ZEBRA CAPTURE YOUR EDGE

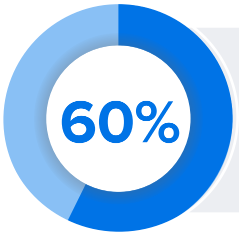
Zebra Mobile Computing Security

Secure Mobile Devices with Industry Best Practices

Table of Contents

Follow Mobile Computing Security Best Practices with Zebra

Mobile initiatives are among the top priorities for most businesses. According to a global survey*:



of respondents believe mobile computing will benefit their business within the next five years.

However, with more organizational mobility comes an increase in users accessing and using devices at various locations, including remote locations. And while users are able to be more productive and efficient both in and out of the office, security teams are fighting to protect a growing number of endpoints and securing data from myriad devices.

Smartphones | Tablets | Laptops | Printers

Organizations looking to safeguard mobile devices such as **smartphones, tablets, laptops and printers** can do so by following Zebra's mobile computing security best practices.

*Source

Zebra: Taking a Proactive Approach to Security

Securing devices and data is critical to smooth workflows and strong business performance. Zebra mitigates security risks and vulnerabilities by integrating devices with multiple layers of protection. Each of our solutions, devices and services are all designed to protect against common **security threats such as malware, phishing, cryptographic failures, insecure design and more**—without hindering productivity or accessibility.

As organizations become more interconnected, their network and sensitive data become more susceptible to unlawful access and numerous security vulnerabilities. Zebra mitigates security risks by following trusted pillars of cybersecurity principles and implementation of a defense-in-depth approach in our architecture and design process. With our smart, configurable technology, Zebra empowers businesses to strike a perfect balance between operational objectives and security.

From Zebra LifeGuard™
to Zebra Mobility DNA™

From Zebra LifeGuard™ to Zebra Mobility DNA™, Zebra ensures all devices are secure and compliant by following industry and internal best practices for robust security across enterprise devices.

Protect against common security threats:

Malware

Phishing

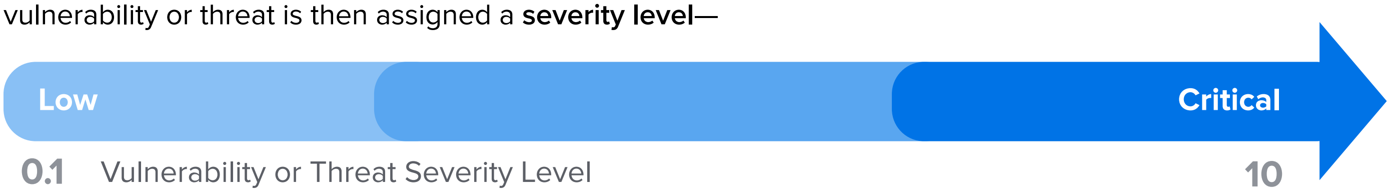
Cryptographic Failures

Insecure Design

Leveraging Past Vulnerabilities to Build Smarter Solutions

From the 2014 Zombie Zero attack method to the BlueBorne Bluetooth vulnerabilities found in 2017, Zebra is constantly analyzing and learning from past mobile device vulnerabilities. The insight has enabled us to build smarter, more robust security solutions specifically designed for today's unique mobile computing security challenges.

Each time a new vulnerability is detected, Zebra's team takes prompt action to prepare a patch based on the vulnerability classification, which is described and categorized based on the common vulnerabilities exposure (CVE) list. This list is rigorously managed by and contained in the National Vulnerability Database. The vulnerability or threat is then assigned a **severity level**—ranging from 0.1 for low and 10 for critical—from the **common vulnerability scoring system** (CVSS) and details what actions businesses must take to protect against the new threat.



Zebra also carefully monitors the Open Web Application Security Project (OWASP) which analyzes and reports on the top mobile vulnerabilities each year.

Among the top ten global vulnerabilities in 2021 were broken access control and injection flaws. To combat this, Zebra ensures that every top mobile vulnerability is thoroughly analyzed and the entire eco-system—both hardware and software—on our devices address existing mobile vulnerabilities. Our devices undergo many phases of security testing including internal security testing which involves analysis of the entire code (static and dynamic code analysis) as well as third party penetration testing. Our external third party pen testing is to ensure that security controls are in place as pen testers makes an attempt to bypass various layers of security controls just like a hacker in real world would try the various methods to hack the device.

Zebra ensures that every top mobile vulnerability is **thoroughly analyzed** and the entire eco-system—both hardware and software—on our devices address existing mobile vulnerabilities.

Zebra devices are developed in accordance with a corporate mandated software development lifecycle (SDLC), that ensure all Zebra software is developed and tested in accordance with strict security guidelines that needs to be followed in our SDLC. Strict implementation of principle of least privilege and application programming interface (API) controls ensure unauthorized users cannot access devices and thorough end-to-end testing of applications further enhances security. Zebra is continuously adding to our portfolio of security features each time a new threat is found.

Zebra meticulously tracks Android™ vulnerabilities and threats by monitoring CVE and OWASP and collaborates with vendors to provide appropriate patches, ensuring all mobile devices are protected against threats—both low and critical—via Zebra LifeGuard.

