *The Remove command will only remove the device from the Device page. This will not issue an uninstall command to the Agent. The agent needs to be uninstalled at the endpoint.*

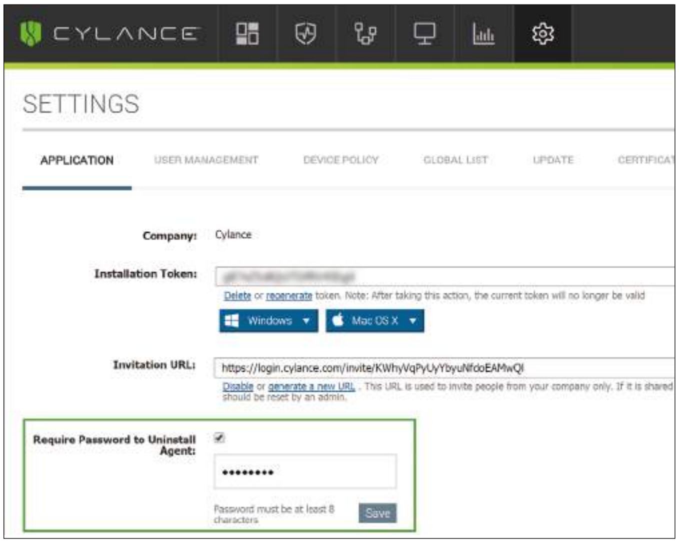
Password-Protected Uninstall

Settings > Application

Administrators can require a password for uninstalling the Agent. When users attempt to uninstall the Agent under this setting, they will be presented with a dialog box prompting for the uninstall password. If the uninstall is being performed using a command line, the following entry needs to be added to the uninstall string: UNINSTALLKEY = [MyUninstallPassword].

To Create an Uninstall Password

1. Log in to the Console as an Administrator.
2. Select **Settings > Application**.
3. Click the **Require Password to Uninstall Agent** checkbox.
4. Type a password, then click **Save**.



Company: Cylance

Installation Token: [redacted]

Delete or regenerate token. Note: After taking this action, the current token will no longer be valid

Invitation URL: https://login.cylance.com/invite/KWhyVqPyUyYbyuNfdoEAMwQI

Disable or generate a new URL . This URL is used to invite people from your company only. If it is shared should be reset by an admin.

Require Password to Uninstall Agent: ☑

••••••••

Password must be at least 8 characters

Figure 22: Configure Password-Protected Uninstall

Agent Update

Maintenance and management of Agents are hassle-free. Agents automatically download updates from the Console, and the Console is maintained by Cylance.

The Agent checks in with the Console every 1-2 minutes. The Console reports the agent's current state (Online or Offline, Unsafe or Protected), version information, operating system, and threat status.

Cylance releases updates to the Agent on a monthly basis. These updates can include configuration revisions, new modules, and program changes. When an Agent update is available (as reported by the Console under **Settings > Agent Updates**), the Agent automatically downloads and applies the update. In order to control network traffic during Agent updates, all organizations are set to accommodate a maximum of 1000 device updates simultaneously. Users can also disable the Auto Update feature if they prefer.

> **NOTE:** *The maximum number of devices for simultaneous update can be modified by Cylance Support.*

Zone-Based Updating

Zone-Based updating allows an organization to evaluate a new agent on a subset of devices before deploying it to the whole environment (Production). One or more current zones can be temporarily added to one of two testing zones (Test and Pilot) which can use a different agent than Production.

To Configure Zone-Based Updates:

1. Log in to the Console as an Administrator.

2. Select **Settings > Update**. If the Production Zone is set to **Auto-Update**, the Test and Pilot Zones are not available. Change Auto-Update in the Production Zone to something else to enable the Test and Pilot Zones.

3. Select a specific agent version in the Production dropdown list. For Production, the user can select also Auto-Update or Do Not Update.

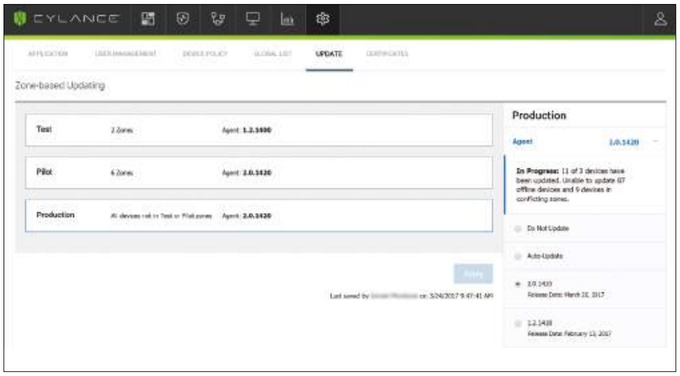
    a. **Auto-Update** will allow all Production devices to automatically update to the latest version in the Supported Agent Versions list.

    b. **Do Not Update** will prohibit all Production devices from updating the Agent.

4. For the Test Zone, choose one or more Zones from the Zone dropdown list, then select a specific Agent version from the version dropdown list

5. If desired, repeat step 4 for the Pilot Zone.

> **NOTE:** *When a device is added to a Zone that is part of the Test or Pilot Zone, that device will start using the Test or Pilot Zone's agent version. If a device belongs to more than one Zone, and one of those Zones belongs to either the Test or Pilot Zone, the Test or Pilot Zone agent version will take precedence. The priority is: Test, Pilot and then Production.*



Zone-based Updating

Test	2 Zones	Agent: 1.2.1400
Pilot	6 Zones	Agent: 2.0.1420
Production	All devices not in Test or Pilot zones	Agent: 2.0.1420

Last saved by [redacted] on: 5/24/2017 9:47:41 AM

Production

Agent 2.0.1420

In Progress: 11 of 3 devices have been updated. Unable to update 87 offline devices and 9 devices in conflicting zones.

○ Do Not Update

○ Auto-Update

● 2.0.1420
Release Date: March 20, 2017

○ 1.2.1410
Release Date: February 13, 2017

Figure 23: Agent Updates

To Trigger an Agent Update

An agent update can be triggered without having to wait for the next hourly interval. This requires accessing the device.

- Right-click the Agent icon (in the system tray), then select **Check for Updates**.
- Restart the **CylancePROTECT** service. This will force it to immediately check in with the Cylance Console.
- Alternatively, updates can also be initiated from the command line (run CylanceUI.exe –update from the Cylance directory).

Dashboard

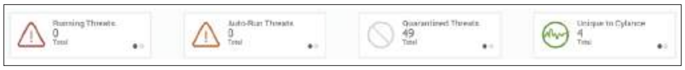
The Dashboard page displays once you log in to the Console. The Dashboard provides an overview of threats in your environment and provides access to different console information from one page.

Threat Statistics

Threat Statistics provide the number of threats found within the Last 24 Hours and the Total for your organization. Clicking on a Threat Statistic takes you to the Protection page and displays the list of threats related to that statistic.

- **Running Threats:** Files identified as threats that are currently running on devices in your organization.
- **Auto-Run Threats:** Threats set to run automatically.
- **Quarantined Threats:** Threats quarantined within the last 24 hours and the total.

Unique to Cylance: Threats identified by Cylance but not by other antivirus sources.



Running Threats
0
Total

Auto-Run Threats
0
Total

Quarantined Threats
49
Total

Unique to Cylance
4
Total

Figure 24: Policy Details > File Actions

Protection Percentages

Displays percentages for Threat Protection and Device Protection.

- **Threat Protection:** The percentage of threats on which you have taken action (Quarantine, Global Quarantine, Waive, and Safe Lists).
- **Device Protection:** The percentage of devices associated with a policy that has Auto-Quarantine enabled.

Threats By Priority

Displays the total number of threats that require an action (Quarantine, Global Quarantine, Waive, and Safe Lists). The threats are grouped by priority (High, Medium and Low). This overview displays the total number of threats that require an action, separates that total by priority, provides a percentage total, and how many devices are affected.

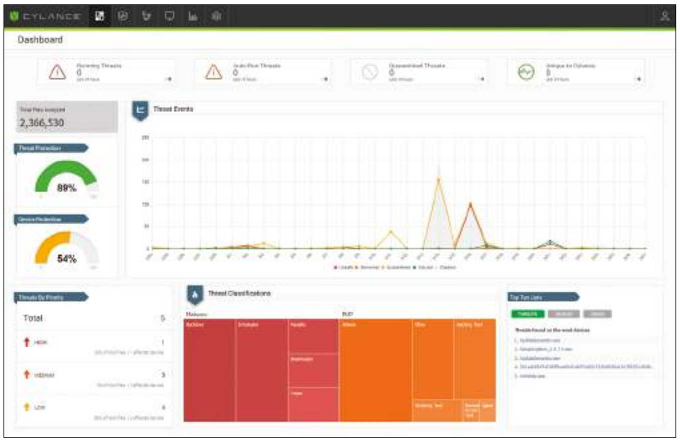


Figure 25: Cylance Dashboard

Threats are listed by priority in the lower left corner of the Dashboard page. Specified are the total number of threats in an organization grouped by their priority classifications.

A threat is classified as Low, Medium, or High based on the number of the following attributes it has:

- The file has a Cylance score greater than 80.
- The file is currently running.
- The file has run previously.
- The file is set to auto run.
- The priority of the zone where the threat was found.

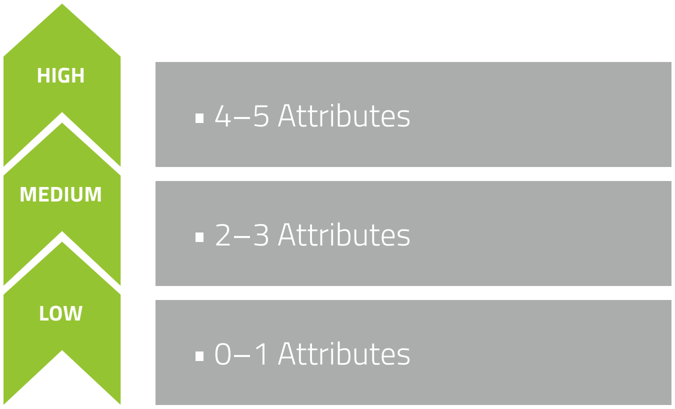


Figure 26: Threat Classifications

This classification helps Administrators determine which threats and devices to address first. Threat and device details can be viewed from this section of the Dashboard by clicking on either the threat or device number.

Threat Events

Displays a line graph with the number of threats discovered over the last 30 days. Lines are color-coded for Unsafe, Abnormal, Quarantined, Waived, and Cleared files.

- Hover over a point on the graph to view the details.
- Click on one of the colors in the legend to show/hide that line.

Threat Classifications

Displays a heat map of the types of threats found in your organization, like viruses or malware. Clicking on an item in the heat map takes you to the Protection page and displays a list of threats of that type.

Top Ten Lists

Displays lists for the Top 10 Threats found on the most devices, the Top 10 Devices with the most threats, and the Top 10 Zones with the most threats in your organization. Click on a list item for more details.

The Top 10 lists on the dashboard highlight Unsafe Threats in your organization that have not been acted upon (Unsafe files that have not been quarantined or waived). Most of the time these lists should be empty. While Abnormal Threats should also be acted upon, the focus of the Top 10 lists is to bring critical threats to your attention.

Protection — Threats

CylancePROTECT can do more than simply classify files as Unsafe or Abnormal. It can provide details on the static and dynamic characteristics of files. This allows administrators to not only block threats, but to understand threat behavior in order to further mitigate or respond to threats.

File Type

Unsafe: A file with a score ranging from 60-100. An Unsafe file is one in which the **CylancePROTECT** engine finds attributes that greatly resemble malware.

Abnormal: A file with a score ranging from 1-59. An Abnormal file has a few malware attributes but less than an unsafe file, thus is less likely to be malware.

> **NOTE:** *Occasionally, a file may be classified as Unsafe or Abnormal even though the score displayed doesn't match the range for the classification. This could result from updated findings or additional file analysis after the initial detection. For the most up-to- date analysis, enable Auto Upload in the Device Policy.*

Cylance Score

A Cylance score is assigned to each file that is deemed Abnormal or Unsafe. The score represents the confidence level that the file is malware. The higher the number, the greater the confidence.

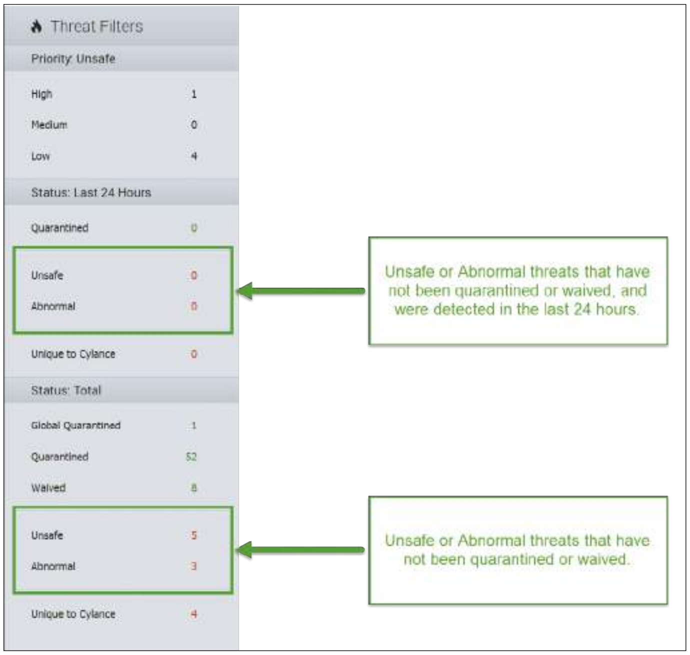
Viewing Threat Information

The Protection tab on the Console displays detailed threat information, the devices where the threats were found, and the actions taken on those devices for those threats.

To View Threat Details

1. Log in to the Console.
2. Click on the **Protection** tab to display a list of threats found in that organization.
3. Use the filter on the left menu bar to filter by Priority (high, medium, or low) and Status (Quarantined, Waived, Unsafe, or Abnormal).

> **NOTE:** *Numbers that are displayed in red on the left pane indicate outstanding threats that have not been quarantined or waived. Filter on those items to view a list of files that need to be examined.*



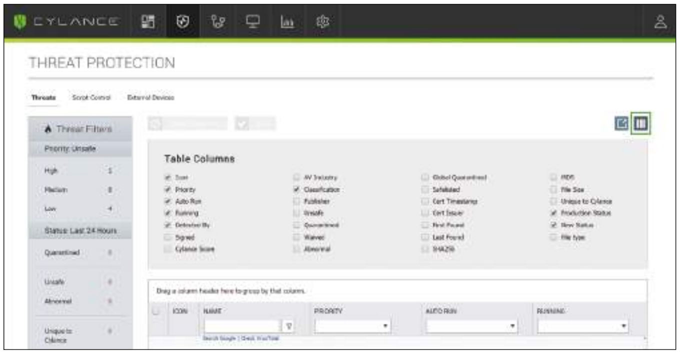
Threat Filters

Priority: Unsafe	
High	1
Medium	0
Low	4
Status: Last 24 Hours	
Quarantined	0
Unsafe	0
Abnormal	0
Unique to Cylance	0
Status: Total	
Global Quarantined	1
Quarantined	52
Waived	8
Unsafe	5
Abnormal	3
Unique to Cylance	4

Unsafe or Abnormal threats that have not been quarantined or waived, and were detected in the last 24 hours.

Unsafe or Abnormal threats that have not been quarantined or waived.

