Feature Focus: Cylance® Management Console Reporting

Interactive Dashboards and Reports for CylancePROTECT®

CYLANCE®

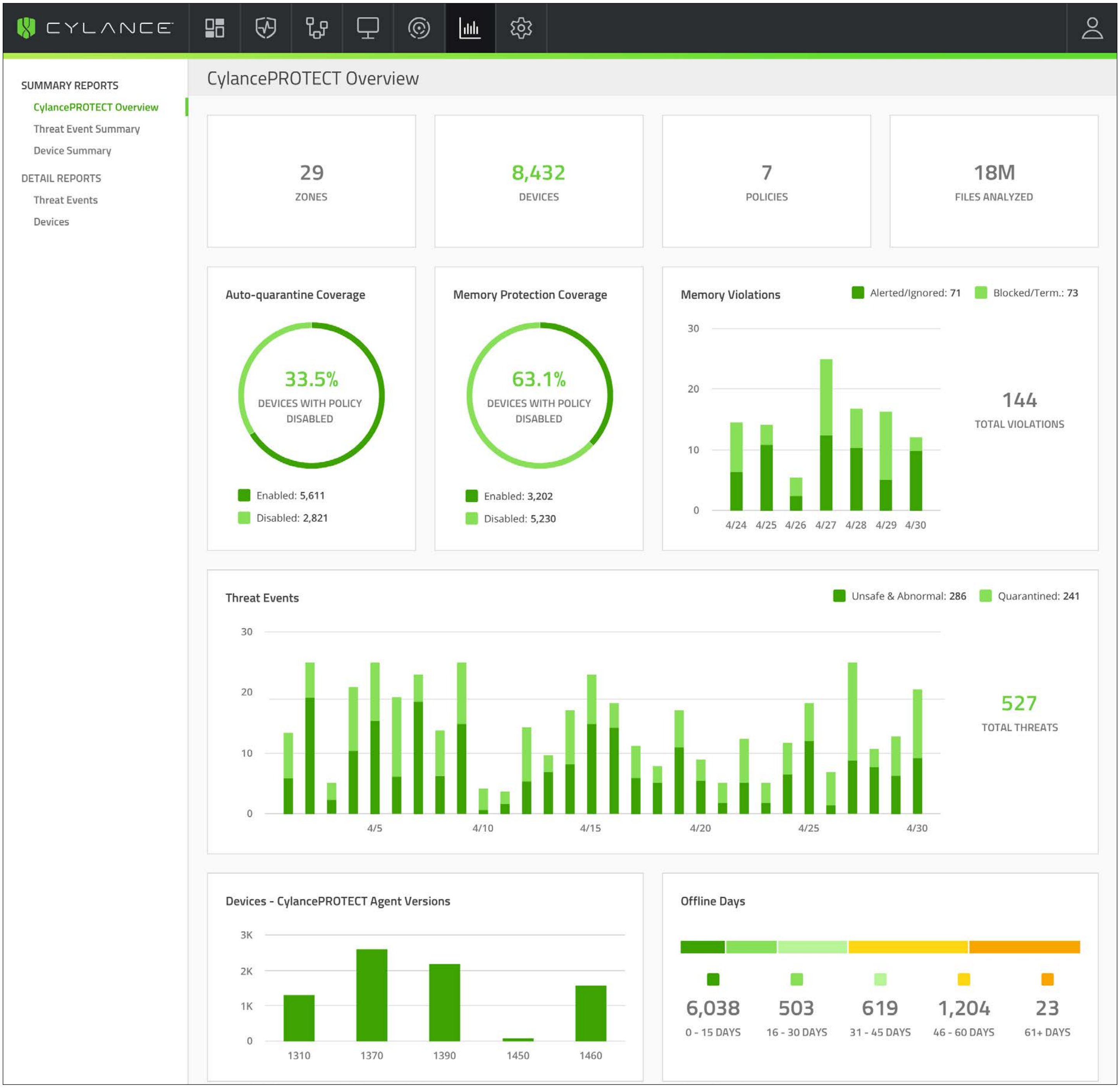
Introduction

Securing an organization's endpoints and servers from compromise is the number one priority of Cylance security solutions. Using patented artificial intelligence and purpose-built security features, CylancePROTECT and CylanceOPTICS™ deliver continuous prevention, ensuring company sensitive data remains secure.

