CROWDSTRIKE

Anti-Virus Comparative

CrowdStrike Falcon Endpoint Protection for Mac

Language: English
November 2017

Last Revision: 20th November 2017

www.av-comparatives.org

Commissioned by CrowdStrike

CrowdStrike Falcon Endpoint Protection for Mac

This report has been commissioned by CrowdStrike.

Overview

Product version reviewed

CrowdStrike Falcon Sensor for Mac OS 3.5.5603.0
CrowdStrike Falcon cloud console as at November 2017

Operating systems supported

Mac OS 10.10, 10.11, 10.12
CrowdStrike Falcon also supports Windows and Linux operating systems.

About the product

CrowdStrike Falcon uses a cloud-based console to manage protection for client devices. A sensor is installed on all clients; this monitors processes run on the client and blocks any that are deemed to be malicious. Please note that all the prevention features need to be turned on for the product to automatically block threats.

Product information on vendor's website

https://www.crowdstrike.com/products/

Online support

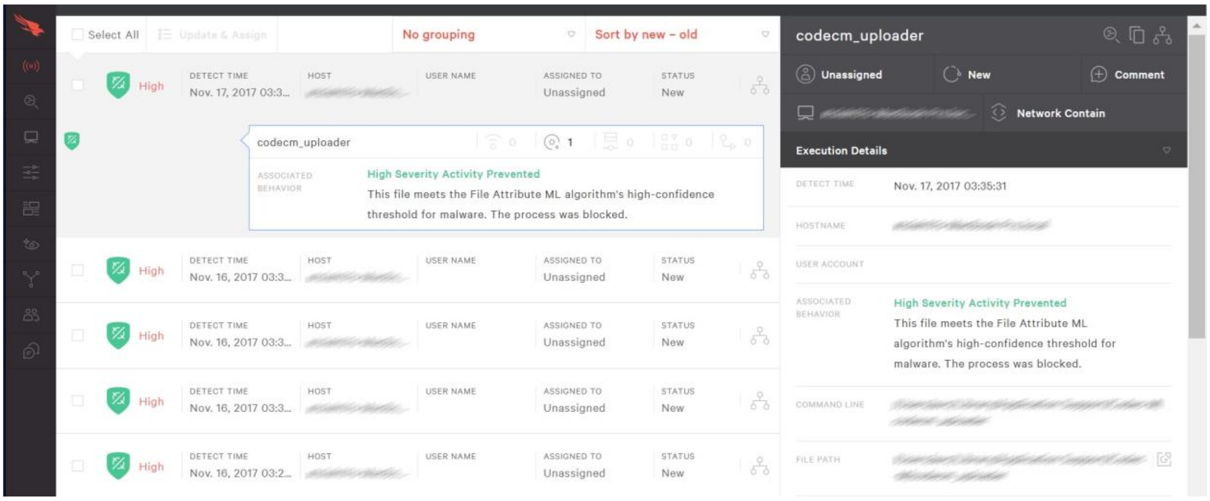
https://supportportal.crowdstrike.com

Summary

The management console is well designed and easy to navigate, allowing administrators to explore the functionality with ease. A wealth of detailed information on threats etc. is provided. Windows and Linux clients can be managed in just the same way as Mac clients, making the product very suitable for companies that use multiple operating systems.

Functionality Test

To verify the prevention capabilities of CrowdStrike Falcon Endpoint Protection for Mac, we conducted a malware detection test using samples belonging to the ten major Mac malware families currently found in the field, such as FakeCo, GetShell, HackBack, KeRanger, KitM, MacDown, NetWeird, Proton, SpyDok and Turla. 100% of the samples were prevented and reported in the CrowdStrike web console. Please note that the number of Mac malware families currently posing a threat is very small compared to their Windows counterparts.



