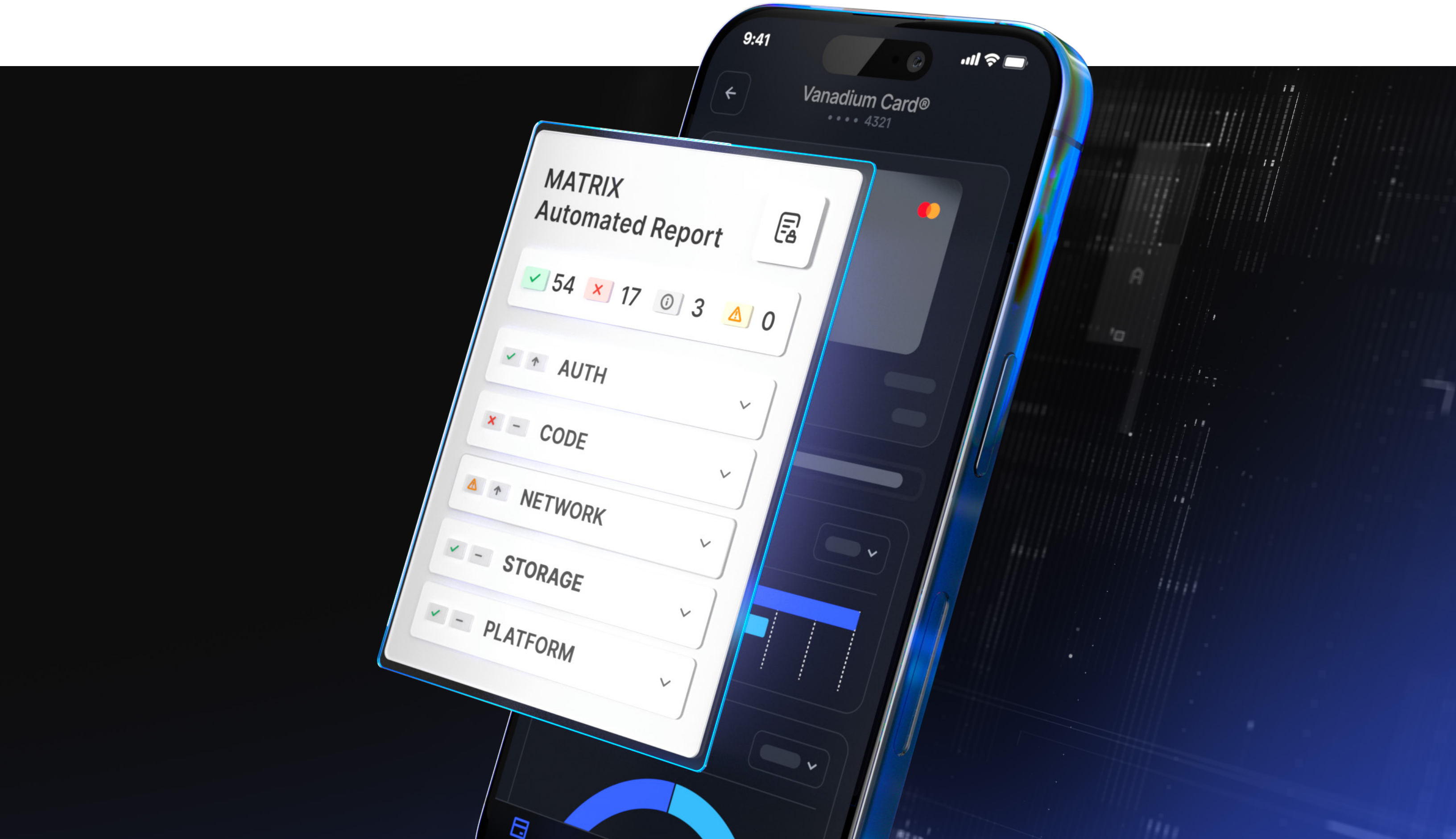
CORELLIUM®

# Corellium MATRIX™ for Mobile Pentesting

Corellium is excited to introduce MATRIX™ (Mobile Automated Testing and Reporting Interface) into the Corellium Virtual Hardware platform. This new technology simplifies and accelerates the work of mobile security testing, validation, and compliance teams.

