ZEBRA

Mobile computing security thought leadership

Uptime is now a security metric

Why endpoint control has become a strategic priority for IT leaders

Risk has moved to your workflows

Understanding the shift

As an IT leader, you ensure your enterprise perimeter is well defended. Your network controls are stronger than they were a decade ago. You mature your identity governance and increase the capabilities and automation of your security operations centers.

Yet, the risk is not shrinking. It is shifting. As work becomes more distributed, so does risk. It moves into the technology that powers everyday operations.

Endpoints are no longer secondary infrastructure

In most industries, workers' technologies sit directly inside essential workflows. They scan medications, verify inventory, print labels, route tasks, update records, and move information across physical and digital environments.

Where control matters most

However, these endpoints often operate outside the direct control of traditional security layers. When those devices are misconfigured, unpatched, or insufficiently controlled, the impact lands immediately on operations. Productivity suffers. Data exposure grows, and incident response becomes more difficult.

The new reality

Security is no longer defined by what is blocked at the perimeter, but by what is controlled at the endpoint. We'll address this core issue in this paper, offering strategic practices to bolster endpoint security, and in turn, business resilience.

90% of successful cyberattacks and as many as 70% of successful data breaches originate from endpoints[1]

Sources:
1. 2023 Mobile Security Index Report, Verizon

Close the security gap

Why your existing stack needs a hardened foundation

Most enterprises don't ignore endpoint security. Instead, they lean on the tools they already trust. Your team has likely invested heavily in identity platforms, network monitoring, MDM, and cloud controls. Each plays a vital role in your defense. However, their center of gravity often sits above the device itself, rather than within it.

That distinction is critical. While a network control identifies traffic and an identity platform authenticates a user, neither can guarantee that the physical endpoint is hardened, restricting local attack surfaces, or aligned with your policy after years of heavy use.

Restoring confidence at the edge

The endpoint gap rarely appears as a sudden crisis; it emerges as "configuration drift" as fleets expand. Bit by bit, security becomes less uniform than leadership assumes. Workers' unmanaged technology creates an outsized opening for attackers, but they also make the environment harder to govern, standardize, and recover.

The good news is that this gap is addressable. By bringing endpoints back into alignment, you restore the consistency your entire security stack relies on.

Integrity by design

Security starts before deployment

The most effective endpoint strategies evaluate how security is built and governed before the technology ever reaches the frontline. You aren't just selecting hardware; you're choosing a security posture your team will manage for years.

Built-in security from policy to practice

Consumer devices prioritize flexibility, but enterprise environments require predictable behavior and enforceable policy at scale. Fortunately, you don't have to choose between performance and security. Zebra delivers endpoints that perform at scale without weakening critical protection.

Engineering for compliance and trust

Zebra embeds security across the software development lifecycle (SDLC), utilizing continuous code analysis and threat modeling validated against CVE, CVSS, and OWASP frameworks. This discipline ensures that regulatory readiness is "baked in". Look for this degree of endpoint support:

- **Government-grade encryption** and secure boot to protect data at rest and in motion
- **Access controls** aligned to FIPS 140-3 and EU RED standards, simplifying compliance without the need for layered, third-party add-ons
- **Traceable supply chains** that reduce tampering risks and ensure technology integrity from the factory to your facility
- **Proactive vulnerability management** to identify and remediate emerging threats with speed and transparency

Enforce control where work happens

Turn policy into consistency

The challenge is not defining policy but ensuring thousands of endpoints in the field behave according to that policy.

Zebra DNA turns your security model into an operational reality. With this comprehensive suite of enterprise tools, you can enforce consistency at the point of use.

