Single Product Test

Panda Adaptive Defense 360

Language: English
December 2016

Last Revision: 12th January 2017

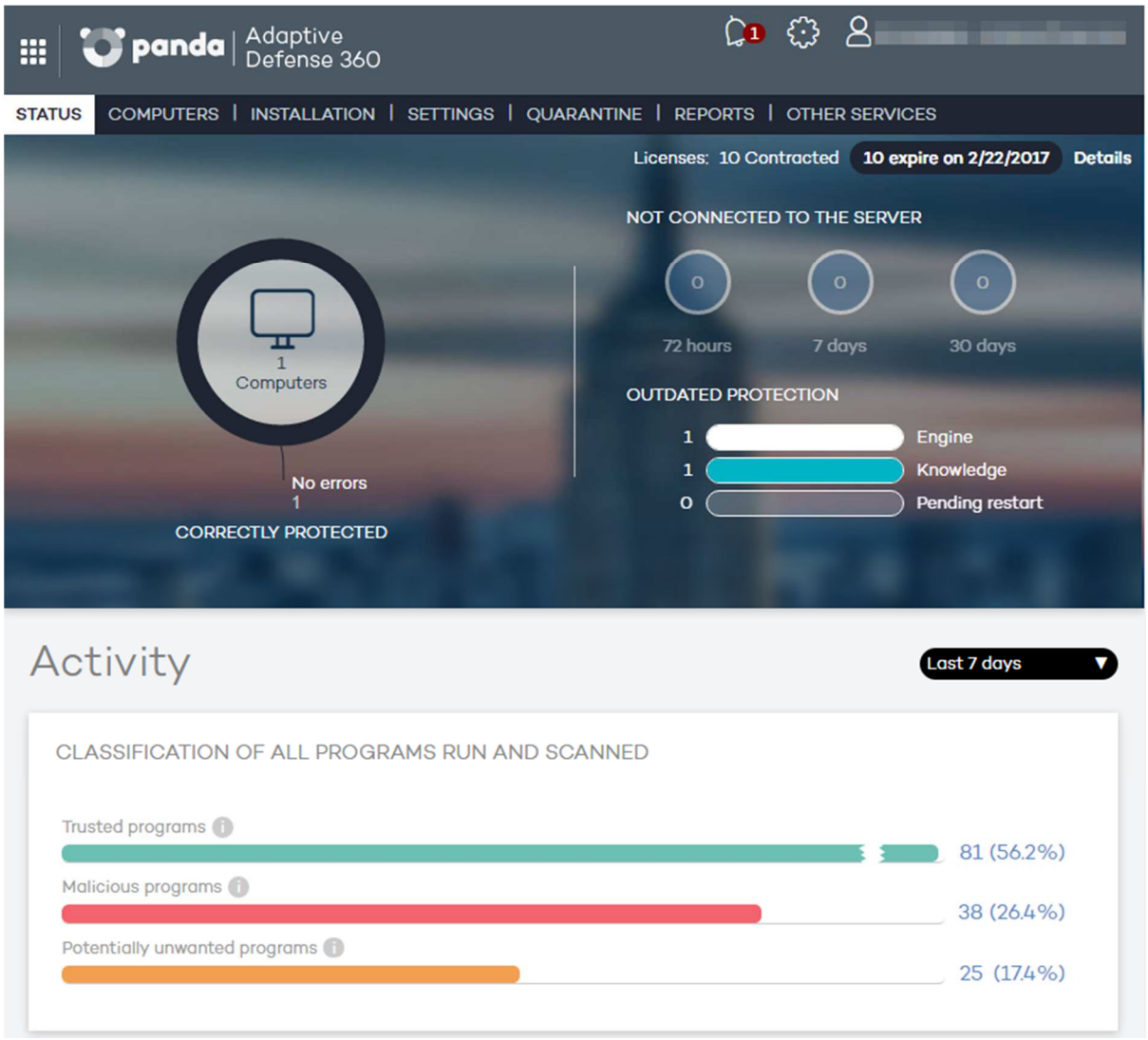
www.av-comparatives.org

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

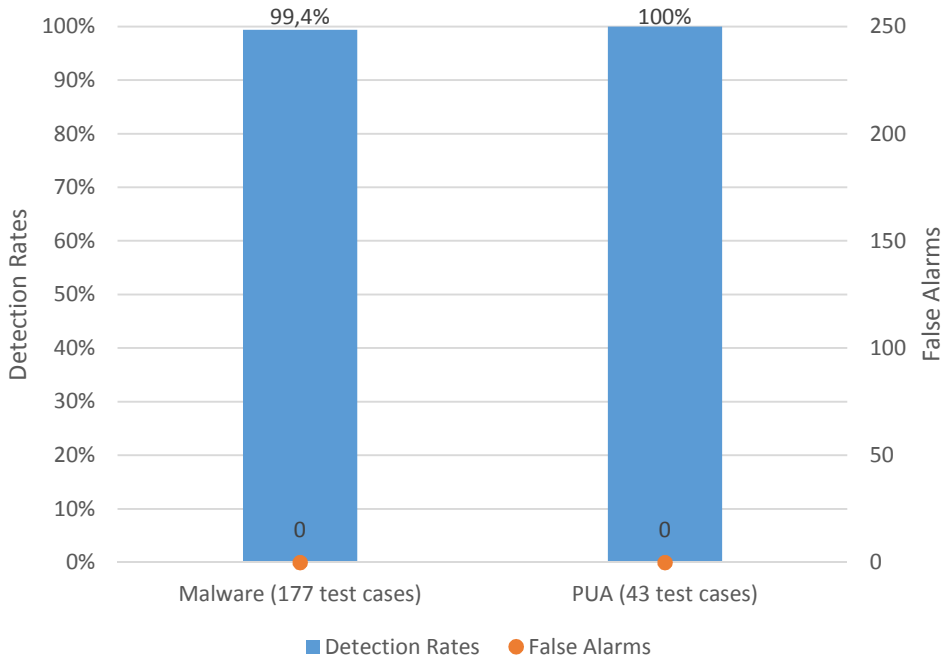
The management console provides a well-structured and intuitive user interface. The event data collected and enriched by Adaptive Defense Platform is presented in a clear way. Activity graphs provide intuitive visualization of the events that occurred during each security incident.

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.