**Introducing Mobile App Security Testing automation and AppSec report generation**



# Automated Security Testing & Reporting for Mobile Apps

Corellium MATRIX™ (Mobile Automated Testing and Reporting Interface) is a core technology of the Corellium Virtual Hardware platform. The innovative technology simplifies and accelerates the work of mobile security pentesting and AppSec compliance teams.

## Accelerate Software Development Lifecycles and Reduce Costs with Corellium

The Corellium platform allows mobile developer, test, and security teams to collaborate and work together on a single, centralized platform that can be powered by Corellium onsite appliances or as a cloud service.

Corellium enables teams to leverage powerful, built-in security tools to not only test apps, but also investigate vulnerabilities discovered, snapshot device states, and share them with other teams for remediation. The MATRIX test automation framework affords significant security penetration testing time savings, allowing for the "automation of the mundane" so that security professionals can focus on the "art" of testing where their expertise shines.

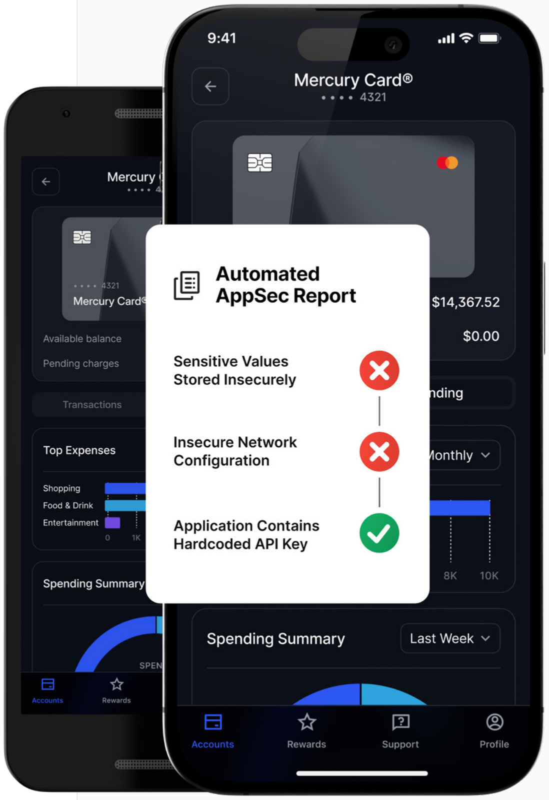
Corellium is changing the entrenched paradigm in mobile security testing by eliminating the limitations of using physical devices, bringing high-cost and high-risk cloud-based testing services in-house, and shifting security left for DevOps continuous security testing.

### Industries

- Enterprise
- Security Service Providers
- Independent Consultants
- Government

### Roles

- Mobile App Pentesters
- AppSec Compliance Teams
- DevOps Continuous Testing



# Secure In-House Testing

Using external cloud-based testing services for mobile apps imposes security risks with sensitive company IP including pre-release binaries, authentication keys and passwords, and often needing access to internal networks and data.

Corellium Server and Desktop appliances provide powerful, onsite, air-gapped solutions with MATRIX built-in. Corellium Servers also allow for centralized workspace access for greater visibility and control.

