SentinelOne™

DATASHEET

Extending Windows Defender ATP to MacOS and Linux with SentinelOne

Executive Summary

SentinelOne and Microsoft have partnered to integrate SentinelOne Endpoint Protection with Microsoft Windows Defender Advanced Threat Protection (WD ATP) to extend WD ATP coverage to Mac and Linux endpoints. The integration allows SentinelOne and Microsoft customers to autonomously prevent, detect, and respond to the most advanced cyber-attacks not only on Windows endpoints - but also on Mac and Linux endpoints - directly from the Microsoft WD ATP Management Console.

Benefits

The integration enables detection, visibility, investigation, and response to advanced cyber-attacks and data breaches on macOS and Linux-based endpoints right from within the Windows Defender Security Center management console. View comprehensive threat intelligence information which includes the following:

- **File and Process Properties:** name, path, size on disk, last write time, hash, file owner: username, pid
- **User and device properties:** name, operating system, domain, logged on users information, logon type (remote, interactive)
- **Network Properties:** NICs and IP addresses, local IP address, http, https, tcp and udp headers and traffic, owner: pid and username
- **Detection Properties:** prevention alerts, post breach detection, cloud detection, machine timeline, process trees, network events
- **Prevention and Mitigation**: file block, file quarantine machine isolation, trigger AV scan.

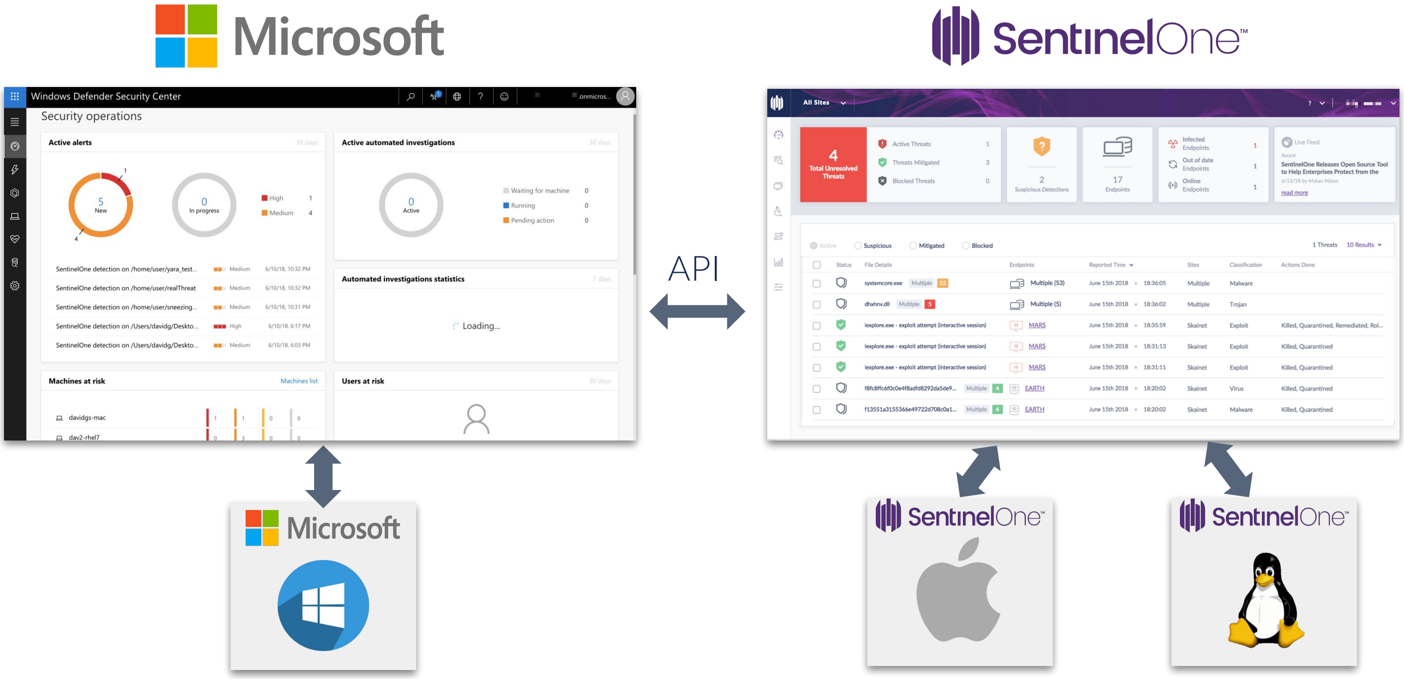
Microsoft + SentinelOne™

Broad Protection Against Diverse Modes of Attack

MALWARE		EXPLOITS		LIVE/INSIDER	
Executables	**Fileless**	**Documents**	**Browser**	**Scripts**	**Credentials**
Trojans, malware, worms, backdoors, payload-based	Memory-only malware, no-disk-based indicators	Exploits rooted in Office documents, Adobe files, macros, spear phishing emails	Drive-by downloads, Flash, Java, Javascript, VBS, IFrame/HTML5, plug-ins	Powershell, WMI, PowerSploit, VBS	Mimikatz, credentials scraping, tokens

How Does it Work?

