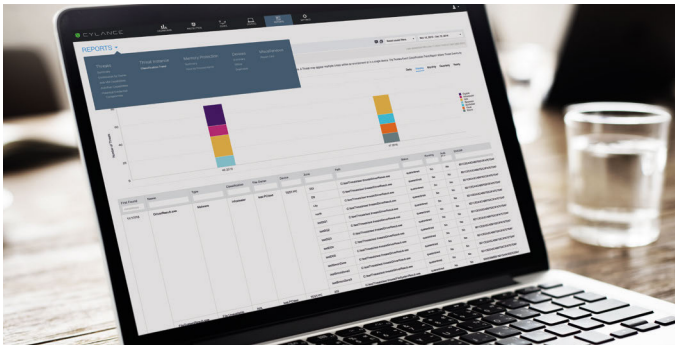


CylancePROTECT® Feature Focus

Reporting

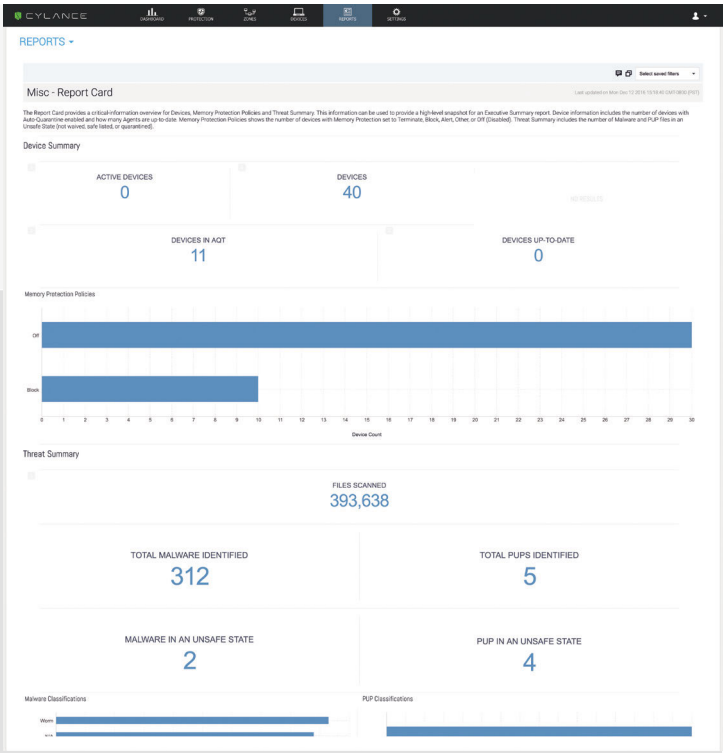
CYLANCE™



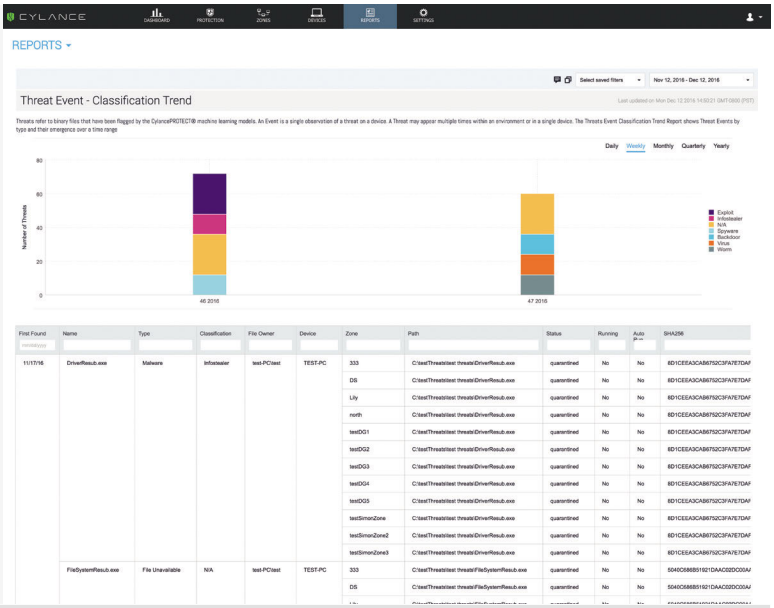
Reporting Overview

The CylancePROTECT release adds comprehensive reporting functionality through the intuitive web-based console. This release offers a summary report called Report Card, drill-down reports in three primary vectors: threats, memory protection, and devices, and some helpful additional features designed to streamline the entire reporting process. The following is a summary of the new reporting features.

Report Card	The Report Card feature summarizes the overall health of your cybersecurity infrastructure in a single, easy to understand screen.
Threats – Summary Report	The Threat Summary Report shows the quantity of files identified in each of the two CylancePROTECT threat families: malware and PUPs (potentially unwanted programs) and includes a breakdown to specific sub-category classifications for each family.
Threats – Distribution by Owner	Threats refer to binary files that have been flagged by the CylancePROTECT machine learning models. The Threats Distribution by Owner Summary Report reveals which user accounts are tagged as threat file owners. This information reveals the rate at which certain users are involved with threat incidents. This information can also provide direction on which accounts may need assistance to improve security (like resetting a password during an incident).
Threats – Anti-VM Capabilities	This report reveals binaries with features that could potentially be used to evade dynamic analysis (sandbox) detection. This information is generated from the presence of Threat Indicators related to Anti-VM capabilities.
Threats – AutoRun	This report reveals binaries with features that indicate they automatically run during system bootup to maintain persistence.
Threats – Potential Credential Compromise	This report reveals binaries with features that could potentially be used as key loggers for capturing and exfiltrating system credentials.



Threat – Classification Trend Report	Threats refer to binary files that have been flagged by the CylancePROTECT machine learning models. An Event is a single observation of a threat on a device. A threat may appear multiple times within an environment or in a single device. The Threats Event Classification Trend Report shows Threat Events by type and their emergence over time.