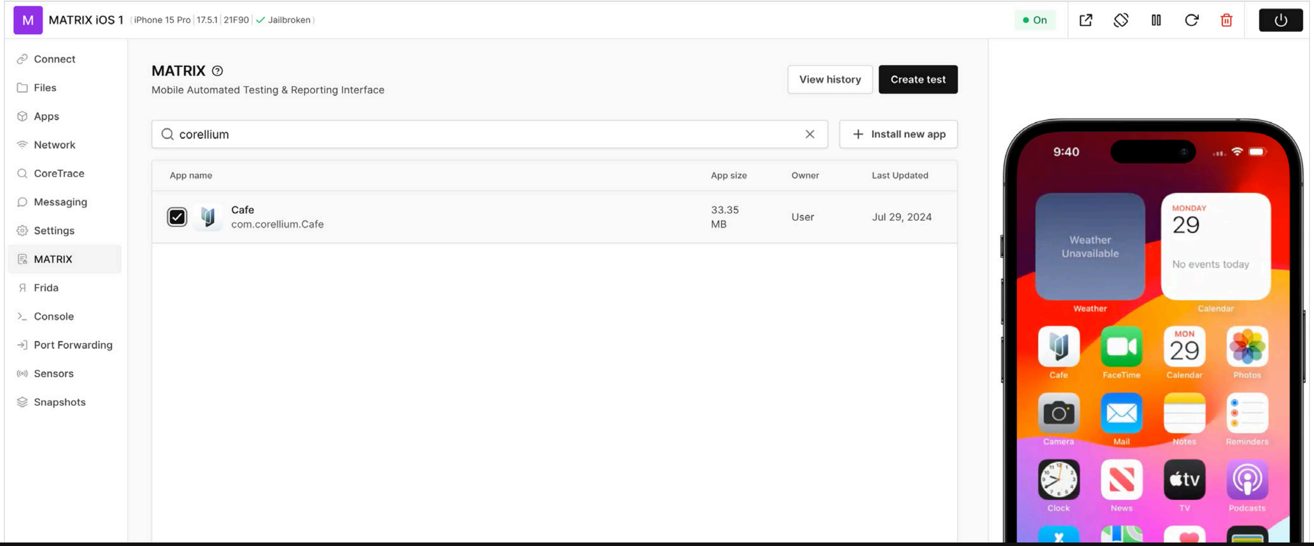
Corellium appliances provide the complete security testing platform for advanced security and penetration testing needs - whether automated or manual. Your security experts have “in-house” total access to the platform for hands-on use, including snapshot and cloning of full virtual device images for superior state restoration, fault reproduction, regression testing, and cross-team sharing.

Corellium Desktop Appliance

# Dynamic Test Automation

Dynamic mobile app security testing often requires teams to repeat many of the same tasks over and over again. Particularly in security and penetration testing, teams are creating dynamic data within a mobile application, then gathering evidence for both data at rest and data in motion. After all the evidence has been gathered, the tester then scours through that data for sensitive information.

The MATRIX automation framework allows for this process to be automated for a significant portion of dynamic testing recommended by the OWASP Mobile Security Testing Guide (MSTG) for both iOS and Android apps. This can alleviate as much as 75% of the mundane, routine work required of pentesters for every mobile app testing run.



MATRIX

Mobile Automated Testing & Reporting Interface

corellium

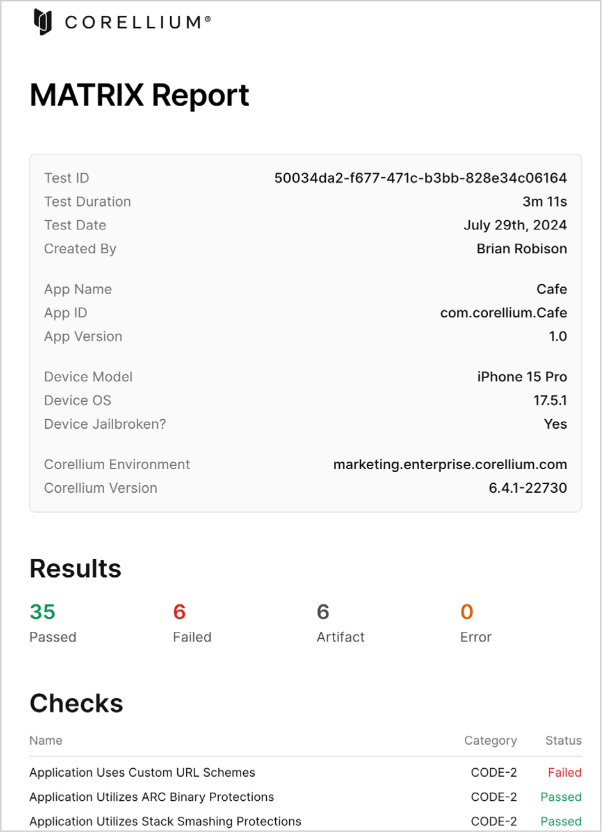
| | App name | App size | Owner | Last Updated |
|---|---|---|---|---|
| ☑ | Cafe<br>com.corellium.Cafe | 33.35 MB | User | Jul 29, 2024 |