1. Once the integration is enabled, the SentinelOne console is connected to Windows Defender Security Center management console via API.
2. Information that is gathered by the SentinelOne console is then sent to the Windows Defender Security Center management console and displayed, like any Windows device.
3. You may perform threat hunting, correlate IOCs and take actions directly from the Windows Defender Security Center management console.



Windows Defender Security Center [redacted].onmicros...

Security operations

Active alerts 30 days

5 New · 0 In progress · High 1 · Medium 4

SentinelOne detection on /home/user/yara_test...	Medium	6/10/18, 10:32 PM
SentinelOne detection on /home/user/realThreat	Medium	6/10/18, 10:32 PM
SentinelOne detection on /home/user/sneezing...	Medium	6/10/18, 10:31 PM
SentinelOne detection on /Users/davidg/Deskto...	High	6/10/18, 6:17 PM
SentinelOne detection on /Users/davidg/Deskto...	Medium	6/10/18, 6:03 PM

Active automated investigations 30 days

0 Active · Waiting for machine 0 · Running 0 · Pending action 0

Automated investigations statistics 7 days

Loading...

Machines at risk Machines list

davidgs-mac	1	1	0	0
dav2-rhel7	0	3	0	0

Users at risk 30 days

All Sites [redacted]

4 Total Unresolved Threats · Active Threats 1 · Threats Mitigated 3 · Blocked Threats 0 · 2 Suspicious Detections · 17 Endpoints · Infected Endpoints 1 · Out of date Endpoints 1 · Online Endpoints 1

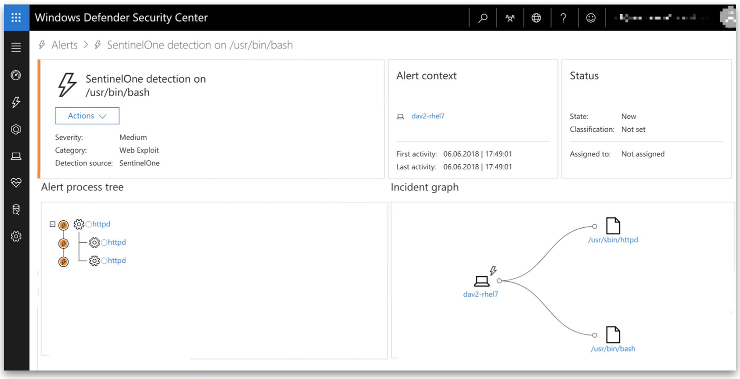
Live Feed · Recent · SentinelOne Releases Open Source Tool to Help Enterprises Protect from the · 6/13/18 by Matan Mates · read more

○ Active ○ Suspicious ○ Mitigated ○ Blocked — 1 Threats · 10 Results

File Details	Endpoints	Reported Time	Sites	Classification	Actions Done
systemcore.exe Multiple 53	Multiple (53)	June 15th 2018 • 18:36:05	Multiple	Malware	
dhxhnv.dll Multiple 5	Multiple (5)	June 15th 2018 • 18:36:02	Multiple	Trojan	
iexplore.exe - exploit attempt (interactive session)	MARS	June 15th 2018 • 18:35:59	Skainet	Exploit	Killed, Quarantined, Remediated, Rol...
iexplore.exe - exploit attempt (interactive session)	MARS	June 15th 2018 • 18:31:13	Skainet	Exploit	Killed, Quarantined
iexplore.exe - exploit attempt (interactive session)	MARS	June 15th 2018 • 18:31:11	Skainet	Exploit	Killed, Quarantined
f8fc8ffc6f0c0e4f8adfd8292da5de9... Multiple 4	EARTH	June 15th 2018 • 18:20:02	Skainet	Virus	Killed, Quarantined
f13551a3155366e49722d708c0a1... Multiple 4	EARTH	June 15th 2018 • 18:20:02	Skainet	Malware	Killed, Quarantined

Use Cases

1 Prevention before, during, and after threats through SentinelOne's multilayered AI-powered approach.


Windows Defender Security Center [redacted]