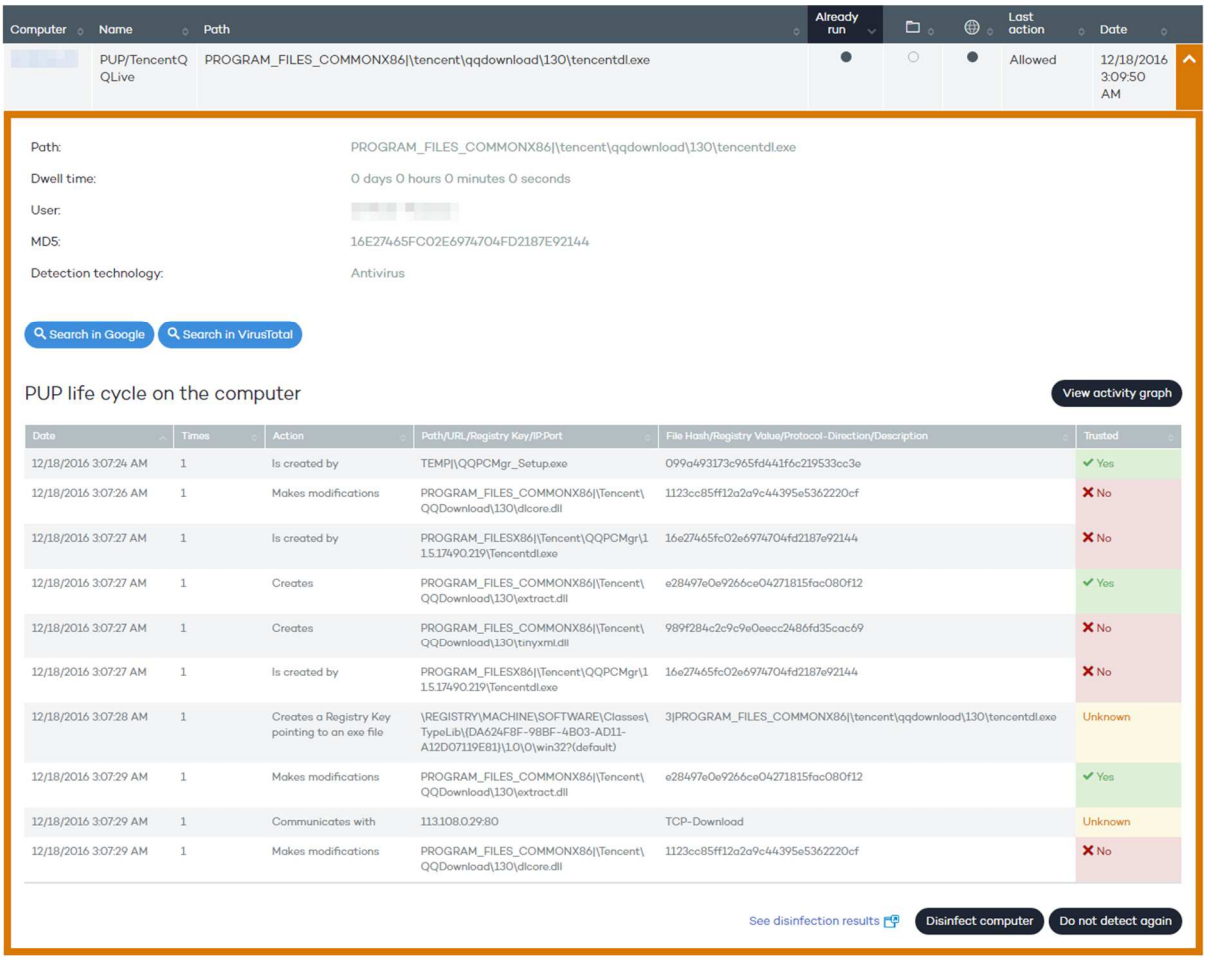


Management Console

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.