# Turnkey AppSec Reports

MATRIX produces a turnkey, easy to understand, AppSec assessment that includes pass/fail results, information about the tests, evidence identified, as well as recommended remediations.

When used for repeated testing, these reports allow for significant savings by allowing high-value security testers to focus more on the “art” areas of testing rather than the mundane portions. Reports are quickly generated for each mobile app, increasing testing consistency and reproducibility.

The reports can be included in AppSec auditing and compliance submissions which otherwise can be cumbersome and time consuming. And they foster best-practices, knowledge sharing, and skills building across development, testing, and security teams.



CORELLIUM®

## MATRIX Report

| | |
|---|---|
| Test ID | 50034da2-f677-471c-b3bb-828e34c06164 |
| Test Duration | 3m 11s |
| Test Date | July 29th, 2024 |
| Created By | Brian Robison |
| App Name | Cafe |
| App ID | com.corellium.Cafe |
| App Version | 1.0 |
| Device Model | iPhone 15 Pro |
| Device OS | 17.5.1 |
| Device Jailbroken? | Yes |
| Corellium Environment | marketing.enterprise.corellium.com |
| Corellium Version | 6.4.1-22730 |

### Results

| 35 | 6 | 6 | 0 |
|---|---|---|---|
| Passed | Failed | Artifact | Error |

### Checks

| Name | Category | Status |
|---|---|---|
| Application Uses Custom URL Schemes | CODE-2 | Failed |
| Application Utilizes ARC Binary Protections | CODE-2 | Passed |
| Application Utilizes Stack Smashing Protections | CODE-2 | Passed |

# Continuous Security Testing

When fully integrated into a CI/CD pipeline, Corellium can be actioned to bring up a virtual mobile device, install an app build, execute the app, click/swipe/enter data, then sift through app data and network transmissions for sensitive data that is provided by the tester or developer.

By utilizing actual data in the dynamic generation, rather than relying on a simple “bill of material” scan to determine vulnerabilities – false positives can be greatly reduced – thus saving the team wasted time. Corellium APIs allow for this process to be fully automated and built into a CI/CD development pipeline to be run as often as desired, all without incurring per-test or per-app costs.

Providing continuous security testing is a critical milestone in shifting-left to achieve DevSecOps for mobile.

