EINPRESSWIRE

ANY.RUN Introduces macOS to Strengthen SOC Operations

CA, UNITED STATES, March 19, 2026 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has announced the introduction of macOS support. Now available in beta for Enterprise Suite users, this update enables SOC and MSSP teams to investigate threats across Windows, Linux, Android, and macOS within a single unified environment.

□□□□□□□□□□ □□□□□□-□□□□□□□□ □□□□□□□□ □□□□□□□□□□

With macOS adoption steadily growing across enterprise environments, attackers are increasingly targeting Apple devices with platform-specific threats. They include credential stealers, phishing campaigns, and business email compromise (BEC) attacks.

With the addition of macOS virtual machines, analysts can now detonate suspicious files and URLs and observe their behavior in real time regardless of the target platform. This unified approach improves visibility, reduces complexity, and accelerates decision-making during incident response.

□□□ □□□□□□□□ □□□ □□□ □□□□□ □□□□□□□:

□ Faster validation of suspicious files and URLs through real-time behavioral analysis
□ Reduced investigation time by eliminating the need for multiple tools
□ Improved detection coverage across Windows, Linux, Android, and macOS
□ Increased analyst productivity with fewer workflow interruptions

□ Lower alert backlog during peak threat activity

See real-world example of macOS malware sample analyzed within Sandbox in ANY.RUN’s blog.

□□□□□□□□□□□ □□□□□□□□ □□□ □□□□□□□□ □□□□□ □□□□□□ □□□□□□□□□

A key advantage of ANY.RUN’s macOS sandbox is its interactive analysis capability.

This approach helps uncover advanced attack techniques, including:

□ Credential harvesting via fake authentication dialogs
□ Multi-stage execution chains triggered by user input
□ Data exfiltration initiated after system access is granted
□ Social engineering tactics embedded within malware behavior

□□□□□ □□□.□□□

ANY.RUN is an interactive malware analysis and threat intelligence platform designed to help security teams detect, investigate, and respond to cyber threats faster. Its cloud-based sandbox enables real-time analysis across Windows, Linux, Android, and macOS environments, while integrated tools such as Threat Intelligence Lookup and TI Feeds provide immediate context for informed decision-making. Trusted by thousands of organizations worldwide, ANY.RUN is SOC 2 Type II certified and committed to delivering secure, efficient, and scalable solutions for modern cybersecurity operations.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
LinkedIn
YouTube
X