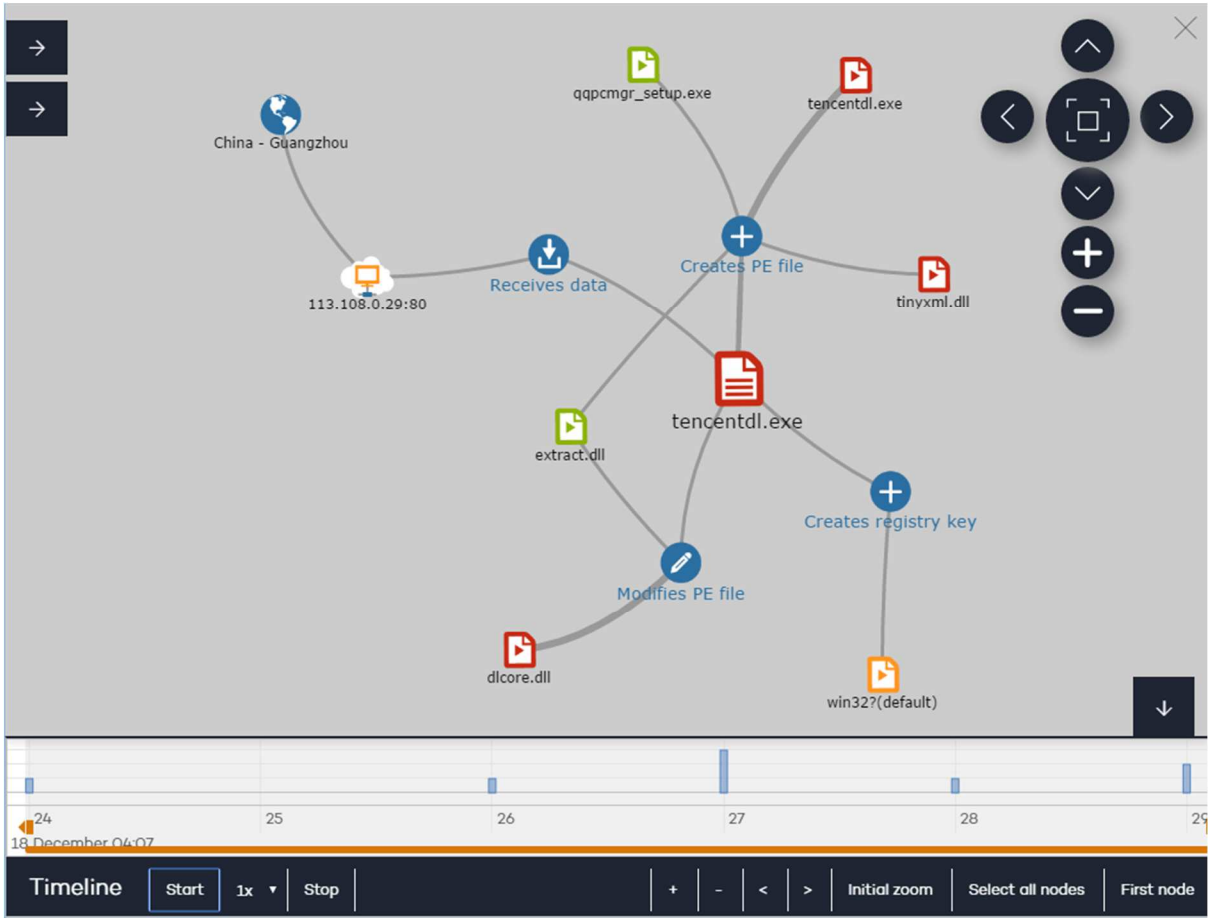
Monitoring the network

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.