And now, with Cylance's new management console reporting capabilities, users can easily get real-time interactive statistics, increasing their situational awareness and gaining insight into their potential attack surface. This document provides a detailed description of the new dashboards and reports available from the Cylance management console.

CylancePROTECT Overview

Provides an executive summary of your CylancePROTECT usage, from the number of zones and devices, to the percentage of devices covered by Auto-Quarantine and Memory Protection, Threat Events, Memory Violations, Agent Versions, and Offline Days for devices.



SUMMARY REPORTS
- CylancePROTECT Overview
- Threat Event Summary
- Device Summary

DETAIL REPORTS
- Threat Events
- Devices

CylancePROTECT Overview

29 ZONES

8,432 DEVICES

7 POLICIES

18M FILES ANALYZED

Auto-quarantine Coverage

33.5% DEVICES WITH POLICY DISABLED

🟩 Enabled: 5,611
🟩 Disabled: 2,821

Memory Protection Coverage

63.1% DEVICES WITH POLICY DISABLED

🟩 Enabled: 3,202
🟩 Disabled: 5,230

Memory Violations

🟩 Alerted/Ignored: 71 🟩 Blocked/Term.: 73

144 TOTAL VIOLATIONS

Threat Events

🟩 Unsafe & Abnormal: 286 🟩 Quarantined: 241

527 TOTAL THREATS

Devices - CylancePROTECT Agent Versions

Offline Days

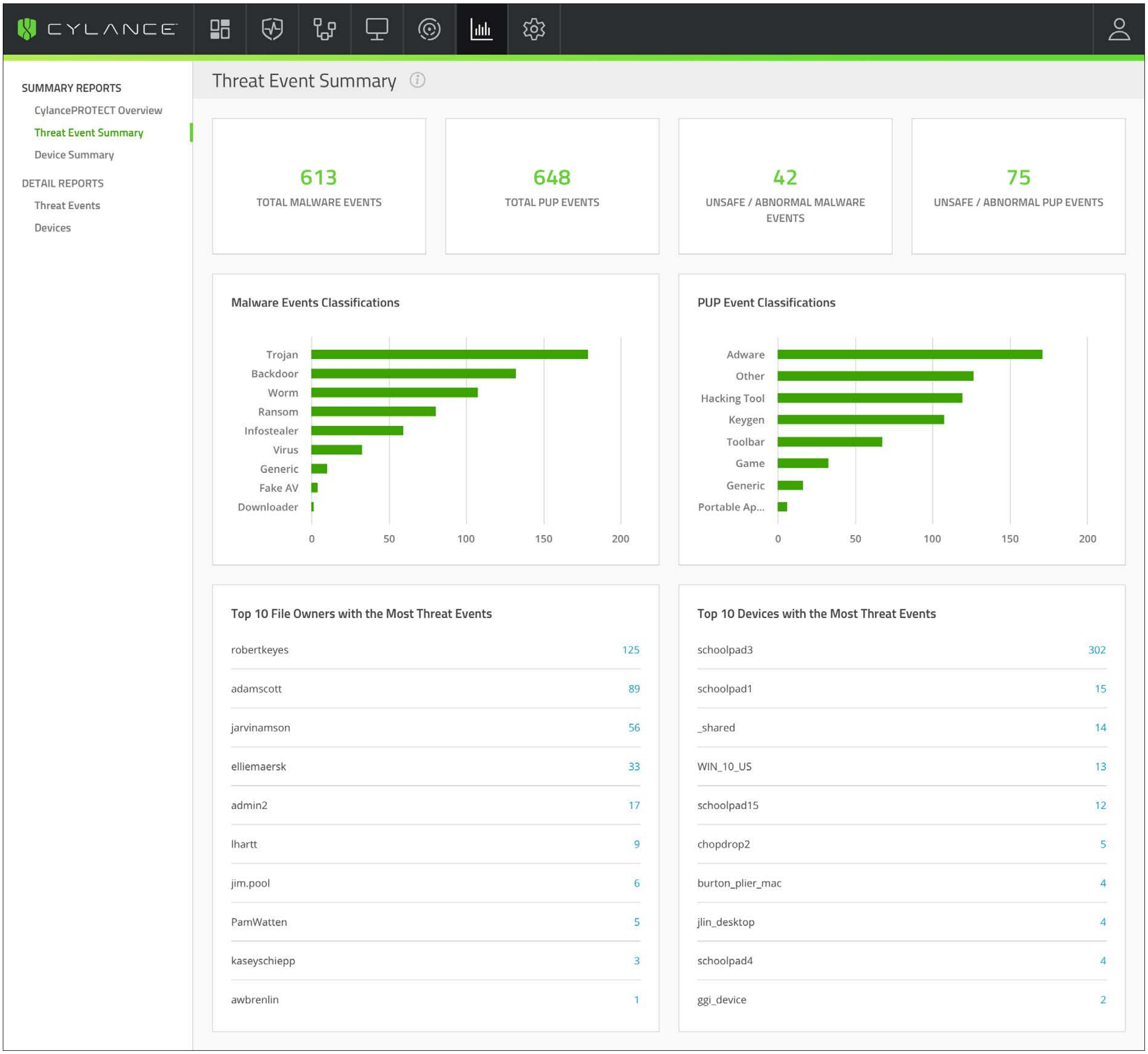
🟩	🟩	🟩	🟨	🟧
6,038	503	619	1,204	23
0 - 15 DAYS	16 - 30 DAYS	31 - 45 DAYS	46 - 60 DAYS	61+ DAYS

