

**ENDGAME.**

## **Anti-Virus Comparative**



### **Endgame 2.3.11**

Language: English  
May 2017

Last Revision: 9<sup>th</sup> June 2017

[www.av-comparatives.org](http://www.av-comparatives.org)

*Commissioned by Endgame*

## Endgame endpoint security platform

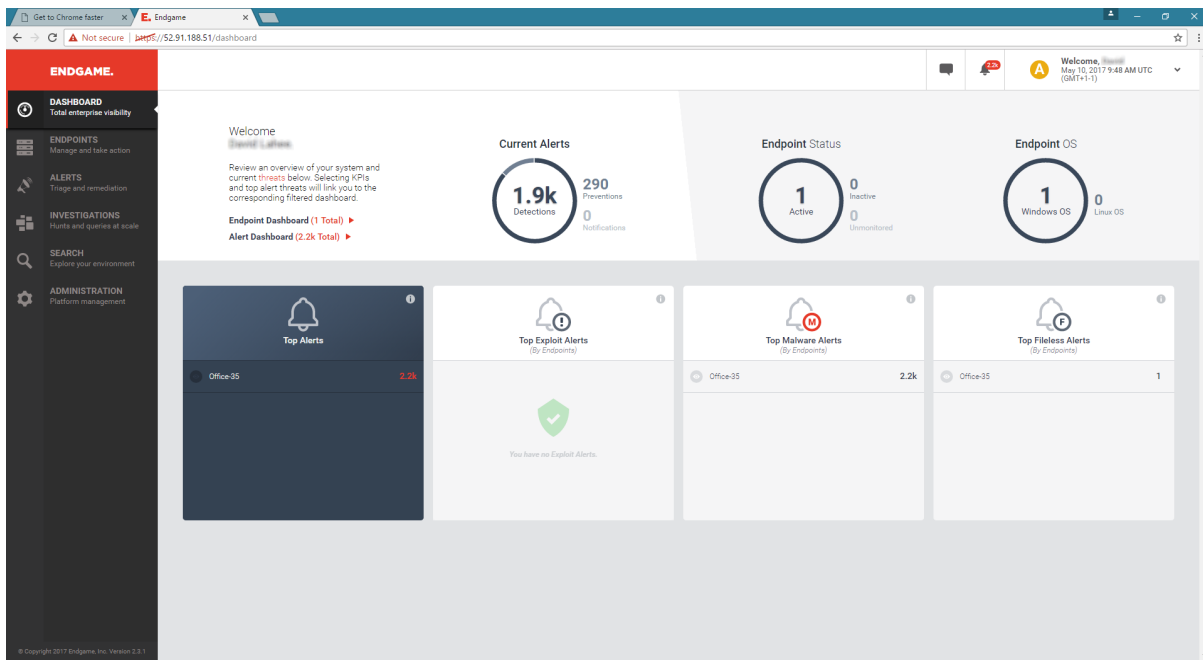
This report was commissioned by Endgame (<https://www.endgame.com>). The Real-World Protection test was performed in May 2017 using Endgame 2.3.11. The product has been configured by Endgame.

### About the product

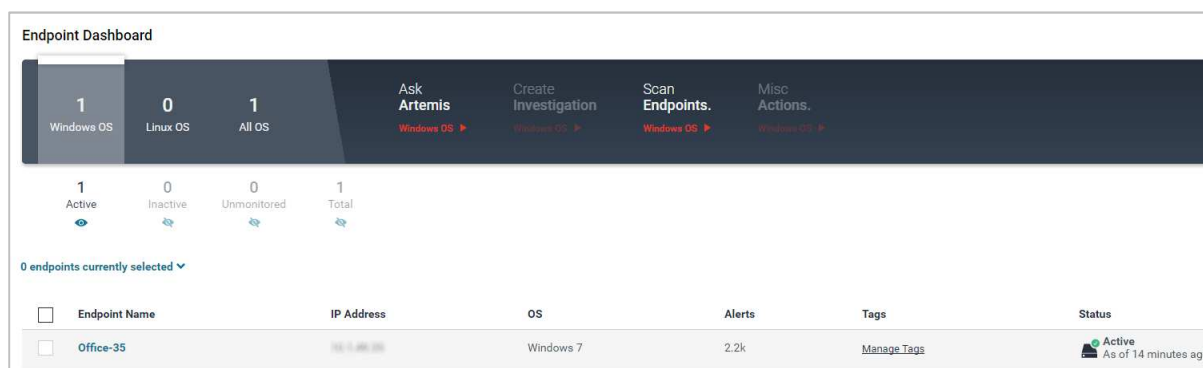
The Endgame endpoint security platform provides detection and prevention for Windows and Linux systems. It uses a server-based console to manage agents installed on endpoints, and employs machine learning and other techniques to detect and block malware, exploits and fileless attacks.

