CORELLIUM®

Corellium Falcon for Government

Corellium provides government agencies and service providers access to a powerful platform for creating Arm-native virtual devices to support their mobile vulnerability research, app penetration testing, malware analysis and forensics needs.

The Corellium Virtual Hardware platform enables never-before-possible testing and research on virtual iOS, Android, and IoT devices. Through high-accuracy, Arm-native virtualization, it empowers researchers and security experts with the cutting-edge technology they need to stay ahead in the cybersecurity arms race.

It’s not an emulator; it’s Arm on Arm virtualization.

Accelerate R&D with Virtual Devices

Corellium is used by over 50 government agencies, mission teams, and service providers worldwide to successfully achieve their objectives. The Corellium Virtual Hardware platform provides unprecedented research, development, and introspection capabilities for iOS, Android and IoT devices.

Mobile Vulnerability Research

Stay ahead of tomorrow's cyber threats with powerful, never-before possible vulnerability research for iOS and Android. Advance mission critical capabilities with integrated development, reverse engineering, and introspection tools. Corellium's high-accuracy, Arm-native virtual devices enable and accelerate real vulnerability discovery and exploit validation. Get instant jailbreak or root access to any OS version, including beta releases. This is not an emulator or simulator - it's Arm-on-Arm virtualization, which provides greater accessibility and control than real devices without sacrificing binary fidelity.

Mobile Malware & Threat Analysis

Enable threat research teams with advanced investigative capabilities on virtual iOS and Android devices. Arm your Security, IT and SOC teams with the cutting-edge tools they need to stay ahead of cyber threats and accelerate incident response. Simplify IoC gathering and threat hunting with root access and control of virtual devices. Safely sandbox and detonate malware while providing real-time system, file, and network level analytics for IoC evidence gathering, malware reverse engineering, and mobile app debugging.

Mobile App Penetration Testing

Virtualize devices for static (SAST) and dynamic (DAST) application security testing. Leverage a powerful suite of built-in tools to simplify OS, app, data, and network layer analysis and introspection in real-time. Spinup any phone model and iOS or Android version on-demand. Replace costly and incomplete sets of physical devices on testers' desktops or device labs. Run production code without modifications, and have complete control over device sensors, conditions, and location. Easily connect virtual devices to your favorite IDEs, developer tools, and CI/CD systems.

Industries

- Government
- Intelligence Community
- Defense & National Security
- Research Agencies
- Service Providers
- Public Sector
- Legal & Law Enforcement

Roles

- Intelligence Teams
- Defense & Cyber Teams
- Threat Response Teams
- Mobile & Security Analysts
- Independent Contractors

Stay Ahead of Cyber Threats

Strengthen your defensive cybersecurity capabilities with in-depth research, testing, and analysis. Discover vulnerabilities and exploits before the bad actors do.

Advanced research

Examine vulnerabilities with powerful debugging, device state, and runtime hooking functionality.

High-fidelity testing

Leverage Arm-native models through high accuracy and fidelity virtualization, not emulation.

Instant root access

Easily jailbreak/root iOS and Android, including the latest versions and beta releases.

Dynamic testing

Analyze, trace, and log encrypted application traffic with built-in network monitoring tools.

Deep introspection

Assess software at the lowest levels with powerful OS, app, file, system call, and network tooling.

Tooling flexibility

Use our browser console and APIs with Frida, Binary Ninja, IDA Pro, Burp Suite, and all of your favorites.

Push Your R&D Forward

Revolutionize and accelerate R&D on iOS, Android and IoT devices through hardware virtualization.

Workspace Security

Manage and support your teams and their workflows through a centralized server solution that unlocks collaboration while providing visibility and control.

- **Visibility** - Eliminate desktop-based R&D that is decentralized and poses security and compliance risks.
- **Procurement** - Eliminate physical device procurement and risks by allocating virtual hardware resources to specific teams with user and project workspace management tools.
- **Collaboration** - Quickly create and deploy pre-configured virtual devices across users and teams with one-click device snapshot, restore, and cloning functionality.
- **Control** - Simplify onboarding, role-based access (RBAC), and offboarding through centralized administration.
- **Sandboxing** - Sandbox with network-isolated virtual hardware for safer threat analytics and malware detonation.

