



Single Product Test

Panda Adaptive Defense 360

Language: English
December 2016

Last Revision: 12th January 2017

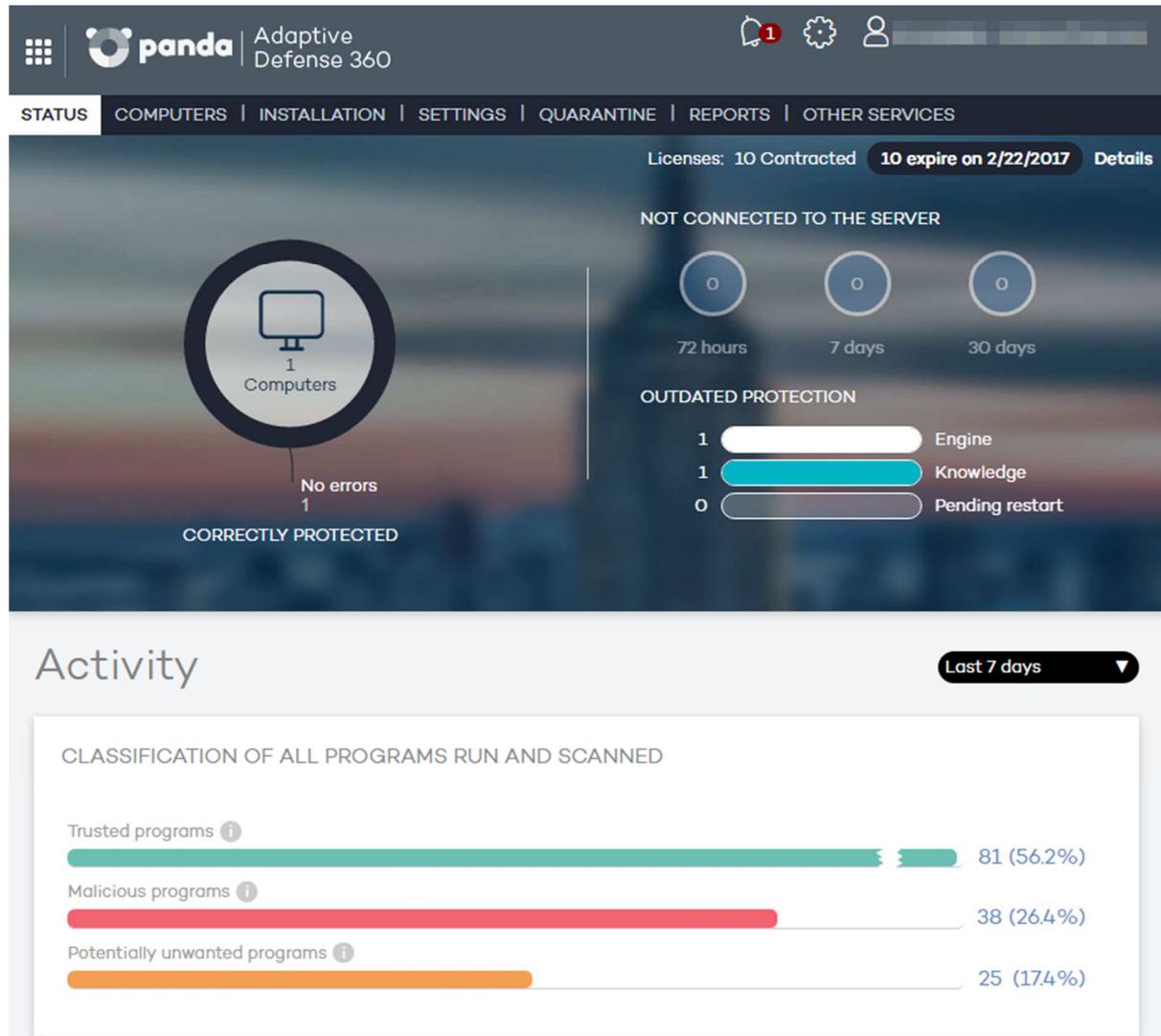
www.av-comparatives.org

Commissioned by Panda Security

Panda Adaptive Defense 360

Introduction

This report was commissioned by Panda Security.



