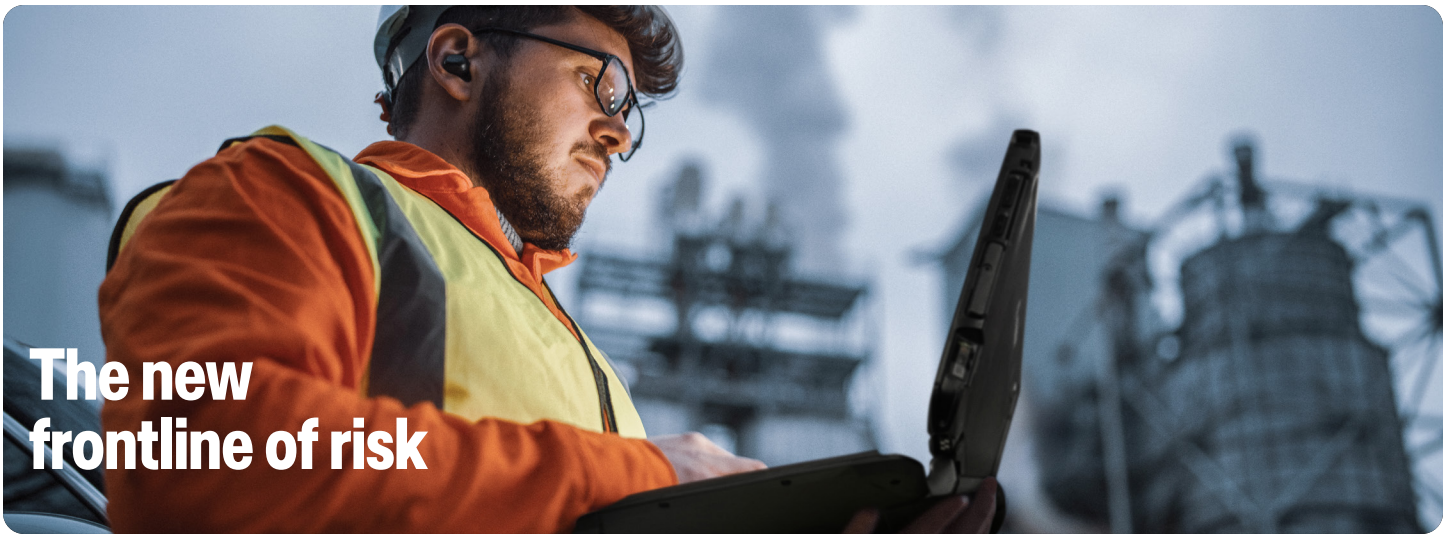
ZEBRA

Mobile computing security thought leadership

Move from risk management to operational resilience

Turn endpoint security into a source of operational strength



The new frontline of risk

Every endpoint—whether it's a mobile computer on the sales floor, a tablet in a patient's room, or a printer in the warehouse—lives inside a workflow. When that endpoint is compromised, the impact is immediate. Tasks are disrupted. Decisions stall and revenue dips.

The cost is measurable

Risk is increasingly tied to endpoints. Google reports that 40% of consumer-grade Android devices are at risk of new malware and spyware attacks[1]. With the average cost of a breach reaching $4.44 million, the implications are significant[2]. At the same time, Microsoft's Digital Defense Report finds that between 80% and 90% of successful ransomware attacks originate from unmanaged devices—the very laptops, phones, and tablets many organizations rely on[3].

Together, these trends point to a clear conclusion: Endpoint security is not just an IT concern; it is a primary driver of business.

Consider the operational impact

As environments grow, security often struggles to keep pace. Controls are layered on after deployment, and tools operate in silos. The result is friction—more workarounds, more IT effort, and less predictable operations.

A better way to think about security

Organizations that move past this pattern take a different view. They treat endpoint security as part of the infrastructure itself, something that keeps systems reliable, usable, and secure as the business scales.