	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Nov. 17, 2017 03:3...	[redacted]		Unassigned	New
High	Nov. 16, 2017 03:3...	[redacted]		Unassigned	New
High	Nov. 16, 2017 03:3...	[redacted]		Unassigned	New
High	Nov. 16, 2017 03:3...	[redacted]		Unassigned	New
High	Nov. 16, 2017 03:2...	[redacted]		Unassigned	New

codecm_uploader 0 1 0 0 0

ASSOCIATED BEHAVIOR: High Severity Activity Prevented
This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was blocked.

codecm_uploader

[redacted]

DETECT TIME: Nov. 17, 2017 03:35:31

HOSTNAME: [redacted]

USER ACCOUNT

ASSOCIATED BEHAVIOR: High Severity Activity Prevented
This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was blocked.

COMMAND LINE: [redacted]

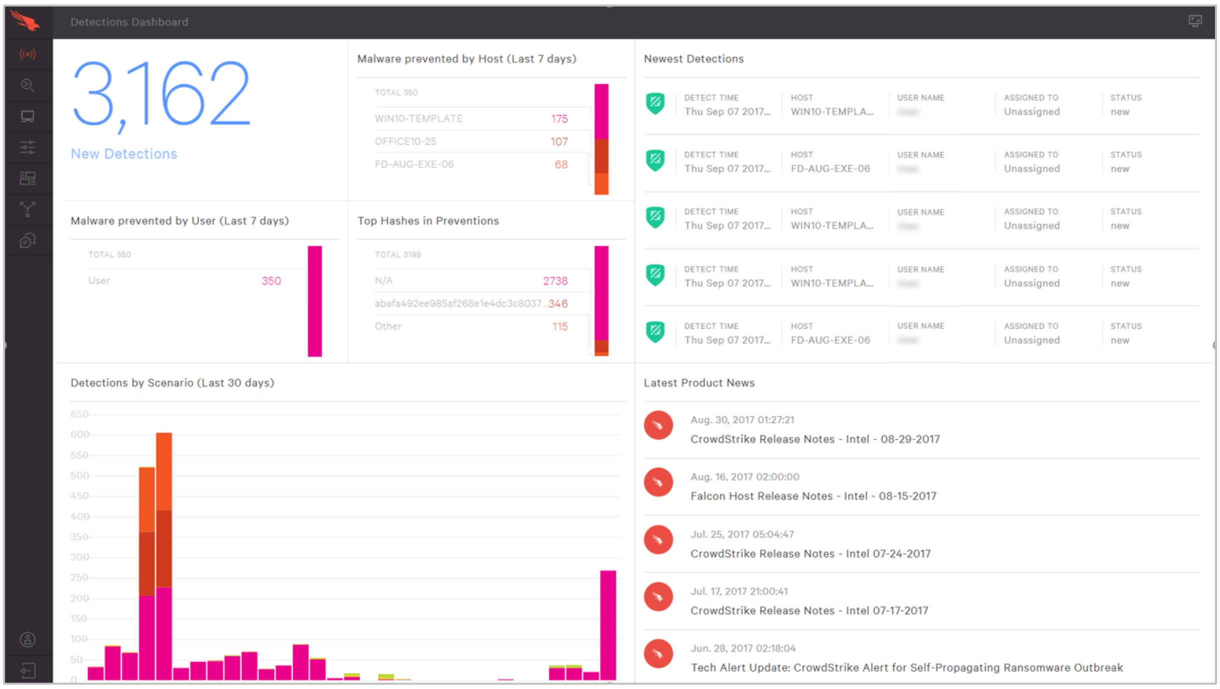
FILE PATH: [redacted]

Management Console

Installation and configuration

The console is cloud-based and so no installation is necessary.

