ERICSSON

In partnership with

TD SYNNEX

IoT survival guide 2026:

Four rules every IT leader needs to know

Practical strategies to prepare your organization for the next wave of IoT challenges

Image courtesy of Adobe Stock

Welcome to uncharted IoT terrain

The year ahead isn't business as usual — it's survival of the fittest.

The 2026 IoT landscape represents new territory. The environment is changing fast: LTE is being phased out, artificial intelligence (AI) is transforming both opportunities and threats, and attackers are more sophisticated than ever. Meanwhile, IT teams are leaner, budgets are tighter, and the number of connected devices continues to climb into the tens of billions.

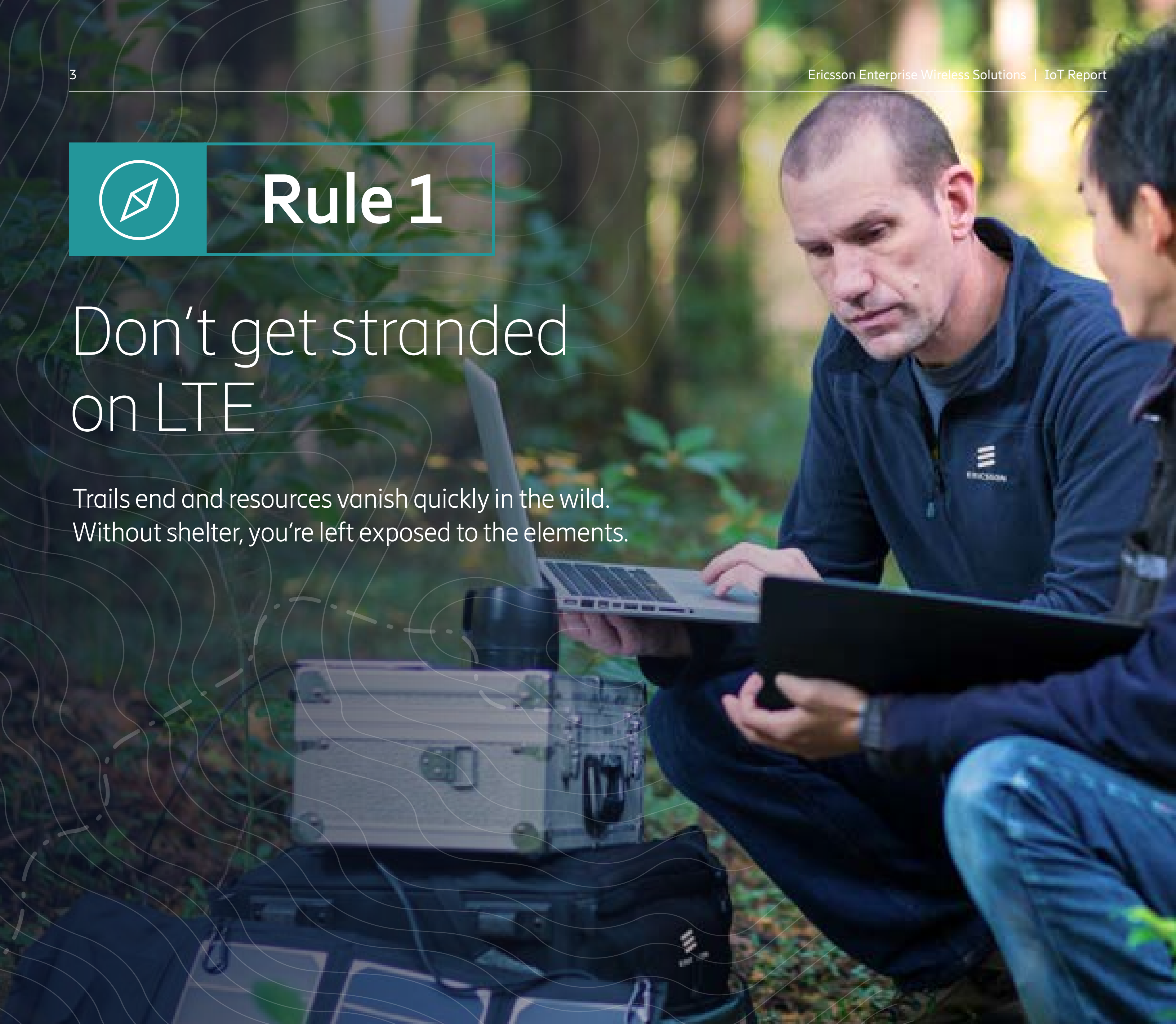
For CIOs and IT leaders, this isn't a gentle hike; it's a high-stakes expedition. The landscape is uncharted, the trails are converging, and the margin for error is razor-thin. Those who wander unprepared risk stranded assets, rising costs, or vulnerabilities that could compromise their entire enterprise.

But those who prepare will do more than endure the excursion. They will be poised to thrive.

That's the purpose of this survival guide. Think of it as your field manual for navigating the dynamic IoT environment in 2026. Each rule is rooted in a core trend that will shape the year ahead: the migration from LTE to RedCap, the need for zero trust security, the rise of AI as a critical tool, and the convergence of networks into one streamlined architecture.

Like any seasoned outfitter worth their salt, Ericsson doesn't just hand you a map; we equip you with the tools, expertise, and support to make the journey with confidence.

Image courtesy of Adobe Stock



Rule 1

Don’t get stranded on LTE

Trails end and resources vanish quickly in the wild. Without shelter, you’re left exposed to the elements.

LTE spectrum is being reframed for 5G. For enterprises that rely on LTE, the risks include degraded performance, increased costs, and ultimately, disconnection. Those who stay put will be stranded. RedCap 5G is the reliable shelter.

