SentinelOne Announces Amazon Linux 2023 Service Ready Designation

March 20, 2023
by Rick Bosworth and Laura Roantree

SentinelOne is pleased to announce support for Amazon Linux 2023 (AL2023) with the latest agent 23.1, and achievement of the Amazon Linux 2023 Service Ready Designation. Amazon Linux 2023 Ready solutions are vetted by AWS Partner Solution Architects to ensure a consistent customer experience.

Singularity Cloud Workload Security for Servers delivers autonomous runtime protection, detection, and response for workloads operating in Amazon EC2, Amazon ECS, and hybrid cloud compute instances. With support for 13 major Linux distributions and operation entirely in user space, SentinelOne delivers frictionless runtime workload security, so you can innovate faster and focus on your core competency. Customer benefits include resource efficiency, high performance risk management, and high availability.

Amazon Linux 2023

AL2023 is optimized for Amazon EC2 and is well integrated with the latest AWS features. Based on Fedora, AL2023 provides frequent, flexible quarterly updates, and provides customers the control over how and when to absorb these updates

New Amazon Linux major versions are generally available every 2 years, and each major version, including AL2023, comes with 5 years of long-term support. Moreover, AL2023 sets a high security and hardening standard, with features such as SELinux, kernel live-patching (x86-64 and ARM), OpenSSL 3.0, and revised cryptographic policies. Major apps within AL2023 come with pre-configured SELinux policies to help meet compliance needs. Finally, AL2023 allows users to set security policies at boot time.

High-Performance Runtime Security

SentinelOne is cloud-native, built and run on AWS infrastructure. Working with AWS allows us to focus on our core competency, which is runtime security against advanced threats such as ransomware and crypto mining malware.

Our autonomous runtime Linux agent regularly shines in 3rd party benchmark testing, such as that by MITRE Engenuity ATT&CK®, which for the last 2 years has included Linux as part of its testing. The results may be found on the MITRE Engenuity™ webpage (see, Carbanak+FIN7 (2021), Wizard Spider + Sandworm (2022)). Discussion of the results and their significance can be found at SentinelOne here. In short, SentinelOne customers can expect the most analytic enrichment of detections, which helps accelerate triage and forensic investigation in the event of an incident.

Our latest Linux agent releases offer compelling enhancements to our already market-leading, AI-driven detection technology including support for Amazon Linux 2023. While earlier revisions did well in detecting execution of crypto mining malware, the latest releases detect crypto mining malware during setup/installation phase, before mining actually begins. Detecting such malware sooner not only simplifies incident response but also boosts customer confidence.

As customers like to remind us, and it's a mission on which we remain singularly focused, "Innovation is king, and we have to move fast." SentinelOne customers running Linux workloads have the confidence to go fast and secure.

Operational Efficiency

Back in July 2022, SentinelOne announced our AWS Graviton Ready Designation. The AWS Graviton3 processor itself delivers compelling improvement in energy, computational and memory efficiency.

Being continuous innovators ourselves, the R&D team at SentinelOne too had been working diligently to improve the resource efficiency of our fully capable Linux agent. The 22.x version shows dramatic improvement in both memory and CPU usage when compared to its 21.x predecessor. Both memory and CPU usage are nearly halved, without impairing its primary mission – workload protection – one iota.

The resource efficiency story is even more compelling for Kubernetes customers. Our specialized Singularity Cloud Workload Security for Kubernetes agent protects the host OS of the worker node, all its pods, and all their containers: no sidecars or pod instrumentation, just powerful visibility into and security for your Kubernetes workloads. This efficiency is very compelling for digital natives running workloads at scale.

Parting Thoughts

We are thrilled to protect our customers' workloads on AWS by pushing the boundaries of machine learning, behavioral AI-driven detection, and autonomous response against runtime threats. Our sincere thanks to AWS for the opportunity to be part of the Amazon Linux 2023 launch, and for the Amazon Linux 2023 Service Ready Designation.

Our Linux and Kubernetes agents operate entirely in user space, completely free of any kernel dependency hassles, a fact which DevOps appreciate because it does not slow them down. Moreover, the agent is resource-efficient, high performance, and easy to deploy and manage, facts which SecOps appreciate for obvious reasons.

To learn more about our cloud workload protection solution and the importance of CWP in a cloud defense-in-depth strategy, visit Singularity Cloud Workload Security.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Securing Amazon EKS Anywhere Bare Metal with SentinelOne Singularity
- Cloud Credentials Phishing | Malicious Google Ads Target AWS Logins
- Email Security and XDR | Simple Integration, Powerful Results
- Reduce Risk with Unified EDR and Cyber Asset Management
- EDR for Cloud Workloads Running on AWS Graviton
- SentinelOne Integrates With Amazon Security Lake to Power Cloud Investigations

©2023 SentinelOne. All Rights Reserved.
Privacy Policy Master Subscription Agreement