Layout and functionality



Detections Dashboard

3,162

New Detections

Malware prevented by Host (Last 7 days)

TOTAL 350	
WIN10-TEMPLATE	175
OFFICE10-25	107
FD-AUG-EXE-06	68

Malware prevented by User (Last 7 days)

TOTAL 350	
User	350

Top Hashes in Preventions

TOTAL 3199	
N/A	2738
abafa492ee985af268e1e4dc3c8037...	346
Other	115

Newest Detections

DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Thu Sep 07 2017...	WIN10-TEMPLA...	[redacted]	Unassigned	new
Thu Sep 07 2017...	FD-AUG-EXE-06	[redacted]	Unassigned	new
Thu Sep 07 2017...	WIN10-TEMPLA...	[redacted]	Unassigned	new
Thu Sep 07 2017...	WIN10-TEMPLA...	[redacted]	Unassigned	new
Thu Sep 07 2017...	FD-AUG-EXE-06	[redacted]	Unassigned	new

Detections by Scenario (Last 30 days)

Latest Product News

Aug. 30, 2017 01:27:21
CrowdStrike Release Notes - Intel - 08-29-2017

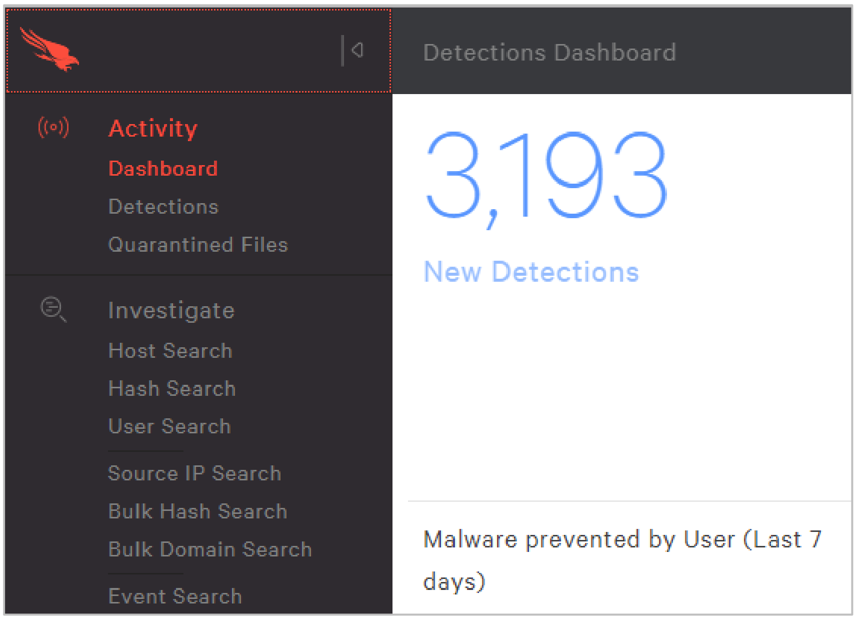
Aug. 16, 2017 02:00:00
Falcon Host Release Notes - Intel - 08-15-2017

Jul. 25, 2017 05:04:47
CrowdStrike Release Notes - Intel 07-24-2017

Jul. 17, 2017 21:00:41
CrowdStrike Release Notes - Intel 07-17-2017

Jun. 28, 2017 02:18:04
Tech Alert Update: CrowdStrike Alert for Self-Propagating Ransomware Outbreak

The console is navigated by means of a left-hand menu bar, with the main items *Activity, Investigate, Hosts, Configuration, Dashboards, Intelligence* and *Support*. This can be expanded by clicking the red Falcon graphic in the top left-hand corner, thus displaying the names and sub-pages for each of the items:



