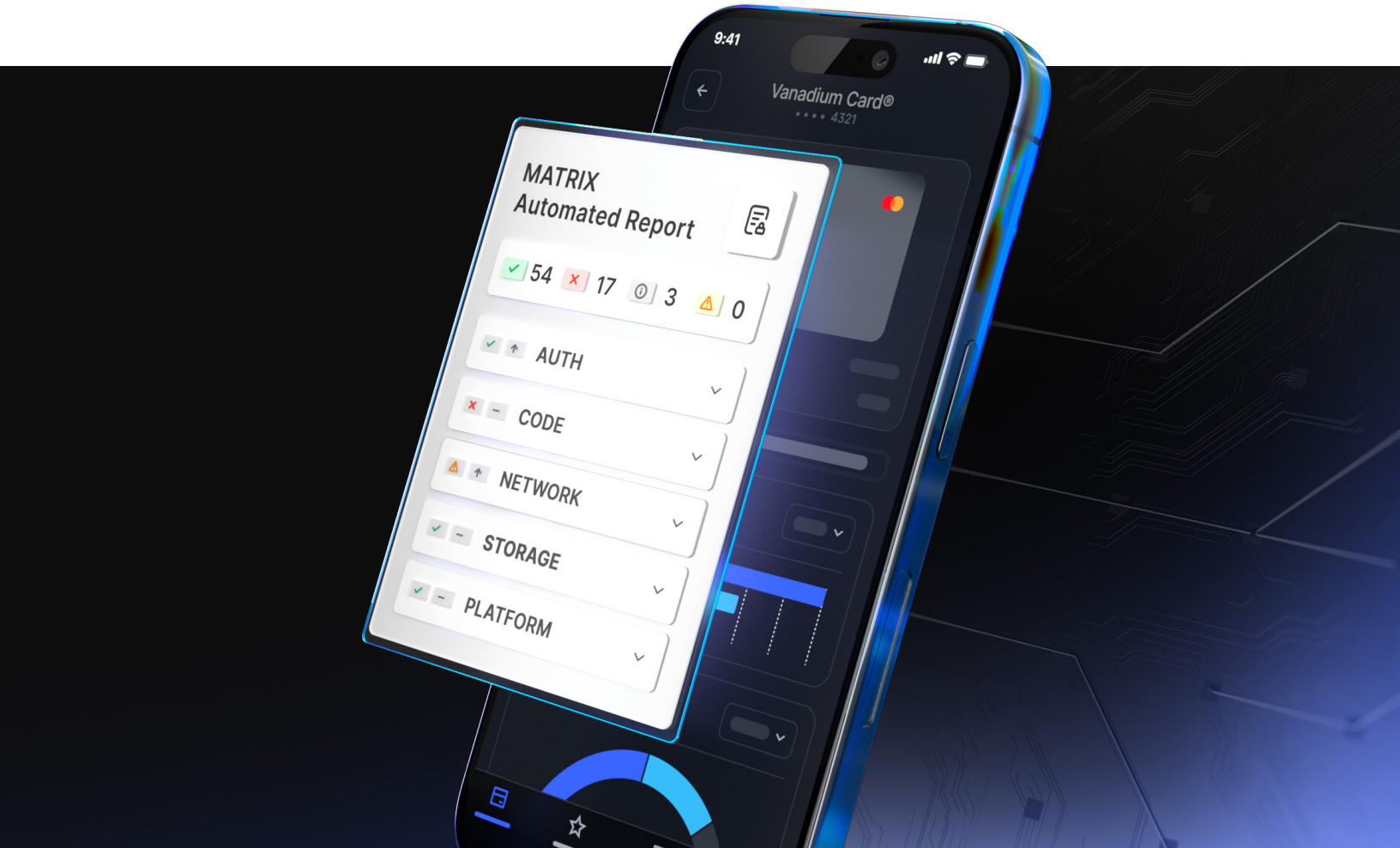
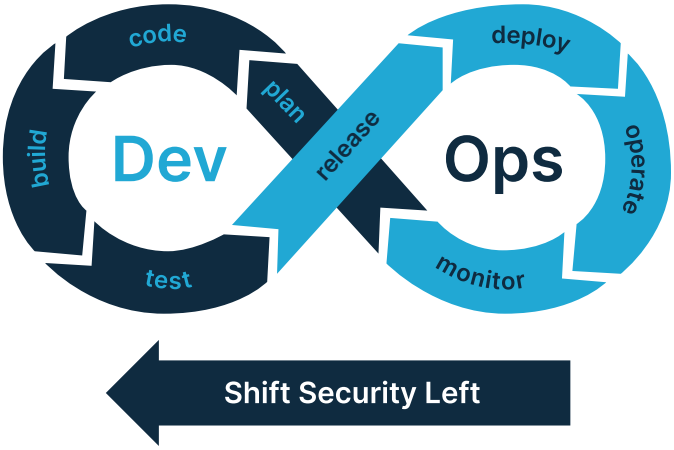
CORELLIUM®

Corellium Viper for Enterprise

Corellium Viper is designed for mobile app security testing (MAST) for iOS and Android. Viper provides virtual devices that enable pentesting capabilities, speed, and cost savings not achievable with physical phones. Equip your security team with unprecedented tools for both manual and automated testing, freeing up valuable engineering time and saving money.