Overview

Product version reviewed

Adaptive Defense 360 Version 2.3.5
Windows protection version 7.60

Operating systems supported

Windows XP SP2 and later, Windows Vista, Windows 7, 8, 8.1, 10; Windows Server 2003, 2008, 2012.
Partially supported: Linux, Mac OS X, and Android

About the product

Panda Adaptive Defense 360 provides a cloud-based, centrally managed endpoint security platform. It combines classical security features such as Anti-Malware, Firewall, and Web- and E-Mail Filtering, with a combination of a Next-Generation Endpoint Protection and a Cloud Platform that provides Endpoint Detection and Response service (EDR). The EDR component continuously monitors all applications running on devices within the company network, and aims to protect those devices from known and unknown threats. For this, the EDR employs automatic classification of all running processes based on the recorded events using machine learning techniques in a Big Data environment. Applications which cannot be classified automatically are analysed by Panda's threat researchers.

The combination of these elements constitute the essence of Panda Adaptive Defense's Cloud Service and Platform.

Product page on vendor's website

<http://www.pandasecurity.com/intelligence-platform/solutions.htm>

Description of the product

Panda Adaptive Defense 360 is a combination of an Endpoint Protection Platform (EPP) that includes "traditional" antivirus software, and a combination of a Next-Generation Endpoint Protection and a Cloud Platform that provides Endpoint Detection and Response service (EDR).

The cloud-based console displays an overview of the status of the network, and all individual endpoints and servers, etc. where the solution is deployed.

While the EPP detects and blocks malware using existing methods such as signatures and behavioural detection, the Next Generation Endpoint Protection monitors and classifies 100% of processes that run on network computers, generating forensic information that can be used to determine the root cause, the affected assets and the actions taken by the incident actor, such as how the threat started, what processes were created and when, opened connections, etc. All that information is available through the console in real time.

All processes will be categorized as either Trusted Programs, Malicious Programs or Potentially Unwanted Programs (this can be seen on the same page, under "Activities"). The Malicious Programs and Potentially Malicious Programs lists show the admin if any such programs have been successfully executed, if they have made external connections or have accessed data. As this solution classifies all executed processes, it cannot fail to record any malware. Even if the product misclassifies a malicious process as Trusted, as it is being monitored in real time, when malicious activity is identified or suspicious behaviour found it will be classified as malware. If the malware was already on the system before Adaptive Defense 360 was installed, when the malware acts the product will realize it is there and provide information about what it has been doing since Adaptive Defense 360 was installed in the system. Adaptive Defense 360 provides its own Advanced Reporting Tool (ART), a service based on Big Data that provides total visibility and insights of the activities at the endpoints, processes, users and IT resources misuse. It also has a SIEM connector to feed all the information to an existing SIEM (such as QRADAR). As Panda Adaptive Defense 360 is a managed service, quarantine, suspicious files and disinfection all looked after by Panda technicians.

Documentation

From the web management console of the product, administrators have access to a comprehensive online help feature, as well as detailed administration and user guides.

Good points

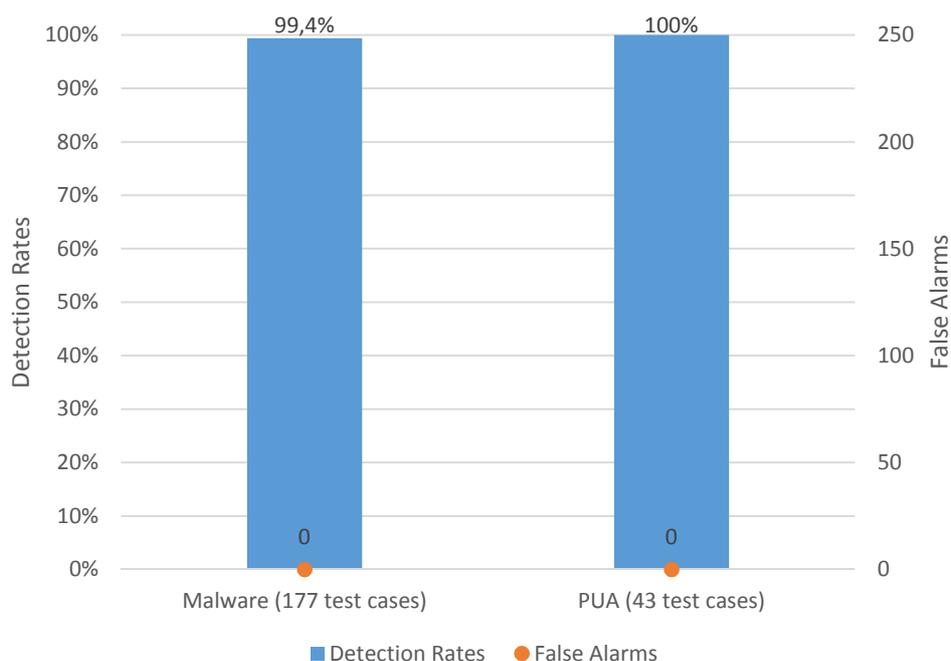
The management console provides a well-structured and intuitive user interface. The event data collected and enriched by Adaptive Defense Platform is presented in a clear way. Activity graphs provide intuitive visualization of the events that occurred during each security incident.