Corellium
Server Appliance

Government Proven

Corellium technology has been extensively government battle-tested, designed from its inception to meet the most stringent security and compliance needs.

- **Adopted** - Numerous U.S. and international agencies rely on Corellium virtualization technology for their critical security, compliance, and privacy research work.
- **On-Site** - Maintain security compliance with a completely on-site and air-gapped solution. The Corellium platform is available as pre-configured, Arm-powered server appliances for centralized management and control.
- **Flexible** - A single platform can support all Arm device virtual workloads, and enable defensive and offensive research, exercises, and cyber range programs.
- **Training** - The Corellium virtual hardware platform is an excellent hands-on teaching platform for developing security skill sets and best practices, all through simple browsers.

Extensible Platform

The Corellium Virtual Hardware platform is based on our innovative Corellium Hypervisor for Arm (CHARM) technology and can support many types of Arm-powered device models:

- **Included** - We provide iOS and Android virtual device models that are ready to go.
- **Extended** - Create custom extensions to our standard device models.
- **Custom** - Develop entirely new virtual models of your own IoT devices.

Corellium Desktop Appliance

Flexible Deployment Options

Corellium Appliances

Corellium's on-site appliances use the latest NVIDIA Grace™ servers. On-site servers can be air-gapped for use in high-security locations.

Corellium Cloud

Corellium's cloud service is hosted at AWS, using Amazon's Graviton Arm servers. Private AWS deployments are also supported.

Corellium Virtual Hardware Platform

VIRTUAL DEVICES
Arm-powered phones and IoT devices with endless OS and model combinations.

HYPERVISOR
Corellium Hypervisor for Arm (**CHARM**) is a type 1 hypervisor and the only one of its kind.

ARM SERVER
Virtual models run on Arm, just like real devices, combining native fidelity with on-demand availability.

TOOLING
Simplified connection of IDE, debugging, network and security toolsand comprehensive APIs.

NETWORK ANALYSIS
HTTP/S traffic inspection, tracing, and logging.

X-RAY VISION
Powerful OS, app, file, system call, and console access and control.

INTROSPECTION
Advanced OS, kernel and boot controland tooling.

CONTROL
Configure device buttons, sensors, location, environment, battery, device IDs, ports, cameras and mics.

REPLICATION
Snapshot, clone, and restore device states.

TEAMING
Easy project workspace management and team collaboration.

ROOT ACCESS
Root or jailbreak devices instantly, no need to add code or apply security vulnerabilities.

Corellium Falcon

Purpose-built for research and government organizations providing OS-level capabilities and powerful introspection tools not available with physical devices. Falcon enables mobile vulnerability research, exploit introspection, and malware analysis not possible on physical iOS and Android devices.

	Falcon Essentials • Security Research • Malware & Threat Research • App Pentesting	**Falcon Premium** • Vulnerability Research • Introspection & Reversing • Exploit Analysis & Verification
Team & workspace management	✓	✓
Jailbreak/root any OS	✓	✓
App & file system tools	✓	✓
Frida and Cydia integration	✓	✓
Snapshot & cloning	✓	✓
CoreTrace process tracing	✓	✓
HTTPS Network Monitor	✓	✓
MATRIX test automation	✓	✓
MATRIX AppSec reports	✓	✓
Snapshot Sharing	✓	✓
Advanced Network Monitor	✓	✓
OS kernel and filesystem tools	✓	✓
Run self-signed binaries	✓	✓
Kernel debugging	✓	✓
Kernel patch management	✓	✓
Boot control and modification	✓	✓
Device tree configuration	✓	✓
KASLR configuration	✓	✓
Trust cache modification	✓	✓
OS Beta support		✓
Kernel hooking		✓
Program flow & coverage tracing		✓
MicroSnapshots		✓
IMEI, IMSI, and SN modification		✓
Virtual MMIO		✓
SEP debugging		✓
iBoot/BootROM debugging		✓

Free trials at **Corellium.com**

Free trials at **Corellium.com**