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



Mobile 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.

Mobile devices run on Arm. Corellium does, too.

Unlike servers and desktops that run on Intel x86 processors, nearly 95% of smartphones 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 mobile apps on AWS servers or onsite appliances to revolutionize how they are built and tested. It's time to replace inadequate emulators or costly device farms for security testing.

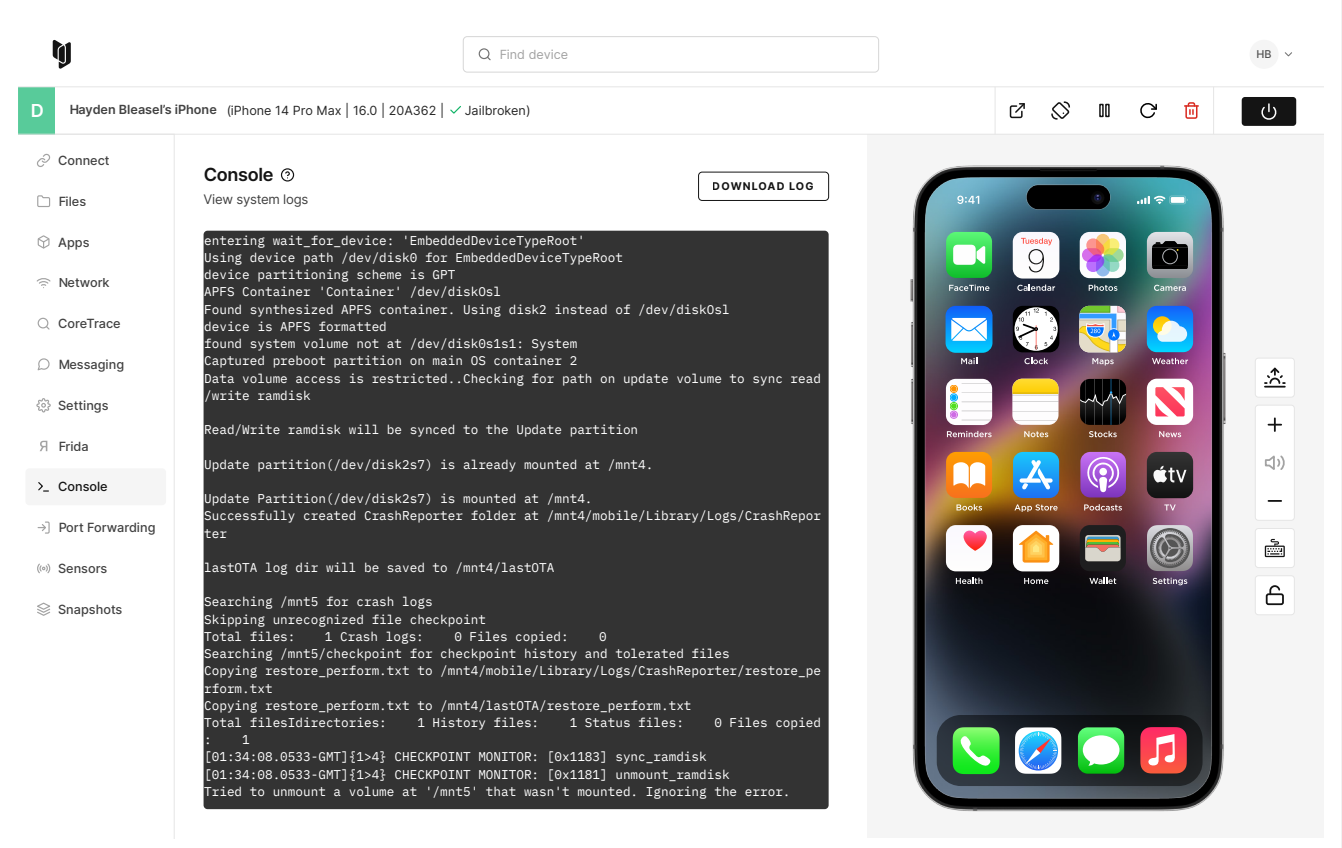
Access iOS & Android Devices On-Demand

Corellium provides high-precision virtual devices for mobile security testing. With highly performant, scalable, and accurate virtual models, Corellium enables powerful capabilities not possible on physical hardware. This is not an emulator or simulator — it's 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.