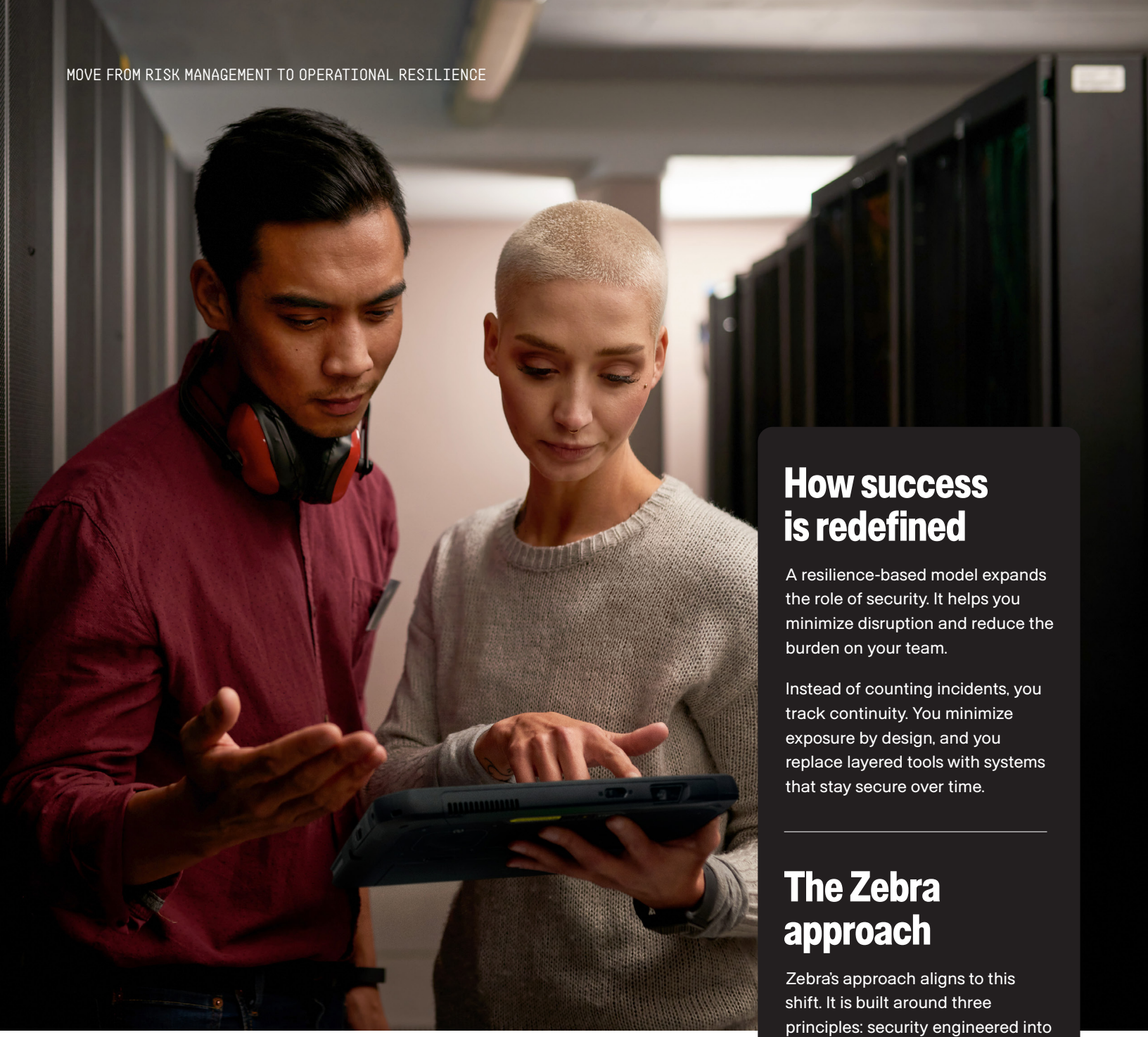
Exposure across endpoints

If a device connects to your network, handles data or supports frontline work, it's part of your endpoint environment and risk surface.