Figure 27: Protection Page Threat Filters



THREAT PROTECTION

Threats Script Control External Devices

Table Columns

- ☑ Icon
- ☑ Priority
- ☑ Auto Run
- ☑ Running
- ☑ Detected By
- □ Signed
- □ Cylance Score
- □ AV Industry
- ☑ Classification
- □ Publisher
- □ Unsafe
- □ Quarantined
- □ Waived
- □ Abnormal
- □ Global Quarantined
- □ Safelisted
- □ Cert Timestamp
- □ Cert Issuer
- □ First Found
- □ Last Found
- □ SHA256
- □ MD5
- □ File Size
- □ Unique to Cylance
- ☑ Production Status
- ☑ New Status
- □ File type

Drag a column header here to group by that column.

□	ICON	NAME	PRIORITY	AUTO RUN	RUNNING

Search Google | Check VirusTotal

Figure 28: Protection Page Threat Information

4. To view additional threat information, add columns by clicking the Table Column icon (see image above), then select a column name.

5. Additional information on a specific threat can be viewed either by clicking on the threat name link (details display on a new page) or by clicking anywhere in the threat's row (details display at the bottom of the page). Both views show the same content but have different presentation styles. The details include an overview of file metadata, a list of devices with the threat, and evidence reports.

a. File Metadata

- Classification (assigned by the Cylance Advanced Threat and Alert Management (ATAM) Team)
- Cylance score (confidence level)
- AV Industry conviction (links to VirusTotal.com for comparison to other vendors)
- Date first found, Date last found
- SHA256
- MD5
- File Information (author, description, version, etc.)
- Signature Details

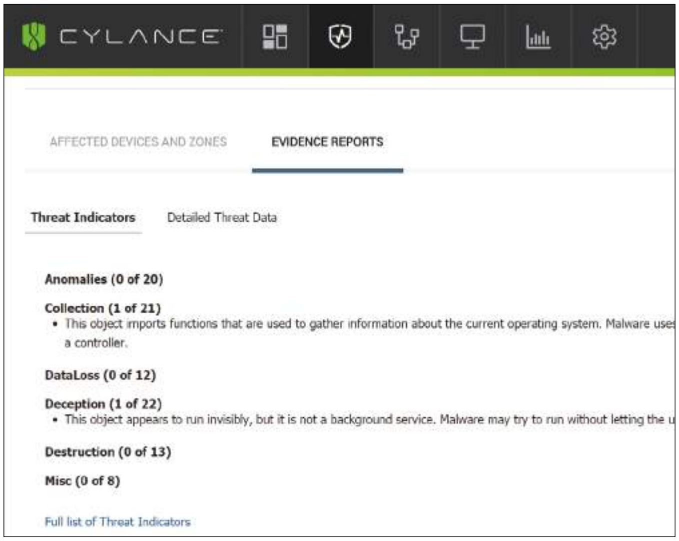
b. Devices

The Device/Zone list for a threat can be filtered by the threat's state (Unsafe, Quarantined, Waived, and Abnormal). Clicking on the state filter links will show the devices with the threat in that state.

- **Unsafe:** The file is classified as Unsafe, but no action has been taken.
- **Quarantined:** The file was already quarantined due to a policy setting.
- **Waived:** The file was waived or whitelisted by the Administrator.
- **Abnormal:** The file is classified as Abnormal, but no action has been taken.

c. Evidence Reports

- **Threat Indicators:** Observations about a file that the Cylance OEM Engine has analyzed. These indicators help understand the reason for a file's classification and provide insight into a file's attributes and behavior. Threat Indicators are grouped into categories to aid in context.
- **Detailed Threat Data:** Detailed Threat Data provides a comprehensive summary of the static and dynamic characteristics of a file, including additional file metadata, file structure details, and dynamic behaviors such as files dropped, registry keys created or modified, and URLs with which it attempted to communicate.



Anomalies (0 of 20)

Collection (1 of 21)

- This object imports functions that are used to gather information about the current operating system. Malware uses a controller.

DataLoss (0 of 12)

Deception (1 of 22)

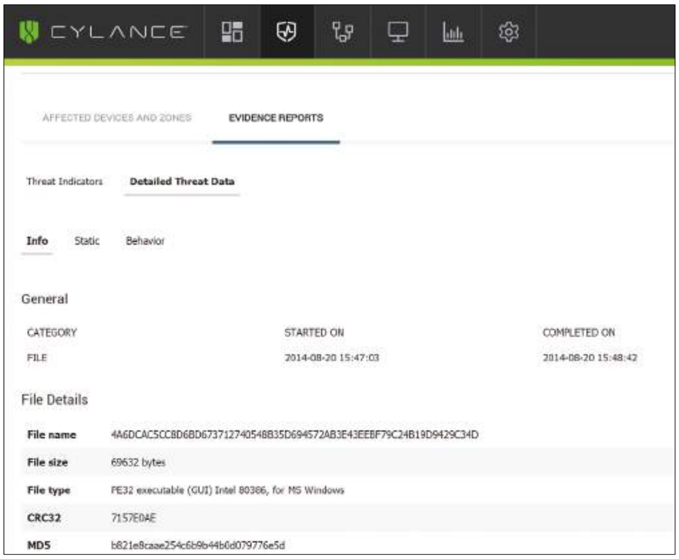
- This object appears to run invisibly, but it is not a background service. Malware may try to run without letting the u

Destruction (0 of 13)

Misc (0 of 8)

Full list of Threat Indicators

Figure 29: Threat Indicators



General

CATEGORY	STARTED ON	COMPLETED ON
FILE	2014-08-20 15:47:03	2014-08-20 15:48:42

File Details

File name	4A6DCAC5CC8D6BD67371274054BB35D694572AB3E43EEBF79C24B19D9429C34D
File size	69632 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	7157E0AE
MD5	b821e8caae254c6b9b44b0d079776e5d

Figure 30: Detailed Threat Data

To Save a Filter

After you have filtered for the threats you want to view, you can save these filters by bookmarking the page. The table columns selected and the filters applied creates a unique URL in the Console. Bookmarking the results page and then opening that bookmark later will apply the same columns and filters to the latest threat data.

You can share your saved filters by sharing the bookmark with other Console users in your organization. The results from using a filter might vary depending on the user role assigned to the user: Administrators can see everything in the Console, while Zone Managers and Users can only see the zones to which they are assigned (this includes devices and threats).

To View Threat Indicators:

1. Log in to the Console.
2. View a list of threats, click **Protection** in the top menu. Or click **Devices**, then select a device.
3. Click on the name of any threat. The Threat Details page displays.
4. Click on **Evidence Reports**.

Threat Indicator Categories

Each category represents an area that has been frequently seen in malicious software and is based on deep analysis of over 100 million binaries. The Threat Indicators report indicates how many of those categories were present in the file.

Anomalies

The file has elements that are inconsistent or anomalous in some way. Frequently, there are inconsistencies in the structure of the file.

Collection

The file has evidence of data collection. This can include enumeration of system configuration or collection of sensitive information.

Data Loss

The file has evidence of data exfiltration. This can include outgoing network connections, evidence of acting as a browser, or other network communications.

Deception

The file has evidence of attempts to deceive. Deception can be in the form of hidden sections, inclusion of code to avoid detection, or indications of improper labeling in metadata or other sections.

Destruction

The file has evidence of destructive capabilities. Destruction includes the ability to delete system resources such as files and directories.

Miscellaneous

All other indicators that do not fit into the aforementioned categories. For more detailed information on each Threat Indicator Category, refer to:

- https://support.cylance.com/hc/en-us/articles/203664403

> **NOTE:** *Occasionally, the Threat Indicators and Detailed Threat Data sections have no results or are not available. This happens when the file has not been uploaded. Debug logging may provide insight as to why the file was not uploaded.*

Addressing Threats

Determining the type of action to take on some threats may depend on a device's assigned user. Actions applied to threats can be applied at the device level or at a global level. Below are the different actions that can be taken against detected threats or files:

- **Quarantine:** Quarantining a specific file will prevent the file from being executed on that device.
- **Global Quarantine:** Globally quarantining a file will prevent the file from being executed on any device across the entire organization.

> **NOTE:** *Quarantining a file will move the file from its original location to the Cylance Quarantine directory (C:\ ProgramData\ Cylance\Desktop\q).*

- **Waive:** Waiving a specific file will allow that file to run on the device specified.
- **Global Safe:** Globally Safe Listing a file will allow that file to run on any device across the entire organization.

> **NOTE:** *Occasionally*, **CylancePROTECT** *may quarantine or report a "good" file (this could happen if the features of that file strongly resemble those of malicious files). Waiving or Globally Safe Listing the file can be useful in these instances.*

- **Upload File:** Manually upload a file to CylanceINFINITY for analysis. If Auto-Upload is enabled, new files (ones that have not been analyzed by Cylance) are automatically uploaded to CylanceINFINITY. If the file exists in CylanceINFINITY, then the Upload File button is unavailable (grayed out).
- **Download File:** Download a file for your own testing purposes. This feature must be enabled for your organization. The user must be an Administrator. The threat must be detected using Agent version 1320 or higher.

> **NOTE:** *The file must be available in CylanceINFINITY and all three hashes (SHA256, SHA1 and MD5) must match between CylanceINFINITY and the Agent. If not, then the Download File button is not available.*

Address Threats on a Specific Device

1. Log in to the Console.
2. Click on the **Devices** tab.
3. Search for and select the Device. Alternately, a link to the device may be available from the Protection tab if it is listed with an associated threat.
4. All threats on that device will be listed on the bottom of the page. Select the threat to either Quarantine or Waive the file on that device.

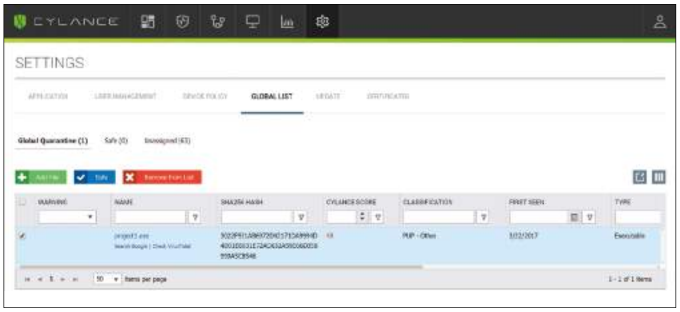
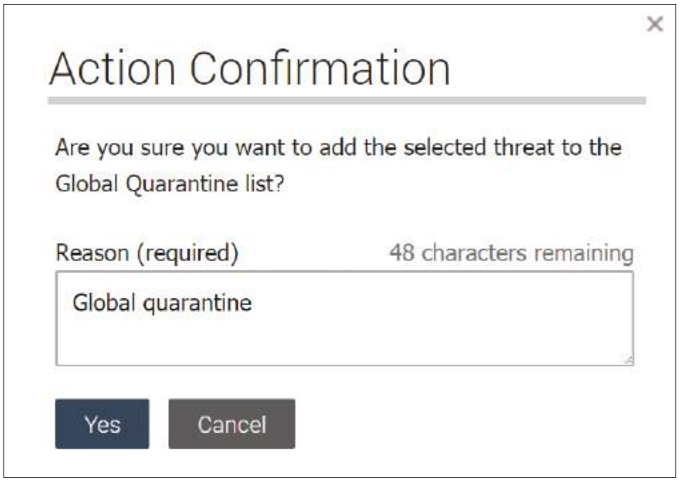


Figure 31: Global Quarantine List

Address Threats Globally

Files added to the Global Quarantine List or Global Safe List will either quarantine or allow the file on all systems across all zones.

1. Log in to the Console as an Administrator.
2. Click on **Settings > Global List**.
3. Click on **Global Quarantine or Safe**.
4. Click **Add File**.
5. Add the file's SHA256 (required), MD5, name, and the reason it's being placed on the global list.
6. Click **Submit**.



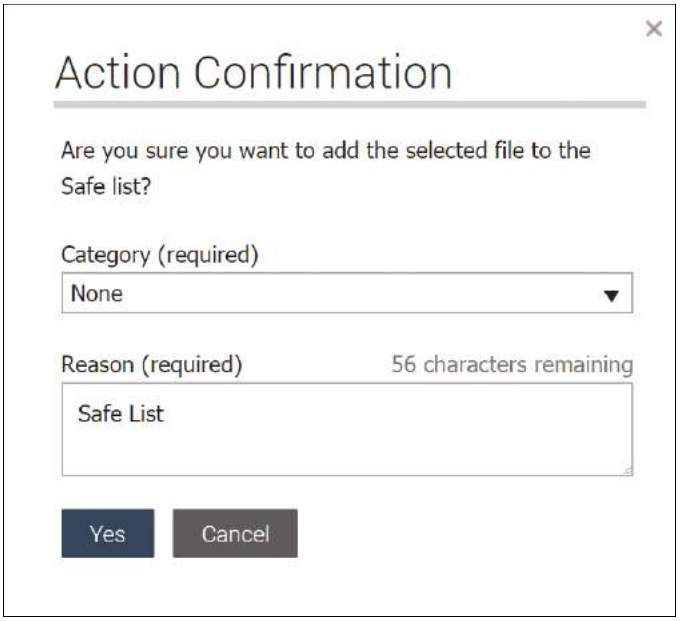
Action Confirmation

Are you sure you want to add the selected threat to the Global Quarantine list?

Reason (required) 48 characters remaining

Global quarantine

Figure 32: Global Quarantine List



Action Confirmation

Are you sure you want to add the selected file to the Safe list?

Category (required)

None

Reason (required) 56 characters remaining

Safe List

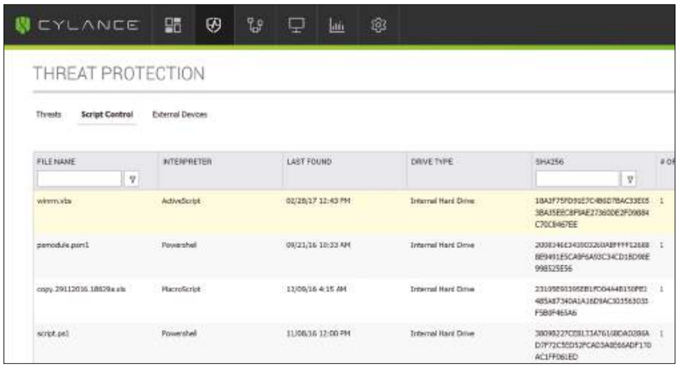
Figure 33: Global Safe List

Protection — Script Control

CylancePROTECT also provides details about Active scripts, PowerShell scripts, and Microsoft Office macros that have been blocked or alerted upon. With Script Control enabled, the results display on the Script Control tab on the Protection page. This provides details about the script and the devices affected.

To View Script Control Results

1. Log in to the Cylance Console as an Administrator.
2. Click on **Protection**, then click **Script Control**.
3. Select a script in the table. This updates the Details table with a list of affected devices.



THREAT PROTECTION

FILE NAME	INTERPRETER	LAST FOUND	DRIVE TYPE	SHA256	# OF
winrm.vbs	ActiveScript	02/28/17 12:43 PM	Internal Hard Drive	18A3F75FD91E7C4B6D7BAC33E05 3BA35EEC8F9AE273600E2F09884 C70C8467EE	1
pemodule.psm1	Powershell	09/21/16 10:33 AM	Internal Hard Drive	2008346E3430032E0ABFFFF12688 BE9491E5CA9F6A93C34CD18D98E 998525E56	1
copy.29112016.18829a.xls	MacroScript	12/09/16 4:15 AM	Internal Hard Drive	23105E90396EB1FD04A4B150FE1 485A87340A1A18D9AC303563033 F5B0F465A6	1
script.ps1	Powershell	11/08/16 12:00 PM	Internal Hard Drive	3809822?CE8133A761GBDAD286A D7F72C55D52FCAD3A8E66ADF170 AC1FF061ED	1

Figure 34: Script Tab — Protection Page

Script Control Column Descriptions

- **File Name:** The name of the script.
- **Interpreter:** The script control feature that identified the script.
- **Last Found:** The date and time the script was last run.
- **Drive Type:** The type of drive on which the script was found (example: Internal Hard Drive).
- **SHA256:** The SHA 256 hash of the script.
- **# of Devices:** The number of devices affected by this script.
- **Alert:** The number of times the script has been alerted upon. This could be multiple times for the same device.
- **Block:** The number of times the script was blocked. This could be multiple times for the same device.

