

Securing Linux

The need to Secure Linux devices

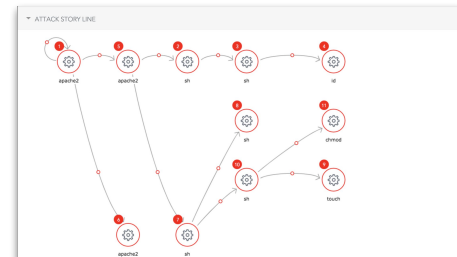
There are many different ways that attackers can go after Linux devices - breaches via web servers or SQL servers, command injection, SSH compromise, and more. Also, cryptominers and ransomware is an emerging threat to the open source operating system now that attacks are evolving.

SentinelOne Linux offering

The Linux agent by SentinelOne has the same core security approach as other SentinelOne agents, including Static AI, Behavioral AI, and Visibility. It was designed for low CPU and memory consumptive and to provide the needed protection to answer security threats as seen today.

- Pre-execution and post-infection: Increased visibility into the endpoints
- Focused on stability and decreased attack surface
- Seamlessly managed by the SentinelOne console

<input type="checkbox"/>	MACHINE NAME	LAST LOGGED I...	GROUP	POLICY	DOMAIN	CONSOLE ...	AGENT VE...
<input type="checkbox"/>	allina_SLES12_1	N/A	4msft-int	IOC	localdom...	62.219.14...	2.5.0.1336
<input type="checkbox"/>	RanTestCentos	N/A	4msft-int	IOC	localdom...	62.219.14...	2.5.0.1315
<input type="checkbox"/>	ubuntu1404vic	N/A	Chris Bat...	Chris Bat...	localdom...	73.11.61.49	2.5.0.1336
<input type="checkbox"/>	dav-ubuntu16	N/A	4msft-int	IOC	auto.sent...	62.219.14...	2.5.0.1336
<input type="checkbox"/>	dav2-rhel7	N/A	4msft-int	IOC	sentinelo...	31.154.17...	2.5.0.1336



Wide support

- Amazon Linux AMI
- Red Hat Enterprise Linux RHEL v5.5-5.11, 6.5+, 7.0+
- Ubuntu 12.04, 14.04, 16.04, 16.10
- CentOS 6.5+, 7.0+
- Oracle Linux OL (Oracle Enterprise Linux or OEL) v6.5-6.9 & v7.0+
- OpenSUSE, 42.2
- SUSE Linux Enterprise Server - 12 SP1+

Selected by Microsoft to protect the ATP customers

SentinelOne and Microsoft have partnered to integrate SentinelOne Endpoint Protection with Microsoft Windows Defender Advanced Threat Protection. 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.