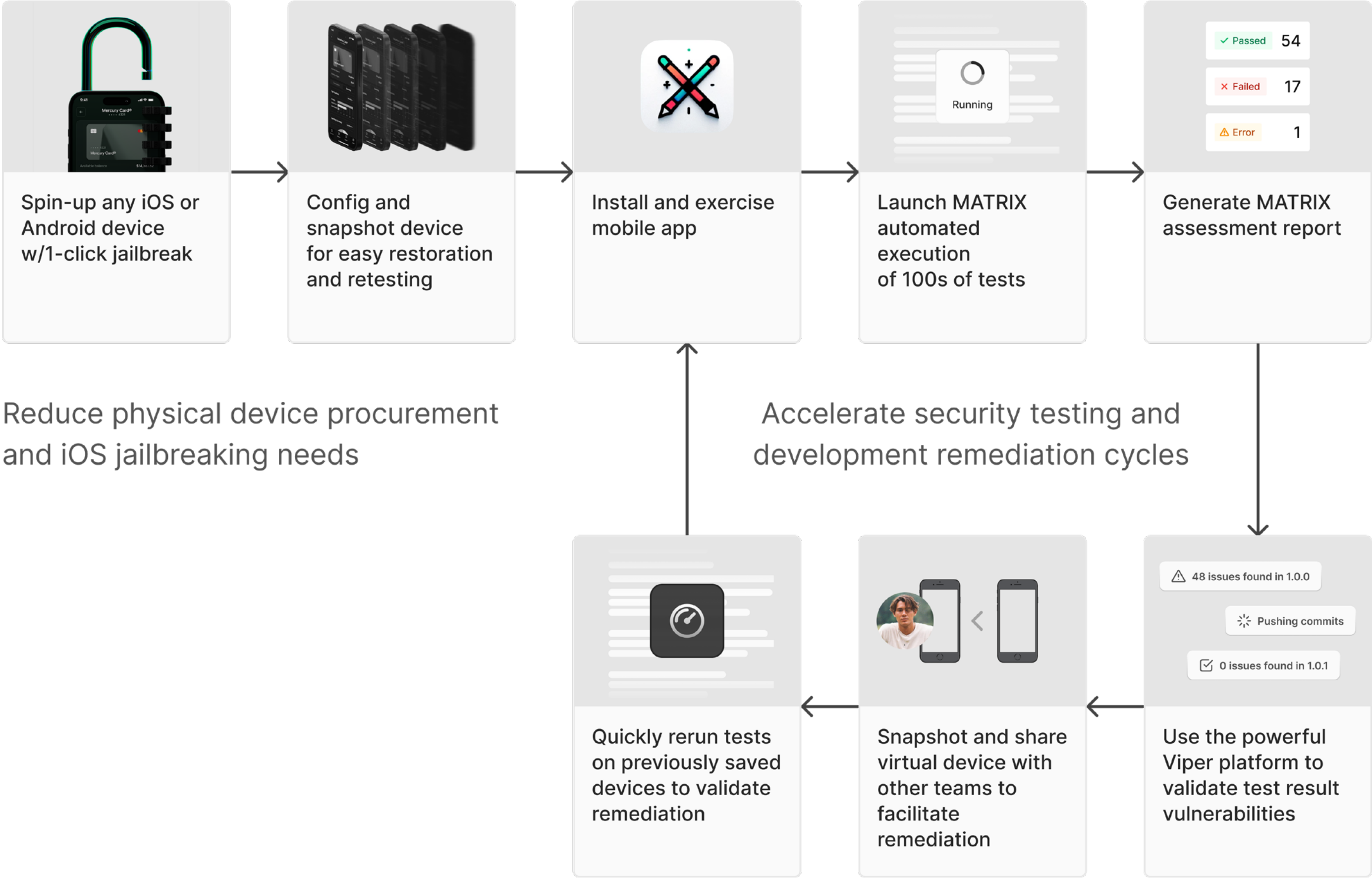
# iOS and Android Virtual Devices On-Demand

The Corellium hypervisor for Arm (CHARM) runs on native Arm processors, available in the cloud or as onsite server appliances. Corellium provides a single platform for iOS and Android virtual devices that are a drop-in replacement for physical devices. Simply spin-up a near limitless combination of device and OS, from older versions to the very latest, patched or unpatched, jailbroken or not.

# Comprehensive Penetration Testing

Corellium Viper provides a powerful and polished user interface with built-in security tools for root access, forensic analysis, filesystem manipulation, Frida scripting, SSL/TLS stripped network monitoring, application debugging, and much more. A comprehensive API and USBFlux technology enables integration with leading development and security tools such as Xcode, Android Studio, IDA Pro, Frida, and Burp Suite.