Details Column Descriptions

- **Device Name:** The name of the device affected by the script. Click on the device name to go to the Device Details page.
- **State:** The state of the device (online or offline).
- **Agent Version:** The Agent version number currently installed on the device.
- **File Path:** The file path from which the script was executed.
- **When:** The date and time when the script was run.
- **Username:** The name of the logged in user when the script was run.
- **Action:** The action take on the script (alert or block).

Global List

Global Lists allow you mark files for quarantine or allow those files on all devices in your organization.

- **Global Quarantine:** All Agents in your organization will quarantine any file on the Global Quarantine list that is discovered on the device.
- **Safe:** All Agents in your organization will allow any file on the Safe List that is discovered on the device.
- **Unassigned:** Any threat identified in your organization that is not assigned to either the Global Quarantine or Safe List.

Change Threat Status

To change a threat status (Global Quarantine, Safe or Unassigned):

1. Log in to the Console as an Administrator.
2. Select **Settings > Global List**.
3. Select the list to which the threat is currently assigned.

   > **EXAMPLE:** *Click Unassigned to change an unassigned threat to either Safe or Global Quarantine.*

4. Click the checkboxes for the threats you want to change, then click a status button.
   a. **Safe:** Moves the files to the Safe List.
   b. **Global Quarantine:** Moves the files to the Global Quarantine List.
   c. **Remove from List:** Moves the files to the Unassigned List.

Add a File

You can manually add a file to the Global Quarantine or the Safe List. You must have the SHA256 hash information for the file you want to add.

1. Log in to the Console as an Administrator.
2. Select **Settings > Global List**.
3. Select the list to which you want to add the file (Global Quarantine or Safe).
4. Click **Add File**.
5. Type the SHA256 hash information. Optionally, type in the MD5 and File Name information.
6. Type a reason for adding this file.
7. Click **Submit**.

Export a List

You can export a Global List to a CSV file.

1. Log in to the Console as an Administrator.
2. Select **Settings > Global List**.
3. Select a list you want to export. You can filter the data before you export.
4. Click the **Export** icon.
5. Select **Everything** or **Current Filters**, then click **Export**.

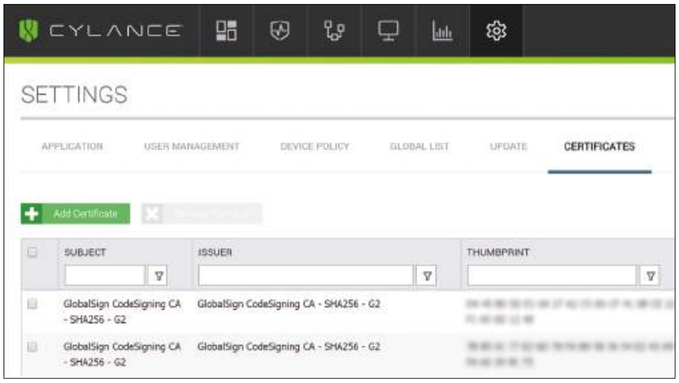
Safe List By Certificate

Customers have the ability to safe list files by signed certificate, allowing any custom software that is properly signed to run without interruption.

- This functionality allows customers to establish a white list/safe list by signed certificate which is represented by the SHA1 thumbprint of the certificate.
- Certificate information is extracted by the Console (Timestamp, Subject, Issuer, and Thumbprint). The certificate is not uploaded or saved to the Console.
- The certificate timestamp represents when the certificate was created.
- The Console does not check if the certificate is current or expired.
- If the certificate changes (examples: renewed or new), you should add it to the Safe List in the Console.

> **NOTE:** *This feature currently works with Windows operating systems only.*

1. Add the certificate details to the Certificate Repository.
    a. Identify the certificate thumbprint for the signed Portable Executable (PE).
    b. Select **Settings > Certificates**.
    c. Click **Add Certificate**.
    d. Either click **Browse for certificates to add** or drag-and-drop the certificate to the message box. If you browse for the certificates, the Open window displays and allows you to select them.
    e. Optionally, you can add notes about this certificate.
    f. Click **Submit**. The Issuer, Subject, Thumbprint, and Notes (optional) are added to the repository.
2. Add the Certificate to the Safe List.
    a. Select **Settings > Global List**, then select the **Safe** tab.
    b. Click **Certificates**, then click **Add Certificate**.
    c. Select a certificate from the Safe List. You can also select a Category and add a Reason for adding this certificate.
    d. Click **Submit**.



□	SUBJECT	ISSUER	THUMBPRINT
□	GlobalSign CodeSigning CA - SHA256 - G2	GlobalSign CodeSigning CA - SHA256 - G2	[redacted]
□	GlobalSign CodeSigning CA - SHA256 - G2	GlobalSign CodeSigning CA - SHA256 - G2	[redacted]

Figure 35: Certificate Repository

Viewing Thumbprints for a Threat

On the Protection tab, Threat Details now display the certificate thumbprint. From the screen, select **Add to Certificate** to add the certificate to the Repository.

Privileges

Add to Certificate is a function available to Administrators only. If the certificate is already added to the Certificate Repository, the Console displays **Go to Certificate**. Certificates are view only by Zone Managers, who will see the option **Go to Certificate**.

Integrations

The Console provides integration with some third party programs.

Syslog/SIEM

CylancePROTECT can integrate with Security Information Event Management (SIEM) software using the Syslog feature. Syslog events are persisted at the same time the Agent events are persisted to the Console.

See SIEM/Syslog for more information.

Custom Authentication

Use external Identity Providers (IdP) to log in to the Console. This requires configuring settings with your IdP to obtain an X.509 certificate and a URL for verifying your IdP login. Custom Authentication works with Microsoft SAML 2.0. This feature has been confirmed to work with OneLogin, Okta, Microsoft Azure, and PingOne. This feature also provides a Custom setting and should work with other Identity Providers who follow Microsoft SAML 2.0.

> **NOTE:** *Custom Authentication does not support Active Directory Federation Services (ADFS).*

- **Strong Authentication:** Provides multi-factor authentication access.
- **Single Sign-On:** Provides single sign-on (SSO) access.

> **NOTE:** *Selecting Strong Authentication or Single Sign-On does not affect the Custom Authentication settings, because all configuration settings are handled by the Identity Provider (IdP).*

- **Allow Password Login:** Selecting this option allows you to log in to the Console directly and using SSO. This allows you to test your SSO settings without being locked out of the Console. Once you have successfully logged into the Console using SSO, it is recommended that you disable this feature.
- **Provider:** Select the service provider for the custom authentication.
- **X.509 Certificate:** Enter the X.509 certification information.
- **Login URL:** Enter the URL for the custom authentication.

Threat Data Report

Comma-separated value files (CSV) that contain the following information about your organization:

- **Threats:** Lists all threats discovered in your organization. This information includes File Name and File Status (Unsafe, Abnormal, Waived, and Quarantined).
- **Devices:** Lists all devices in your organization that have an Agent installed. This information includes Device Name, OS Version, Agent Version, and Policy applied.
- **Events:** Lists all events related to the Threat Events Graph on the Dashboard, for the last 30 days. This information includes File Hash, Device Name, File Path, and the Date the event occurred.
- **Indicators:** Lists each threat and the associated threat characteristics.
- **Cleared:** Lists all files that have been cleared in your organization. This information includes files that were Waived, added to the Safe List, or deleted from the quarantine folder on a device.

When this feature is enabled, the report is automatically updated at 1:00 AM Pacific Standard Time (PST).

The Threat Data Report provides URLs and a token that can be used to download each report without requiring a login to the Console. You can also delete or regenerate the token, as needed, allowing you to control who has access to the report.

Profile

The profile menu (upper-right corner) allows you to manage your account, view Console audit logs, and find product help.

My Account

You can change your password and change your email notification setting on the My Account page.

1. Log in to the Console.
2. Click the profile menu in the upper-right corner, then select **My Account**.
3. To change your password:
   a. Click **Change Password**. Password fields display.
   b. Type your old password.
   c. Type your new password, then retype it to confirm it.
   d. Click **Update**.
4. To enable or disable Email Notifications, click the checkbox. Enabling and disabling the checkbox is automatically saved. Email Notifications are available for Administrators only.

Audit Logging

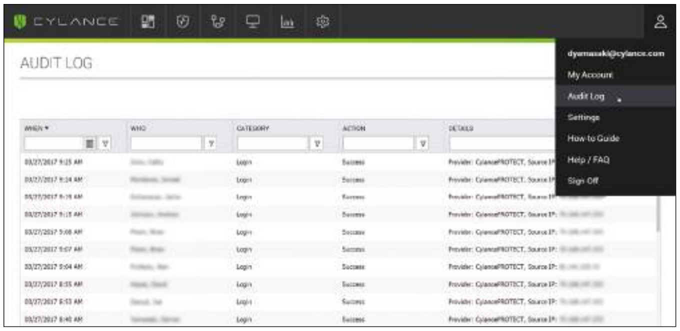
User Icon Dropdown list (upper-right hand corner of console)

The Audit Log contains information pertaining to the following actions performed from the console interface:

- Log in (Success, Failure)
- Policy (Add, Edit, Remove)
- Device (Edit, Remove)
- Threat (Quarantine, Waive, Global Quarantine, Safe List)
- User (Add, Edit, Remove)
- Agent Update (Edit)

The Audit Log can be viewed from the console by navigating to the profile dropdown list on the upper-right side of the console, and selecting **Audit Log**. Audit logs are available for Administrators only.

The Audit Log can be exported as a CSV file for use in other applications. Click the **Export** button on the Audit Log page.



AUDIT LOG

WHEN ▾	WHO	CATEGORY	ACTION	DETAILS
03/27/2017 9:25 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP
03/27/2017 9:24 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP
03/27/2017 9:16 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP
03/27/2017 9:15 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]
03/27/2017 9:08 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]
03/27/2017 9:07 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]
03/27/2017 9:04 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]
03/27/2017 8:55 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]
03/27/2017 8:53 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]
03/27/2017 8:40 AM	[redacted]	Login	Success	Provider: CylancePROTECT, Source IP: [redacted]

Figure 36: Audit Log

Settings

Takes you to the Settings page with the Application, User Management, Device Policy, Global List, and Agent Update tabs. The Settings menu item is available for Administrators only.

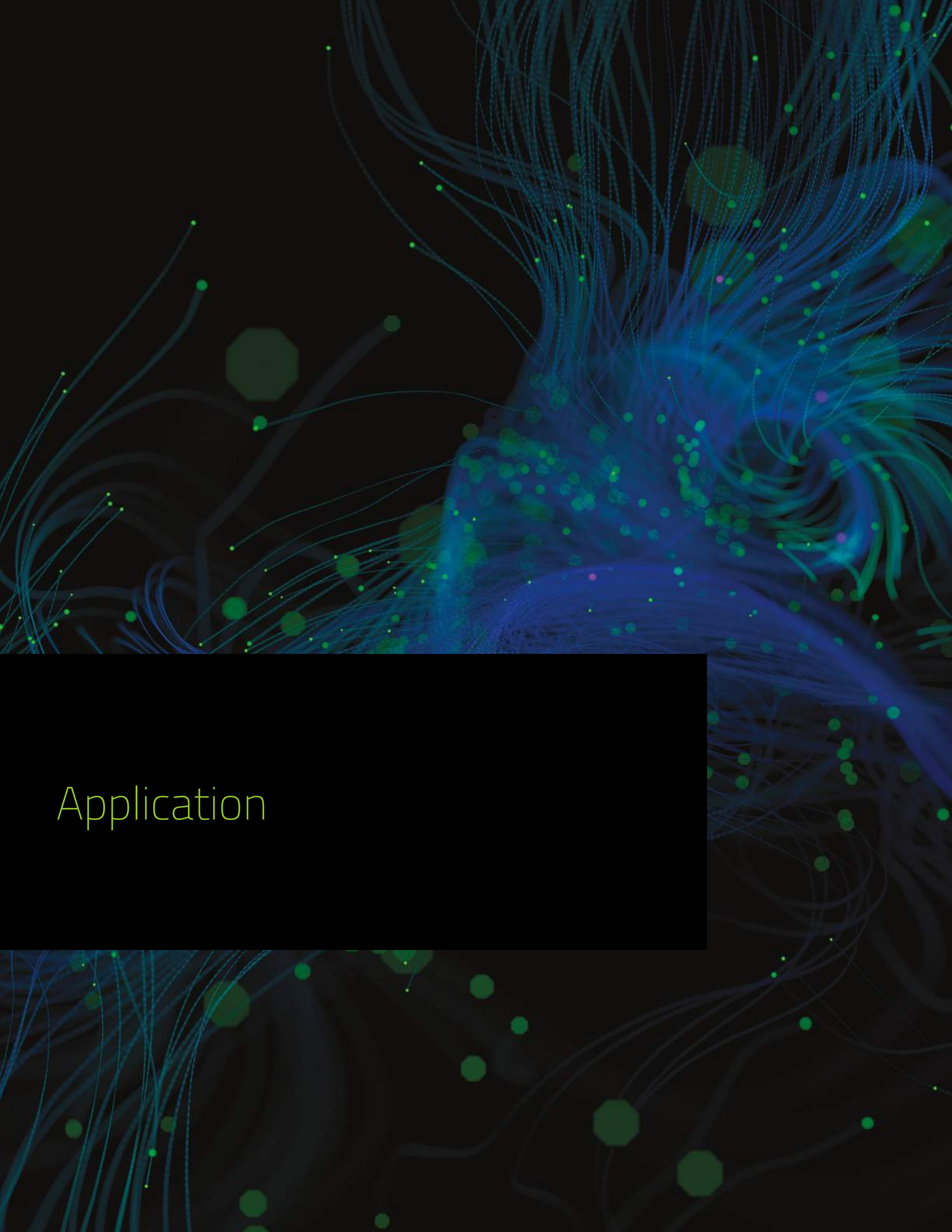
How-To Guide

Online guide with section-by-section tutorials for using the Console.

Help and FAQ

Help and Frequently Asked Questions (FAQ) are hosted on the Support website. Clicking the Help/FAQ link in the profile menu (upper-right corner of the Console) takes you to the Cylance Support homepage

Application



Devices are added to your organization by installing the **CylancePROTECT** Agent on each system. Once connected to the Cylance Console, you can apply policies (to manage identified threats) and organize your devices based on your needs.

The Agent is designed to use a minimal amount of system resources. The Agent treats files or processes that execute as a priority because these events could be malicious. Files that are simply on disk (in storage but not executing) take a lower priority because while these could be malicious, these do not pose an immediate threat.

