

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



ins

emails

(I) SentinelOne

+ 1 855 868 3733 sales@sentinelone.com

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.



Use Cases

1

2

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

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.



묘 Machines > 묘	' J-wlaptop					
Actions V Domain: sentinelone.loc OS: MacOS 64-bit Machine IP addresses >	aptop R Logged on u 2 > Most frequent: R is g Claned user	SerS (last 30 days) ▲ A Active Remoteinteractive © [2] Other ⊙ [0] Check	Aachine Risk - Medium alerts: 0 h 0 0 0 0 Medium 0 0 Azure ATP Integration	n	chine reporting days ago minutes ago	
Alerts related to th	is machine	User	Severity Stat	us Investigation State	Assigned to	
06.13.2018 /priva 08:10:32 kage. Malwa	elOne detection on te/tmp/PKInstallSandbox.SIfvA(/Scripts/com.micros Microsoft_AutoUpdate.app.SulxOp/postinstall re	oft.pac	Informational Nev	v Unsupported OS	Not assigned	
06.12.2018 Suspe 15:05:56 Suspic	cted spambot ous Network Traffic		Medium Nev	v Unsupported OS	Not assigned	

3

1

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.

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

Windows Defender Security Center		م	* 0	? 🙂		
${\mathscr P}$ Alerts > ${\mathscr P}$ SentinelOne detection > \Box File						
File Actions Switz B038Hbd286570053/03446B422617111977c Switz B038Hbd286570053/03446B422617111977c	Mał File n	Malware detection File not found in VinaTotal		Prevalence worldwide 2 First seen: 7 months app Latt seen: 2 dipt seps		
MOS: 34065374;ck08c58991095ebdd87655c0 Star: 511.3 KB Signer: unisigned Issuer: unisigned	• Wi No de					
Deep analysis						
Deep analysis request 🕥				File type n	ot supported	
Alerts related to this file	Machine and user	Severity	Status	Investigation State	Assigned to	
06.06.2018 SentinelOne detection on /usr/bin/bash 17:49:01 Web Exploit	□ dav2-rhel7	Medium	New	Unsupported OS	Not assigned	
File in organization						

iii Windows Defender	Security Center	♪ ★ ⊕ ? 0	
	Security operations > Security operati	ers/davidg/Downloads/	
Dashboards Security operations Secure score	SentinelOne detection on (/users/davidg/Downloads/eica	Alert context	Status State: New Classification: Not set
Prreat analytics Alerts queue Automated investigations	Investigate Investigate alert on affected machine Print alert	First activity: 06.11.2018 09.41:39 Last activity: 06.11.2018 09.41:39	Assigned to: Not assigned
교 Machines list 양 Service health 륁 Advanced hunting	Description SentinelOne detection on /Users/davidg/Downloads/eicar.com: scanner	Recommended actions 1. Preform a mitigation action	

How to Enable the Integration

manage tags.

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



Supported
 Operating
 Systems

MacOS

- MacOS 10.12x
- MacOS 10.13 (High Sierra)

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.

Se	ntinelOne	SETTINGS		
	Dashboard	POLICIES CONFIGURATION EXCLUSIONS UPDATES NOTIFICATIONS USERS INTEGRATIONS SMTP SYSLOG ACTIVE DIRECTORY SSO MICROSOFT WDATP		
	Visibility	Microsoft WDATP 💿		
	Activity	Test passed		
	Analyze			
	Network	Events Zagent		
	Black / White	🗾 Usar		
Pul	Reports	💆 Deep Visibility		
÷	Settings			

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+

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

2

+1 855 868 3733 sales@sentinelone.com