CylancePROTECT Overview Report Details

Report Section	Description
Auto-Quarantine Coverage	Displays the number of devices with a policy that has both Unsafe and Abnormal selected for Auto-Quarantine; these devices are considered Enabled. Disabled devices are assigned to a policy that has one or both options disabled. The pie chart displays the percentage of devices assigned to a policy with Auto-Quarantine disabled for Unsafe, Abnormal, or both. Click on this widget to see a detailed list of devices by Auto-Quarantine enablement status.
Devices	Displays the number of devices in your organization. A device is an endpoint with a registered CylancePROTECT Agent. Click on this widget to see a detailed list of devices.
Devices - CylancePROTECT Version Stats	Displays a bar chart representing the number of devices running an Agent version. Hovering over a bar in the chart displays the number of devices running that specific Agent version. Click on this widget to see a detailed list of devices filtered by agent version.
Files Analyzed	Displays the number of files analyzed across all devices in your organization.
Memory Protection Coverage	Displays the number of devices with a policy that has Memory Protection set to Block or Terminate for 11 or more of the 16 memory violation types listed in a policy; these devices are considered Enabled. Disabled devices are assigned to a policy that has Memory Protection set to Block or Terminate for 10 or less of the memory violation types. The pie chart displays the percentage of devices assigned to a policy with 10 or less memory violation types set to Block or Terminate. Click on this widget to see a detailed list of devices by Memory Protection enablement status.
Memory Violations	Displays a bar chart with memory violations that were either Alerted/Ignored (**Alert/Ignore**) or Blocked/Terminated (**Block/Term**) over the last seven days. Hovering over a bar in the chart displays a breakdown of each data type.
Offline Days	Displays the number of devices that have been Offline for a range of days (from 0-15 Days, up to 61+ Days). Also displays a bar chart color-coded with each range of days.
Policies	Displays the number of policies created in your organization.
Threats Events	Displays a bar chart with the number of threat events, grouped by day, for the last 30 days. Hovering over a bar in the chart displays a breakdown of the events for that day. Click on this widget to see a detailed threats list.
Zones	Displays the number of zones in your organization.

Threat Event Summary

The Threat Event Summary Report shows the quantity of files identified in each of the two CylancePROTECT threat families, malware and potentially unwanted programs (PUPs), and includes a breakdown to specific sub-category classifications for each family.