Windows Agent

System Requirements

> **NOTE:** *It is recommended that system hardware (CPU, GPU, etc.) meets or exceeds the Recommended Requirements of the target operating system. Exceptions are noted below (RAM, available hard drive space and additional software requirements).*

Operating Systems	▪ Windows XP SP3 with KB 968730 (32-bit & 64-bit) ▪ Windows Vista (32-bit & 64-bit) ▪ Windows 7 (32-bit & 64-bit) ▪ Windows 8 and 8 .1 (32-bit & 64-bit) ▪ Windows 10 (32-bit & 64-bit; Enterprise, Pro and Home) • Windows 10 Anniversary Update requires Agent 1400 or higher ▪ Windows Server 2003 SP2 with KB 968730 (32-bit & 64-bit) ▪ Windows Server 2008 and 2008 R2 (32-bit & 64-bit) • Server Core is not supported ▪ Windows Server 2012 and 2012 R2 (64-bit) • Server Core and Minimal Server Interface are not supported ▪ Windows Server 2016 (Standard, Data Center and Essentials) • Windows Server 2016 requires Agent 1410 or higher
RAM	2 GB
Available Hard Drive Space	300 MB
Additional Software/Requirements	▪ .NET Framework 3 .5 (SP1) or higher (Windows only) ▪ Internet Browser ▪ Internet access to log in, access the installer, and register the product ▪ Local administrator rights to install the software
Other	▪ TLS 1.2 is supported with Agent version 1420 or higher

Table 1: System Requirements for Windows

To Download the Install File

1. Log in to the Console.
2. Select **Settings > Application**.
3. Copy the **Installation Token**. The Installation Token is a randomly generated string of characters that enables the Agent to report to its assigned account on the Console. The Installation Token is required during installation, either in the installation wizard or as an installation parameter setting.
4. Download the Installer. Click on the **Operating System**, then select the file type to download. For Windows, it is recommended to use the MSI file for installing the Agent.

> **TIP:** *If you set up a Zone Rule, devices can be automatically assigned to a zone if the device matches the rule criteria.*

Install the Agent — Windows

1. Double-click the **CylancePROTECT** install file (MSI or EXE). The **CylancePROTECT** install window displays.
2. Click **Install**.
3. Enter or copy/paste the Installation Token, then click **Next**. The Destination Folder step displays.

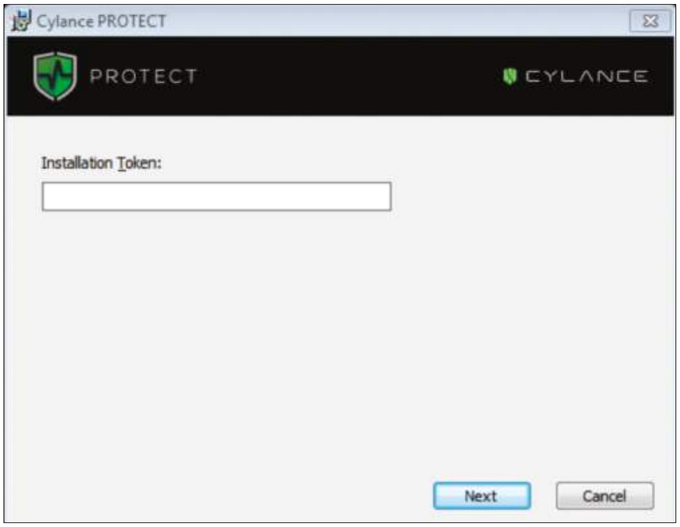


Figure 37: Enter the Installation Token

4. Click **OK**. When installation is done, the Completed step displays.
5. Click **Finish**. *The Agent does not require a reboot when it is installed.*

> **NOTE:** *The Agent can run with Windows Defender installed on a device. This requires Agent version 1370 (and higher), a fresh installation of the Agent (not an upgrade), and Windows Defender must be running.*

Installation Parameters — Windows

The Agent can be installed interactively or non-interactively through GPO, SCCM, MSIEXEC, etc. The MSIs can be customized with built-in parameters (shown in the table below) or the parameters can be supplied from the command line.

Property	Value	Description
LAUNCHAPP	0 or 1	0: The System Tray icon and the Start Menu folder is hidden at run-time 1: The System Tray icon and Start Menu folder is not hidden at run-time (default)
SELFPROTECTIONLEVEL	1 or 2	1: Only Local Administrators can make changes to the registry and services. 2: Only the System Administrator can make changes to the registry and services. This is the default setting.
APPFOLDER	<Target Installation Folder>	Specifies the agent install directory The default location is: C:\Program Files\Cylance\Desktop
REGWSC	0 or 1	0: Indicates that CylancePROTECT is not registered with Windows as an anti-virus program. Allows CylancePROTECT and Windows Defender to run at the same time on the device. 1: Indicates that CylancePROTECT is registered with Windows as an antivirus program.
VENUEZONE	“zone_name”	Assigns the device to the zone. Requires Agent version 1380 or higher. Replace zone_name with the name of the zone. If the zone_name does not exist, the zone is created with the given name. **NOTE:** *Adding spaces before or after the zone name will create a new zone.*

Table 2: Installation Parameters for Windows

The following command line example shows how to run the Microsoft Windows Installer Tool (MSIEXEC) passing it the PIDKEY, APPFOLDER, and LAUNCHAPP installation parameters:

```
▪ msiexec /i CylancePROTECT_x64.msi /qn PIDKEY=<INSTALLATION TOKEN> LAUNCHAPP=0 /L *v C:\temp\install.log
```

The install will be silent and the installation log will be saved to C:\temp. When the Agent is running, both the System Tray icon and the Start Menu Cylance folder will be hidden. Additional information regarding different command line switches accepted by MSIEXEC can be found on KB 227091.

Uninstall the Agent — Windows

To uninstall the Agent on a Windows system, use the Add/Remove Programs feature or use the Command Line. The Agent does not require a system reboot when it is uninstalled.

> **NOTE:** *The Agent uses msiexec to uninstall. There are some events, unrelated to the Agent, that require msiexec to reboot the system. If one of these events happens during a session when the Agent is uninstalled, then the system must be rebooted.*

Uninstalling the Agent on the device does not remove the device from the Console. You must manually remove the device from the Console.

Before you attempt to uninstall the Agent:

- If **Require Password to Uninstall Agent** (Settings > Application) is enabled, make sure you have the password to uninstall the product.
- If **Prevent Service Shutdown from Device** (Settings > Device Policy > Protection Settings) is enabled, either disable it in the policy or apply a different policy to the devices from which you want to uninstall the agent. Another method is to delete the device from the Console and then restart the device. This should unregister the device and allow you to uninstall the Agent.

To Uninstall Using Add/Remove Programs

1. Select **Start > Control Panel**.
2. Click **Uninstall a Program**. If you have Icons selected instead of Categories, then click Programs and Features.
3. Select **CylancePROTECT**, then click **Uninstall**.

To Uninstall Using the Command Line

1. Open the Command Prompt as an Administrator.

2. Use the following commands, based on the installation package you used to install the Agent.

   a. **CylancePROTECT**_x64.msi

      - **Standard uninstall:** msiexec /uninstall **CylancePROTECT**_x64.msi
      - **Windows Installer:** msiexec /x **CylancePROTECT**_x64.msi

   b. **CylancePROTECT**_x86.msi

      - **Standard uninstall:** msiexec /uninstall **CylancePROTECT**_x86.msi
      - **Windows Installer:** msiexec /x **CylancePROTECT**_x86.msi

   c. **CylancePROTECT**Setup.exe

      - **CylancePROTECT**Setup.exe /uninstall

3. The following commands are optional:

   a. **For quiet uninstall:** /quiet

   b. **For quiet and hidden:** /qn

   c. **For password protection uninstall:** UNINSTALLKEY=<password>

   d. **For uninstall log file:** /Lxv* <path>

This creates a log file at the designated path (<path>). Include the filename. Example: C:\Temp\Uninstall.log

OS X Agent

System Requirements

> **NOTE:** *It is recommended that system hardware (CPU, GPU, etc.) meets or exceeds the Recommended Requirements of the target operating system. Exceptions are noted below (RAM, available hard drive space and additional software requirements).*

Operating Systems	▪ Mac OS X 10.9 ▪ Mac OS X 10.10 ▪ Mac OS X 10.11 ▪ macOS 10.12 • macOS 10.12 requires Agent 1410 or higher
RAM	▪ 2 GB
Available Hard Drive Space	▪ 300 MB
Other	▪ TLS 1.2 is supported with Agent version 1420 or higher

Table 3: System Requirements for Windows

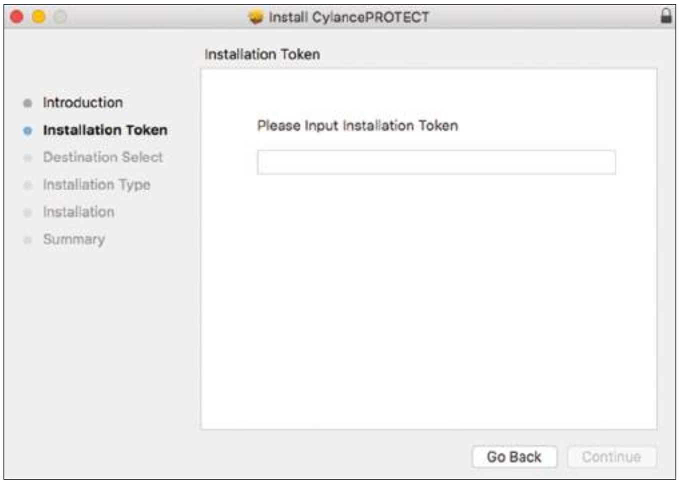
To Download the Install File

1. Log in to the Console.
2. Select **Settings > Application.**
3. Copy the **Installation Token**. The Installation Token is a randomly generated string of characters that enables the Agent to report to its assigned account on the Console. The Installation Token is required during installation, either in the installation wizard or as an installation parameter setting.
4. Download the Installer. Click on the **Operating System**, then select the file type to download.

> **TIP:** *If you set up a Zone Rule, devices can be automatically assigned to a zone if the device matches the Zone Rule criteria.*

Install the Agent — OS X

1. Double-click the **CylancePROTECT** setup file (PKG or DMG). The **CylancePROTECT** setup displays.
2. Click **Install**.
3. Enter or copy/paste the Installation Token, then click **Next**. The Destination Folder step displays.



Please Input Installation Token

Figure 38: Enter the Installation Token

4. Click **OK**. When installation is done, the Completed step displays.
5. Click **Finish**.

Installation — System Management

The Agent can be installed directly on each system or through a system management software. Examples: GPO, SCCM, and MSIEXEC. When installing the Agent, Installation Parameters are provided to configure some installation settings.

> **NOTE:** *Ensure the target devices meet System Requirements and that you have the proper credentials for installing software.*

Install the Agent

Install Without the Installation Token

```
sudo installer –pkg CylancePROTECT.pkg –target/
```

Install with the Installation Token

```
echo[install_token]>cyagent_install_token sudo
installer –pkg CylancePROTECT.pkg –target/
```

> **NOTE:** *Replace [install_token] with your Installation Token. The echo command outputs a cyagent_install_token file, which is a text file with one installation option per line. This file must be in the same folder as the installation package.*

Optional Installation Parameters

You can type the following in Terminal to create a file (cyagent_install_token) that the installer will use and apply the options you entered. Each parameter must be on its own line. This file must be in the same folder as the installation package.

The following is simply an example. You do not need to include all of the parameters in your file. Terminal will include everything contained within the single quotes into the file. Be sure to press Return after each parameter to keep each parameter on its own line in the file.

You can also create a file with a text editor that includes each parameter (on its own line). Just make sure the file is in the same folder as the installation package.

Example:

```
echo ‘InstallToken

NoCylanceUI SelfProtectionLevel=2

LogLevel=2’> cyagent_install_token

sudo installer –pkg CylancePROTECT.pkg –target/
```

Installation Parameters — OS X

The Agent can be installed using command line options in the Terminal. The examples below use the PKG installer. For the DMG, simply change the file extension in the command.

To use the Optional Installation Parameters

Property	Value	Description
InstallToken		Installation token available in the Console.
NoCylanceUI		The Agent icon should not appear on startup. The default is Visible.
SelfProtectionLevel	1 or 2	1: Only Local Administrators can make changes to the registry and services. 2: Only the System Administrator can make changes to the registry and services. This is the default setting.
LogLevel	0, 1, 2, or 3	0: Error — Only error messages are logged. 1: Warning — Error and warning messages are logged. 2: Information (default) — Error, warning, and information messages are logged. This may provide some details during troubleshooting. 3: Verbose — All messages are logged. When troubleshooting, this is the recommended log level. However, verbose log file sizes can grow very large. It is recommended to turn Verbose on during troubleshooting and then change it back to Information when troubleshooting is complete.
VENUEZONE	“zone_name”	Assigns the device to the zone. Requires Agent version 1380 or higher. Replace zone_name with the name of the zone. If the zone_name does not exist, the zone is created with the given name. **NOTE:** *Adding spaces before or after the zone name will create a new zone.*

Table 4: Installation Parameters for OS X

Uninstall the Agent — OS X

> **NOTE:** *Uninstalling the Agent on the device does not remove the device from the Console. You must manually remove the device from the Console.*

Before you attempt to uninstall the Agent:

- If **Require Password to Uninstall Agent** (Settings > Application) is enabled, make sure you have the password to uninstall the product.
- If **Prevent Service Shutdown from Device** (Settings > Device Policy > Protection Settings) is enabled, either disable it in the policy or apply a different policy to the devices from which you want to uninstall the agent. Another method is to delete the device from the Console and then restart the device. This should unregister the device and allow you to uninstall the Agent.

Without Password

```
sudo /Applications/Cylance/Uninstall\
CylancePROTECT.app/Contents/MacOS/
Uninstall\ CylancePROTECT
```

With Password

```
sudo /Applications/Cylance/Uninstall\
CylancePROTECT.app/Contents/MacOS/
Uninstall\ CylancePROTECT --pass-
word=thisismypassword
```

> **NOTE:** *Replace thisismypassword with the uninstall password created in the Console.*

Agent Service

Start Service

```
sudo launchctl load /Library/launchdaemons/
com.cylance.agent_service.plist
```

Stop Service

```
sudo launchctl unload /Library/launchdaemons/
com.cylance.agent_service.plist
```

Installation Verification

Users can verify the Agent installation was successful by checking the following:

1. The program folder was created.
    - **Windows default:** C:\Program Files\Cylance\Desktop
    - **OS X default:** /Applications/Cylance/
2. The Agent icon is visible in the System Tray of the target device.

    This doesn't apply if parameter LAUNCHAPP=0 (Windows) or NoCylacneUI (OS X) was used.
3. There is an Agent folder under Start Menu\ All Programs on the target device.

    This doesn't apply if parameter LAUNCHAPP=0 (Windows) or NoCylacneUI (OS X) was used.
4. The Agent service was added and is running.

    There should be a Cylance service listed as running in the Windows Services panel of the target device.
5. The CylanceUI.exe process is running.

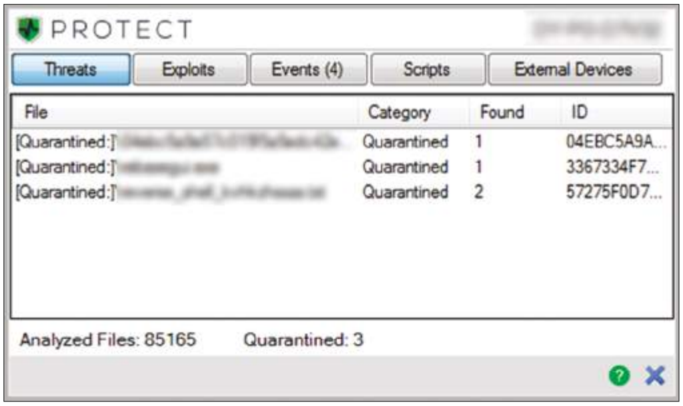
    There should be a CylanceUI.exe process listed under the Processes tab in the Windows Task Manager of the target device.
6. The device is reporting to the Console.