How Zebra DNA strengthens your security posture

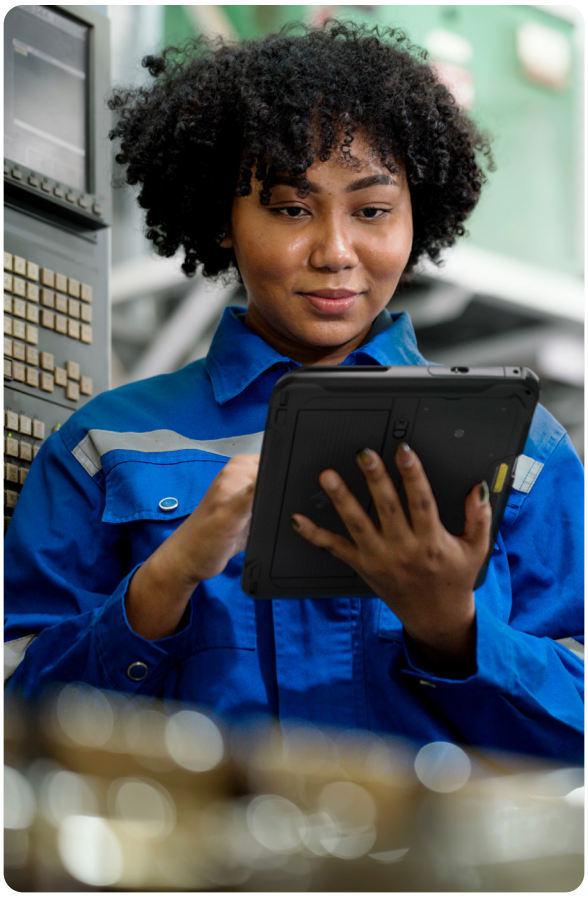
Operational Challenge	Zebra DNA
Unauthorized data transfer	**Restricted hardware access:** Lock down USB, Bluetooth and NFC at the firmware level.
Untrusted network entry	**Certificate-based authentication:** Ensure only validated users and devices gain access.
Expanded attack surface	**Govern interfaces:** Lock down the UI to mission-critical apps and disable unused services.

Extend governance to the printer fleet

Printers often process sensitive data, connect to your network, and operate continuously in critical workflows. Yet, they are a frequently overlooked risk surface.

Zebra PrintSecure—part of the Zebra DNA ecosystem for printers—applies the same rigorous standards of endpoint-level integrity to your thermal print ecosystem.

With it, your team can actively assess vulnerabilities against best practices, block unauthorized access, and automate certificate management, as well as security configurations.



Critical endpoints are out of compliance with internal security and performance policies 22% of the time[2].

Sources:
2. Absolute Security Research, 2025

Sustain security across the device lifecycle

Keep devices secure with controlled updates

Mobile computers, tablets, wearable devices and kiosks remain in service for years, often in operational settings where uptime is critical and change must be carefully managed. Over time, security degrades without proper governance.

Consumer-grade models only compound the issue. They prioritize rapid refresh cycles, not multi-year enterprise lifecycles. Their updates follow vendor timelines, making consistency difficult to sustain.

Inconsistency becomes systemic at scale

At smaller scales, manual correction is possible. At larger scales, however, inconsistency becomes systemic. That's why endpoint management requires a more integrated approach.

Manage updates as a controlled process

Zebra LifeGuard™ for Android gives you a structured, reliable way to maintain security on a monthly basis. Instead of reacting to updates as they appear, you manage them as part of a coordinated, repeatable process aligned to your operational requirements.

You control how and when updates are applied. You can test, stage, and roll out changes in controlled waves, reducing disruption, while keeping devices current well beyond typical support windows.

Maintain visibility and control

LifeGuard also simplifies lifecycle management at scale. You gain visibility into patch levels, compliance status, and rollout progress across your fleet. This lets you identify gaps and take action without manual effort. Single-file update packaging streamlines deployment, helping you maintain consistency across thousands of endpoints.

Preserve uptime while staying current

When change is required, you move between Android versions with minimal disruption, preserving uptime and user productivity. Instead of managing drift, you maintain consistency, sustaining endpoint security over time.

55 days

Avg. time for IT teams to remediate 50% of critical vulnerabilities[3]