Threat Event Summary

613	648	42	75
TOTAL MALWARE EVENTS	TOTAL PUP EVENTS	UNSAFE / ABNORMAL MALWARE EVENTS	UNSAFE / ABNORMAL PUP EVENTS

Top 10 File Owners with the Most Threat Events

robertkeyes	125
adamscott	89
jarvinamson	56
elliemaersk	33
admin2	17
lhartt	9
jim.pool	6
PamWatten	5
kaseyschiepp	3
awbrenlin	1

Top 10 Devices with the Most Threat Events

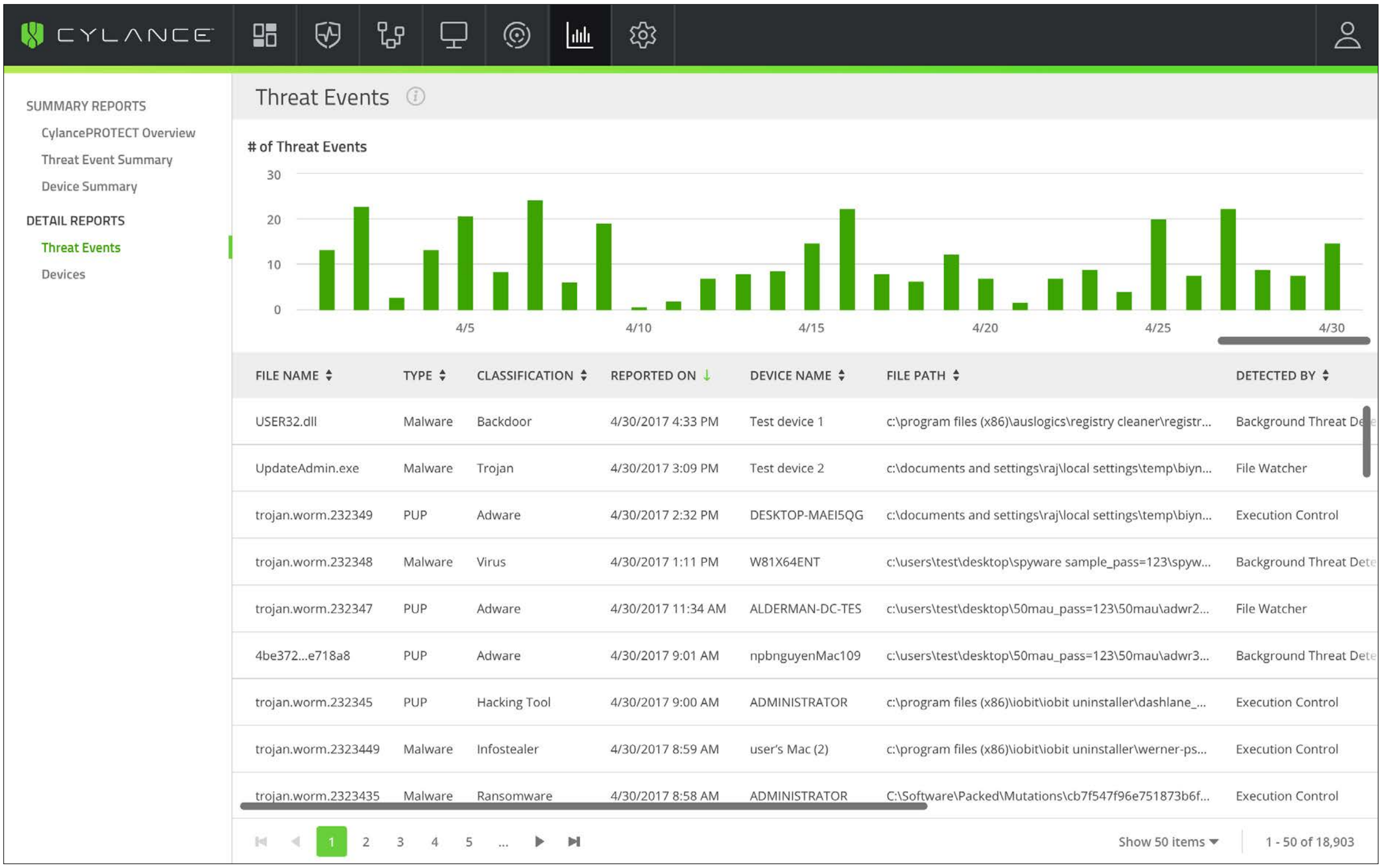
schoolpad3	302
schoolpad1	15
_shared	14
WIN_10_US	13
schoolpad15	12
chopdrop2	5
burton_plier_mac	4
jlin_desktop	4
schoolpad4	4
ggi_device	2