Efficacy Test

For big installations, Panda recommends that after installing Panda Adaptive Defense 360, the product should be run for a period of time in audit mode, so that Adaptive Defense can learn about the ordinary usage in the working environment.

For our test, we used the same method that Panda use with their customers, which is as follows. The system administrator deploys a small Adaptive Defense agent on the company's servers/endpoints. Company staff continue working on their machines as normal, and Adaptive Defense gets to know the usual behavior of all the machines, classifies running processes, etc. So, we did some "normal" work on our test machines (e.g. opening different applications, restarting it a couple of times).

We tested Panda Adaptive Defense 360 against **220** test cases. Of those, **177** were new **malicious websites**, pointing either to ransomware, backdoors, password-stealers, worms, viruses or other Trojans. Panda Adaptive Defense 360 blocked the threats in all but one case (a password-stealer) that was later identified as malware due to its malicious behavior. All **43** potentially unwanted programs (**PUA**) included in the set were also blocked by Panda Adaptive Defense 360. **No false alarms** were observed on the test system during the testing period.



Management Console

The web management console opens on the *Status* page, displaying an overview of recorded activity and detections. The other pages of the console are accessible via the menu at the top of the console. Due to the fact that that Adaptive Defense service classifies all running processes, the dashboard shows the total amount of good software applications that were run in the last year, month, week or day, along with the total amount and percentage of malware and potentially unwanted programs detected in the enterprise.

Monitoring the network

The *Activity* section on the *Status* page shows an overview of security incidents recorded within the network. Adaptive Defense 360 records all events that occurred during each incident, allowing administrators to reproduce the system’s automatic classification and the incident as a whole.

The screenshot displays the Management Console interface for a detected PUP. At the top, a table lists the process details:

Computer	Name	Path	Already run	Last action	Date
	PUP/TencentQQLive	PROGRAM_FILES_COMMONX86\Tencent\qqdownload\130\tencentdl.exe	●	Allowed	12/18/2016 3:09:50 AM