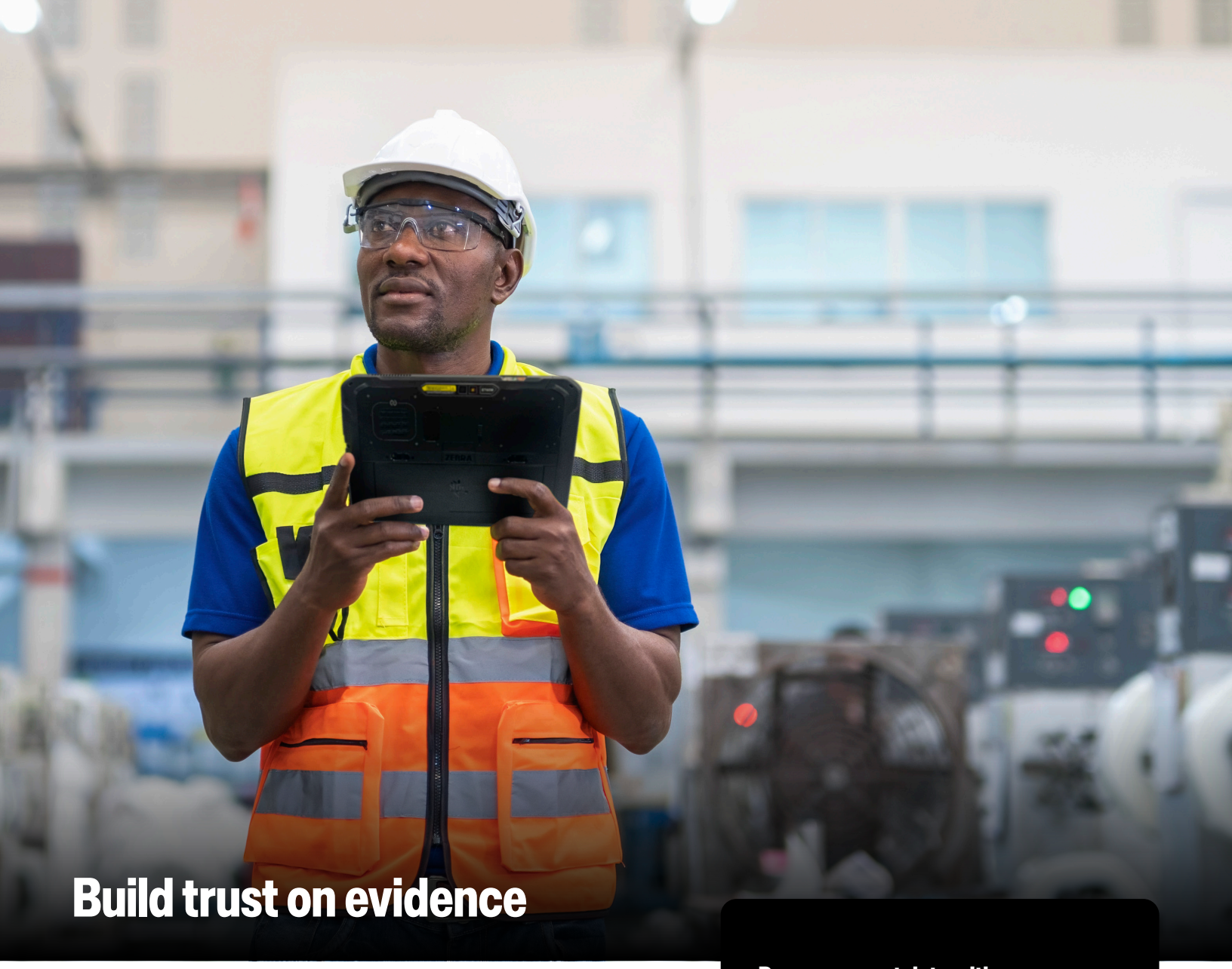
versus

48 hours

Avg. time for bad actors to weaponize code[4]

Sources:

3. 2024 Data Breach investigations Report, Verizon;
4. Hackers Are Getting Faster—48 Minutes and You're Cooked, Davey Winder, Forbes, Jan. 28, 2025



Build trust on evidence

Verify at the edge

As an IT leader, you understand that trust must be grounded in evidence. A strong design and disciplined lifecycle reduce risk, but validation ensures those controls hold under real-world conditions.

Measurable security for immeasurable confidence

Vulnerabilities are identified and prioritized using standard scoring methods, then addressed through a structured remediation process with coordinated disclosure. This external validation makes trust measurable, reinforcing your confidence that your endpoints will perform securely in production.

Remove uncertainty with real-world testing

To ensure your fleet can withstand evolving threats, Zebra employs continuous third-party penetration testing. This includes ethical hacking simulations that target the following attack surfaces:

- **Device firmware** and core system integrity
- **Operating system layers** to ensure hardening remains effective
- **Application interfaces** where data is most vulnerable

Turn security into your strongest asset

Your existing security investments remain essential. Extending that control to the point of work completes the model.

By choosing frontline technology that is secure from the start, controlled in use, sustained over time, and continuously validated, you turn protection into a source of operational strength. Operations run with fewer disruptions. Teams spend more time on strategic initiatives, and compliance becomes easier to maintain. That's a foundation upon which you can build your uptime, reputation, and competitiveness.

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