Threat Event Summary Report Details

Report Section	Description
Malware Event Classifications	Displays a bar chart with each type of malware classification for threat events found on devices in your organization. Hovering over a bar in the chart displays the total number of malware events found for that classification. Click on this widget to see a detailed malware list.
Potentially Unwanted Program (PUP) Event Classifications	Displays a bar chart with each type of PUP classification for threat events found on devices in your organization. Hovering over a bar in the chart displays the total number of PUP events found for that classification. Click on this widget to see a detailed PUP list.
Top 10 Devices with the Most Threat Events	Displays a list of the top 10 devices that have the most threat events. Click on this widget to see a detailed list of threats filtered by Device Name.
Top 10 File Owners with the Most Threat Events	Displays a list of the top 10 file owners that have the most threat events. Click on this widget to see a detailed list of threats filtered by File Owner.
Total Malware Events	Displays the total number of malware events identified in your organization. Click on this widget to see a detailed list of malware events.
Total PUP Events	Displays the total number of PUP events identified in your organization. Click on this widget to see a detailed list of PUP events.
Unsafe/Abnormal Malware Events	Displays the total number of Unsafe and Abnormal malware events found in your organization. Click on this widget to see a detailed list of malware events that are in an Unsafe/Abnormal state.
Unsafe/Abnormal PUP Events	Displays the total number of Unsafe and Abnormal PUP events found in your organization. Click on this widget to see a detailed list of PUP events that are in an Unsafe/Abnormal state.

Threat Events

The Threat Events Report provides data for threats found in your environment, per day, over the last 30 days.



FILE NAME	TYPE	CLASSIFICATION	REPORTED ON	DEVICE NAME	FILE PATH	DETECTED BY
USER32.dll	Malware	Backdoor	4/30/2017 4:33 PM	Test device 1	c:\program files (x86)\auslogics\registry cleaner\registr...	Background Threat De
UpdateAdmin.exe	Malware	Trojan	4/30/2017 3:09 PM	Test device 2	c:\documents and settings\raj\local settings\temp\biyn...	File Watcher
trojan.worm.232349	PUP	Adware	4/30/2017 2:32 PM	DESKTOP-MAEI5QG	c:\documents and settings\raj\local settings\temp\biyn...	Execution Control
trojan.worm.232348	Malware	Virus	4/30/2017 1:11 PM	W81X64ENT	c:\users\test\desktop\spyware sample_pass=123\spyw...	Background Threat Dete
trojan.worm.232347	PUP	Adware	4/30/2017 11:34 AM	ALDERMAN-DC-TES	c:\users\test\desktop\50mau_pass=123\50mau\adwr2...	File Watcher
4be372...e718a8	PUP	Adware	4/30/2017 9:01 AM	npbnguyenMac109	c:\users\test\desktop\50mau_pass=123\50mau\adwr3...	Background Threat Dete
trojan.worm.232345	PUP	Hacking Tool	4/30/2017 9:00 AM	ADMINISTRATOR	c:\program files (x86)\iobit\iobit uninstaller\dashlane_...	Execution Control
trojan.worm.2323449	Malware	Infostealer	4/30/2017 8:59 AM	user's Mac (2)	c:\program files (x86)\iobit\iobit uninstaller\werner-ps...	Execution Control
trojan.worm.2323435	Malware	Ransomware	4/30/2017 8:58 AM	ADMINISTRATOR	C:\Software\Packed\Mutations\cb7f547f96e751873b6f...	Execution Control