Meet Zebra LifeGuard

Designed to protect Zebra Android devices from cyberattacks, Zebra LifeGuard regularly delivers security patch updates to mobile computers. Organizations gain peace of mind knowing their devices are prepared for the latest security threats and enjoy the flexibility of updating devices on their own schedule.

LifeGuard features a number of tools designed to secure Zebra mobile devices, including:

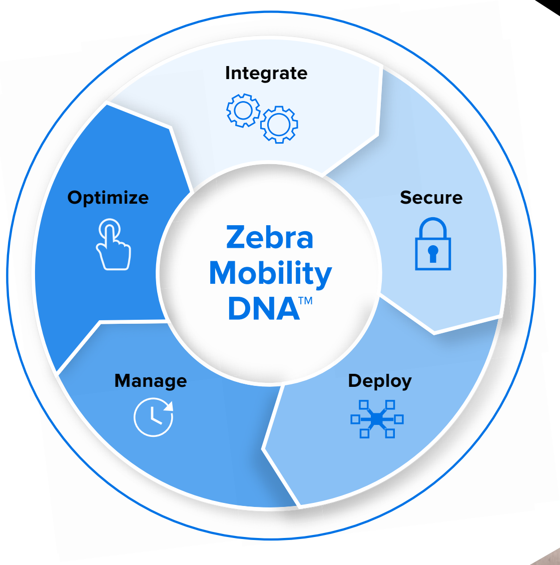
1. **Timely updates** to address new and emerging security threats
2. **Flexible update options**, enabling businesses to update devices based on their own needs
3. **Complete migration support** to minimize productivity disruptions
4. **Report-enabled visibility** for faster, easier management of the update process
5. **Single file updates** via Zebra Dynamic Packaging
6. **Detailed LifeGuard policies** for comprehensive security

LifeGuard was designed to follow security patch hygiene best practices as recommended by NIST guidelines. The Zebra team rigorously checks the latest vulnerabilities on the CVE and automatically sends out security patches, ensuring devices are protected against the latest vulnerabilities and organizations are maintaining good cyber hygiene.

With LifeGuard, **businesses enjoy comprehensive security and powerful security updates designed to protect all mobile devices, data and solutions**—all with the power to choose how, when and where updates take place.

LifeGuard

Simplify Device Lifecycle Management with Zebra Mobility DNA



Designed from thousands of use cases and decades of R&D, Zebra Mobility DNA is a suite of enterprise solutions that maximize mobile user productivity while minimizing IT complexities over the device lifecycle. The suite features numerous solutions designed to simplify and streamline mobile device lifecycle management—from integration to security and beyond. Zebra Mobility DNA optimizes your IT team's ability to respond to new and emerging security threats with features such as:

Principle of least privilege: In addition to limiting device access, Zebra goes a step further, enhancing the feature with detection of any escalation of privilege for system, application or components calls, etc.

Defense in-depth: Zebra's layered approach to security ensures data is completely secure—both in motion and at rest. Zebra's architecture protects each layer of a mobile device from vulnerabilities and analyzes them to provide protection for a true "defense-in-depth" approach. Zebra offers greater device protection against a world of security threats, reducing your risk and extending the lifespan of your device, hardware backed protection of firmware storage to ensure the OS and bootloader are not modified, end-to-end secure communications, and more.

LifeGuard for Android: Extend OS security support for up to 10 years of timely security updates.

LifeGuard OTA (Over the Air): Control and schedule device updates over the air via your enterprise mobility management software tool (EMM) to meet your business requirements for device security.

Compliance: With Zebra's security patch hygiene and automatic updates, organizations have peace of mind knowing their devices can help them comply with ever-shifting regulations such as Health Insurance Portability and Accountability Act (HIPAA) or Cybersecurity Maturity Model Certification (CMMC).

Enterprise Home Screen: Prevent operational disruptions and protect workforce productivity by customizing user views/access on device—specify apps users can access, disable device features and automatically launch apps.

Zebra Mobility DNA

Suite of enterprise solutions that maximize mobile user productivity while minimizing IT complexities over the device lifecycle.

Increasing Confidence in Mobile Device Security

Zebra strictly follows the **IT pillars of cybersecurity, providing confidentiality, integrity, availability, authenticity and non-repudiation with our products**. Zebra is trusted by heroes in public safety, first responders and federal and state customers. Zebra holds a number of security certificates, all of which increase user confidence in device security, including:

FIPS 140-2:

The Federal Information Processing Standard (140-2) defines security requirements related to the design and implementation of a cryptographic module. Zebra mobile computers employ multiple cryptographic modules that have been FIPS 140-2 validated, ensuring cryptographic operations perform as expected.

> Zebra's mobile computers have a FIPS 140-2 certificate, showing its capability in safely and securely managing encryption.

Common Criteria (CC):

Common Criteria (CC) for Information Technology Security Evaluation is an international standard (ISO/IEC IS 15408) for computer security certification. This certification is used by international governments, US federal agencies, financial institutions and other organizations that deal with sensitive data.