Alerts > SentinelOne detection on /usr/bin/bash

SentinelOne detection on /usr/bin/bash

Actions

Severity: Medium
Category: Web Exploit
Detection source: SentinelOne

Alert context

dav2-rhel7

First activity: 06.06.2018 | 17:49:01
Last activity: 06.06.2018 | 17:49:01

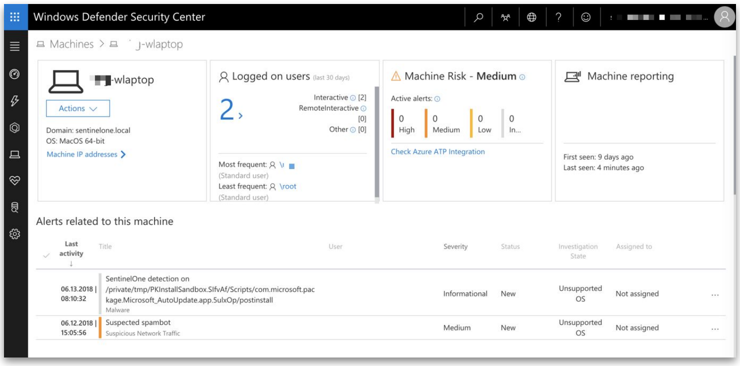
Status

State: New
Classification: Not set
Assigned to: Not assigned

Alert process tree

Incident graph

2 Gain rich machine data within the Windows Defender Security Center management console. Understand each machine risk score, logged on users (including their type and commonalities), see active alerts, machine reporting, and timeline of events.


Windows Defender Security Center [redacted]

Machines > [redacted]-wlaptop

[redacted]-wlaptop

Actions

Domain: sentinelone.local
OS: MacOS 64-bit
Machine IP addresses

Logged on users (last 30 days)

2 · Interactive [2] · RemoteInteractive [0] · Other [0]

Most frequent: [redacted] (Standard user)
Least frequent: \root (Standard user)

Machine Risk - **Medium**

Active alerts: 0 High · 0 Medium · 0 Low · 0 In...

Check Azure ATP Integration

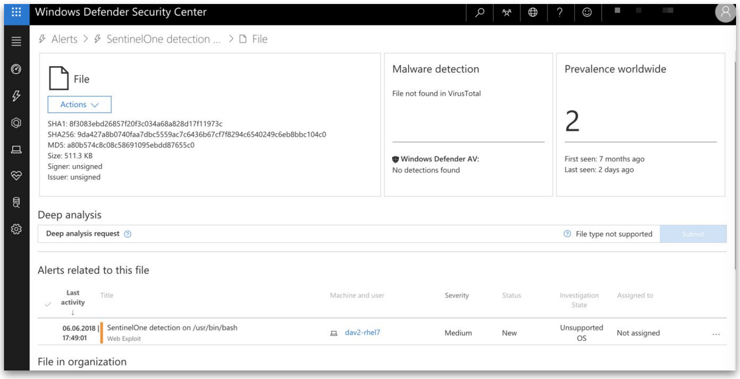
Machine reporting

First seen: 9 days ago
Last seen: 4 minutes ago

Alerts related to this machine

Last activity	Title	User	Severity	Status	Investigation State	Assigned to
06.13.2018 | 08:10:32	SentinelOne detection on /private/tmp/PKInstallSandbox.SlfvAf/Scripts/com.microsoft.package.Microsoft_AutoUpdate.app.5ulxOp/postinstall Malware		Informational	New	Unsupported OS	Not assigned
06.12.2018 | 15:05:56	Suspected spambot Suspicious Network Traffic		Medium	New	Unsupported OS	Not assigned

3 View event and threat storylines. Analyze each event, including the process tree, and other associated IOCs. See how each activity is observed worldwide or in your organization. See related alerts and request in-depth analysis report.


Windows Defender Security Center
Alerts > SentinelOne detection ... > File
Actions
Submit

File

SHA1: 8f3083ebd26857f20f3c034a68a828d17f11973c
SHA256: 9da427a8b0740faa7dbc5559ac7c6436b67cf7f8294c6540249c6eb8bbc104c0
MD5: a80b574c8c08c58691095ebdd87655c0
Size: 511.3 KB
Signer: unsigned
Issuer: unsigned