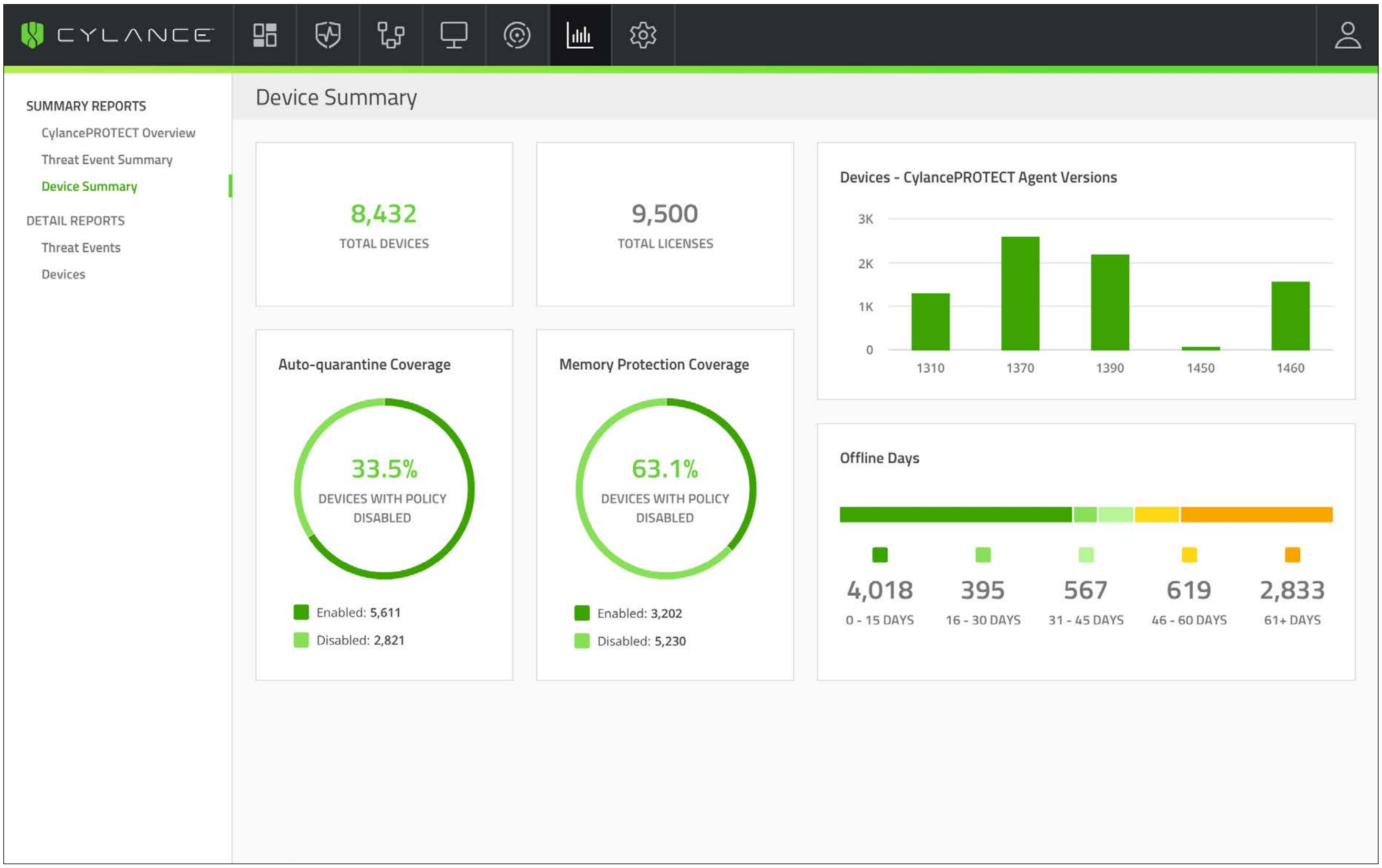
|◀ ◀ 1 2 3 4 5 ... ▶ ▶|

Threat Event Report Details

Report Section	Description
# of Threat Events	Displays a bar chart with the threat events reported in your organization. Hovering over a bar in the chart displays the total number of threat events reported on that day. The bar chart displays the last 30 days. Clicking on any bar will filter the table below by the Reported-On date. Click on the bar again to remove the filter.
Threat Events Table	Displays threat event information. Clicking on a table heading will sort the list (ascending or descending) by the column.