    Log in to the console and click on the Devices tab. The target device should show up and be listed in the online state.

Agent UI

The Agent user-interface is enabled by default and available by clicking on the Agent icon in the system tray. You can install the Agent and hide the Agent icon from the system tray.

Threats Tab



File	Category	Found	ID
[Quarantined:] [redacted]	Quarantined	1	04EBC5A9A...
[Quarantined:] [redacted]	Quarantined	1	3367334F7...
[Quarantined:] [redacted]	Quarantined	2	57275F0D7...

Analyzed Files: 85165 Quarantined: 3

Figure 39: Agent User Interface

Displays all threats discovered on the device and the action taken. Unsafe means no action has been taken on the threat. Quarantined means the threat has been modified (to keep the file from executing) and has been moved to the quarantine folder.

Waived means a file is deemed safe by your administrator and allowed to run on the device.

Events Tab

Displays any threat events that have occurred on the device.

Scripts Tab

Displays any malicious scripts that have run on the device and any action taken on the script.

Agent Menu

The Agent menu provides access to help and updates for **CylancePROTECT**. You can access the Advanced UI that provides more menu options.

Agent Menu

The Agent menu allows users to perform some actions on the device. Right-click the Agent icon to see the menu.

- **Visit Cylance.com:** Opens the Cylance website (cylance.com) in your default web browser.
- **Help/FAQ:** Opens the Cylance Support website (support.cylance.com) in your default web browser.
- **Check for Updates:** The Agent will check for and install any updates available. Updates are restricted to the Agent version allowed for the zone to which the device belongs.
- **About:** Displays a dialog box with the Agent version, name of the policy assigned to the device, the last time the Agent checked for an update, and the installation token used during installation.
- **Exit:** Closes the Agent icon in the system tray. This does not turn off any of the Cylance services.
- **Options > Show Notifications:** Selecting this option will display any new events as notifications.

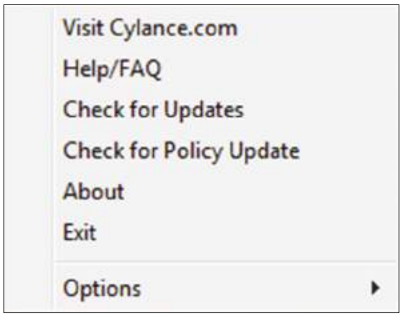


Figure 40: Agent Menu

Enable Agent UI Advanced Options

The Agent provides some advanced options via the UI to provide features on systems without connectivity to the Console. The CylanceSVC.exe must be running when you enable the Advanced Options.

1. If the Agent icon is visible in the system tray, right-click the icon, then select Exit.
2. Launch the Command Prompt.
3. Type cd C:\Program Files\Cylance\desktop, then press Enter. If the application was installed in a different location, you must navigate to that location in the command prompt.
4. Type CylanceUI.exe –a, then press Enter. The Agent icon will appear in the system tray.
5. Right-click the icon. You can now see Logging, Run a Detection, and Threat Management options.

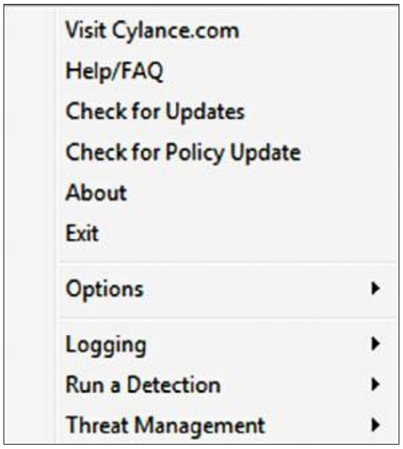


Figure 41: Agent Advanced UI Options

Logging

Select the level of log information to collect from the Agent. The default is Information. For troubleshooting, it is recommended to set the log level to All (Verbose). When troubleshooting is complete, change this back to Information because logging All information can generate very large log files.

Run a Detection

Allows users to specify a folder to scan for threats. Select Run a Detection > Specify Folder. Select a folder to scan, then click **OK**. Any threats found appear in the Agent UI.

Threat Management

Allows users to delete quarantined files on the device. Select Threat Management > Delete Quarantined, then click **OK** to confirm.

Enable Submitting Helpdesk Tickets

Add a menu item to the Agent UI to submit a ticket to your internal helpdesk for a threat. The ticket is sent using the default web browser.

Prerequisites

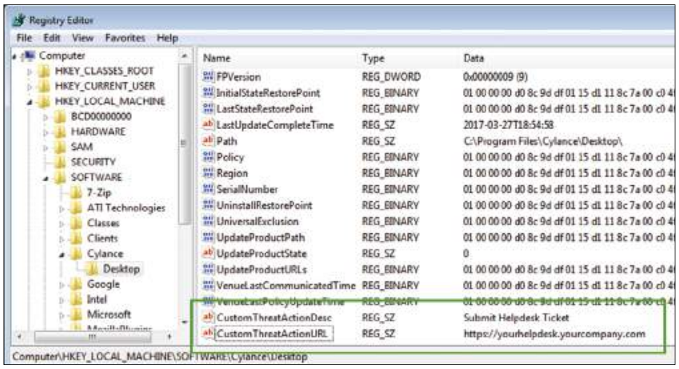
- Agent version 1300 and higher
- URL with an HTTP GET request (for submitting tickets)

Create a Custom Action

1. On the device, open the Registry Editor.

> **NOTE:** *Self Protection might need to be disabled to perform this step.*

2. Navigate to the Cylance Desktop folder. HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
3. Right-click inside the Registry Editor, then select **New > String Value**. A new string value is added to the registry.
4. Type CustomThreatActionDesc to name the value, then press **Enter**. This renames the value.
5. Double-click **CustomThreatActionDesc**, type a message to display and then click **OK**. This message displays when users right-click a threat in the Agent UI. Example: Submit Helpdesk Ticket.
6. Right-click inside the Registry Editor, select **New > String Value**, type CustomThreatActionURL, then press **Enter**.
7. Double-click **CustomThreatActionURL**, type the URL to which you wish to send the ticket information, then click **OK**.
8. Exit and restart the Agent UI.



Name	Type	Data
FPVersion	REG_DWORD	0x00000009 (9)
InitialStateRestorePoint	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
LastStateRestorePoint	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
LastUpdateCompleteTime	REG_SZ	2017-03-27T18:54:58
Path	REG_SZ	C:\Program Files\Cylance\Desktop\
Policy	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
Region	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
SerialNumber	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
UninstallRestorePoint	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
UniversalExclusion	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
UpdateProductPath	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
UpdateProductState	REG_SZ	0
UpdateProductURLs	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
VenueLastCommunicatedTime	REG_BINARY	01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4
~~VenueLastPolicyUpdateTime~~	~~REG_BINARY~~	~~01 00 00 00 d0 8c 9d df 01 15 d1 11 8c 7a 00 c0 4~~
CustomThreatActionDesc	REG_SZ	Submit Helpdesk Ticket
CustomThreatActionURL	REG_SZ	https://yourhelpdesk.yourcompany.com

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop

Figure 42: Add a Custom Action

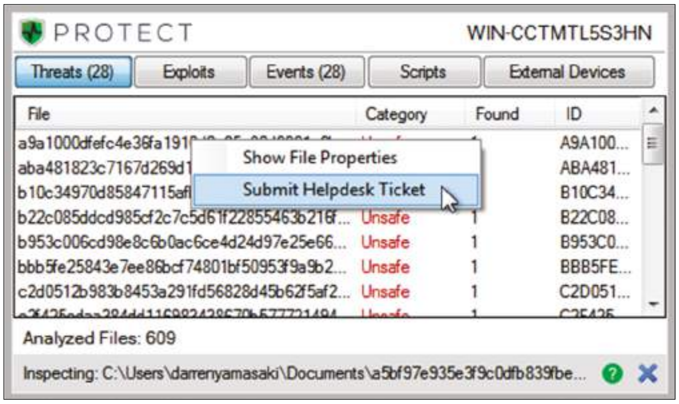
URL Structure

The URL accepts four tokens which are substituted with the values associated with the threat.

- **CY_THREAT:** The SHA256 of the threat.
- **CY_PATH:** The path (location) where the file was found. **Example: C:\Temp\malware\thisisthemalware.exe.**
- **CY_SCORE:** The Cylance Score assigned to the threat. A score from 60 to 100 is considered Unsafe. A score from 1 to 59 is considered Abnormal.
- **CY_STATE:** The state of the threat. Could be Unsafe, Abnormal, Waived, Safelisted, or Quarantined.
- **CY_MACHINENAME:** The name of the machine on which the threat was found.

Using the Action

1. On the device, click on the Agent icon in the system tray.
2. Make sure the Threats tab is selected.
3. Right-click the threat for which you want to submit a ticket, then click the menu item to submit the ticket. The default web browser opens to the URL.



File	Category	Found	ID
a9a1000dfefc4e36fa191			A9A100...
aba481823c7167d269d1			ABA481...
b10c34970d85847115afl			B10C34...
b22c085ddcd985cf2c7c5d61f22855463b216f...	Unsafe	1	B22C08...
b953c006cd98e8c6b0ac6ce4d24d97e25e66...	Unsafe	1	B953C0...
bbb5fe25843e7ee86bcf74801bf50953f9a9b2...	Unsafe	1	BBB5FE...
c2d0512b983b8453a291fd56828d45b62f5af2...	Unsafe	1	C2D051...

Analyzed Files: 609

Inspecting: C:\Users\darrenyamasaki\Documents\a5bf97e935e3f9c0dfb839fbe...

Figure 43: Submit a Ticket

Changing the Help/FAQ Link in the Agent UI

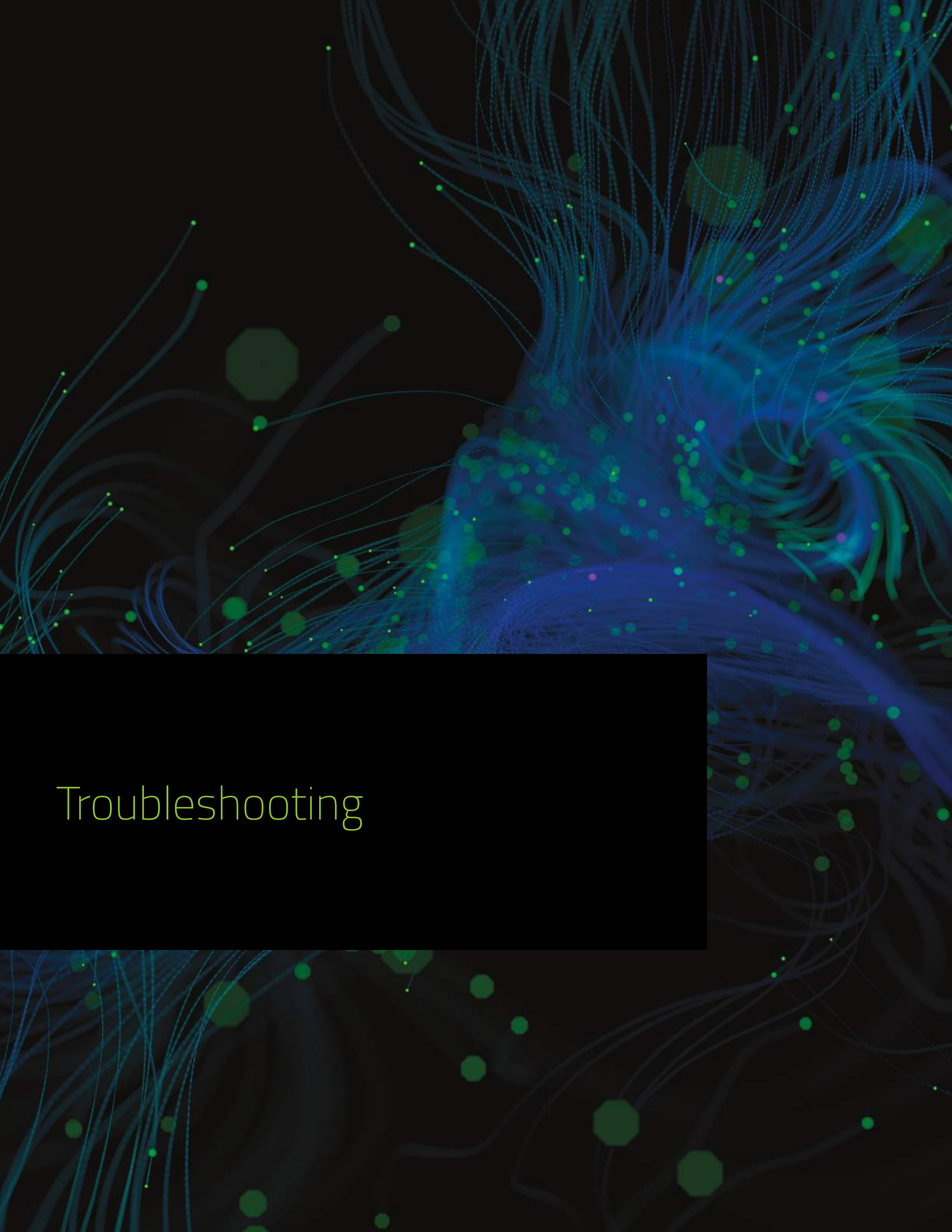
By default, the Help/FAQ link in the Agent user-interface takes you to the Cylance Support site. With Agent versions 1380 and higher, you can add a registry item to redirect this link to your own support site. This is helpful for organizations that want to use their own support or IT teams to field questions from their users before contacting Cylance Support.

1. On the device, right-click the Agent icon, then select **Exit**.
2. Stop the Cylance Service. While restarting the UI will load the new value, the service protects the registry from being changed, so the service must be stopped to set the new value. If **Prevent Service Shutdown** is enabled, you can't stop the service. You must disable the **Prevent Service Shutdown** feature, create the help link, then re-enable the **Prevent Service Shutdown** feature.
3. Run the Registry Editor, then take ownership of the Cylance Desktop. HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\ Desktop.
4. Right-click inside the Registry Editor, then select **New > String Value**. A new string value is added to the registry.
5. Type CustomHelpFaqUrl to name the value, then press **Enter**. This renames the value.
6. Double-click **CustomHelpFaqUrl**, type the URL for the help website, then click **OK**.
7. Exit, restart the Cylance Service, then restart the Agent UI.

Virtual Machines

Below are some recommendations for using the **CylancePROTECT** Agent on a virtual machine image.

- When creating a virtual machine image to be used as a template, disconnect the virtual machine network settings before installing the Agent. This prevents the Agent from communicating with the Console and configuring the Device Details. This prevents duplicate devices in the Console.
- Some virtual machine software has security settings that conflict with **CylancePROTECT**'s Memory Protection feature. This conflict may result in an unresponsive virtual machine. If this happens, it is recommended to either disable the Memory Protection feature or use different virtual machine software.



Troubleshooting

This section provides a list of questions to answer and files to collect when troubleshooting issues with **CylancePROTECT**. This information will enable Cylance Support to assist in resolving any issues.

For up-to-date information about **CylancePROTECT**, visit the Cylance Support Knowledge Base at https://support.cylance.com.