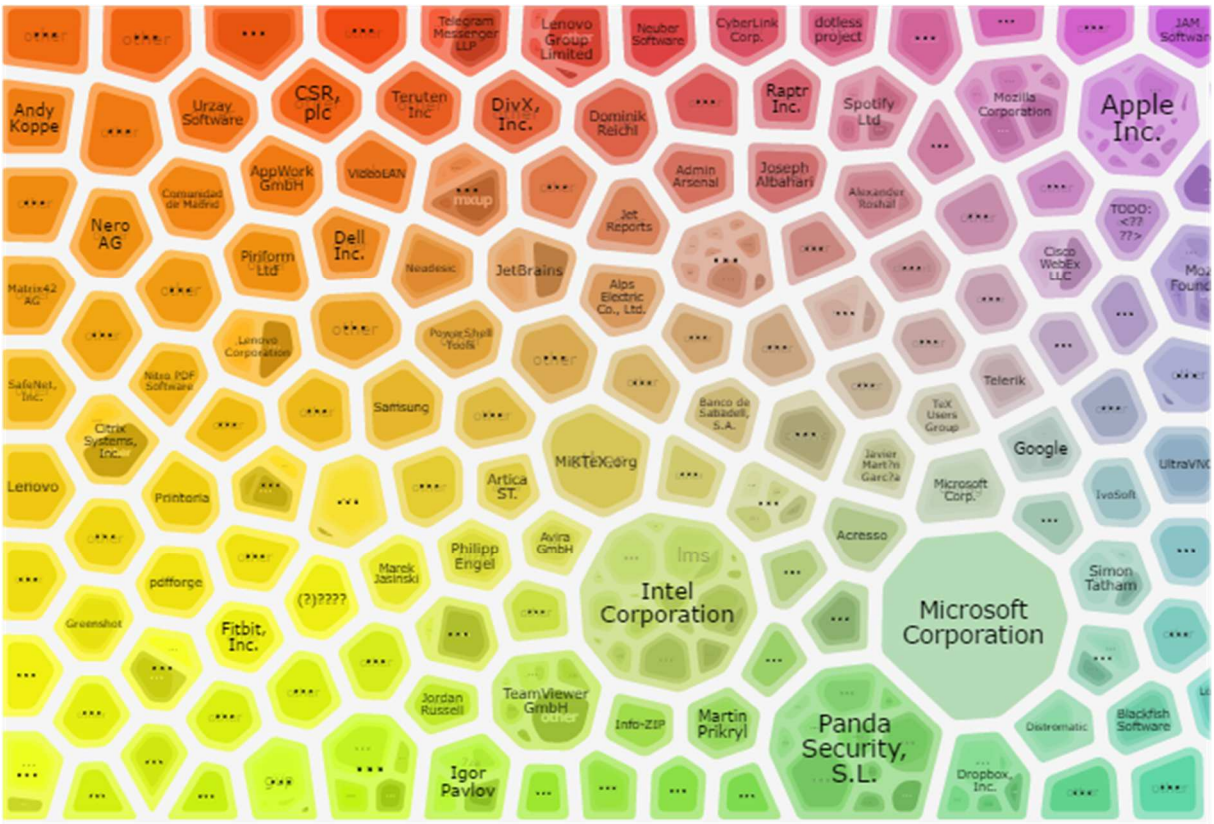


PUP detection life cycle

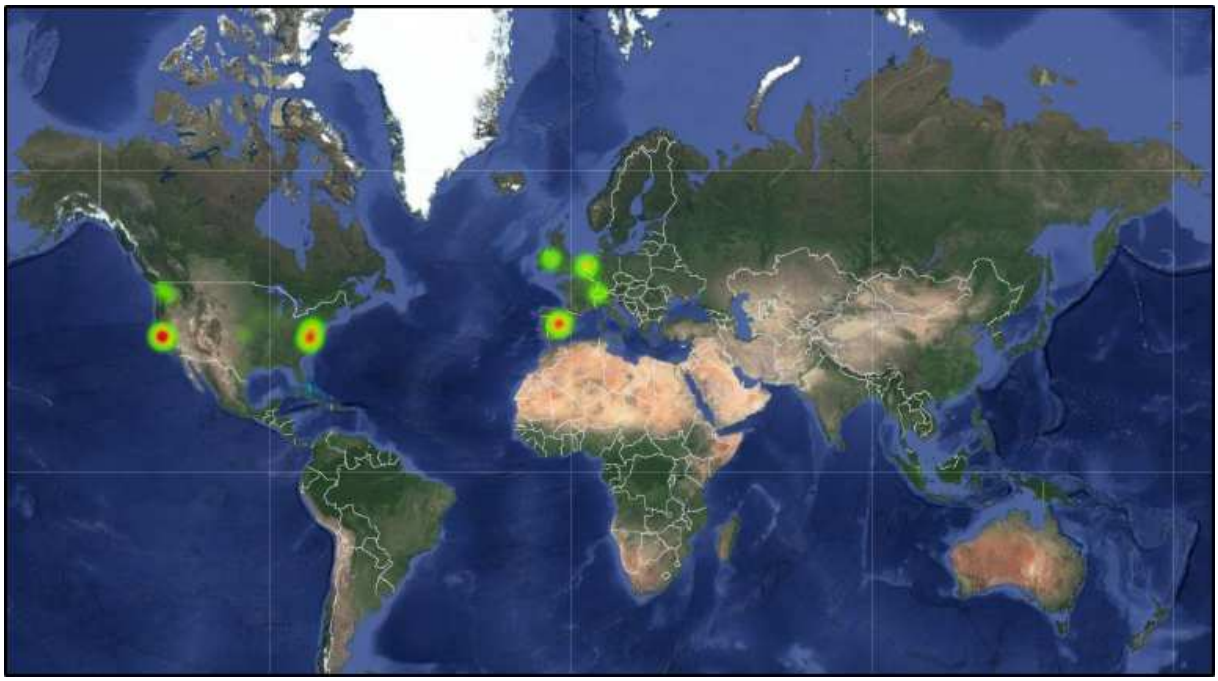
This information is further complemented by an activity graph of the recorded events. The activity graph visualizes the relationship between different events and their actors during the incident. The graph also allows administrator to follow the