> All Zebra products as listed on the NIAP website meet the international standard for IT products and have been carefully evaluated for proper security features.

DoD STIG:

The Security Technical Implementation Guide (STIG) is a configuration standard consisting of information assurance (IA) and interoperability (IO) guidelines for hardening systems and devices to improve security posture.

> Zebra mobile devices meet configuration standards for IA and IO as well as Department of Defence (DoD) devices and systems. Zebra places particular emphasis on defining compliance to various risk categories and developing usage guides that are consistent with DoD policies.

DoDIN APL:

The Defense Information Systems Agency maintains the DoD Information Network (DoDIN) Approved Products List (APL) process on behalf of the US Department of Defense. This process provides a single, consolidated list of products that meet cybersecurity and interoperation certification requirements.

> Many Zebra products have qualified to be on the DoDIN APL list and are compliant with DoDIN APL security standards.

Elevated Trust with Trusted Execution Environment (TEE)

One mechanism organizations utilize to protect cryptographic operations and material is a trusted execution environment. This environment runs separately from a device's rich execution environment (REE) which executes the device's operating system and respective applications. In the TEE, code is able to execute with a high level of trust knowing that the environment is completely isolated from rest of the system. Any threats found in the rest of the device environment cannot impact TEE. Even if the REE is compromised, data within the TEE remains secure.

Zebra provides an additional layer of security to organization's TEEs with features such as the Enterprise Home Screen and others. For example, Zebra's Enterprise Home Screen allows admins to control which users have access to the environment, ensuring sensitive or confidential data is kept secure. And by following TEE best practices (which are included in all recently produced Zebra devices), TEEs are protected against new and emerging security threats.

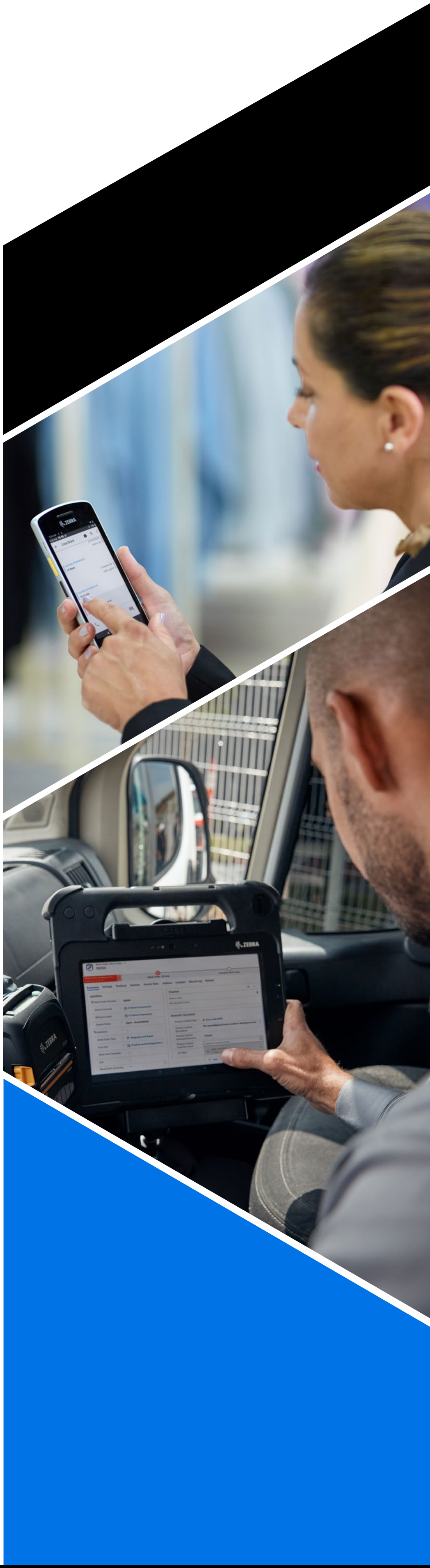
Zebra Enterprise Home Screen

1.	2.	3.
Allows admins to control users access	Ensures secure sensitive material	TEE's are protected against security threats

Zebra's Ethical Hacking Program

Zebra takes a proactive approach to security. Rather than waiting for security threats to happen, we regularly attempt to hack into our own devices in order to identify code vulnerabilities or system weaknesses. Once identified, Zebra quickly rectifies the issue—patching holes or creating a security patch to eliminate the vulnerability. This decreases the likelihood of cybercriminals identifying vulnerabilities and exploiting them, which could cause potentially devastating consequences.

Rather than waiting for security threats to happen, **we regularly attempt to hack into our own devices in order to identify code vulnerabilities or system weaknesses.**



Enhance Mobile Computing Security with Zebra

For more than **50** years we've been a leader in mobile device security, and have been committed to providing organizations with comprehensive security designed around industry best practices.

Our entire security solution portfolio is designed from the ground up to provide total security without compromising accessibility or scalability. When it comes to mobile device security, **no one provides more than Zebra**.

To learn more about how Zebra's safeguards your mobile devices with best-in-class security features, visit **www.zebra.com/product-security**

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
zebra.com/locations
la.contactme@zebra.com