> **NOTE:** *In the Console, there is a How-To Guide that explains product features. Access this guide from the Account drop-down list (upper-right corner of the Console menu).*

Installation Parameters

- **What is the installation method? Provide any parameters used.**
  - **Example — Windows:** Using LAUCHAPP=0 when installing from the command line hides the Agent icon and Cylance Start Menu folder at run time.
  - **Example — OS X:** Using SelfProtectionLevel=1 when installing from the command line disables Self Protection on the Agent.
- **Which steps of the installation could be verified?**
  - **Example — Windows:** Was the MSI or EXE installer used?
  - **Example — Any OS:** Where any command line options used, such as Quiet Mode or No Agent UI?
- **Enable verbose logging for the installation (Windows only).**
  - In the Registry Editor, go to HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer
  - Create a new String with Logging for the value name and voicewarmupx for the value data.
  - Reproduce the issue by attempting the installation or uninstallation.
  - Collect the log files from the temp folder. C:\<user_profile>\AppData\Local\Temp.

> **NOTE:** *The Temp folder location may vary depending on the user who logged on and the Environment variable settings in Windows.*

Performance Concerns

- Capture a screenshot of the Task Manager (Windows) or Activity Monitor (OS X) showing the Cylance processes and memory consumption.
- Capture a dump of the Cylance process.
- Collect debug logs.
- Collect output of System Information during the issue.
  - **For Windows:** msinfo32 or winmsd
  - **For OS X:** System Information
- Collect any relevant Event Logs (Windows) or Console information (OS X).

Update, Status, and Connectivity Issues

- Ensure that port 443 is open on the firewall and the device can resolve and connect to Cylance.com sites
- Is the device listed in the Devices page of the Cylance console? Is it Online or Offline? What is its Last Connected time?
- Is a proxy being used by the device to connect to the Internet? Are the credentials properly configured on the proxy?
- Restart the **CylancePROTECT** service so that it attempts to connect to the Cylance console
- Collect debug logs
- Collect the output of System Information during the issue.
  - **For Windows:** msinfo32 or winmsd
  - **or OS X:** System Information

Enabling Debug Logging

By default, **CylancePROTECT** maintains log files stored in C:\Program Files\Cylance\Desktop\log. For troubleshooting purposes, **CylancePROTECT** can be configured to produce more verbose logs via KB Debug Logging.

Script Control Incompatibilities

Issue:

When Script Control is enabled on some devices, it can cause conflicts with other software running on those devices. This conflict is typically due to the Agent injecting into certain processes that are being called by other software.

Solution:

Depending on the software, this issue can be resolved by adding in specific process exclusions to the Device Policy in the Console. Another option is to enable Compatibility Mode (registry key) on each affected device. However, if exclusions are not effective, it is recommended to disable Script Control in the Device Policy affecting the devices to restore normal system functionality.

> **NOTE:** *This Compatibility Mode solution is for Agent 1360 and 1370. Starting with Agent 1380 and higher, the injection process has been updated for compatibility with other products.*

Compatibility Mode

Add the following registry key to enable Compatibility Mode:

1. Using the Registry Editor, go to HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop.
2. Right-click **Desktop**, click **Permissions**, then take ownership and grant yourself Full Control.
3. Right-click **Desktop**, then select **New > Binary Value**.
4. For the name, type CompatibilityMode.
5. Open the registry setting and change the value to 01.
6. Click **OK**, then close Registry Editor.
7. A restart of the system may be required.

Command Line Options

Using Psexec:

```
psexec -s reg add HKEY_LOCAL_MACHINE\
SOFTWARE\Cylance\Desktop /v
CompatibilityMode /t REG_BINARY /d 01
```

To perform a command on multiple machines, you can use the Invoke-Command cmdlet:

```
psexec -s reg add HKEY_LOCAL_MACHINE\
SOFTWARE\Cylance\Desktop /v
CompatibilityMode /t REG_BINARY /d 01
```

```
$credential = Get-Credential -Credential
{UserName}\administrator
```

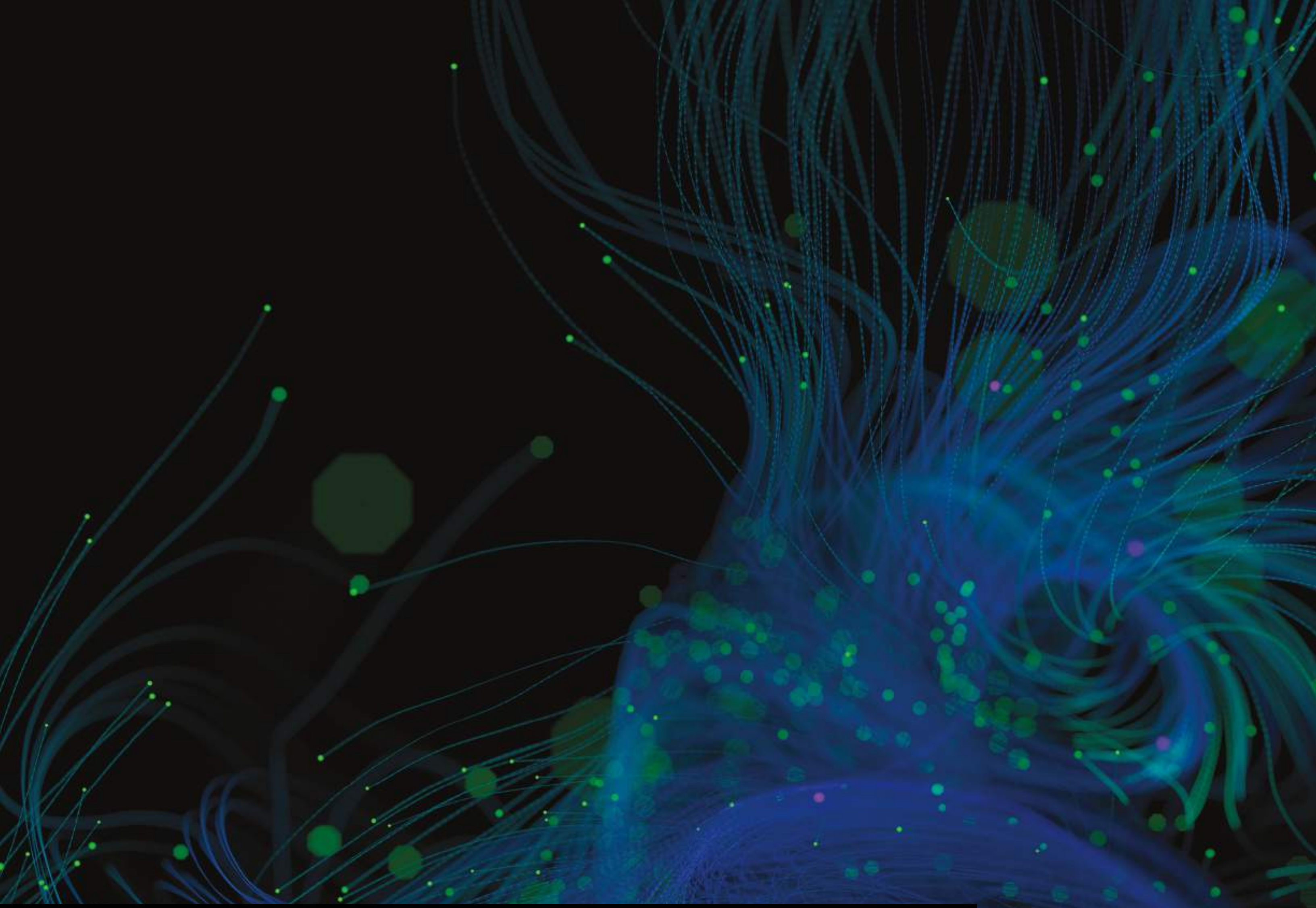
```
Invoke-Command -ComputerName $servers
-Credential $credential -ScriptBlock {New-Item
-Path HKCU:\Software\ Cylance\Desktop -Name
CompatibilityMode -Type REG_BINARY -Value
01}
```

Enable Support Login

Allows Support to help users troubleshoot Console issues by providing Support access to the user's tenant and act on behalf of the user. This allows Support to see what the user sees, with the same level of permission as the user. All actions taken by Support are tracked in the Audit Log.

To Enable Support Login:

1. Log in to the Console as an Administrator.
   An Administrator can enable this
   feature for their organization.
2. Select **Settings > Application**.
3. Select **Enable Support Login**.



Memory Protection Violation Types

Stack Pivot — The stack for a thread has been replaced with a different stack. Generally the system will only allocate a single stack for a thread. An attacker would use a different stack to control execution in a way that is not blocked by Data Execution Prevention (DEP).

Stack Protect — The memory protection of a thread's stack has been modified to enable execution permission. Stack memory should not be executable, so usually this means that an attacker is preparing to run malicious code stored in stack memory as part of an exploit, an attempt which would otherwise be blocked by Data Execution Prevention (DEP).

Overwrite Code — Code residing in a process's memory has been modified using a technique that may indicate an attempt to bypass Data Execution Prevention (DEP).

RAM Scraping — A process is trying to read valid magnetic stripe track data from another process. Typically related to point of sale systems (POS).

Malicious Payload — A generic shellcode and payload detection associated with exploitation has been detected.

Remote Allocation of Memory — A process has allocated memory in another process. Most allocations will only occur within the same process. This generally indicates an attempt to inject code or data into another process, which may be a first step in reinforcing a malicious presence on a system.

Remote Mapping of Memory — A process has introduced code and/or data into another process. This may indicate an attempt to begin executing code in another process and thereby reinforce a malicious presence.

Remote Write to Memory — A process has modified memory in another process. This is usually an attempt to store code or data in previously allocated memory (see OutOfProcessAllocation) but it is possible that an attacker is trying to overwrite existing memory in order to divert execution for a malicious purpose.

Remote Write PE to Memory — A process has modified memory in another process to contain an executable image. Generally this indicates that an attacker is attempting to execute code without first writing that code to disk.

Remote Overwrite Code — A process has modified executable memory in another process. Under normal conditions executable memory will not be modified, especially by another process. This usually indicates an attempt to divert execution in another process.

Remote Unmap of Memory — A process has removed a Windows executable from the memory of another process. This may indicate an intent to replace the executable image with a modified copy for the purpose of diverting execution.

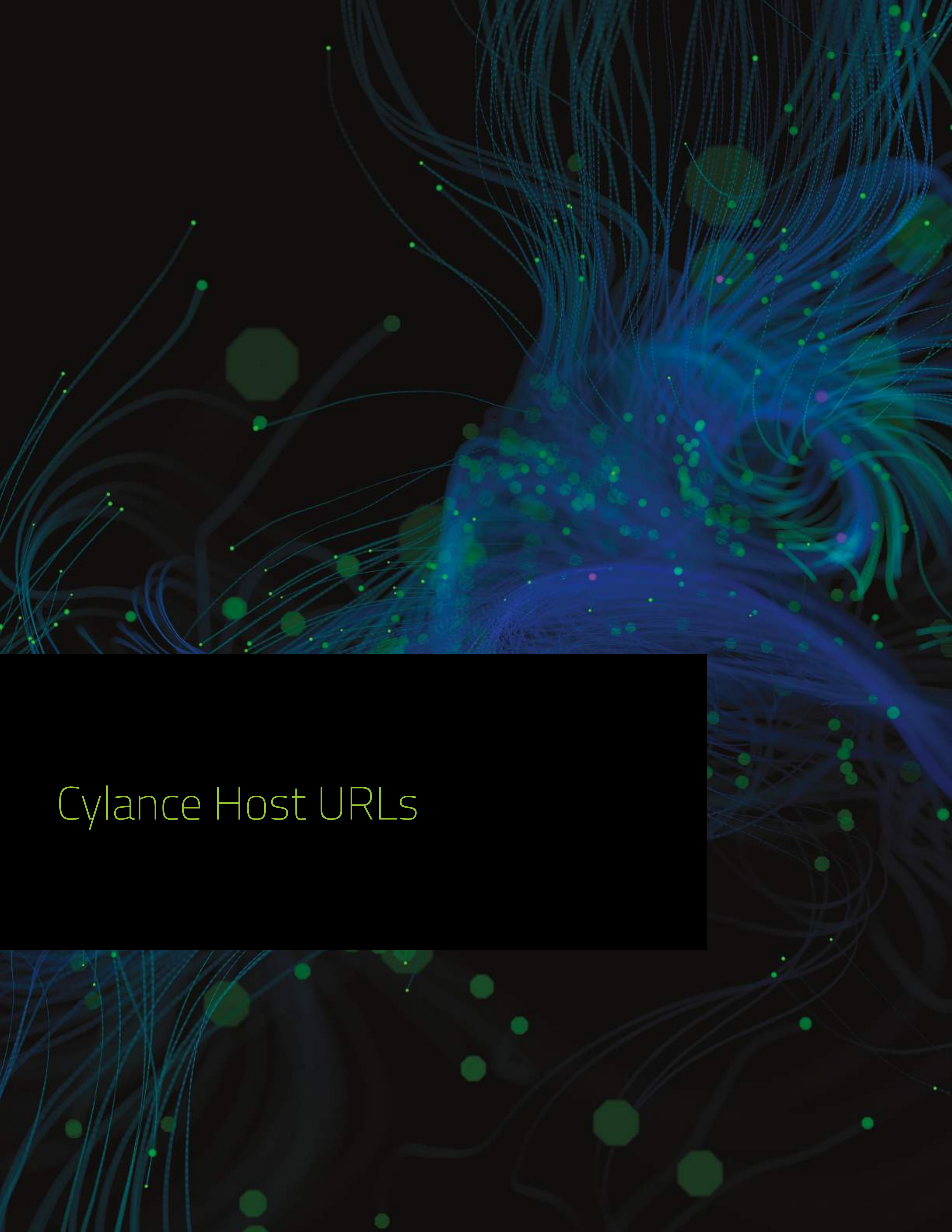
Remote Thread Creation — A process has created a new thread in another process. A process's threads are usually only created by that same process. This is generally used by an attacker to activate a malicious presence that has been injected into another process.

Remote APC Scheduled — A process has diverted the execution of another process's thread. This is generally used by an attacker to activate a malicious presence that has been injected into another process.

DYLD Injection — An environment variable has been set that will cause a shared library to be injected into a launched process. Attacks can modify the plist of applications like Safari or replace applications with bash scripts, that cause their modules to be loaded automatically when an application starts.

LSASS Read — Memory belonging to the Windows Local Security Authority process has been accessed in a manner that indicates an attempt to obtain users' passwords.

Zero Allocate — A null page has been allocated. The memory region is typically reserved, but in certain circumstances it can be allocated. Attacks can use this to setup privilege escalation by taking advantage of some known null de-reference exploit, typically in the kernel.



Cylance Host URLs

The Agents report to, and are managed by, the Console. For environments that must allow domains through a firewall, use the list of domains below, based on the region to which your organization belongs.

To verify the domain to which you belong, log in to the Console and check the URL, then match that information to the correct list below.

> **NOTE:** *When logging in to the Console, you must use the correct login URL, which is based on the region to which your organization belongs. If you are using the correct login credentials but cannot log in, check the URL.*

Asia-Pacific North East

- login-apne1.cylance.com
- data-apne1.cylance.com and data-vs1-apne1.cylance.com
- protect-apne1.cylance.com
- update-apne1.cylance.com
- protect-api-apne1.cylance.com
- download.cylance.com

Asia-Pacific South East

- login-au.cylance.com
- data-us.cylance.com
- protect-au.cylance.com
- update-au.cylance.com
- api-au.cylance.com or api2-au.cylance.com
- download.cylance.com

Europe Central

- login-euc1.cylance.com
- data- euc1.cylance.com
- protect-euc1.cylance.com
- update-euc1.cylance.com
- protect-api-euc1.cylance.com
- download.cylance.com

North America

- login.cylance.com
- data.cylance.com
- protect.cylance.com
- update.cylance.com
- api.cylance.com or api2.cylance.com
- download.cylance.com

SIEM / Syslog

CylancePROTECT can integrate with your Security Information Event Management (SIEM) software using Syslog. Syslog events will be persisted at the same time the Agent events persist to the Console.

