ZEBRA

Security Thought Leadership

Endpoint security is now business-critical

Why the modern threat landscape makes robust protection a business imperative

Work no longer happens within a fixed network perimeter. It now moves across warehouses, delivery routes, retail floors, healthcare environments, and more—powered by a growing ecosystem of endpoints.

From mobile computers, to scanners, kiosks, POs solutions, and printers, these endpoints act as gateways to systems, data, and operational continuity across the world. Organizations have invested heavily in securing networks, cloud services, and data centers, but **endpoint security** hasn't always been prioritized. Failing to block compromised firmware and prevent privilege escalation that allow harmful applications to execute, together with neglecting essential encryption and patching, all create critical vulnerabilities that often remain invisible until it's too late. The average cost of a data breach **exceeds $4 million** globally, with impact extending beyond immediate financial loss. Operational downtime, supply chain disruption, regulatory exposure, and long-term damage to brand trust can all originate from a single compromised endpoint.

Endpoint risk is everywhere, and often invisible. This paper shows where risk hides, what's missing, and how to secure it.

Every endpoint tells a security story

As organizations scale operations, security challenges shift. Businesses now rely on fleets of distributed endpoints across locations, networks, and use cases. Though they are essential to productivity and efficiency, they also introduce new points of exposure that are difficult to see and control. The accumulation of small, often overlooked gaps compounds into a broader, harder-to-detect risk. Here are some examples:

Insecure endpoint foundation

If an endpoint allows a modified operating system to run because of an insecure boot process, attackers can bypass security controls before it is even fully operational.

Broken chain of trust

When applications can't verify endpoint security, sensitive workflows like payments or authentication become vulnerable.

Unknown or unverified applications

Pre-installed or downloaded apps may introduce unknown behaviors, including unauthorized communication outside the organization.

Weak or absent integrity checks

Without reliable attestation, applications can't confirm whether an endpoint has been compromised, putting sensitive workflows at risk.

Unsecured data in transit

Without encryption, communications can be intercepted, altered or blocked, impacting both security and operations.

Individually, these issues may seem manageable. Together, they create an environment where trust is uncertain. That's when a single compromised endpoint can quickly cascade across the business—impacting finance, workflows, uptime, and, ultimately, customer trust.

The hidden risk of "lower-cost" endpoints

Investing in budget-friendly endpoints may seem like a smart decision. But when it comes to security, the true cost is revealed over time.

Many lower-cost endpoints are designed with a focus on upfront affordability, not on long-term protection. Though features and specs look good on the surface, when it comes to performance and security in the real world, that's when they start falling short and can easily become expensive liabilities.

Complex and costly breach recovery

Security gaps not only increase exposure but also create ongoing operational challenges:

Regulatory fines

Significant financial penalties for non-compliance with strict, data protection regulatory standards (e.g., FIPS, HIPAA, PCI).

Operational downtime

Direct business disruption and lost productivity due to compromised endpoints.

Brand damage and loss of customer trust

Erosion of reputation and customer loyalty.

Increased cyber insurance premiums

Increased costs or reduced coverage for cybersecurity insurance.

Unplanned hardware upgrades

Premature replacement of endpoints due to lack of long-term security support.

Reduced IT productivity

Diversion of IT resources from strategic initiatives to reactive troubleshooting

Lost business opportunities

Inability to meet security mandates required for key contracts.

A different way to look at cost

When security is treated as optional, organizations end up compensating elsewhere: through added controls, reactive fixes, or incident response.

In today's mobile-first enterprise landscape, the proliferation of mobile endpoints is a double-edged sword. While these endpoints have unlocked unprecedented productivity and efficiency, they have also introduced a host of new security vulnerabilities. A single compromised endpoint can be a gateway for malicious actors, leading to data breaches, operational disruptions, and significant financial and reputational damage. It is then imperative to evaluate endpoints not just by purchase price but, most importantly, by built-in protection, ability to verify endpoint integrity, consistency over time, and total cost of ownership across the lifecycle.

The most cost-effective endpoint is the one you can trust, manage, and secure over time, not the one with the lowest upfront cost.

An intelligent approach to security: Defense in Depth

"Defense in Depth" is the foundation of Zebra's approach to security. This approach is based on the fact that attackers look for small gaps through which they can connect. When those gaps are linked together, they can move from limited access to full control, leading to data breaches, operational disruptions, and significant financial and reputational damage.

This is how to respond to these threats

This approach moves beyond creating a single layer, such as relying solely on network security like firewalls that are useless once breached or bypassed. True security requires building a series of defensive barriers directly into the endpoint itself in addition to network defenses. This multi-layered approach is what cybersecurity experts call Defense in Depth.

Zebra brings this Defense in Depth approach to life through a comprehensive, six-layer security framework—designed to protect endpoints from the moment they are built to the end of their operational life.

The Zebra 6-layer security framework

This is not a collection of isolated features. It's a comprehensive multi-layered framework where each layer strengthens the others, creating a resilient security system. Together, these six layers provide a continuous chain of trust, control, and visibility.

Layer 1 — Secure by design: A rigorous process

Mandatory security requirements
Apply to all software deliverables with proof of compliance demanded before any code can be integrated.

Intensive code scanning
Validated through both automated scanning (SAST/DAST) and intensive manual peer reviews. Identified vulnerabilities are tracked and remediation is managed at the highest levels of the organization.

Consistent auditing
Done by multiple groups outside the development team to ensure compliance and effectiveness. This ensures the security is embedded into the DNA of every product, enabling all the technical layers that follow.

What this means for you

Security built in early gives you more confidence in the endpoints you deploy.

Layer 2 — Endpoint integrity: Immutable hardware Root of Trust

The attackers first move is to try and replace the operating system

The attack
An attempt to boot the endpoint with a custom, unsigned OS loaded with malicious software.

