

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.



Broad Protection Against Diverse Modes of Attack

MALWARE

EXPLOITS

LIVE/INSIDER



Executables

Trojans, malware, worms, backdoors, payload-based



Fileless

Memory-only malware, no-disk-based indicators



Documents

Exploits rooted in Office documents, Adobe files, macros, spear phishing emails



Browser

Drive-by downloads, Flash, Java, Javascript, VBS, IFrame/HTML5, plug-ins



Scripts

Powershell, WMI, PowerSploit, VBS

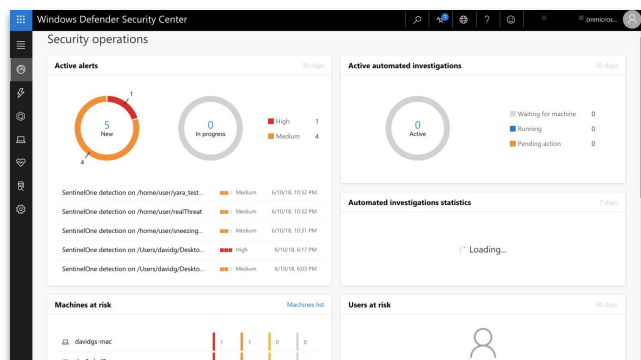


Credentials

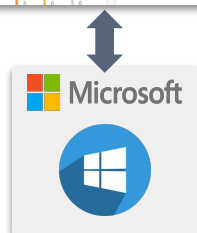
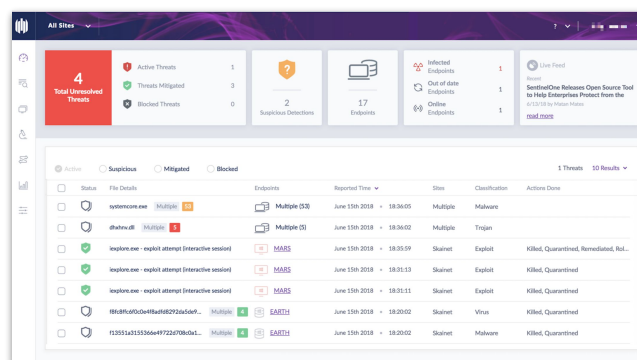
Mimikatz, credentials scraping, tokens

► 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 IOC's and take actions directly from the Windows Defender Security Center management console.