The Syslog server IP addresses are static to ensure communication with your Syslog servers. Allow all IP addresses for the region to which your organization belongs. There are multiple IP addresses for fail-over solutions and future expansion.

If you do not use a Syslog server, then you do not need to allow this IP address through your firewall.

Asia-Pacific North East (my-apne1.cylance.com)

- 10.13.0.144
- 10.13.1.34

Asia-Pacific South East (my-au.cylance.com):

- 52.63.15.218
- 52.65.4.232

Europe Central (my- euc1.cylance.com):

- 52.28.219.170
- 52.29.102.181
- 52.29.213.11

North America (my.cylance.com):

- 52.2.154.63
- 52.20.244.157
- 52.71.59.248
- 52.72.144.44
- 54.88.241.49

Undeliverable Messages

If the **CylancePROTECT** Syslog integration cannot successfully deliver syslog messages to your server, an email notification will be sent to any Administrators in the organization with a confirmed email address. The email notification is to alert any Administrators about the Syslog issue. If no action is taken, Syslog messaging is disabled after 20 minutes.

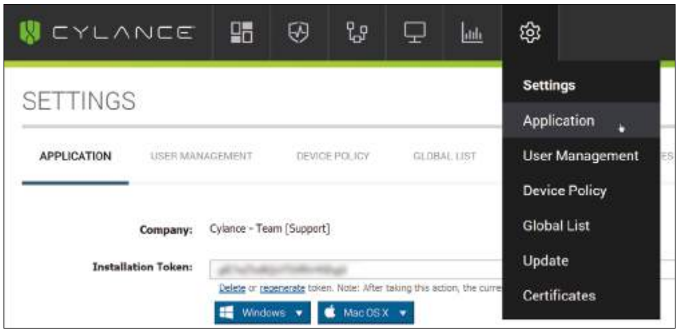
If the issue is resolved before the 20 minute time period has ended, then syslog messages will continue to be delivered. If the issue is resolved after the 20 minute time period, an Administrator in your organization must re-enable Syslog messaging in the Console (**Settings > Application > Syslog/SIEM**).

CylancePROTECT Syslog Settings

CylancePROTECT can be configured to forward events to a Syslog server. The content of each event is Unicode plain text consisting of key-value pairs, separated by commas. Due to the size limitation of most Syslog servers, the details of each message (Cylance-specific payload) is limited to 2048 characters.

Change Syslog Settings

1. Log in to the **CylancePROTECT** Console.
2. Select **Settings > Application**.

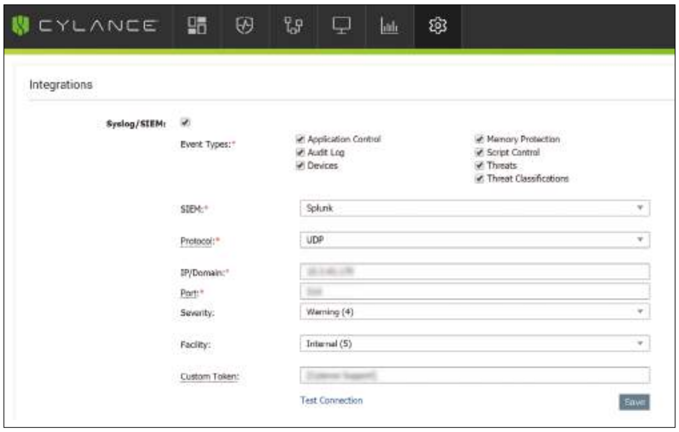


Company: Cylance - Team (Support)

Installation Token: [redacted]

Delete or regenerate token. Note: After taking this action, the curre

3. Under Integrations, click **Syslog/SIEM**.



Syslog/SIEM: ☑

Event Types:* ☑ Application Control ☑ Audit Log ☑ Devices ☑ Memory Protection ☑ Script Control ☑ Threats ☑ Threat Classifications

SIEM:* Splunk

Protocol:* UDP

IP/Domain:* [redacted]

Port:* [redacted]

Severity: Warning (4)

Facility: Internal (5)

Custom Token: [redacted]

4. Select the options you want and type in any server information needed.
5. Click **Save**.

Event Types

Syslog events have standard fields like timestamp, severity level, facility, and a Cylance-specific payload (message). Examples provided in this section only contain the Cylance-specific message.

Application Control

This option is only visible to users who have the Application Control feature enabled. Application Control events represent actions occurring when the device is in Application Control mode. Selecting this option will send a message to the Syslog server whenever an attempt is made to modify or copy an executable file, or when an attempt is made to execute a file from an external device or network location.

Example Message for Deny PE File Change

```
CylancePROTECT: Event Type: AppControl,
Event Name: pechange, Device Name: WIN-
7entSh64, IP Address: (192.168.119.128),
Action: PEFileChange, Action Type: Deny, File
Path: C:\Users\admin\AppData\Local\Temp\
MyInstaller.exe, SHA256:04D4DC02D96673EC
A9050FE7201044FDB380E3CFE0D727E
93DB35A709B45EDAA
```

Example Message for Deny Execution from External Drive

```
CylancePROTECT: Event Type: AppControl,
Event Name: executionfromexternaldrives,
Device Name: WIN-7entSh64, IP Address:
(192.168.119.128), Action:

PEFileChange, Action Type: Allow, File
Path: \\shared1\psexec.exe, SHA256:
F8DBABDFA03068130C277CE49C60E35C02
9FF29D9E3C74C362521F3FB02670D5
```

Audit Log

Selecting this option will send the audit log of user actions performed in the **CylancePROTECT** Console (website) to the Syslog server. Audit log events will always appear in the Audit Log screen, even when this option is unchecked.

Example Message for Audit Log Being Forwarded to Syslog

```
CylancePROTECT: Event Type: AuditLog, Event
Name: ThreatGlobalQuarantine, Message: SHA2
56:A1E92E2E84A1321F499A5EC500E8B
9A9C0CA28701668BF13EA56D3995A96153F,
1CCC95B7B2F78

1D55D538CA01D6049762FDF6A75B32A06DF
3CC2EDC1F1573BFA; Reason: Manually
blacklisting these 2 threats., User:
(johnsmith@contoso.com)
```

Devices

Selecting this option sends device events to the Syslog server.

- When a new device is registered, you will receive two messages for this event: Registration and SystemSecurity.Example Message for Device Registered Event

Example Message for Device Registered Event

```
CylancePROTECT: Event Type: Device, Event
Name: Registration, Device Name: WIN-
55NATVQHBUU

CylancePROTECT: Event Type: Device, Event
Name: SystemSecurity, Device Name: WIN-
55NATVQHBUU, Agent Version: 1.1.1270.58,
IP Address: (10.3.0.154), MAC Address:
(005056881877), Logged On Users: (WIN-
55NATVQHBUU\Administrator), OS: Microsoft
Windows Server 2008 R2 Standard Service Pack
1 x64 6.1.7601
```

- When a device is removed.

Example Message for Device Removed Event

- When a device's policy, zone, name, or logging level has changed.

Example Message for Device Updated Event

```
Cyl CylancePROTECT: Event Type: ExploitAttempt,
Event Name: blocked, Device Name: WIN-
7entSh64, IP Address: (192.168.119.128), Action:
Blocked, Process ID: 3804, Process Name: C:\
AttackTest64.exe, User Name: admin, Violation
Type: LSASS Read
```

Memory Protection

Selecting this option will log any Memory Exploit Attempts that might be considered an attack from any of the Tenant's devices to the Syslog server.

There are four types of Memory Exploit actions:

- **None:** Allowed because no policy has been defined for this violation.
- **Allowed:** Allowed by policy.
- **Blocked:** Blocked from running by policy.
- **Terminated:** Process has been terminated.

Example Message of Memory Protection Event

```
Cyl CylancePROTECT: Event Type: ExploitAttempt,
Event Name: blocked, Device Name: WIN-
7entSh64, IP Address: (192.168.119.128), Action:
Blocked, Process ID: 3804, Process Name: C:\
AttackTest64.exe, User Name: admin, Violation
Type: LSASS Read
```

Threats

Selecting this option will log any newly found threats, or changes observed for any existing threat, to the Syslog server. Changes include a threat being removed, quarantined, waived, or executed.

There are five types of Threat Events:

- **threat_found:** A new threat has been found in an Unsafe status.
- **threat_removed:** An existing threat has been removed.
- **threat_quarantined:** A new threat has been found in the Quarantine status.
- **threat_waived:** A new threat has been found in the Waived status.
- **threat_changed:** The behavior of an existing threat has changed (examples: score, quarantine status, running status).

Example Message of Threat Event

```
CylancePROTECT: Event Type: Threat, Event
Name: threat_found, Device Name: SH-
Win81- 1, IP Address: (10.3.0.132), File Name:
virusshare_00fbc4cc4b42774b50a9f71074b
79bd9, Path: c:\ruby\host_automation\test\data\
test_files\, SHA256:

1EBF3B8A61A7E0023AAB3B0CB24938536A1
D87BCE1FCC6442E137FB2A7DD510B, Status:
Unsafe,

Cylance Score: 100, Found Date: 6/1/2015
10:57:42 PM, File Type: Executable, Is Running:
False, Auto Run: False, Detected By: FileWatcher
```

Threat Classifications

Each day, Cylance will classify hundreds of threats as either Malware or potentially unwanted programs (PUPs). By selecting this option, you are subscribing to be notified when these events occur.

Example Message of Threat Classification

```
CylancePROTECT: Event Type:
ThreatClassification, Event Name:
ResearchSaved, Threat Class: Malware,
Threat Subclass: Worm, SHA256:
1218493137321C1D1F897B0C25BEF17C
DD0BE9C99B84B4DD8B51EAC8F979 4F65
```

Security Information and Event Management (SIEM)

Specifies the type of Syslog server or SIEM to which events are being sent.

Protocol

This must match what you have configured on your Syslog server. The choices are UDP or TCP. UDP is generally not recommended as it does not guarantee message delivery. TCP is the default, and we encourage customers to use it.

TLS/SSL

Only available if the Protocol specified is TCP, TLS/SSL ensures the Syslog message is encrypted in transit from **CylancePROTECT** to the Syslog server. We encourage customers to checkmark this option. Be sure your Syslog server is configured to listen for TLS/SSL messages.

IP/Domain

Specifies the IP address or fully-qualified domain name of the Syslog server that you have setup. Consult with your internal network experts to ensure firewall and domain settings are properly configured

Port

Specifies the port number on the machines that the Syslog server will listen to for messages. It must be a number between 1 and 65535. Typical values are: 512 for UDP, 1235 or 1468 for TCP, and 6514 for Secured TCP (example: TCP with TLS/SSL enabled).

Severity

Specifies the severity of the messages that should appear in the Syslog server. This is a subjective field, and you may set it to whatever level you require. The value of severity does not change the messages that are forwarded to Syslog.

Facility

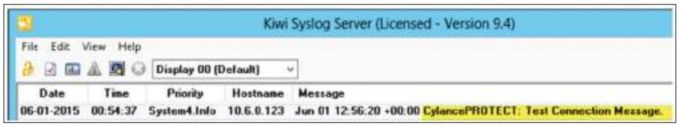
Specifies what type of application is logging the message. The default is Internal (or Syslog). This is used to categorize the messages when they are received by the Syslog server.

Testing the Connection

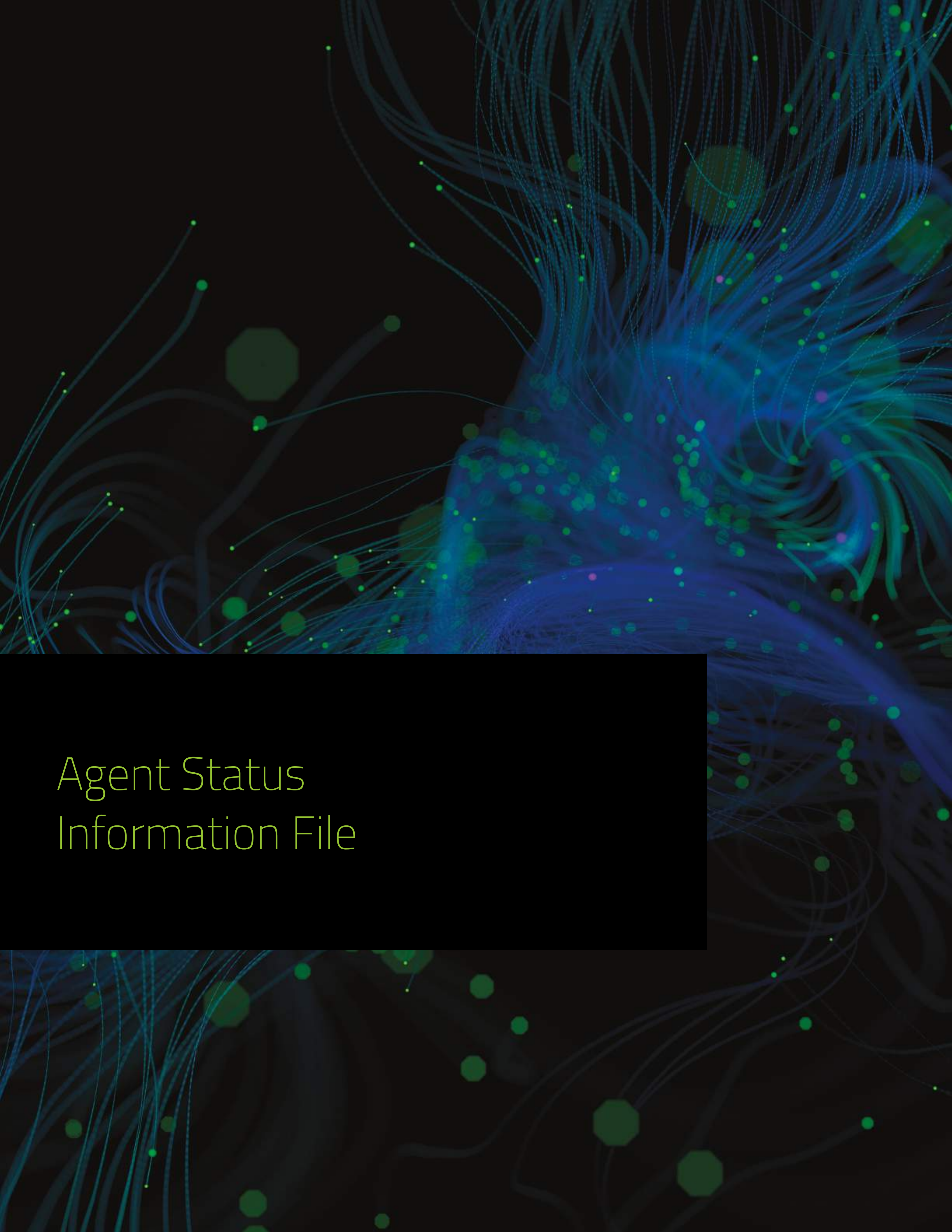
Click **Test Connection** to test the IP/Domain, Port, and Protocol settings. If you entered valid values, after a couple of moments, you should see a success confirmation pop-up.

Connection was successful.