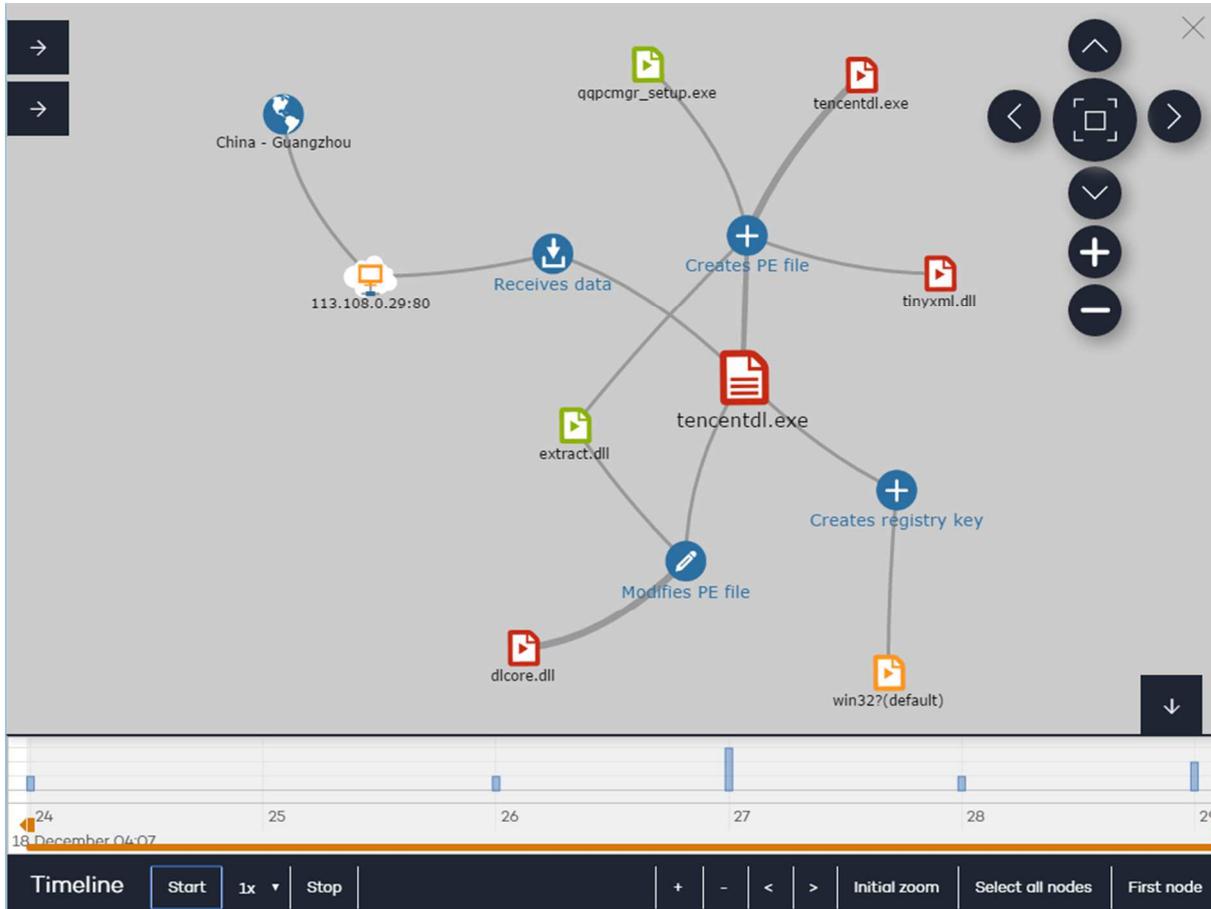
Below this, a detailed view of the PUP life cycle is shown. It includes fields for Path, Dwell time, User, MD5, and Detection technology. Search buttons for Google and VirusTotal are provided. A table titled "PUP life cycle on the computer" details the following actions:

Date	Times	Action	Path/URL/Registry Key/IP/Port	File Hash/Registry Value/Protocol-Direction/Description	Trusted
12/18/2016 3:07:24 AM	1	Is created by	TEMP\QQPCMgr_Setup.exe	099a493173c965fd441f6c219533cc3e	✓ Yes
12/18/2016 3:07:26 AM	1	Makes modifications	PROGRAM_FILES_COMMONX86\Tencent\QQDownload\130\dlcore.dll	1123cc85ff12a2a9c44395e5362220cf	✗ No
12/18/2016 3:07:27 AM	1	Is created by	PROGRAM_FILES_X86\Tencent\QQPCMgr\1.5.17490.219\Tencentdl.exe	16e27465fc02e6974704fd2187e92144	✗ No
12/18/2016 3:07:27 AM	1	Creates	PROGRAM_FILES_COMMONX86\Tencent\QQDownload\130\extract.dll	e28497e0e9266ce04271815fac080f12	✓ Yes
12/18/2016 3:07:27 AM	1	Creates	PROGRAM_FILES_COMMONX86\Tencent\QQDownload\130\trnyxml.dll	989f284c2c9c9e0eccc2486fd35cac69	✗ No
12/18/2016 3:07:27 AM	1	Is created by	PROGRAM_FILES_X86\Tencent\QQPCMgr\1.5.17490.219\Tencentdl.exe	16e27465fc02e6974704fd2187e92144	✗ No
12/18/2016 3:07:28 AM	1	Creates a Registry Key pointing to an exe file	\REGISTRY\MACHINE\SOFTWARE\Classes\TypeLib\{DA624F8F-98BF-4B03-AD11-A12D07119E81}\1.0.0\win32?(default)	3\PROGRAM_FILES_COMMONX86\Tencent\qqdownload\130\tencentdl.exe	Unknown
12/18/2016 3:07:29 AM	1	Makes modifications	PROGRAM_FILES_COMMONX86\Tencent\QQDownload\130\extract.dll	e28497e0e9266ce04271815fac080f12	✓ Yes
12/18/2016 3:07:29 AM	1	Communicates with	113.108.0.29:80	TCP-Download	Unknown
12/18/2016 3:07:29 AM	1	Makes modifications	PROGRAM_FILES_COMMONX86\Tencent\QQDownload\130\dlcore.dll	1123cc85ff12a2a9c44395e5362220cf	✗ No