Malware detection

File not found in VirusTotal

Windows Defender AV:
No detections found

Prevalence worldwide

2

First seen: 7 months ago
Last seen: 2 days ago

Deep analysis

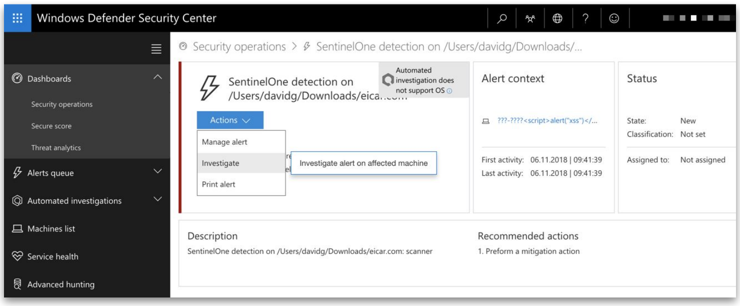
Deep analysis request — File type not supported

Alerts related to this file

Last activity	Title	Machine and user	Severity	Status	Investigation State	Assigned to
06.06.2018 | 17:49:01	SentinelOne detection on /usr/bin/bash Web Exploit	dav2-rhel7	Medium	New	Unsupported OS	Not assigned

File in organization

4 Take actions on your MacOS and Linux machines directly from the Windows Defender Security Center management console including run malware scan, isolate device, and manage tags.



SentinelOne detection on /Users/davidg/Downloads/eica...

Automated investigation does not support OS

Alert context

???-????<script>alert("xss")</...

First activity: 06.11.2018 | 09:41:39
Last activity: 06.11.2018 | 09:41:39

Status

State: New
Classification: Not set
Assigned to: Not assigned

Description

SentinelOne detection on /Users/davidg/Downloads/eicar.com: scanner

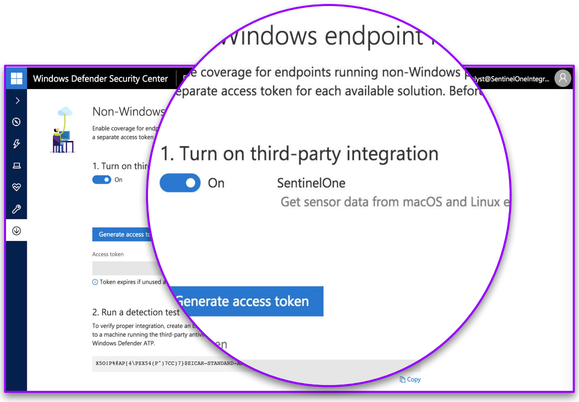
Recommended actions

1. Preform a mitigation action

How to Enable the Integration

1 Go to "Non-Windows" in your Windows Defender Security Center management console and generate a token for SentinelOne

2 In the SentinelOne console, enable the Microsoft Integration. Go to Settings, Integrations, Microsoft WDATP and insert the token. After this configuration process, use the Windows Defender Security Center management console to holistically manage Windows, Mac, and Linux endpoints.


Windows Defender Security Center
...lyst@SentinelOneIntegr...
Copy

Non-Windows endpoint

Enable coverage for endpoints running non-Windows ... a separate access token for each available solution. Befor...

1. Turn on third-party integration

On — SentinelOne
Get sensor data from macOS and Linux e...

Generate access token

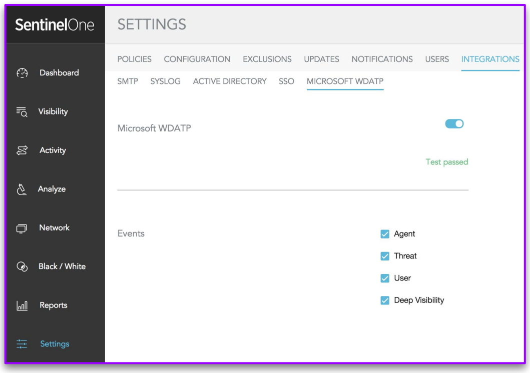
Access token

Token expires if unused a...

2. Run a detection test

To verify proper integration, create an E... to a machine running the third-party antivi... Windows Defender ATP.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-A...
```



SETTINGS

Microsoft WDATP — On

Test passed

Events
- ☑ Agent
- ☑ Threat
- ☑ User
- ☑ Deep Visibility

Supported Operating Systems

MacOS

- MacOS 10.12x MacOS 10.13 (High Sierra)
- Mac OS X 10.9.x, 10.10.x, 10.11x

Linux

- Red Hat Enterprise Linux 6.5, 7.0, 7.2
- Ubuntu 12.04, 14.04, 16.04, 16.10
- SUSE Linux Enterprise Server 12SP1
- openSUSE 42.2
- Oracle Linux 6.5 - 6.9, 7.0+
- Amazon Linux (AMI) 2016.09+, 2017.03+
- Debian 8+
- Fedora 23+

SentinelOne™

To sign up, visit http://bit.ly/S1-ATP

+ 1 855 868 3733
sales@sentinelone.com