On the Syslog server console, you should see the **CylancePROTECT**: Test Connection Message like this:



Date	Time	Priority	Hostname	Message
06-01-2015	00:54:37	System4.Info	10.6.0.123	Jun 01 12:56:20 +00:00 CylancePROTECT: Test Connection Message.



Agent Status Information File

The Agent provides a way for users to get Agent Status information from a device. This file provides information about the Agent that users would see in the Agent user interface, except for Events information. This allows users to get Agent information without needing to go directly to the Agent UI.

Enabling this feature requires adding a few registry keys and is available with Agent version 1370 and higher. The file is available in XML and JSON file formats.

> **NOTE:** *The Status file contains the latest information only. It does not contain any historical status information. The file is over-written at a set interval.*

1. On the device, open the Registry Editor and navigate to:
   - HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop
   - You might need to change the registry permissions to add these keys.
2. Create the following keys in the Desktop folder. Use DWORD (32-bit) and Hexadecimal.
   - **StatusFileEnabled:** File is written if the registry value is greater than zero. Default value is 1, so the file is written by default.
   - **StatusFileType:** The file format written. If the value is zero (0), then a JSON file is written. If the value is 1, then an XML file is written. The default value is 1.
   - **StatusFilePath:** Location of the Status file. The default path is: <CommonAppData>\Cylance\Status\Status.json (or Status.xml)
   - **Example:** C:\ProgramData\Cylance\Status.
   - **StatusPeriod:** How often the file is written. The default value is 60, so the file is over-written every 60 seconds. The minimum value is 15 for a 15-second interval.

Status Information Type	Description
snapstop_time	The date and time the Status information was collected. The date and time are local to the device.
ProductInfo	▪ version: **CylancePROTECT** Agent version on the device. ▪ last_communicated_timestamp: Date and time of the last check for an Agent Update. ▪ serial_number: Installation Token used to register the Agent. ▪ device_name: Name of the device on which the Agent is installed.
Policy	▪ type: Status of the Agent, whether it is Online or Offline. ▪ id: Unique identifier for the policy. ▪ name: Policy name.
ScanState	▪ last_background_scan_timestamp: Date and time of the last Background Threat Detection scan. ▪ drives_scanned: List of drive letters scanned.
Threats	▪ count: The number of threats found. ▪ max: The maximum number of threats included in the Status file. ▪ Threat: • file_hash_id: Displays the SHA256 hash information for the threat. • file_md5: The MD5 hash information. • file_path: The path where the threat was found. Includes the file name. • is_running: Is the threat currently running on the device? True or False. • auto_run: Is the threat file set to run automatically? True or False. • file_status: Displays the current state of the threat, like Allowed, Running, or Quarantined. See the **Threat: FileStatus** table below. • o file_type: Displays the type of file, like Portable Executable (PE), Archive, or PDF. See the **Threat: FileType** table below. • o score: Displays the Cylance Score. The score displayed in the Status file ranges from 1000 to -1000. In the Console, the range is 100 to -100. • o file_size: Displays the file size, in bytes.

Status Information Type	Description
Exploits	▪ count: The number of exploits found. ▪ max: The maximum number of exploits included in the Status file. ▪ Exploit • ProcessId: Displays the process ID of the application identified by Memory Protection. • ImagePath: The path from which the exploit originates. Includes the file name. • ImageHash: Displays the SHA256 hash information for the exploit. • FileVersion: Displays the version number of the exploit file. • Username: Displays the name of the user who was logged in to the device when the exploit occurred. • Groups: Displays the group with which the logged in user is associated. • Sid: The Security Identifier (SID) for the logged in user. • ItemType: Displays the exploit type, which relates to the Violation Types (KB 204295888). See the **Exploit: ItemType** table below. • State: Displays the current state of the exploit, like Allowed, Blocked, or Terminated. See the **Exploit: State table** below. • MemDefVersion: The version of Memory Protection used to identify the exploit. This is typically the Agent version number. • Count: The number of times the exploit attempted to run.
Scripts	▪ count: The number of scripts run on the device. ▪ max: The maximum number of scripts included in the Status file. ▪ Script • script_path: The path from which the script originates. Includes the file name. • file_hash_id: Displays the SHA256 hash information for the script. • file_md5: Displays the MD5 hash information for the script, if available. • file_sha1: Displays the SHA1 hash information for the script, if available. • drive_type: Identifies the type of drive from which the script originated, like Fixed. • last_modified: The date and time the script was last modified. • interpreter: • name: The name of the script control feature that identified the malicious script. • version: The version number of the script control feature. • username: Displays the name of the user who was logged in to the device when the script was launched. • groups: Displays the group with which the logged in user is associated. • sid: The Security Identifier (SID) for the logged in user. • action: Displays the action taken on the script, like Allowed, Blocked, or Terminated . See the Script: Action table below.

Threat: FileStatue	Value
None	0x00
Threat	0x01
Suspicious	0x02
Allowed	0x04
Quarantined	0x08
Running	0x10
Corrupt	0x20

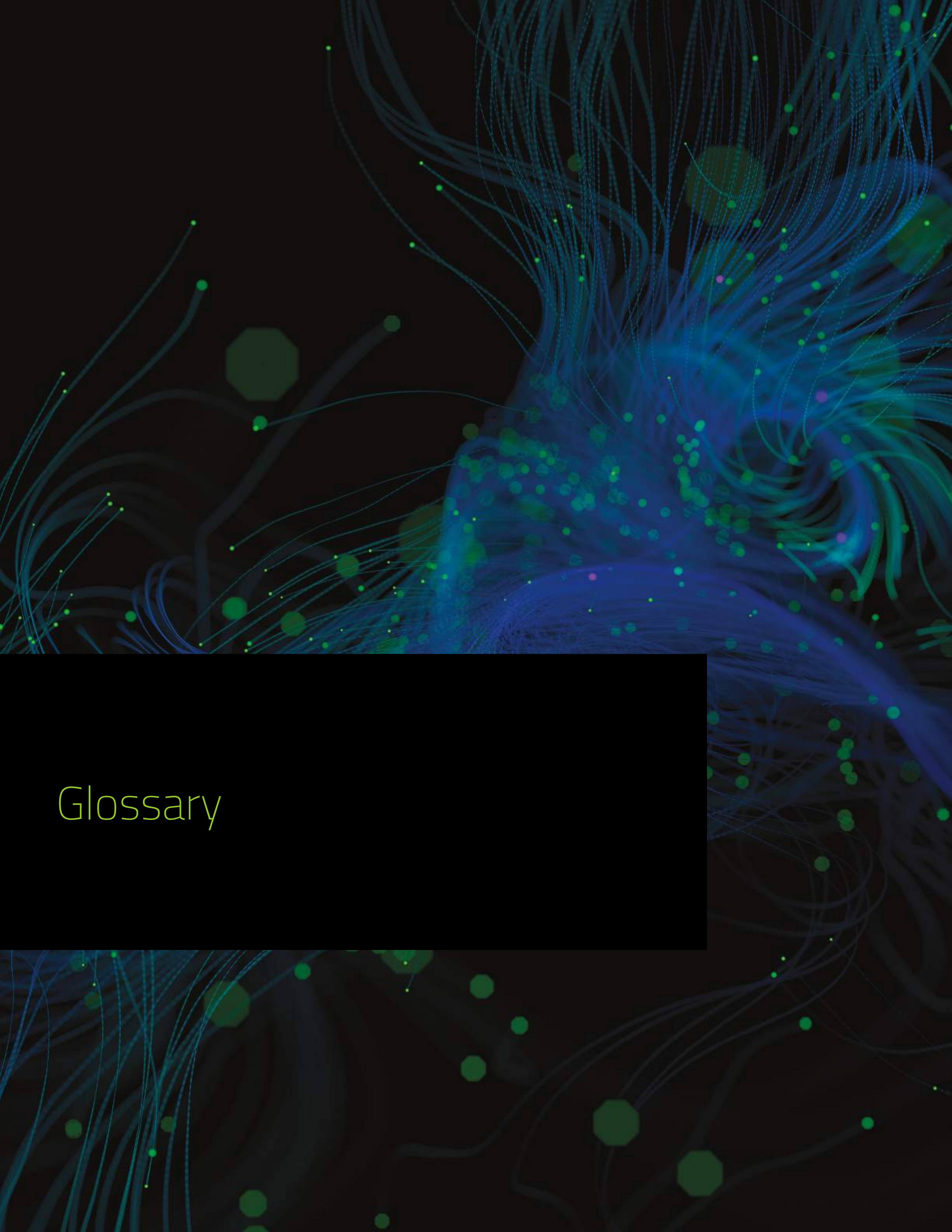
Threat: FileType	Value
Unsupported	0
PE	1
Archive	2
PDF	3
OLE	4

Exploit: ItemType	Value	Related Violation Type
None	0	n/a
StackPivot	1	Stack Pivot
StackProtect	2	Stack Protect
OverwriteCode	3	Overwrite Code
OopAllocate	4	Remote Allocation of Memory
OopMap	5	Remote Mapping of Memory
OopWrite	6	Remote Write to Memory
OopWritePe	7	Remote Write PE to Memory
OopOverwriteCode	8	Remote Overwrite Code
OopUnmap	9	Remote Unmap of Memory
OopThreadCreate	10	Remote Thread Creation
OopThreadApc	11	Remote APC Scheduled
LsassRead	12	LSASS Read
TrackDataRead	13	RAM Scraping
CpAllocate	14	Remote Allocation of Memory
CpMap	15	Remote Mapping of Memory
CpWrite	16	Remote Write to Memory
CpWritePe	17	Remote Write PE to Memory
CpOverwriteCode	18	Remote Overwrite Code
CpUnmap	19	Remote Unmap of Memory
CpThreadCreate	20	Remote Thread Creation
CpThreadApc	21	Remote APC Scheduled
ZeroAllocate	22	Zero Allocate
DyldInjection	23	DYLD Injection
MaliciousPayload	24	Malicious Payload

Oop = Out of Process; Cp = Child Process

Exploit: State	Value
None	0
Allowed	1
Blocked	2
Terminated	3

Script: Action	Value
None	0
Allowed	1
Blocked	2
Terminated	3



Glossary

Abnormal — A suspicious file with a lower score (1 – 59) that is less likely to be malware

Administrator — Tenant manager for **CylancePROTECT**

Agent — CylancePROTECT Endpoint Host that communicates with the Console

Application Control — Device Policy setting that enables administrator to implement system lockdown for organization's devices

Audit Log — Log that records actions performed from the **CylancePROTECT** console interface

Auto-Quarantine — Automatically prevent execution of all Unsafe and/or Abnormal files

Auto Upload — Automatically upload any unknown Portable Executable (PE) files to the CylanceINFINITY Cloud for analysis.

Background Threat Detection — Full Disk Scan that is lightweight and is used to detect dormant threats

Console — CylancePROTECT Management User Interface

CylanceINFINITY — The **CylancePROTECT** Mathematical Model used to score files

Device Policy — CylancePROTECT policy that can be configured by organization administrator that defines how threats will be handled on all devices

File Watcher — Feature that will detect and analyze any new files on disk

Global Quarantine — Prevent execution of a file globally (across all devices in an organization)

Global Safe List — Allow execution of a file globally (across all devices in an organization)

Memory Protection — Device Policy setting that monitors and blocks exploit attempts

Organization — A tenant account using the **CylancePROTECT** service

Quarantine — Prevent execution of a file locally on a specific device

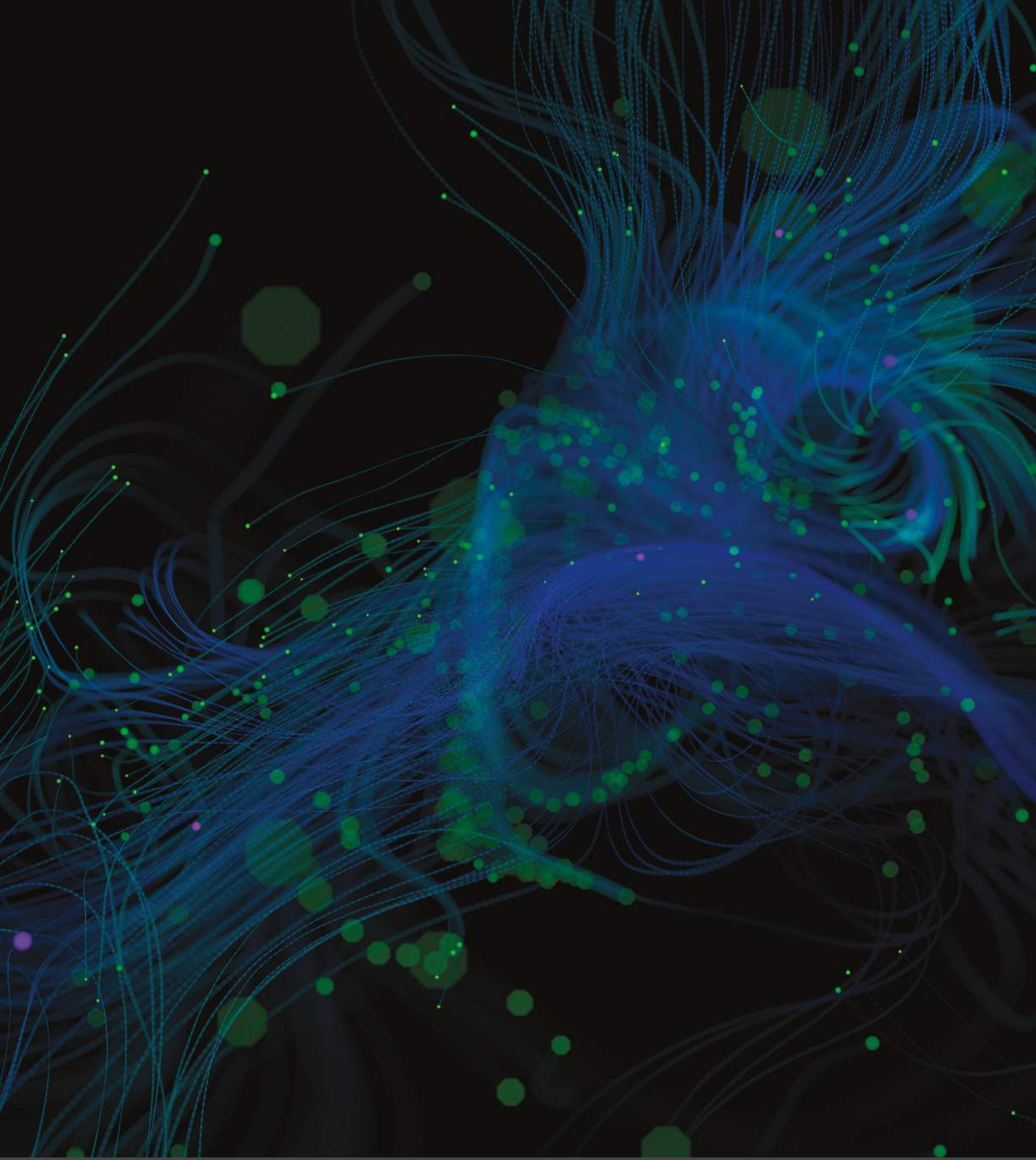
Threats — Potentially and malicious files detected by **CylancePROTECT** and classified either as Unsafe or Abnormal

Unsafe — A suspicious file with a high score (60 – 100) that is likely to be malware

Waive — Allow execution of a file locally on a specific device

Zone — A way to organize and group devices within an organization according to priority, functionality, etc.

Zone Rule — Feature that enables automation of assigning devices to specific zones based on IP addresses, operating system, and device names



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

CYLANCE™