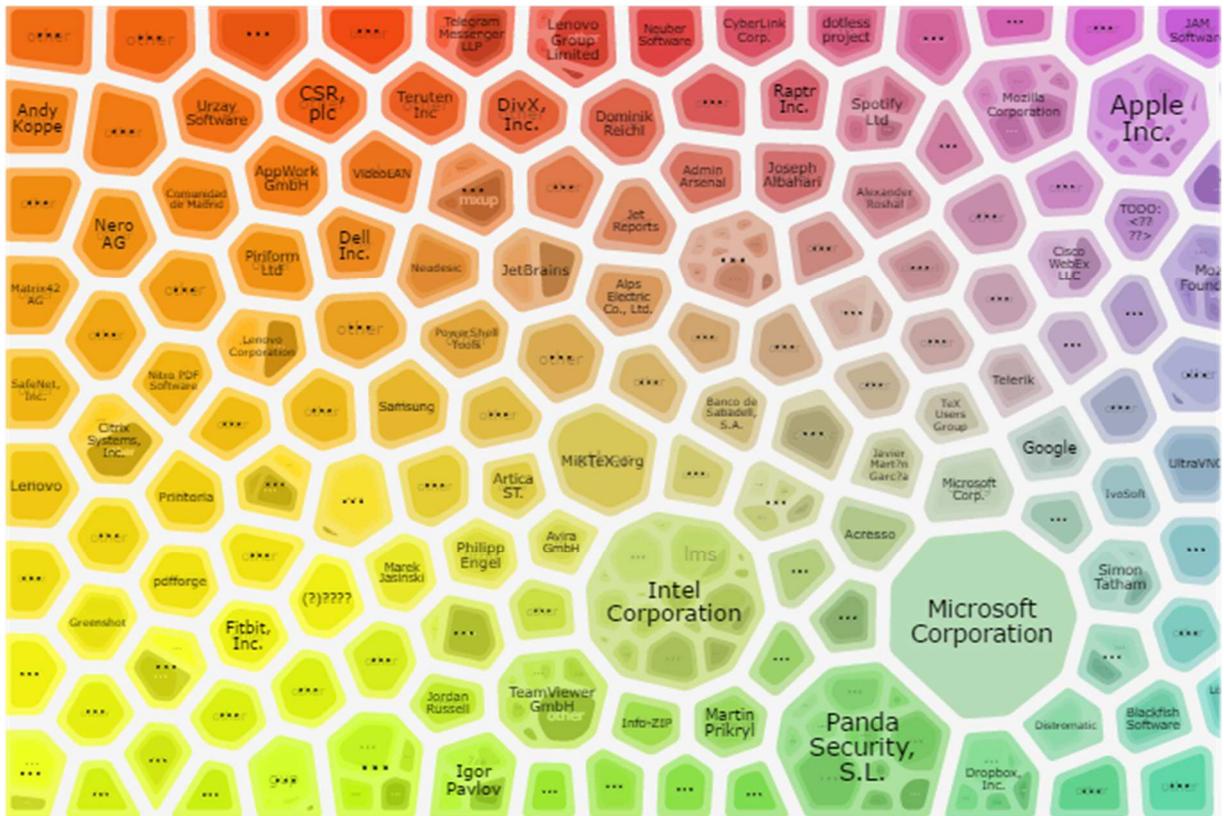
At the bottom of the detailed view, there are buttons for "See disinfection results", "Disinfect computer", and "Do not detect again".