chronological sequence of events in an intuitive way, by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



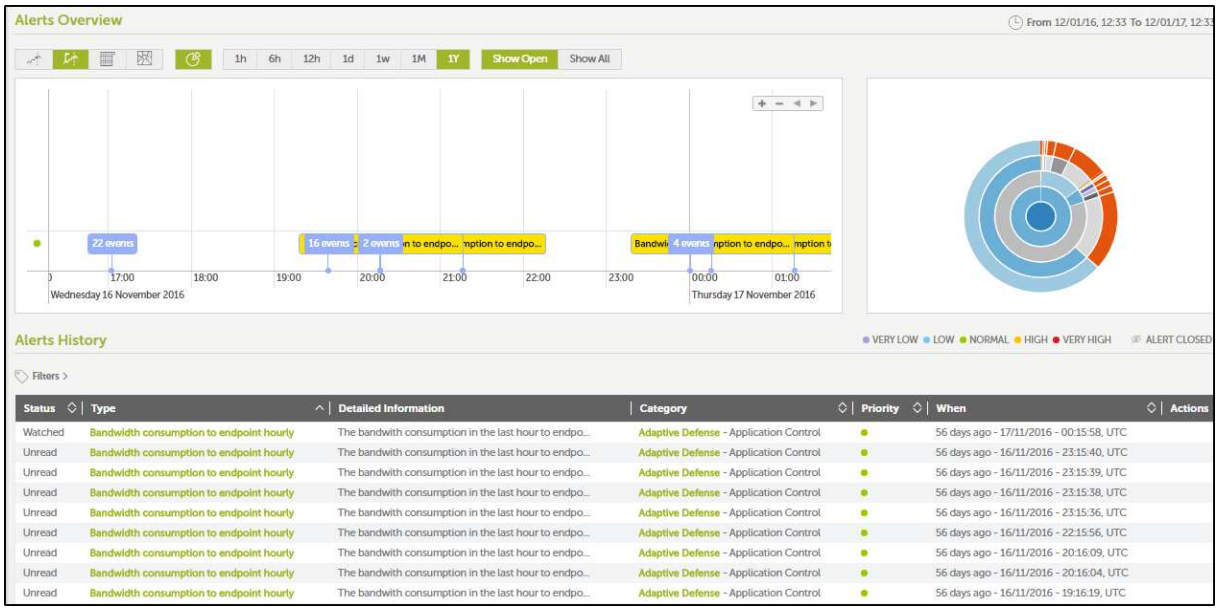
Incident Timeline



Dashboard – Voronoi Graphs



Dashboard – Heat Map Graphs



Alerts Panel

Copyright and Disclaimer

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

AV-Comparatives (January 2017)