Detections Dashboard

3,193

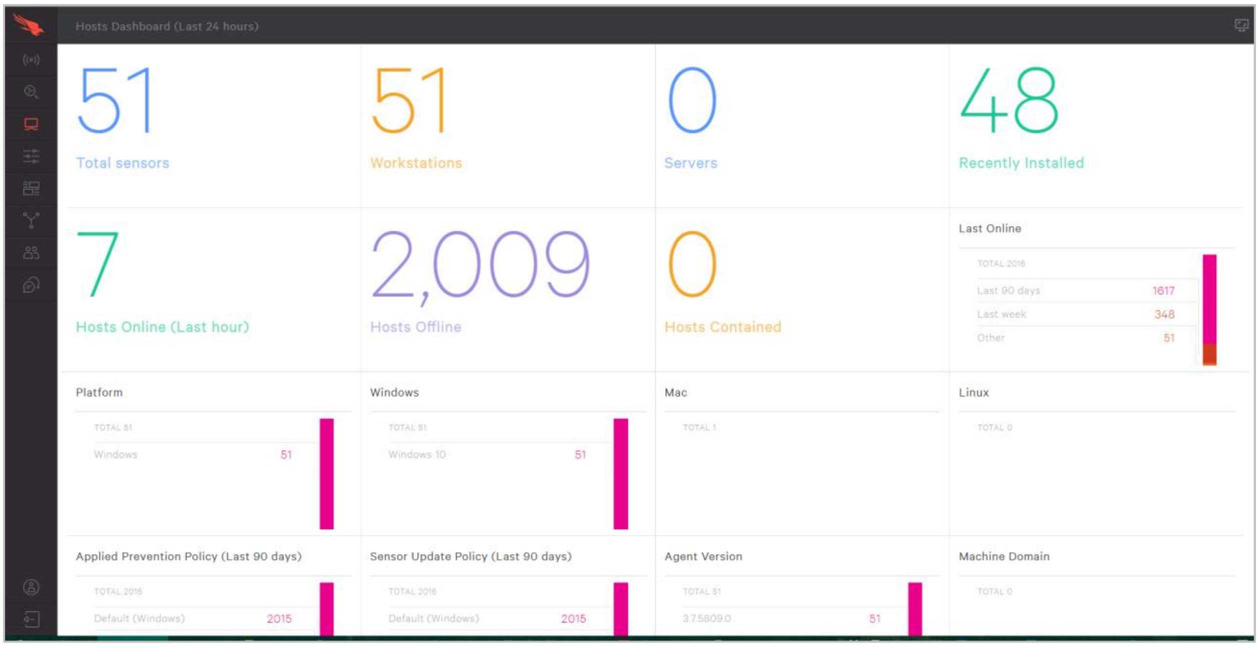
New Detections

Malware prevented by User (Last 7 days)

The *Activity Dashboard* (home) page of the console shows a variety of detection statistics, including *New Detections, Malware prevented by Host, Newest Detections* and *Detections by Scenario*.

The *Investigations* page allows the admin to search for any item collected by the Falcon agent, including hosts, hashes, users and source IP.

The *Hosts Dashboard* displays statistics relating to clients:



Hosts Dashboard (Last 24 hours)

51 Total sensors

51 Workstations

0 Servers

48 Recently Installed

7 Hosts Online (Last hour)

2,009 Hosts Offline

0 Hosts Contained

Last Online

TOTAL 2016

Last 90 days	1617
Last week	348
Other	51

Platform

TOTAL 51

Windows	51

Windows

TOTAL 51

Windows 10	51

Mac

TOTAL 1

Linux

TOTAL 0

Applied Prevention Policy (Last 90 days)

TOTAL 2016

Default (Windows)	2015

Sensor Update Policy (Last 90 days)

TOTAL 2016

Default (Windows)	2015

Agent Version

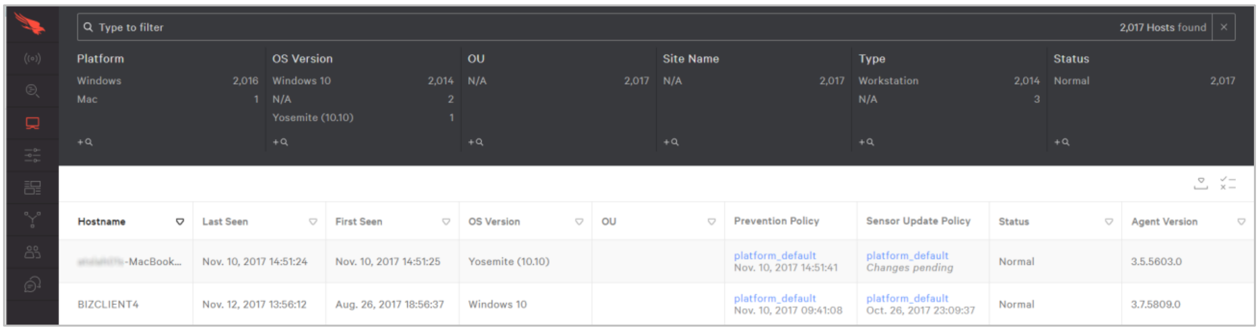
TOTAL 51

3.7.5809.0	51

Machine Domain

TOTAL 0

Hosts Management lists clients on the network:

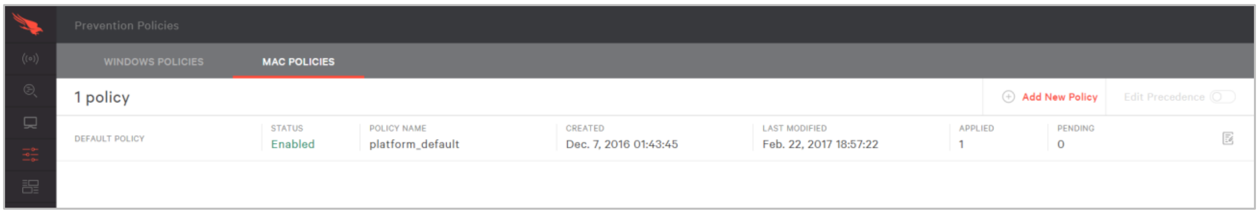


Type to filter — 2,017 Hosts found

Platform		OS Version		OU		Site Name		Type		Status	
Windows	2,016	Windows 10	2,014	N/A	2,017	N/A	2,017	Workstation	2,014	Normal	2,017
Mac	1	N/A	2					N/A	3		
		Yosemite (10.10)	1								

Hostname	Last Seen	First Seen	OS Version	OU	Prevention Policy	Sensor Update Policy	Status	Agent Version
[redacted]-MacBook...	Nov. 10, 2017 14:51:24	Nov. 10, 2017 14:51:25	Yosemite (10.10)		platform_default Nov. 10, 2017 14:51:41	platform_default *Changes pending*	Normal	3.5.5603.0
BIZCLIENT4	Nov. 12, 2017 13:56:12	Aug. 26, 2017 18:56:37	Windows 10		platform_default Nov. 10, 2017 09:41:08	platform_default Oct. 26, 2017 23:09:37	Normal	3.7.5809.0

Configuration, Prevention Policies lists configuration policies to be applied to clients:



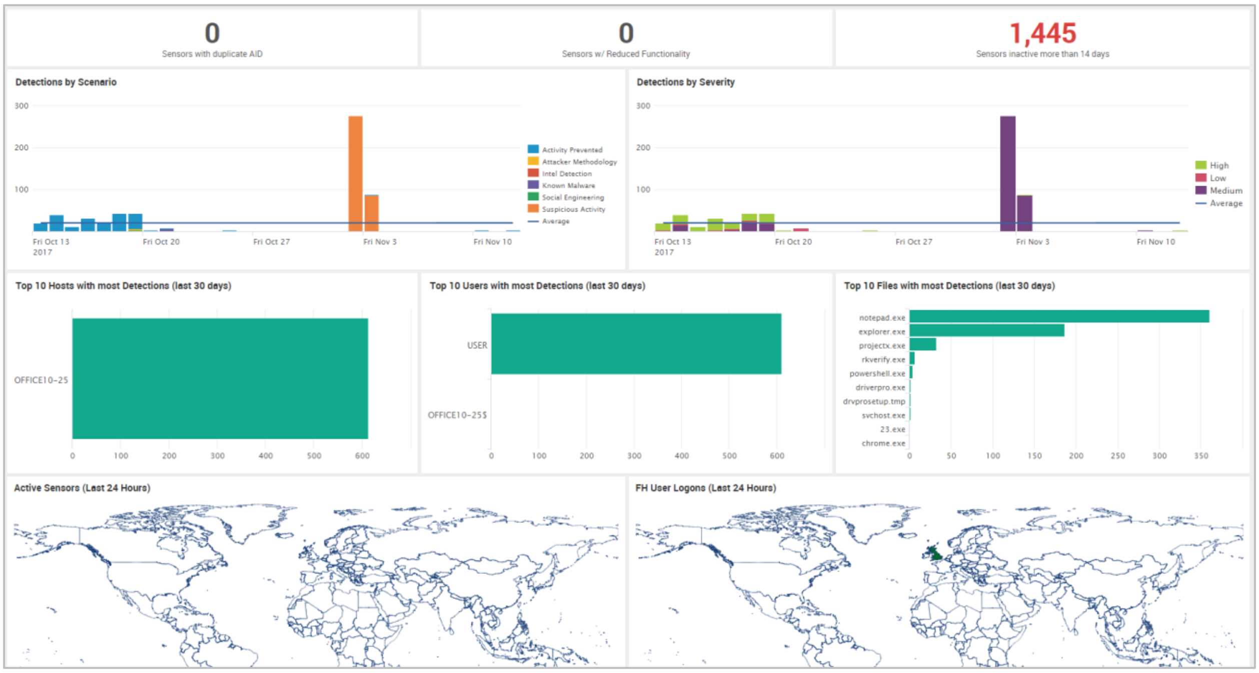
Prevention Policies

WINDOWS POLICIES | MAC POLICIES

1 policy — Add New Policy — Edit Precedence

	STATUS	POLICY NAME	CREATED	LAST MODIFIED	APPLIED	PENDING
DEFAULT POLICY	Enabled	platform_default	Dec. 7, 2016 01:43:45	Feb. 22, 2017 18:57:22	1	0

Under *Dashboards, Executive Summary* the admin can display a detailed breakdown of detections by scenario, severity, host or user:

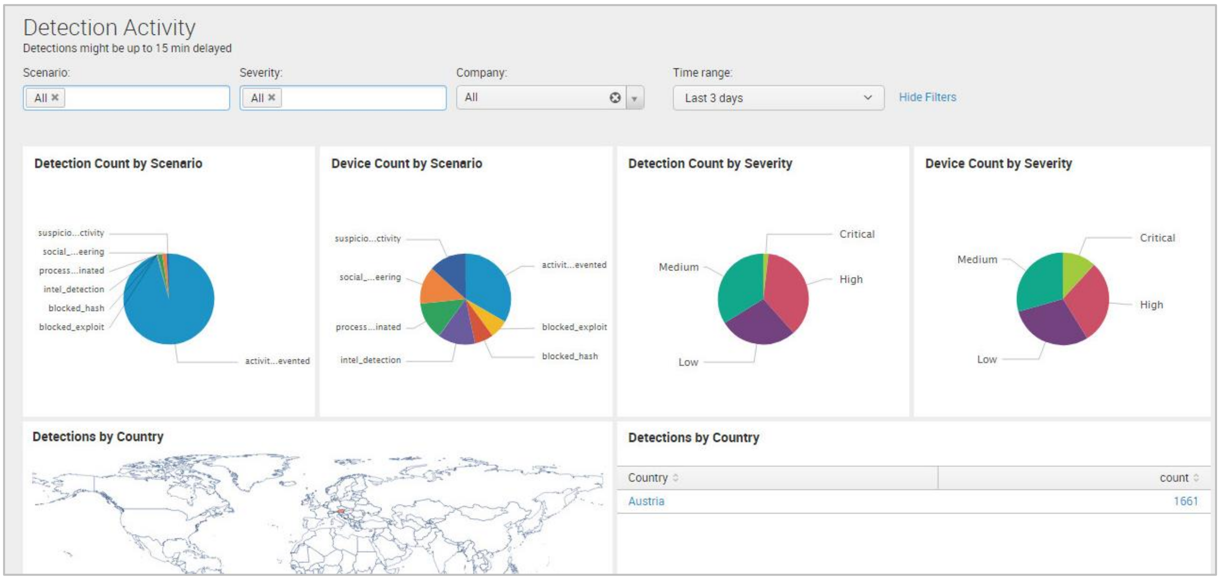


0
Sensors with duplicate AID

0
Sensors w/ Reduced Functionality

1,445
Sensors inactive more than 14 days

Other *Dashboards* pages include *Detection Resolutions* and *Detection Activity* (shown below):