- Smartphones
- Tablets
- Laptops
- Kiosks
- Printers

Sources:

1. Google Issues Android Update—40% of All Phones Now at Risk, Forbes, Feb. 5, 2026
2. Cost of a Data Breach Report 2025, IBM, 2025
3. Microsoft Digital Defense Report 2023



How success is redefined

A resilience-based model expands the role of security. It helps you minimize disruption and reduce the burden on your team.

Instead of counting incidents, you track continuity. You minimize exposure by design, and you replace layered tools with systems that stay secure over time.

The Zebra approach

Zebra's approach aligns to this shift. It is built around three principles: security engineered into the foundation, lifecycle protection, and trust proven in real-world conditions. We'll explore each in the sections that follow.

Together, these create endpoints that are not only secure, but also stable and aligned to how your business run

Shift to proactive business continuity

If you follow a traditional model, you focus on protection: preventing breaches, responding to threats, and maintaining compliance. Those goals still matter. But they're not enough when business continuity defines success.

Security starts in the silicone

Most security issues start much earlier than an attack. They start with design decisions. When security is introduced late, gaps begin to form. Controls don't align. Enforcement varies. Teams compensate with manual workarounds, and small inconsistencies compound into real risk.

Hardened by design

A more effective approach is to build security into the software development lifecycle (SDLC) from the beginning. That means continuously analyzing code to catch issues early and limiting access to only the right people and applications. Security is validated at every stage—not just at the end—so problems are addressed before they can affect your operations.

Zebra's built-in security

Zebra takes this approach a step further by embedding security controls directly into the architecture of its devices. Protection isn't added later; it's part of how we build the system.

That includes firmware-level safeguards that help encrypt sensitive data and prevent unauthorized access. We align with stringent standards such as FIPS and EU RED, so compliance is integrated from the start.

Staying ahead of threats

At the same time, Zebra maintains a continuous security discipline. We monitor global vulnerability sources such as the Common Vulnerabilities and Exposures (CVE) database, prioritize risks using the Common Vulnerability Scoring System (CVSS), and validate against frameworks like the Open Worldwide Application Security Project (OWASP).

Zebra assesses, prioritizes, and addresses each vulnerability through a structured process that includes internal testing and independent testing. The outcome: Your environment becomes more resilient to new emerging threats.

What this prevents and protects

You reduce risk and when issues do arise, they're easier to contain. That is how you protect your reputation at its source. By preventing high-profile breaches before they ever reach your frontline, you avoid the long-term damage to your brand that can take years to recover.