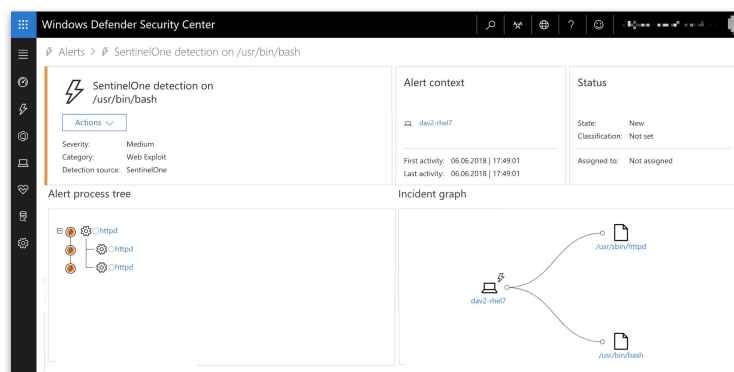


API

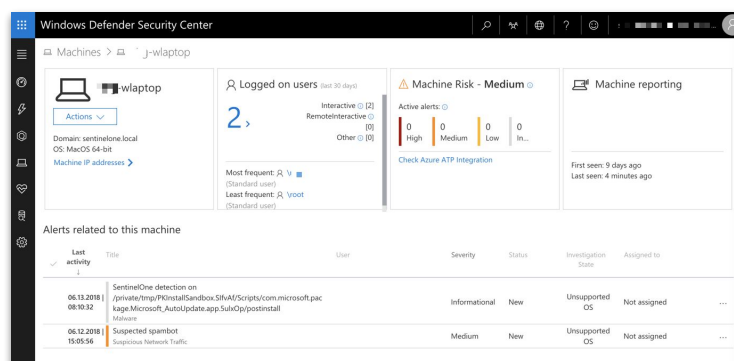


► Use Cases

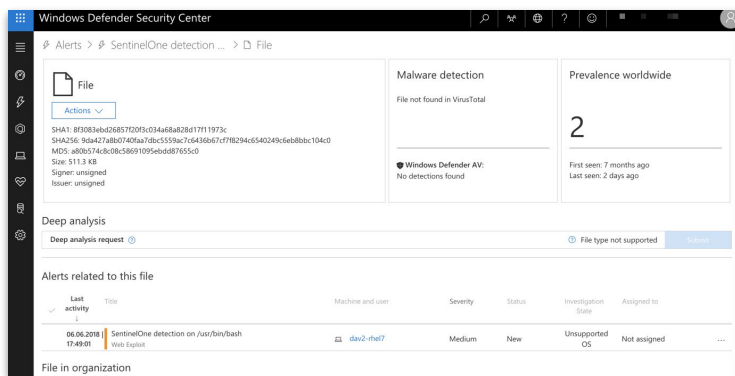
1. Prevention before, during, and after threats through SentinelOne's multilayered AI-powered approach.



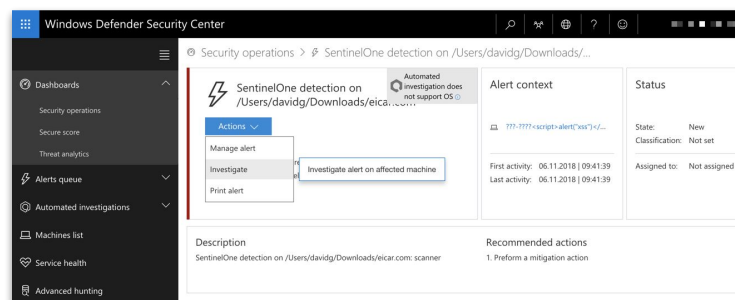
2. Gain rich machine data within the Windows Defender Security Center management console. Understand each machine risk score, logged on users (including their type and commonalities), see active alerts, machine reporting, and timeline of events.



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.

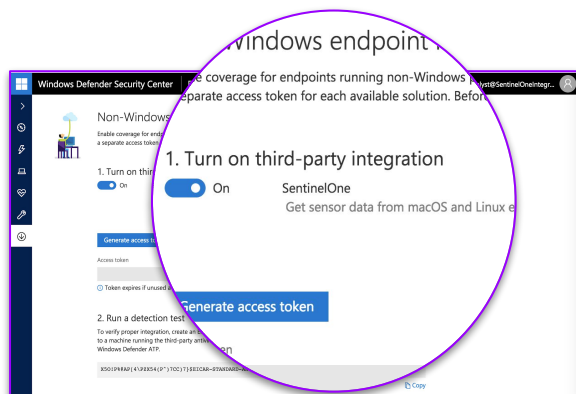


4 Take actions on your MacOS and Linux machines directly from the Windows Defender Security Center management console including run malware scan, isolate device, and manage tags.

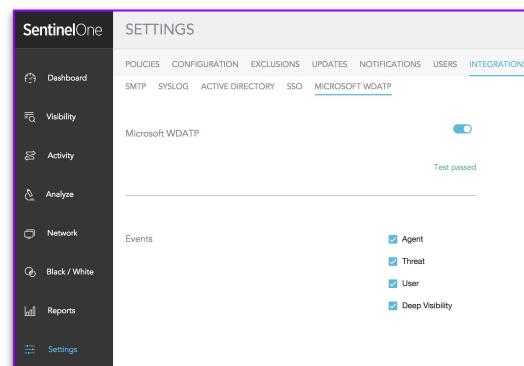


► How to Enable the Integration

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.



► Supported Operating Systems

MacOS

- MacOS 10.12x
- MacOS 10.13 (High Sierra)

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+