# Innovate mobile security testing



Spin-up any iOS or Android device w/1-click jailbreak

Config and snapshot device for easy restoration and retesting

Install and exercise mobile app

Launch MATRIX automated execution of 100s of tests

Generate MATRIX assessment report

Use the powerful Viper platform to validate test result vulnerabilities

Snapshot and share virtual device with other teams to facilitate remediation

Quickly rerun tests on previously saved devices to validate remediation

Reduce physical device procurement and iOS jailbreaking needs

Accelerate security testing and development remediation cycles

# Why Choose Corellium for Mobile App Pentesting

### Virtualization Not Emulation

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

### On Demand Devices & Root Access

Spin-up device models and OSs on-demand, including beta releases, with one-click jailbreak/root access.

### Static & Dynamic Pentesting

Direct root file system access and built-in network monitoring tools enable static and dynamic app security testing.

### Lower Costs

Unlike other solutions and services that are priced per test or app, Corellium provides cost efficient “all-you-can-test” pricing.

### Accelerate Testing

MATRIX can alleviate up to 75% of mundane, routine work with automated security testing and reporting.

### Increase Consistency

Establish base-line test reports to increase test coverage consistency and reproducibility.

### Facilitate Compliance

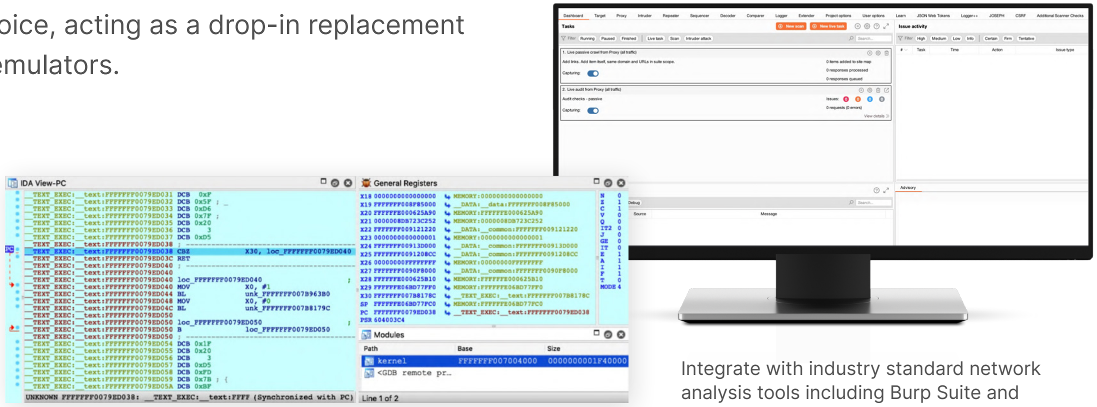
Automatically generated AppSec reporting facilitates standards adherence and compliance submissions.

### API and Integrations

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

## Use with your favorite tools

Corellium’s virtual devices are designed to integrate seamlessly with existing tools of choice, acting as a drop-in replacement for physical devices or emulators.



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued

2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues: 0 0 0 0
0 requests (0 errors)