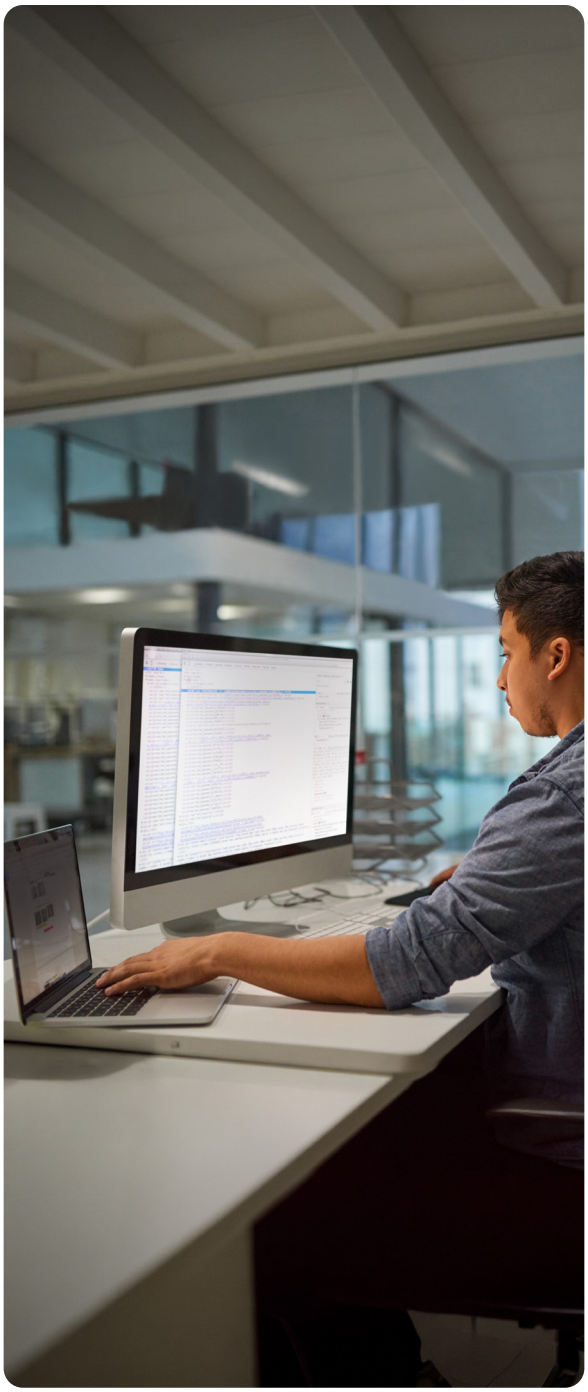
Addressing vulnerabilities at the source

We thoroughly analyze every mobile vulnerability and address it in both our hardware and software.

Security should last as long as your hardware

Your devices don't operate on short timelines. They often remain in service for years. During that time, new risks surface constantly, requiring a consistent and reliable approach to patching and protection.

Yet, this is where gaps often appear. Updates get delayed in hopes of avoiding disruption, and devices fall out of sync. All the while, risk is accumulating quietly in the background.



Turn security into a controlled, repeatable process

Zebra LifeGuard™ for Android™ gives you a structured, reliable way to keep devices secure on a monthly basis. Instead of reacting to updates as they appear, you manage them as part of a coordinated, repeatable system.

With LifeGuard's monthly updates, your endpoints stay current over their full lifecycle—long after consumer support windows. You control how and when updates are applied. Flexible options let you test, stage, and roll out changes in sync with your operations.

LifeGuard also reduces your operational burden. Track progress and address gaps without manual effort. LifeGuard gives you visibility into update status and compliance. Single-file update packaging simplifies deployment across large fleets, helping you maintain consistency at scale.

When change is required, migration support helps you move between Android versions with minimal disruption, preserving uptime and user productivity. What's more, you standardize how updates are governed across devices, so execution stays consistent, even as your environment grows.

Continuity without disruption

When you get this right, protection becomes part of your operating rhythm. Your endpoints stay current, and your risk stays controlled. You maintain operational continuity by avoiding disruptions that can cost up to $100,000 per hour in critical environments[4]. You also eliminate the steady drain caused by outdated or poorly managed endpoints.

Sources:
4. ITIC 2024 Hourly Cost of Downtime, 2024.

Simplify how you manage security at scale

As your endpoint environment grows, so does complexity and risk. Every additional device introduces variation—in configurations, permissions, and update states. Over time, that variation creates inconsistency, and inconsistency weakens even the strongest security strategy. The solution isn't adding more tools. It's creating a more integrated way to manage your environment.

Bringing control and consistency with Zebra DNA

Zebra DNA™ is a suite of enterprise capabilities built into Zebra devices that simplify how you deploy, secure, manage, and optimize your endpoints across their entire lifecycle. It gives you a unified way to manage the full device journey, while reducing reliance on fragmented systems and manual intervention.

Many organizations already depend on enterprise IT and security tools to monitor and protect their environments. Those systems are essential, but they operate at the network, application, or user level. Zebra DNA extends that control directly to the device itself, giving you visibility and enforcement at the point where work happens.