PUP detection life cycle

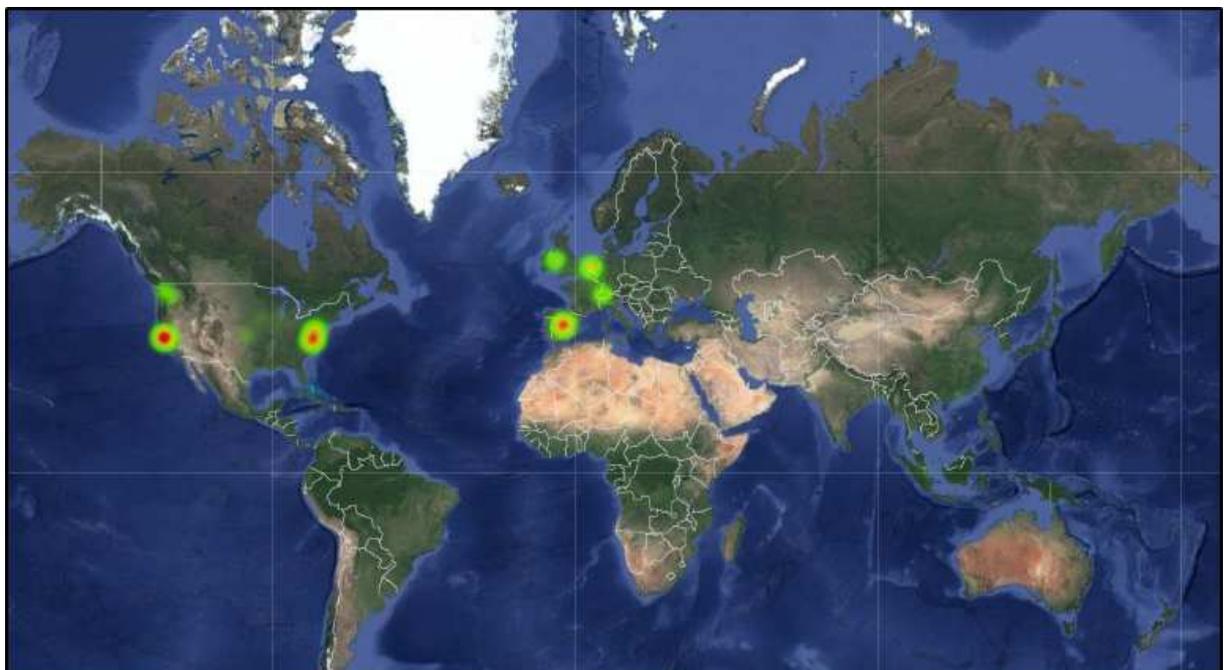
This information is further complemented by an activity graph of the recorded events. The activity graph visualizes the relationship between different events and their actors during the incident. The graph also allows administrator to follow the chronological sequence of events in an intuitive way, by animating the graph according to the incident timeline.



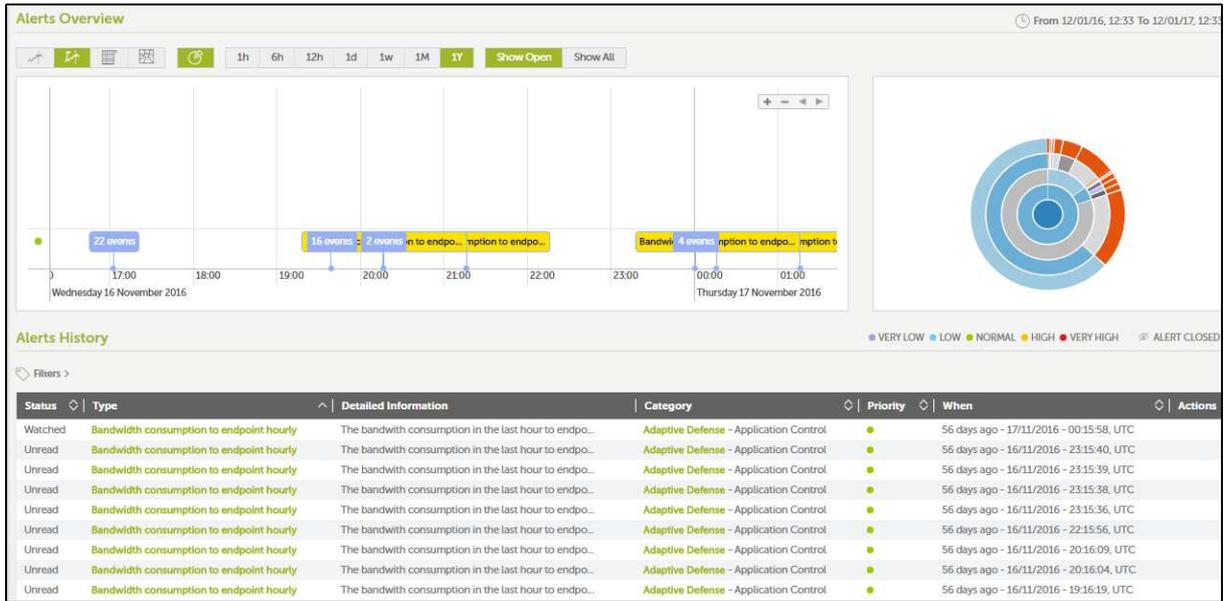
Incident Timeline



Dashboard – Voronoi Graphs



Dashboard – Heat Map Graphs



Alerts Panel

Copyright and Disclaimer

This publication is Copyright © 2017 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (January 2017)