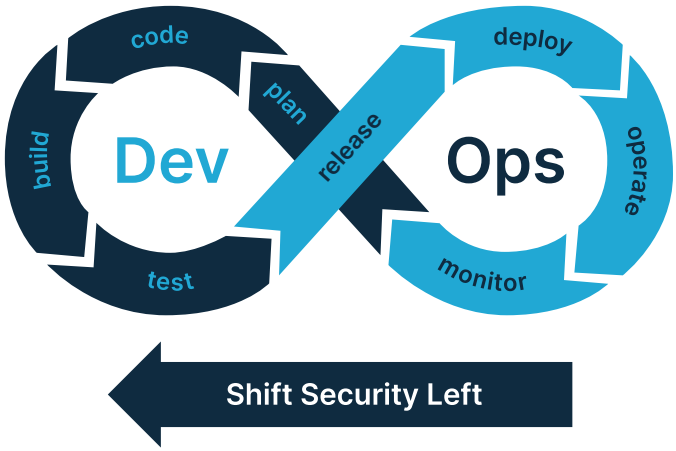
CORELLIUM®

Corellium Solutions for Enterprise

Corellium is used around the world by businesses of all sizes, from small service providers to global enterprises. Corellium is reinventing how mobile applications are being developed and tested in a new cybersecurity and cost efficiency landscape. From developer teams to security teams, the Corellium Virtual Hardware platform accelerates R&D, reduces DevOps costs, and helps shift security left in the software development lifecycle.

Smart devices, cyber security, and shifting left. The risks from inaction are too great.



Smart devices are the new cyber security battlefront. Vulnerabilities lie within mobile apps themselves, exploited by attackers and malware.

Enterprises are moving security practices and accountability further left where apps are first developed.

Smart devices run on Arm. Corellium does, too.

Unlike servers and desktops that run on Intel x86 processors, nearly 95% of smartphones and IoT devices are powered by Arm processors.

We built a unique hypervisor, the Corellium Hypervisor for Arm (CHARM), to run virtual Arm devices on Arm servers.

Developer and security teams can now run phone and IoT apps on Arm-powered development servers to revolutionize how they are built and tested.

Smart device virtualization

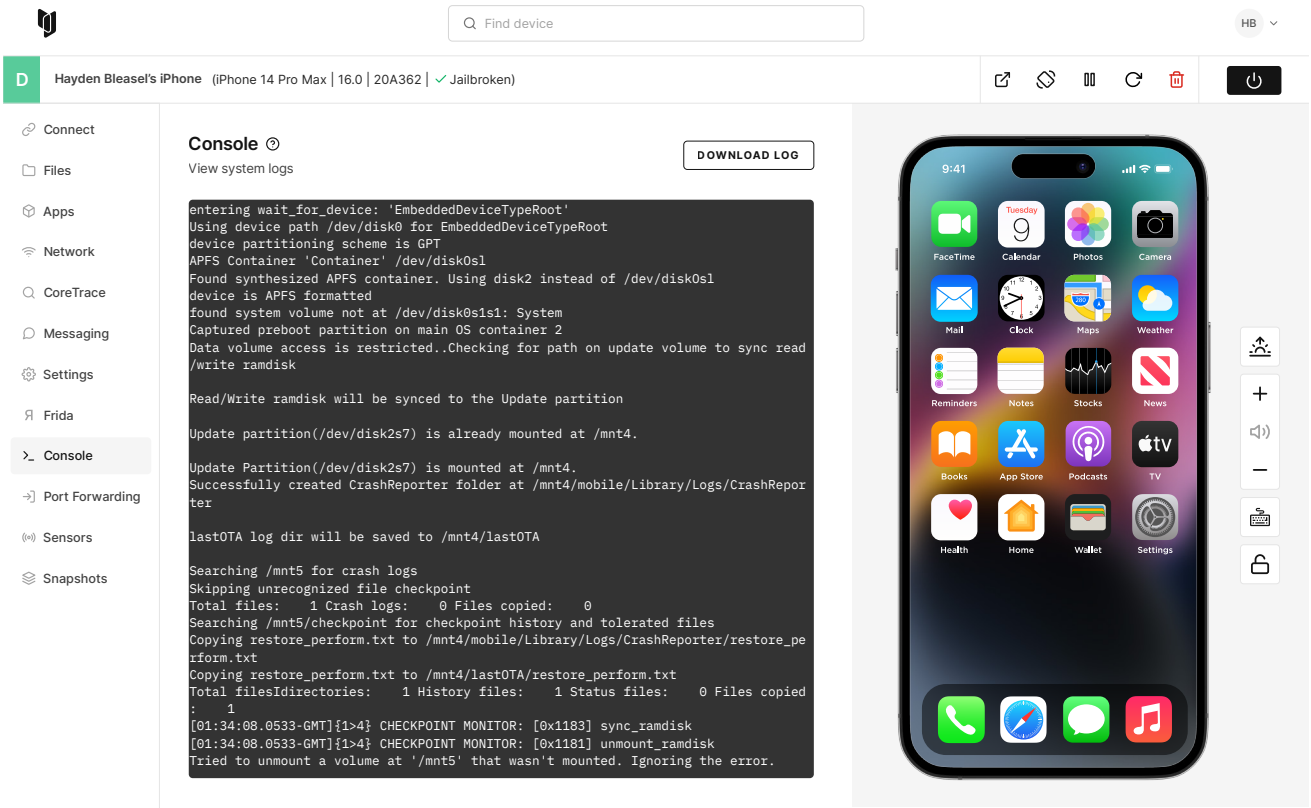
Opens the door for developer and security teams.