At the core of Zebra DNA are Mobility Extensions (Mx), Zebra's enterprise layer that hardens consumer-grade Android. Mx gives you precise control over how your devices are configured, secured, and used.

Unlike consumer operating systems, which prioritize end-user flexibility, an enterprise OS prioritizes control, consistency, and security. With Mx, you shift control to the administrator—defining how devices behave, what users can access, and how data is handled. This is especially critical in frontline environments.

You can automate configuration and certificate deployment, enforce consistent policies across your fleet, and control user access through tools such as Enterprise Home Screen, ensuring each device is used exactly as intended.

This approach reinforces the principle of least privilege, so every device, application, and user has only the access required—nothing more. Combined with a layered, defense-in-depth model, security is applied consistently across hardware, OS, and applications without adding operational complexity.

Operational stability at scale

As a result, security becomes easier to manage—and more reliable. You can support compliance with evolving requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Cybersecurity Maturity Model Certification (CMMC), without constant manual effort.

You spend less time managing exceptions and more time maintaining control. That stability supports continuity across your operations, helping your teams perform without interruption.

Ensure your security is ready for the real world

In your environment, trust has to be proven, validated, and continuously verified. That means going beyond internal validation and aligning with recognized standards.

Standards that matter

Know that Zebra devices are validated against government-grade requirements. Zebra designs its endpoints to meet frameworks such as FIPS 140-3 for cryptographic validation. It also performs Common Criteria (CC), an internationally recognized benchmark for security evaluation. Configuration guidance is generated by DISA in their Security Technical Implementation Guides (STIG), helping you harden systems based on proven practices. These validations reinforce government's use in highly secure and mission-critical environments.

Beyond certification

Certification alone is not enough. Zebra reinforces this with active third-party penetration testing. This includes ethical hacking programs that simulate real-world attack scenarios. Vulnerabilities are identified, disclosed transparently, and addressed before the products are ever shipped.

This same commitment extends to how devices are built and delivered. Zebra maintains a secure, traceable supply chain, validated by enterprise and government customers. That translates into trust in how your endpoints perform as well as where they originate. Such confidence extends beyond IT. It strengthens trust in your systems, your data, and your brand.

Zebra proactively tests our own devices

We regularly attempt to hack into our own devices to identify weaknesses in the code or system.

The fortress stack: protection from firmware to cloud

Some endpoints operate in dynamic environments. Networks change and threats evolve. A single layer of protection cannot keep up with that complexity.

Defense in depth explained

You need a layered approach—often called defense in depth—where protection spans hardware, operating system, application, and data layers.

Zebra implements this across the stack. Hardware-level safeguards help prevent unauthorized modification of firmware and core system components. Secure communication protocols protect your data as it moves and while it is stored.