| # | Task | Time | Action | Issue type |
|---|---|---|---|---|

| Source | Message |
|---|---|

```
__TEXT_EXEC:__text:FFFFFFF0079ED031 DCB  0xF
__TEXT_EXEC:__text:FFFFFFF0079ED032 DCB 0x5F ; _
__TEXT_EXEC:__text:FFFFFFF0079ED033 DCB 0xD6
__TEXT_EXEC:__text:FFFFFFF0079ED034 DCB 0x7F ;
__TEXT_EXEC:__text:FFFFFFF0079ED035 DCB 0x20
__TEXT_EXEC:__text:FFFFFFF0079ED036 DCB    3
__TEXT_EXEC:__text:FFFFFFF0079ED037 DCB 0xD5
__TEXT_EXEC:__text:FFFFFFF0079ED038 ; ---------------------------------------
__TEXT_EXEC:__text:FFFFFFF0079ED038 CBZ             X30, loc_FFFFFFF0079ED040
__TEXT_EXEC:__text:FFFFFFF0079ED03C RET
__TEXT_EXEC:__text:FFFFFFF0079ED040 ; ---------------------------------------
__TEXT_EXEC:__text:FFFFFFF0079ED040
__TEXT_EXEC:__text:FFFFFFF0079ED040 loc_FFFFFFF0079ED040                    ;
__TEXT_EXEC:__text:FFFFFFF0079ED040 MOV             X0, #1
__TEXT_EXEC:__text:FFFFFFF0079ED044 BL              unk_FFFFFFF007B963B0
__TEXT_EXEC:__text:FFFFFFF0079ED048 MOV             X0, #0
__TEXT_EXEC:__text:FFFFFFF0079ED04C BL              unk_FFFFFFF007B8179C
__TEXT_EXEC:__text:FFFFFFF0079ED050
__TEXT_EXEC:__text:FFFFFFF0079ED050 loc_FFFFFFF0079ED050                    ;
__TEXT_EXEC:__text:FFFFFFF0079ED050 B               loc_FFFFFFF0079ED050
__TEXT_EXEC:__text:FFFFFFF0079ED050 ; ---------------------------------------
__TEXT_EXEC:__text:FFFFFFF0079ED054 DCB 0x1F
__TEXT_EXEC:__text:FFFFFFF0079ED055 DCB 0x20
__TEXT_EXEC:__text:FFFFFFF0079ED056 DCB    3
__TEXT_EXEC:__text:FFFFFFF0079ED057 DCB 0xD5
__TEXT_EXEC:__text:FFFFFFF0079ED058 DCB 0xFD
__TEXT_EXEC:__text:FFFFFFF0079ED059 DCB 0x7B ; {
__TEXT_EXEC:__text:FFFFFFF0079ED05A DCB 0xBF
UNKNOWN FFFFFFF0079ED038: __TEXT_EXEC:__text:FFFF (Synchronized with PC)
```

```
X18 0000000000000000  ↳ MEMORY:0000000000000000                        N    0
X19 FFFFFFF008F85000  ↳ __DATA:__data:FFFFFFF008F85000                 Z    1
X20 FFFFFFE000625A90  ↳ MEMORY:FFFFFFE000625A90                        C    1
X21 0000008DB723C252  ↳ MEMORY:0000008DB723C252                        V    0
X22 FFFFFFF009121220  ↳ __DATA:__common:FFFFFFF009121220               Q    0
X23 0000000000000001  ↳ MEMORY:0000000000000001                        IT2  0
X24 FFFFFFF00913D000  ↳ __DATA:__common:FFFFFFF00913D000               J    0
X25 FFFFFFF0091208CC  ↳ __DATA:__common:FFFFFFF0091208CC               GE   0
X26 00000000FFFFFFFF  ↳ MEMORY:00000000FFFFFFFF                        IT   0
X27 FFFFFFF0090F8000  ↳ __DATA:__common:FFFFFFF0090F8000               E    1
X28 FFFFFFE000625B10  ↳ MEMORY:FFFFFFE000625B10                        A    1
X29 FFFFFFE06BD77FF0  ↳ MEMORY:FFFFFFE06BD77FF0                        I    1
X30 FFFFFFF007B8178C  ↳ __TEXT_EXEC:__text:FFFFFFF007B8178C            F    1
SP  FFFFFFE06BD77FC0  ↳ MEMORY:FFFFFFE06BD77FC0                        T    0
PC  FFFFFFF0079ED038  ↳ __TEXT_EXEC:__text:FFFFFFF0079ED038            MODE 4
PSR 604003C4
```

| Path | Base | Size |
|---|---|---|
| kernel | FFFFFFF007004000 | 0000000001F40000 |
| <GDB remote pr… | | |

Line 1 of 2

Integrate with your favorite tools for binary disassembly including IDA Pro.

Integrate with industry standard network analysis tools including Burp Suite and Charles Proxy.

# 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 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.

## Deployments

### Onsite Appliances

Corellium server and desktop appliances use the latest Arm processors and are air-gapped for use in high-security environments.

### Cloud Service

The Corellium cloud service runs on AWS using the latest Amazon Graviton servers.

### Private Servers

Customers can host Corellium servers in their own AWS cloud, or we can host them in our AWS cloud.