At-a-Glance

Corellium Viper

- Enable Mobile Application Security Testing on a Virtualized Hardware Platform
- Gain Visibility into Data Security Risk and Compliance During Mobile Application Development

CORELLIUM®

THE CHALLENGE

Secure Mobile Application Development is Complex and Costly

Mobile applications and devices are more embedded into business-critical workflows than ever before. However, ensuring mobile applications meet security compliance requirements and protecting against data leakage and compromise within them has never been more complex. Vulnerabilities lie within applications and are exploited by attackers and malware to access sensitive data.

Aligning cross-functional teams for application security, development, and pen testing to build, test, and deploy mobile applications securely is a complex and costly process.

In depth secure mobile application development requires building the application securely and incorporating testing across multiple mobile devices and OS versions. However, it is resource, time, and cost intensive to purchase and test every potential combination of device and operating system and update. Organizations are also challenged to incorporate this level of testing into every mobile application development cycle, leaving applications at risk.

In the past few years alone, 200 malicious applications were distributed in the official Android store[1].

THE SOLUTION

Save Time and Money Leveraging Corellium Viper for Mobile Security Application Testing

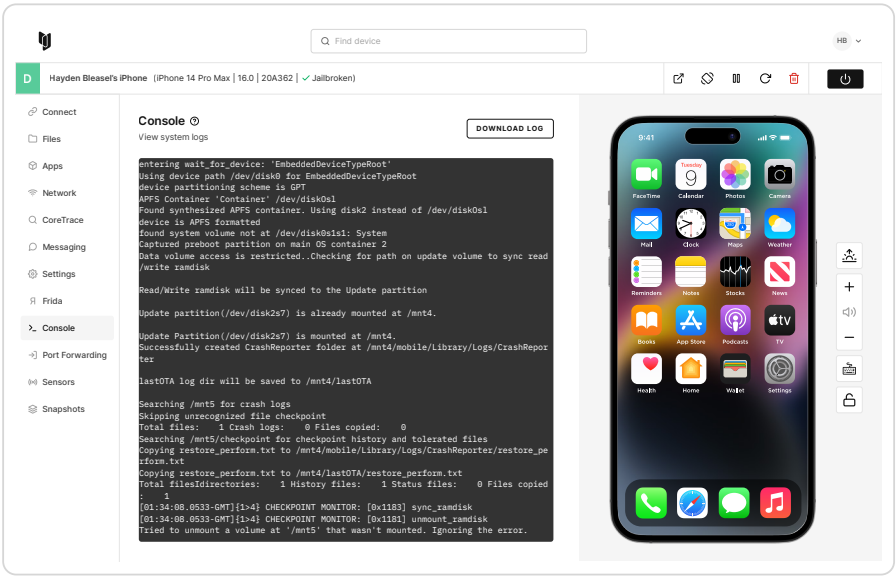
Corellium Viper is a virtualized hardware platform designed to facilitate mobile application security testing across iOS and Android operating systems and devices. Not an emulator or simulator, it is a scalable virtual device platform that enables automated pen testing with static (SAST) and dynamic (DAST) security testing and validation. Unlike emulators or simulators, it runs the actual binaries and delivers high fidelity results for pentesting. Corellium Viper integrates with common development tools so you can easily bring continuous mobile application and device testing into development cycles. An easy-to-use platform, it enables cross-functional collaboration, reducing time and cost for development.

[1] https://www.bleepingcomputer.com/news/security/over-200-malicious-apps-on-google-play-downloaded-millions-of-times/

At-a-Glance

Corellium Viper

- Automate OWASP Mobile Security Testing Guide static and dynamic testing
- Accelerate routine testing by as much as 50% with automation of repetitive tasks, and reduce development cycles
- Reduce risk by freeing up time to enable deep vulnerability and exploit investigation
- Reduce costs, eliminate the need for third- party testing services and hardware devices
- Integrate with a wide variety of API and CLI development tools



Easily Spin-Up Combinations of Device, OS, and Applications for Thorough Testing

- Run ARM devices on ARM servers using on-site appliances, private cloud, or public cloud
- Remove physical device limitations with 300+ device modes and versions supported
- Replace inadequate emulators and costly device farms for security testing

Secure In-House Testing with Greater Visibility and Control

- Deploy using server and desktop appliances for powerful, onsite, air-gapped solutions
- Eliminate the need to provide third-parties access to internal networks and data
- Avoid time spent writing custom scripts so apps can be tested using third-party services

Accelerate Quality Testing and Development using Advanced Tools with Deep Visibility

- Automate OWASP checklist testing to enable time for deep exploit investigation
- Accelerate time to remediation with easy-to-understand results and evidence
- Leverage continuous security testing and report generationto simplify audit and compliance

Next Steps

Contact your Corellium sales representative for more information.

Find out more at **https://www.corellium.com/products/viper**

CORELLIUM®