Containing risk in practice

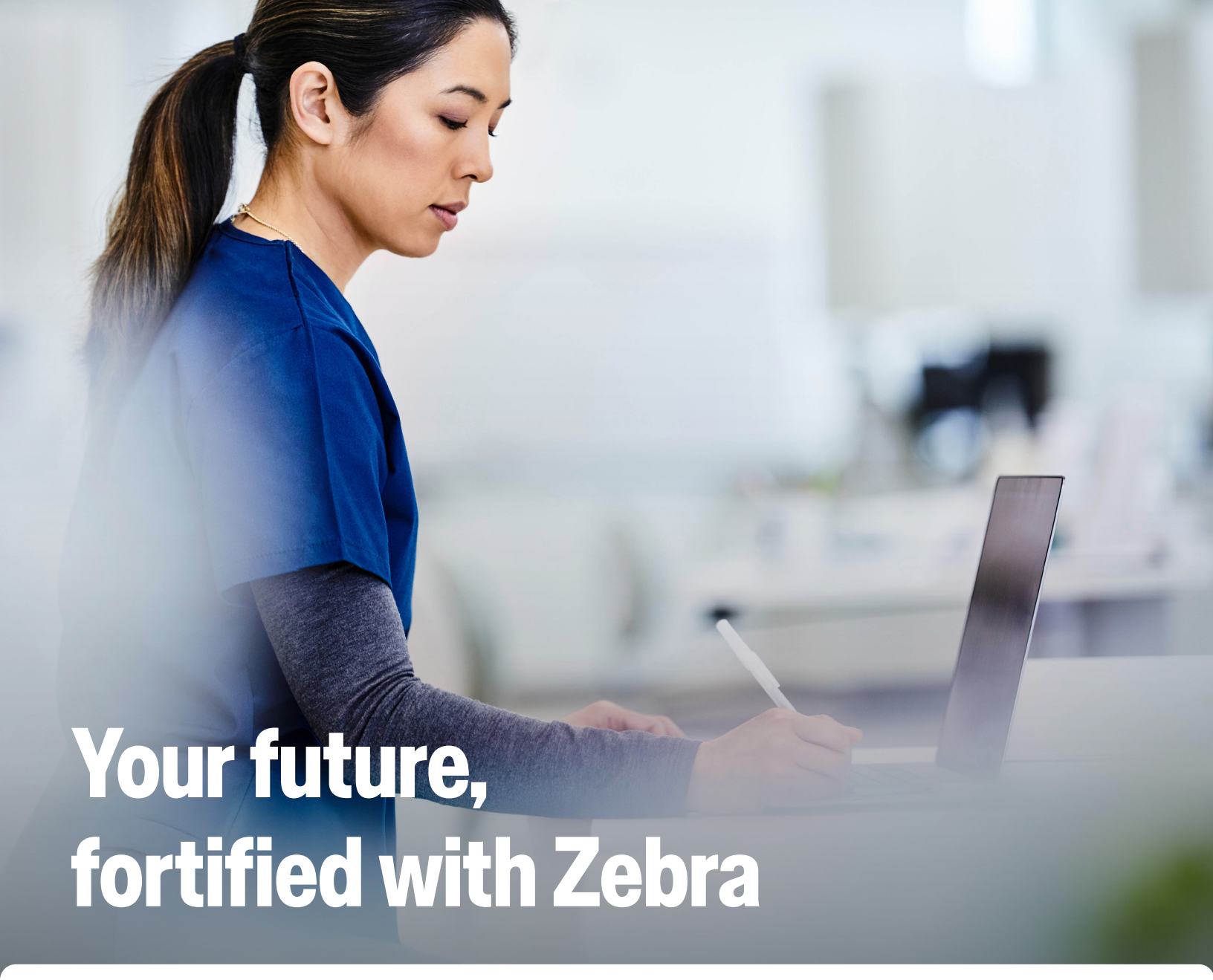
At the same time, sensitive processes are isolated within trusted execution environments (TEE). These environments run independently from the main system. Even if another part of the device is compromised, critical operations and sensitive data remain protected.

This isolation is applied to high-trust functions, such as authentication and encryption. It ensures these processes execute in a secure enclave that is separated from everyday applications and the operating system.

Administrative controls further reinforce this model. You can define how devices are used and what users can access, helping prevent misuse before it becomes risk. This containment model changes how risk behaves in your environment. Instead of a single issue escalating into a larger incident, it is isolated and contained.

Safeguarding innovation

That is what resilience looks like in practice. It also protects your innovation, safeguarding the data, intellectual property, and investments that define your competitive advantage, ensuring integrity across every interaction.



Your future, fortified with Zebra

Combining these capabilities not only strengthens endpoint security, but also establishes a foundation for uninterrupted uptime, consistent data integrity, and better protected brand reputation.

A root of trust across your environment

Zebra delivers enterprise-grade governance across your entire endpoint portfolio. Backed by more than 55 years of experience in frontline environments, this approach reflects a deep understanding of how security must perform in the real world. At the core is a verifiable root of trust—a security model designed to ensure your devices behave as expected from the moment they power on and throughout their lifecycle.

ZEBRA

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