The defense
Security starts with an unchangeable hardware Root of Trust embedded in the endpoint. This foundation triggers Secure Boot and Android Verified Boot, creating a chain where each component verifies the next. If any software is altered or not properly signed, the chain breaks and the endpoint won't boot.

What this means for you

Each endpoint starts in a known, trusted state, every time.

Layer 3 – Trusted operation and lockdown

Blocked from replacing the OS, the attacker shifts their focus on getting a malicious application running or reconfiguring the endpoint to weaken its defenses.

The attack
An attempt to copy a malicious application or access management tools to reconfigure the endpoint.

The defense
Zebra's lockdown policies turn the endpoint into a purpose-built tool by creating multiple layers of defense. They block unauthorized file transfers, prevent unapproved apps from appearing or being launched, and enforce allowlists at the OS level so only trusted applications can run.

Even if an attacker bypasses one layer, additional controls stop execution, and the endpoint's own management tools are secured to prevent tampering or reconfiguration—ensuring security holds at every step.

What this means for you

A tightly controlled environment that minimizes unintended behavior and reduces exposure.

Layer 4 – Privilege escalation prevention

The attacker finds a vulnerability in a legitimate, approved application and attempts to escalate its privileges.

The attack
Through an exploit, the attacker's code begins running and attempts to gain powerful, system-level permissions.

The defense
Zebra prevents privilege escalation by never granting third-party apps full system-level access. Instead, MX Access Manager provides precise, controlled permissions, allowing administrators to give trusted apps only what they need.

This keeps any untrusted or malicious code confined to a low-privilege sandbox, unable to escalate access or cause harm.

What this means for you

Threats are contained before they can expand their reach.

Layer 5 – Compromise detection

In the highly unlikely event an attacker bypasses all previous layers, the final layer is to detect the unauthorized activity in real time.

The attack
The attacker's malware is active and attempts to collect sensitive data and transmit it back to their own server, mimicking the data exfiltration seen on less secure endpoints.

The defense
Our defense is built on a local fail-safe called MX Threat Manager. Rather than watching network traffic, it continuously monitors the state of the OS and management client. If it detects a critical integrity breach—such as unauthorized root access or tampering with security settings—it triggers an automated, local countermeasure. This ensures the device is wiped or locked immediately on the endpoint, preventing data exfiltration before a breach can even begin."

What this means for you

You're not guessing; you can verify and respond with confidence.

Layer 6 – Ongoing lifecycle commitment

Security is not a one-time event; it is a commitment that must last for the entire life of the endpoint. An endpoint that is secure on day one can become vulnerable by day one hundred if it is not continuously defended against new threats.

The attack
An attacker waits months or years after an endpoint is deployed, then uses a newly discovered vulnerability against the now outdated and undefended software.

The defense
Zebra's lifecycle security combines long-term patching with proactive threat detection. LifeGuard™ for Android™ delivers up to 10 years of regular security updates, ensuring vulnerabilities are quickly addressed and endpoints remain protected over time.

In parallel, Zebra actively identifies risks through penetration testing and bug bounty programs, fixing potential issues before attackers can exploit them.

What this means for you

Security that stays current without constant endpoint replacement.

Bringing all together

In this complete framework, each layer plays a distinct role but their strength comes from how they work together. From hardware integrity to application control and ongoing validation, Zebra creates a system where trust is established early, maintained continuously, and verified when necessary.

The result is not just stronger security; it's a more stable, predictable, and resilient foundation for your operations.

Verified, not assumed

Security is not something you can afford to assume. It has to be proven.

That's why Zebra's approach goes beyond architecture and design. It is continuously validated through independent certifications, rigorous testing, and ongoing scrutiny to ensure that protection holds up in real-world conditions.

Zebra endpoints are evaluated against globally recognized standards such as:

FIPS 140 and Common Criteria and are trusted in the most demanding environments. These certifications provide objective, third-party verification of security capabilities and are evidence that Zebra endpoints meet the strict requirements of governments and regulated industries worldwide.

Furthermore, Zebra proactively engages in continuous third-party penetration testing and ethical hacking programs to simulate real-world attacks, identifying and addressing potential vulnerabilities before they can impact your operations.

What this means for your business

It creates a foundation that helps your organization:

- **Ensure business continuity and maximize uptime:** By preventing malicious takeovers, unauthorized reconfigurations, and ransomware attacks that can halt operations, keeping endpoints always ready for business-critical tasks.
- **Safeguard your sensitive data and corporate network:** By protecting both data on the endpoint and preventing a compromised endpoint from being used as a beachhead to attack your broader corporate network.
- **Protect your brand and customer trust:** By providing a verifiable, multi-layered security posture that defends against a public data breach so you can maintain customer trust and avoid long-lasting damage.
- **Maximize your return on investment (ROI):** By committing to long-term security through LifeGuard™. This protects your hardware investment for up to a decade and avoids the costly cycle of premature endpoint replacement forced by abandoned security support.

The Zebra commitment to security

Security is a core part of Zebra's culture and engineering processes, not an afterthought. A multi-layered, verifiable defense strategy protects customers' data, operations, and reputation.

Nothing is left to chance across the entire endpoint lifecycle—through ongoing updates, validation, and support that keep pace with evolving threats.

A moment to reconsider your approach

As mobile business environments continue to grow, it's worth asking:

- Do your endpoints start from a foundation you can truly trust?
- Can you verify their integrity, at any moment, across your environment?
- Are they designed to stay secure over time?

Move forward with confidence

Whether you're reassessing your current security environment or planning for the future, Zebra can evaluate where you are today and help you build a foundation that's secure, resilient, and ready to scale.

→ **Contact a Zebra Security expert**

ZEBRA