Device Summary

The Device Summary Report shows multiple device-centric metrics.



Device Summary

8,432
TOTAL DEVICES

9,500
TOTAL LICENSES

Devices - CylancePROTECT Agent Versions

Auto-quarantine Coverage

33.5%
DEVICES WITH POLICY DISABLED

🟩 Enabled: 5,611
🟩 Disabled: 2,821

Memory Protection Coverage

63.1%
DEVICES WITH POLICY DISABLED

🟩 Enabled: 3,202
🟩 Disabled: 5,230

Offline Days

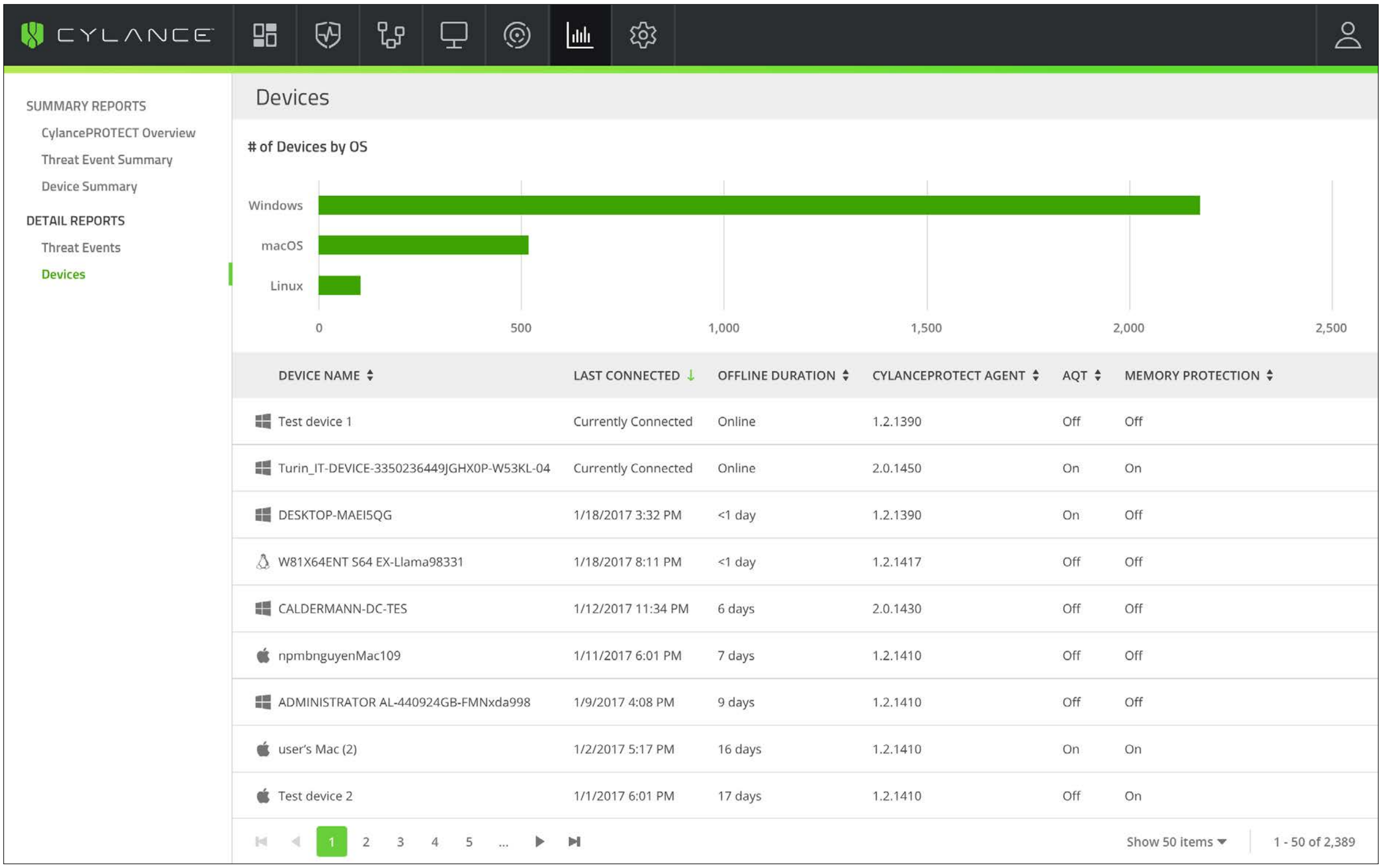
4,018	395	567	619	2,833
0 - 15 DAYS	16 - 30 DAYS	31 - 45 DAYS	46 - 60 DAYS	61+ DAYS