Accelerate R&D and Reduce Costs

The Corellium platform allows mobile developer, test, and security teams to collaborate and work together on a single, centralized platform. Corellium Viper simplifies and accelerates mobile security testing by removing the limitations of physical devices and providing R&D teams with powerful tooling.

Mobile App Security Pentesting

Provide security and testing teams with one place for unprecedented mobile app penetration testing on virtual iOS and Android devices, with static (SAST) and dynamic (DAST) secutity testing and validation. Corellium provides a powerful and polished user interface with unprecedented tools for both manual and automated testing, freeing up valuable engineering time and saving money. Empower your team 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. Our MATRIX automation technology further simplifies application security testing and accelerates the critical work of security teams by as much as 75%.

Mobile Security Continuous Testing

DevOps for iOS and Android apps is challenging as using physical phones in automated workflows imposes high costs and risks. The result is R&D takes longer, and complexity leads to security testing shortcuts and gaps. Corellium provides Arm-native virtual models of iOS and Android devices on a single platform, purpose-built to accelerate the critical work of developer and security teams. Providing continuous security testing is a critical milestone in shifting-left to achieve DevSecOps for mobile. Automated security testing is a capability of the Corellium platform and APIs allow for integration into CI/CD workflows to be run as often as desired.

Secure In-House Testing

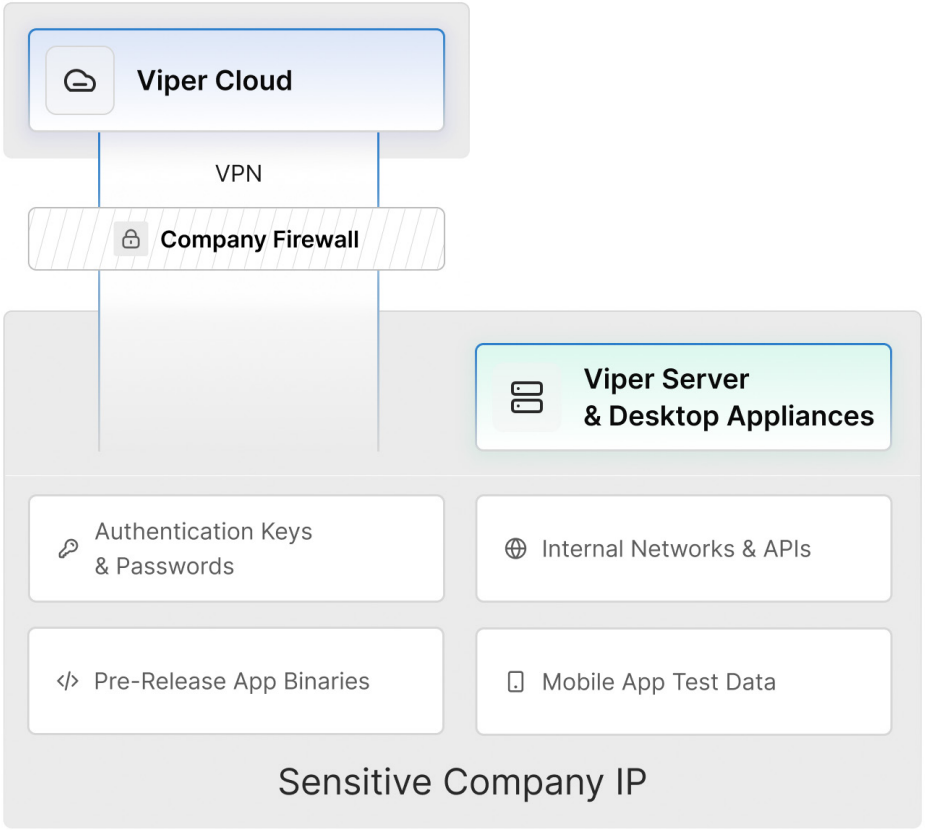
Using external cloud-based testing services for mobile apps imposes security risks with sensitive company IP including pre-release binaries, authentication keys and passwords, and often needing access to internal networks and data.

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

Corellium Viper 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 Viper
Desktop Appliance