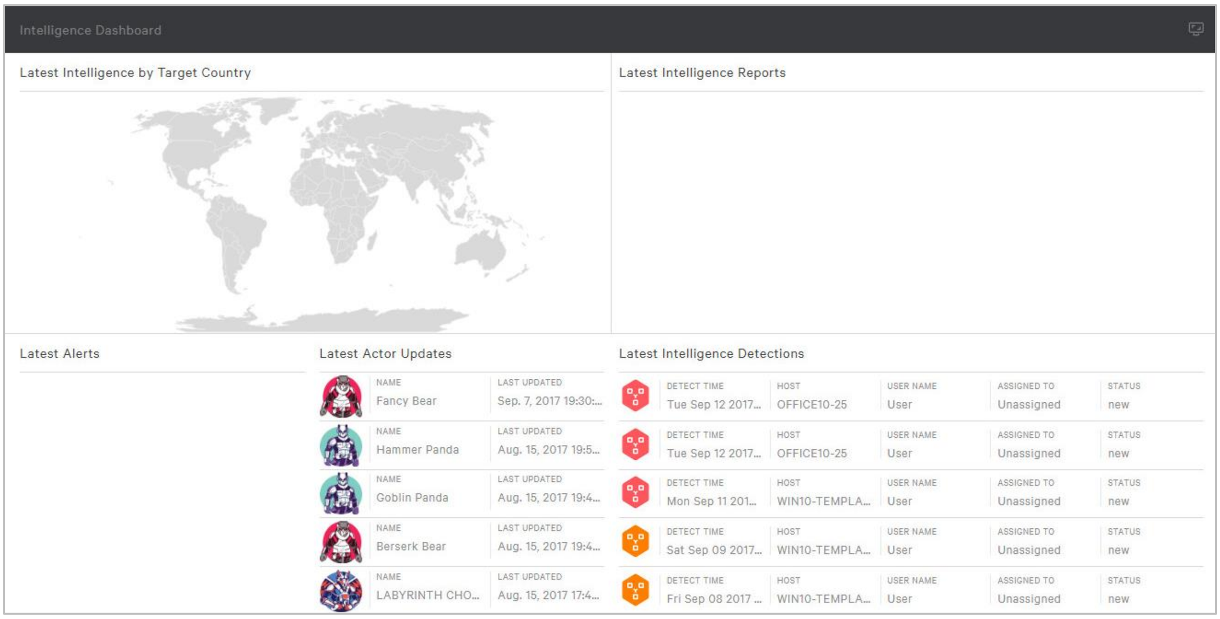
Detection Activity
Detections might be up to 15 min delayed

Scenario: All ×
Severity: All ×
Company: All
Time range: Last 3 days
Hide Filters

Detections by Country

Country	count
Austria	1661

The *Intelligence Dashboard* provides information on the latest threats:


Intelligence Dashboard
Latest Intelligence by Target Country
Latest Intelligence Reports
Latest Alerts