This is not an emulator or simulator — it's Arm-on-Arm native virtualization.

Corellium accelerates software development lifecycles with Arm-native virtual models and a powerful browser interface and APIs.

- Easily spin-up **endless combinations** of device, OS and apps.
- **Instant root access** for iOS and Android, jailbreaks not required.
- Use powerful **built-in security tools** and integrate with your existing developer, security, and DevOps tools.

Corellium enables more secure DevSecOps by simplifying the critical work of developer and security teams, and narrowing the cybersecurity skills gap.



Corellium Virtual Hardware Platform

The R&D platform for the next generation of devices

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 tools and comprehensive APIs.
- **CONTROL**
  Configure device buttons, sensors, location, environment, battery, device IDs, ports, cameras and mics.
- **X-RAY VISION**
  Powerful OS, app, file, system call, and console access and control.
- **INTROSPECTION**
  Advanced OS, kernel and boot control and tooling.
- **NETWORK ANALYSIS**
  HTTP/S traffic inspection, tracing, and logging.
- **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.

Deployment flexibility

aws

- Our Corellium Cloud runs securely on AWS Graviton Arm servers, ready to go.
- If you have a private AWS cloud deployment, we support that too.

AMPERE

- And for onsite or air-gapped needs, Corellium Appliances let you entirely do your own thing.