### Console interface

The *Dashboard* (home) tab of the console shows an overview of alerts and endpoint status:



The *Endpoints* tab shows a list of managed endpoints, along with IP address, operating system, alerts and status:



The *Scan Endpoints* command on the toolbar scans the network for new endpoints, using a specific IP address or address range. When new endpoints are detected, the Endgame agent can be installed on them, enabling them to be managed from the console.

The *Alerts Dashboard* displays a log of malware alerts on the system:

**Alert Dashboard**

2.2k Current | 1.9k Detections | 290 Preventions | 0 Assigned | 2.2k Total

Assign Alerts. | Resolve Alerts. | Dismiss Unactionable Alerts.

Type	Assignee	Severity	IP	Hostname	Status	Date
Malicious File Prevention	NEW Unassigned	Medium	10.1.49.35	Office-35	Active	May 10, 2017 6:56:17 AM UTC
Malicious File Detection	NEW Unassigned	High	10.1.49.35	Office-35	Active	May 10, 2017 6:56:04 AM UTC
Malicious File Detection	NEW Unassigned	High	10.1.49.35	Office-35	Active	May 10, 2017 6:56:03 AM UTC

The *Investigation Dashboard* allows the administrator to “hunt” for threats in the system.

The *Search* tab displays search queries:

**Search Results** | 9K+ TOTAL RESULTS

RESULTS | SAVED SEARCHES

SAVE SEARCH QUERY

1 - 10 of 9,731

Collection Name	Hostname	Collection Type	Status	Endpoint IP	Operating System	Date Created
whitelistResponse	Office-35	config	success	10.1.49.35	Windows 7	May 11, 2017 8:54:43 AM UTC
bundledTasksResponse	Office-35	config	success	10.1.49.35	Windows 7	May 11, 2017 8:54:43 AM UTC
bundledTasksResponse	Office-35	config	success	10.1.49.35	Windows 7	May 11, 2017 8:54:41 AM UTC
whitelistResponse	Office-35	config	success	10.1.49.35	Windows 7	May 11, 2017 8:54:41 AM UTC
whitelistResponse	Office-35	config	success	10.1.49.35	Windows 7	May 11, 2017 8:54:41 AM UTC

The *Administration* tab has multiple subtabs, namely *User Management* (see below), *Sensor Management*, *Alert Management*, *Whitelist Management*, and *Platform Management*.

**Administration**

USER MANAGEMENT | SENSOR MANAGEMENT | ALERT MANAGEMENT | WHITELIST MANAGEMENT | PLATFORM MANAGEMENT

CREATE NEW USER

Name	Username	Role	
David Larkin	david	Admin	<a href="#">Edit User Profile</a>
Phillip Holbach	phillip	Admin	<a href="#">Edit User Profile</a> <a href="#">Remove User</a>
Bill Adams	williams	Admin	<a href="#">Edit User Profile</a> <a href="#">Remove User</a>
Roger Adams	roger	Admin	<a href="#">Edit User Profile</a>

## Real-World Protection Test

The results are based on the test set of **398** live test cases (malicious URLs found in the field), thus exactly the same infection vectors are used as a typical user would experience in everyday life. The test-cases used cover a wide range of current malicious sites and provide insights into the protection given by the product.

For more information about this Real-World Protection Test, please read the details and previous test reports available on <http://www.av-comparatives.org>

## Test Results

Endgame	
<b>Total protection rate</b>	<b>99.5%</b>
<b>Number of false alarms</b>	<b>5</b>

The test results can be compared with results of other products for the month of May 2017 here: <http://chart.av-comparatives.org/chart1.php>

## 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 (June 2017)