

A look at the comprehensive security features of the FR55 First Responder Mobile Computer

Zebra Technologies is known for developing highly secure mobile devices designed for deployment in environments where device security is critical—such as public safety and military applications. When it comes to the security of your mobile devices, their applications and data, and the networks to which they are connected, the FR55 delivers.

Following is a look at the three categories of security features that the FR55 offers: hardware, software and certifications.

Zebra knows security: Zebra has brought over 65 products to market that have achieved the highest level of U.S. government security specifications.



ZEBRA

FR55 security features at-a-glance



FR55 hardware security features

Secure Element

The best physical security available on a mobile device—prevents physical hardware attacks.

Secure Boot/Verified Boot

Prevents malware from loading when a device powers up.

FIPS 140-3 Validated (ISO 19790)

Protects data at rest and in transit.

2nd gen 5G (Rel 16) Cellular

Provides the fastest and most secure cellular connections.

Google Strongbox

Keeps the most sensitive data secure, such as passwords.



FR55 software security features

LifeGuard™ for Android™¹

Delivers regular and timely security updates, over a device's lifespan to protect against the latest cyber threats—complete with priority level.

Nano-SAM slot (Nano Secure Access Module)

Provides a hardened environment to securely handle sensitive data, from storing and securing master keys to performing cryptographic operations and executing mutual authentication processes.

Wireless Insights

Monitors and analyzes the wireless connections on all devices—Wi-Fi and cellular. Presents results on an easy-to-digest dashboard that allows you to identify and resolve critical connectivity issues before they

result in outages that can impact operations and security.

Identity Guardian

Ensures only authorized users can gain access to your Zebra devices through secure technologies, including facial recognition.

Device Guardian

Lost devices can present a major security risk. Device Guardian keeps track of the location of all of your devices, enabling misplaced devices to be located quickly and easily.

Mx (Mobility Extensions)

Provides over 100 features that can be activated to enhance the security of the Android operating system—as well as the ability to disable features to better secure the device, its data and authorized networks.

Device Diagnostic Tool

Tests all main systems on a Zebra mobile device—hardware, software, connectivity and battery—to enable rapid identification and resolution of device issues.

GMS Restricted Mode

Enables control of which GMS apps and services are available on your Zebra devices, increasing security and privacy through better control over your organization's data.

RxLogger

Enables a technician to create in-depth app and system logs on a specific Zebra mobile device to enable rapid troubleshooting and resolution of device issues.



FR55 certifications

MDS Cert (Mobile Device Security Certificate)

Evaluation is complete and certification is in process.

Android Enterprise Recommended

Ensures devices meet strict requirements defined by Google for security updates, as well as performance and ease of management.²

Cyber Resilience Act (CRA)

Compliance with mandated cyber security requirements throughout the lifecycle of a mobile device—from product design to ongoing support.

Common Criteria Certified

This internationally recognized security standard provides a rigorous framework for 3rd party extensive testing to ensure

devices meet defined global security requirements and support compliance.

EU RED (Radio Equipment Directive)

Ensures network protection, personal data, privacy protection, and fraud protection as specified by the EN 18031 specification.

¹ LifeGuard for Android requires a valid Zebra OneCare support agreement.

² Certification completed, announcement pending.