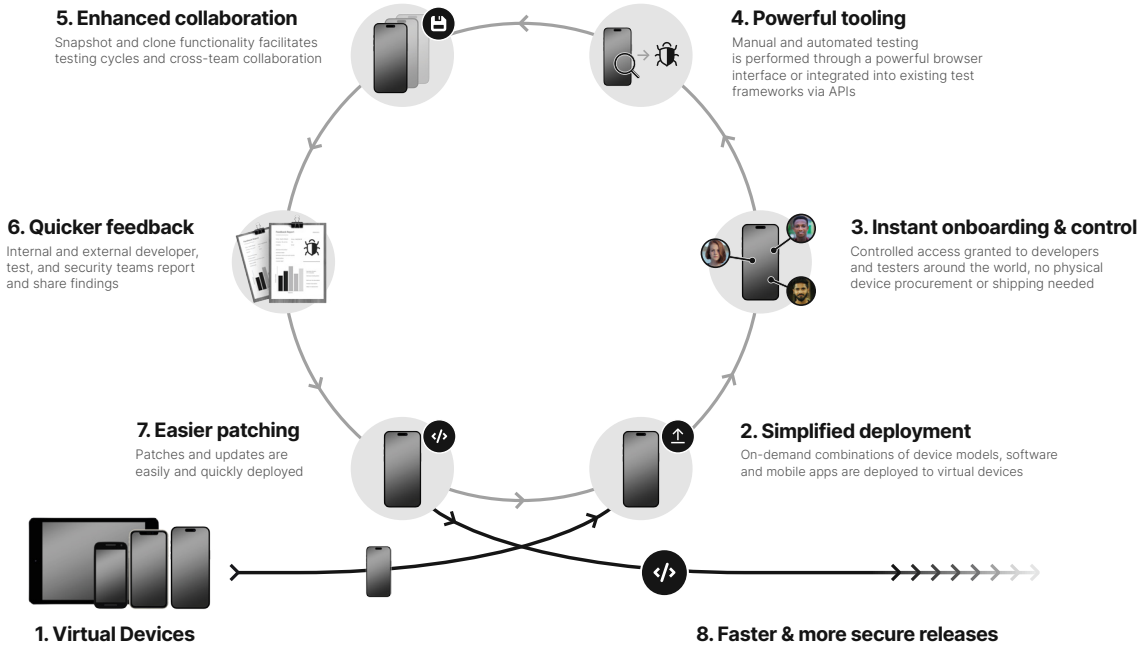
Corellium for Mobile App Development

Mobile app development is challenging as iOS and Android operating systems don't natively run on the laptops of developer and security teams. Emulators are inadequate for keeping up with the new era of cybersecurity threats. And using physical devices with your CI/CD system is too costly. It's time for reinvention.

Virtualize DevOps to reduce costs

It's time to eliminate physical device labs and ditch cloud lab providers.

- They are very costly.
- Very limited in device model and OS availability and combinations.
- Extremely time-consuming to maintain and refresh between testing cycles.
- Root access/jailbreak is needed for comprehensive testing and is not possible or very complicated for iOS.
- Procuring and shipping physical devices wastes time and introduces risks.
- Emulators don't run on Arm, lack security fidelity, require code mods, and lack needed tooling and APIs.
- Batteries cannot support continuous use and pose safety risks.
- The result is R&D takes longer and complexity leads to testing shortcuts and gaps.



Corellium for Mobile App Pentesting

Corellium provides a powerful and polished user interface with built-in security tools for root access, forensic analysis, file system manipulation, Frida scripting, SSL/TLS stripped network monitoring, application debugging, and much more.

Virtualization Not Emulation

ARM-native, this is real pentesting on virtual devices with the ability to quickly load your own binaries.

Instant Root & Jailbreak Access

Root any device configuration, including the latest versions of iOS, even when no public jailbreak is available.

Static Pen Testing

Direct root file system access for Android and iOS devices to perform application static analysis and mobile forensics.

Spin-Up Needed Devices

Easily spin-up near limitless combinations of devices and operating systems, from past models and releases to the very latest.

Dynamic Pen Testing

Built-in network monitoring tools lets you analyze encrypted application traffic instantly.

API and Integrations

Powerful API for scripting and integrations with testing tools such as Frida, Burp, IDA Pro, GDB/LLDB, Xcode, and Android Studio.

Ditch Device Labs and Emulators

Replace costly, incomplete, and undependable physical device labs or cloud farms.

Run Production Code

Emulators often require code modifications that undermine testing integrity.

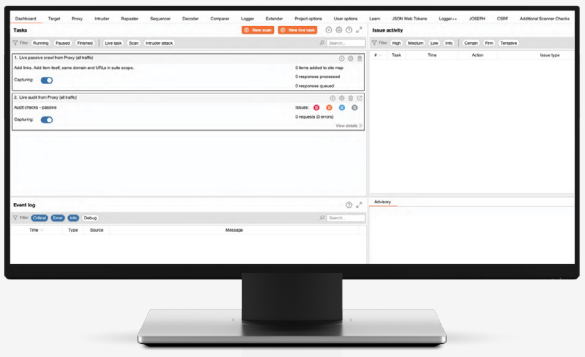
Snapshot & Clone

Instantly restore device states or capture environment conditions for auditing and collaboration.