Latest Actor Updates

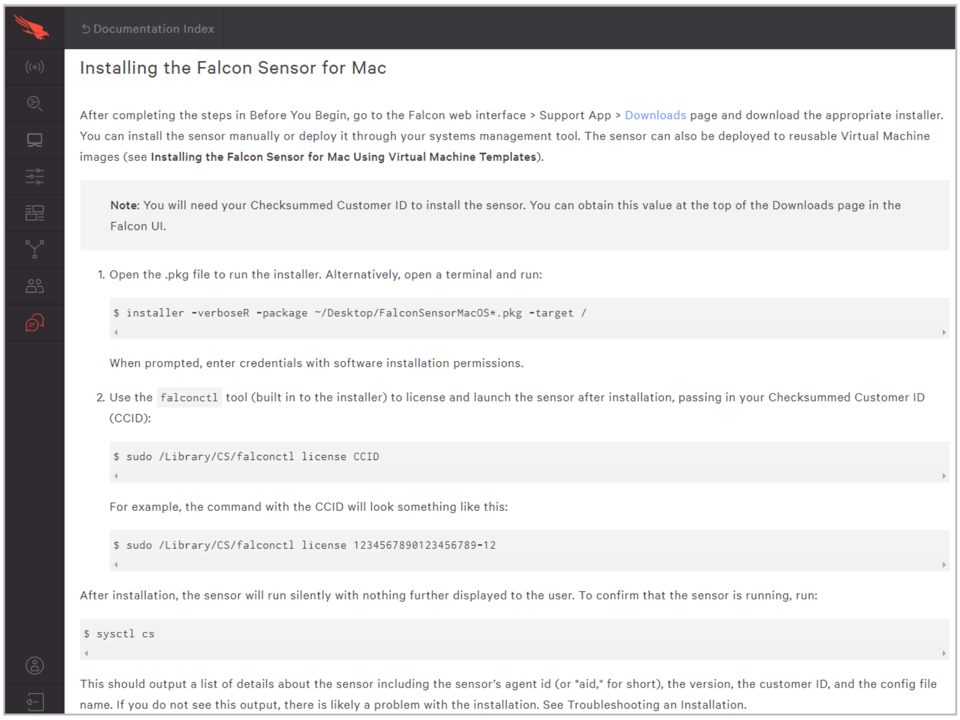
NAME	LAST UPDATED
Fancy Bear	Sep. 7, 2017 19:30:...
Hammer Panda	Aug. 15, 2017 19:5...
Goblin Panda	Aug. 15, 2017 19:4...
Berserk Bear	Aug. 15, 2017 19:4...
LABYRINTH CHO...	Aug. 15, 2017 17:4...

Latest Intelligence Detections

DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Tue Sep 12 2017...	OFFICE10-25	User	Unassigned	new
Tue Sep 12 2017...	OFFICE10-25	User	Unassigned	new
Mon Sep 11 201...	WIN10-TEMPLA...	User	Unassigned	new
Sat Sep 09 2017...	WIN10-TEMPLA...	User	Unassigned	new
Fri Sep 08 2017 ...	WIN10-TEMPLA...	User	Unassigned	new

Deployment of endpoint protection software

Installing the sensor on a Mac client involves downloading the installer file from the console, and running it using the terminal. Full instructions are provided for this in the console's documentation section:



Installing the Falcon Sensor for Mac

After completing the steps in Before You Begin, go to the Falcon web interface > Support App > Downloads page and download the appropriate installer. You can install the sensor manually or deploy it through your systems management tool. The sensor can also be deployed to reusable Virtual Machine images (see **Installing the Falcon Sensor for Mac Using Virtual Machine Templates**).

Note: You will need your Checksummed Customer ID to install the sensor. You can obtain this value at the top of the Downloads page in the Falcon UI.

1. Open the .pkg file to run the installer. Alternatively, open a terminal and run:

```
$ installer -verboseR -package ~/Desktop/FalconSensorMacOS*.pkg -target /
```

When prompted, enter credentials with software installation permissions.

2. Use the `falconctl` tool (built in to the installer) to license and launch the sensor after installation, passing in your Checksummed Customer ID (CCID):

```
$ sudo /Library/CS/falconctl license CCID
```

For example, the command with the CCID will look something like this:

```
$ sudo /Library/CS/falconctl license 1234567890123456789-12
```

After installation, the sensor will run silently with nothing further displayed to the user. To confirm that the sensor is running, run:

```
$ sysctl cs
```

This should output a list of details about the sensor including the sensor's agent id (or "aid," for short), the version, the customer ID, and the config file name. If you do not see this output, there is likely a problem with the installation. See Troubleshooting an Installation.

Mac client endpoint protection software

The Mac client sensor has no user interface and is effectively invisible to the user.

Copyright and Disclaimer

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 (November 2017)