Memory Protection – Summary	Memory Protection refers to the CylancePROTECT function that keeps watch on the system for suspicious memory events. The Memory Protection Summary Report shows unique memory protection event instances by method and their emergence over a time range.
Memory Protection – Pivot by Process Name	This report provides a process-specific view of memory protection event instances.
Devices Summary	The Devices Summary Report shows multiple device-centric measures of importance. Agents Auto Quarantine reveals threat prevention coverage and can be used to show progress. Agent Versions can identify older Agents that should be updated. Device Count and Duplicates indicate overall system usage. Offline Days may indicate devices that are no longer checking in to the CylancePROTECT console and are candidates for removal.
Devices – Unsafe Devices	Malware and PUPs in an Unsafe State are those still considered to be a risk (not contained) because the device is in a non-prevention policy (example: Auto-Quarantine is disabled). The Unsafe Devices Report shows devices that have one or more files considered to be unsafe by the CylancePROTECT Agent. Unsafe threats are handled with prevention policies or by manually quarantining the unsafe threats.
Devices – Duplicates	The Duplicates Report reveals which Device Name has multiple instances associated with it. CylancePROTECT uses a unique fingerprint to identify a device. There are some situations that may cause duplicates for the same device, like cloning a virtual machine or downgrading the CylancePROTECT agent. Identifying duplicates can help you remove redundant, extraneous, or unneeded device information from the console.
Saved Filters Feature	Allows users to avoid repeated filter construction by retaining useful filters in memory.
Redirection Feature	Enables users to immediately access pertinent information on threat reports quickly within the application.
Export Enhancement NEW 1/18/17	Allows users to choose export formats: PDF, CSV, and PNG.



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

©2017 Cylance Inc. Cylance® and CylancePROTECT® and all associated logos and designs are trademarks or registered trademarks of Cylance Inc. All other registered trademarks or trademarks are property of their respective owners.