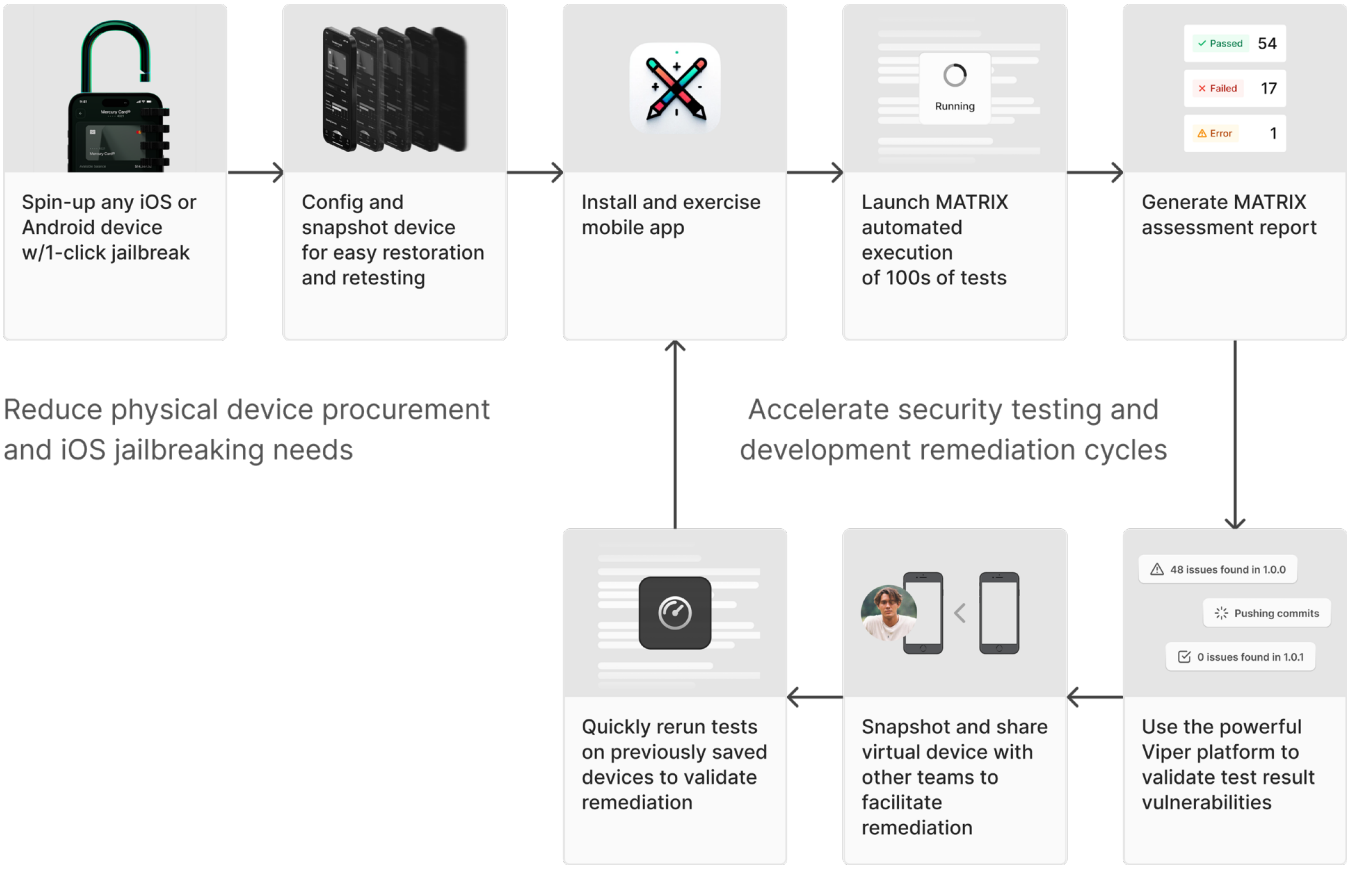
Corellium secure architecture - your data never leaves your datacenter



MATRIX Security Testing Automation

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 by automating a significant portion of static and 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, allowing for the “automation of the mundane” so that security professionals can focus on advanced security testing - where their expertise shines.

MATRIX produces turnkey, easy to understand, AppSec reports that include 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 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.

Corellium Viper

Viper provides virtual iOS and Android devices that enable pentesting capabilities, speed, and cost savings not achievable with physical phones.

	Viper Essentials • Mobile App Security Testing • Physical Device Replacement	**Viper Advanced** • Advanced App Pentesting • Automated Testing & Reporting • AppSec Compliance
Delegated administration	✓	✓
Team management	✓	✓
Project workspaces	✓	✓
Single sign-on	✓	✓
Multi-factor authentication	✓	✓
Jailbreak/root any OS	✓	✓
Root shell access	✓	✓
App & file system tools	✓	✓
Frida integration	✓	✓
Cydia integration	✓	✓
Snapshot & cloning	✓	✓
CoreTrace process tracing	✓	✓
HTTPS Network Monitor	✓	✓
Virtual Wi-Fi	✓	✓
MATRIX test automation		✓
MATRIX AppSec reporting		✓
Snapshot Sharing		✓
Advanced Network Monitor		✓
iOS jailbreak detection bypass		✓
Biometric bypass		✓
iOS update support		✓
Restore iOS backups		✓
UDID & ECID modification		✓
SMS emulation		✓
Port forwarding		✓
Configurable network egress		✓
Location & motion control		✓
Battery & environment control		✓

CORELLIUM®