Control Device Sensors

Control sensors like battery, GPS, and the environment to simulate real-world conditions.

Use virtual devices as drop-in replacements for physical devices with your favorite tools.



Corellium for Malware & Threat Research

The Corellium Arm virtualization platform provides cybersecurity threat and research teams with never-before-possible mobile malware and threat research capabilities on virtualized iOS and Android devices. Its high accuracy, Arm-native device models enable static and dynamic mobile app and OS introspection.

Solutions Highlights

Malware Detonation

Built-in network monitoring tools let you analyze encrypted C2 and app traffic instantly. CoreTrace gives you access to app syscall tracing during execution.

Threat Hunting

Direct root file system access for iOS and Android devices to gather IoC evidence during and after detonation.

Sandboxing

Sandbox with network-isolated virtual hardware for safer mobile threat analysis and malware detonation.

Virtualization Not Emulation

Arm-native, this is real mobile threats and malware running on virtual devices with the ability to quickly restore device snapshots.

Spin Up Needed Devices

Easily spin up near limitless iOS and Android devices, from past models and releases to the very latest.

Instant Root & Jailbreak

Root any device configuration — including the latest versionsof iOS — even when no public jailbreak is available.

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 virtual devices across users and teams with one-click device snapshot, restore, and cloning functionality, eliminating physical device limitations.

Control

Simplify onboarding, role-based access (RBAC), and offboarding through centralized administration.

Conduct Research Faster

Single platform for iOS and Android, faster collaboration, and eliminate shipping physical devices across teams.

Corellium for Cyber Security Training

Corellium gives educational institutions, professors, and trainers a powerful platform to teach computer science and software development without physical devices. Spin up any combination of device and OS and use Corellium's built-in research and teaching tools, all through simple browsers.

The Corellium Arm virtualization platform provides never-before-possible mobile device training environments through the use of virtual iOS and Android phones. Its high accuracy, Arm-native phone virtualization allows instructors to effortlessly provide real-world, hands-on mobile security and app development training without the typical challenges or limitations of using software emulators.

Limitless Teaching On Virtual Phones

Corellium provides a powerful and polished user interface with built-in teaching tools for root access, app forensics, file system manipulation, Frida instrumentation, network traffic analysis, and much more. Corellium's comprehensive API and USBFlux technology streamlines integration with leading development, security, and educational tools — such as Xcode, Android Studio, IDA Pro, Burp Suite, Charles Proxy, and more.

Offer New Courseware

Corellium virtual devices are a drop-in replacement for physical devices, integrating seamlessly with existing curricula. And if you don't currently offer mobile security and research courses, imagine the possibilities. Corellium offers mobile security training classes of its own to help you on your way. Feel free to take our classes, and then contact us for potential use of our syllabi and materials to create or jumpstart your own courseware.

Enterprise teams that use Corellium

Developer teams reporting to the VP of Engineering

- Mobile App R&D
- IoT Device R&D
- Security Testing

Security teams reporting to the CIO/CISO

- Data Security & Compliance
- SOC Teams & Threat Research
- Cyber Security Training

Developer and security teams benefit from the Corellium Virtual Hardware platform to accelerate R&D, lower costs, and increase security for application development and cyber threat research.

500+

CUSTOMERS

Corellium is government battle-tested and security community proven. We have over 500 customers, including many Fortune 1000 companies and government agencies around the world.

- 50+ Fortune 1000 enterprises across finance, automotive, tech, retail, manufacturing, and energy
- 30+ government agencies globally
- 4 of the 5 largest defense contractors
- 2 of the 3 largest telecom companies
- 100's of security services
- 100's of independent professionals

Free trials at **Corellium.com**

CORELLIUM®