Device Summary Report Details

Report Section	Description
Auto-Quarantine Coverage	Displays the number of devices with a policy that has both Unsafe and Abnormal selected for Auto-Quarantine; these devices are considered Enabled. Disabled devices are assigned to a policy that has one or both options disabled. The pie chart displays the percentage of devices assigned to a policy with Auto-Quarantine disabled for Unsafe, Abnormal, or both. Click on this widget to see a detailed list of devices by Auto-Quarantine enablement status.
Devices - CylancePROTECT Version Stats	Displays a bar chart representing the number of devices running an Agent version. Hovering over a bar in the chart displays the number of devices running that specific Agent version. Click on this widget to see a detailed list of devices filtered by agent version.
Memory Protection Coverage	Displays the number of devices with a policy that has Memory Protection set to Block or Terminate for 11 or more of the 16 memory violation types listed in a policy; these devices are considered Enabled. Disabled devices are assigned to a policy that has Memory Protection set to Block or Terminate for 10 or less of the memory violation types. The pie chart displays the percentage of devices assigned to a policy with 10 or less memory violation types set to Block or Terminate. Click on this widget to see a detailed list of devices by Memory Protection enablement status.
Offline Days	Displays the number of devices that have been Offline for a range of days (from 0-15 Days, up to 61+ Days). Also displays a bar chart color-coded with each range of days.
Total Devices	Displays the total number of devices in your organization. A device is a system with a registered CylancePROTECT Agent. Click on this widget to see a detailed list of devices.
Total Licenses	Displays the total number of CylancePROTECT licenses your organization has purchased.

Devices

The Devices Report shows the number of devices per operating system family (Microsoft Windows, Apple macOS, and Linux).



DEVICE NAME	LAST CONNECTED	OFFLINE DURATION	CYLANCEPROTECT AGENT	AQT	MEMORY PROTECTION
Test device 1	Currently Connected	Online	1.2.1390	Off	Off
Turin_IT-DEVICE-3350236449JGHX0P-W53KL-04	Currently Connected	Online	2.0.1450	On	On
DESKTOP-MAEI5QG	1/18/2017 3:32 PM	<1 day	1.2.1390	On	Off
W81X64ENT S64 EX-Llama98331	1/18/2017 8:11 PM	<1 day	1.2.1417	Off	Off
CALDERMANN-DC-TES	1/12/2017 11:34 PM	6 days	2.0.1430	Off	Off
npmbnguyenMac109	1/11/2017 6:01 PM	7 days	1.2.1410	Off	Off
ADMINISTRATOR AL-440924GB-FMNxda998	1/9/2017 4:08 PM	9 days	1.2.1410	Off	Off
user's Mac (2)	1/2/2017 5:17 PM	16 days	1.2.1410	On	On
Test device 2	1/1/2017 6:01 PM	17 days	1.2.1410	Off	On

Devices Report Details

Report Section	Description
# of Devices by OS	Displays a bar chart with devices organized by major OS groups (Microsoft Windows, Apple macOS, Linux). Hovering over a bar in the chart displays the total number of devices in that OS group. Clicking on any bar will filter the table below by OS Group. Click on the bar again to remove the filter.
Devices Table	Displays a list of device names, and device information, for devices in your organization.

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