RedCap (Reduced Capability) 5G is a simplified version of 5G technology designed specifically for IoT. It’s strong, affordable, and designed to last. With routers that are only 10–20% more expensive than LTE, RedCap provides 5G-grade performance without the full 5G price tag. It extends device lifecycles for 5–10 years or more, supports tens of thousands of endpoints in a single network, and adds durability through features such as slicing, better uplink robustness, and LTE fallback.

Any industry deploying IoT at scale can benefit from RedCap 5G.

Where it matters

Any industry deploying IoT at scale can benefit from RedCap 5G’s balance of cost, efficiency, and longevity.

What IT professionals need to know

LTE is a dead-end path. RedCap is the shelter that keeps your deployments protected and operational as the environment shifts.

Ericsson equips you with migration strategies and connectivity solutions that make RedCap a dependable refuge during the 5G transition.

Rule 2

Trust no one, secure everything

In the wilderness, the greatest dangers are often the ones you don't see coming: hidden predators, sudden ambushes, silent hazards.

IoT dramatically expands the attack surface. Every sensor, camera, or controller becomes a potential entry point for malicious activity. IoT devices are typically:

- Limited and low-power, so they're unable to run sophisticated on-device security
- Have the same password they shipped with
- Broadcast their IP address, making them an easy-to-find target
- Unable to run a browser or agent for security
- Physically exposed to tampering
- Interconnected, so one compromised device can put the entire enterprise at risk

Meanwhile, attackers are evolving. Today's AI-driven attacks can probe networks more quickly and creatively than human adversaries. Quantum computing is poised to disrupt encryption standards in the near future. The risks are multiplying as fast as the devices are.

Zero trust networks are an indispensable survival discipline for IoT. Instead of assuming devices are safe once they're "inside the camp," zero trust treats every access attempt as untrusted until proven otherwise.

> Zero trust networks are an indispensable survival discipline for IoT.

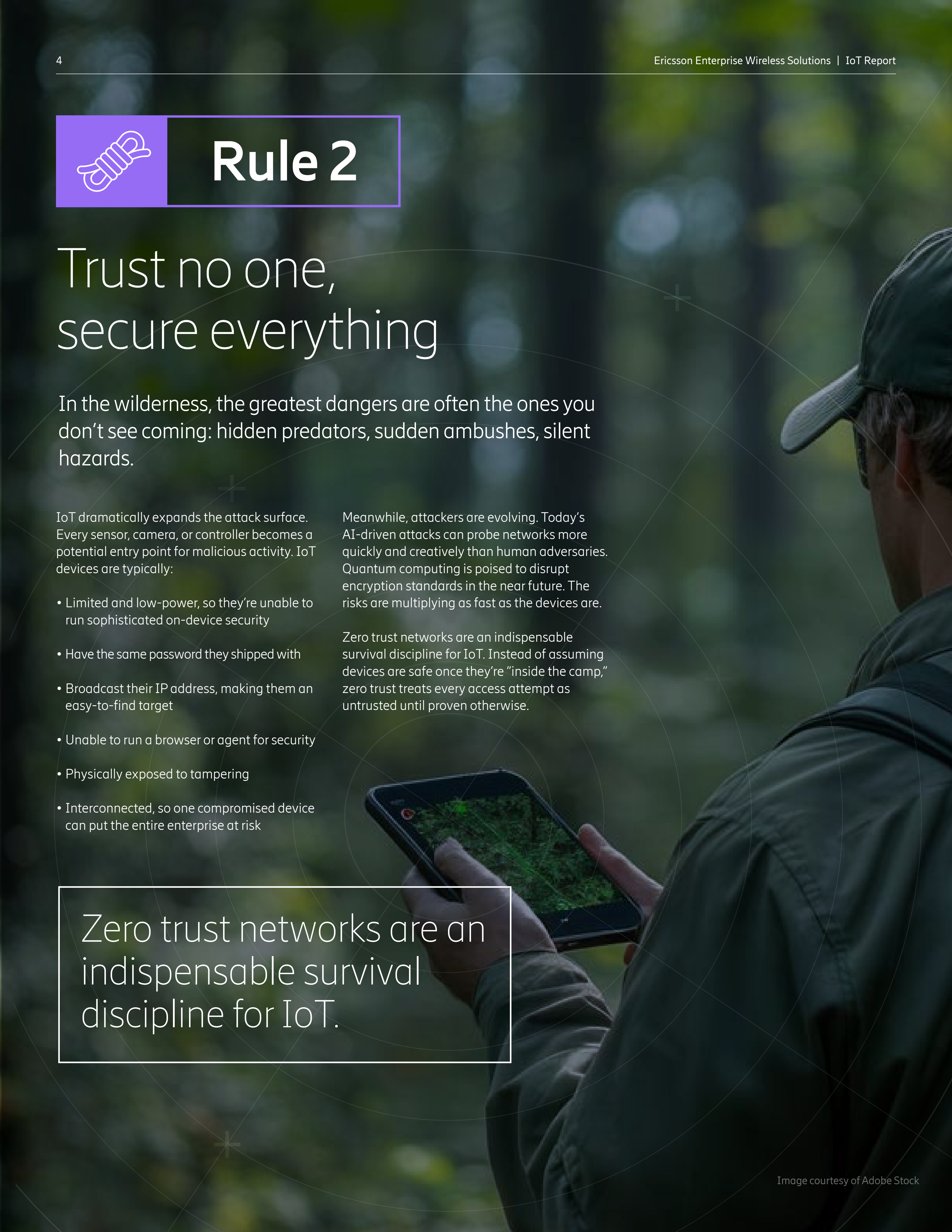
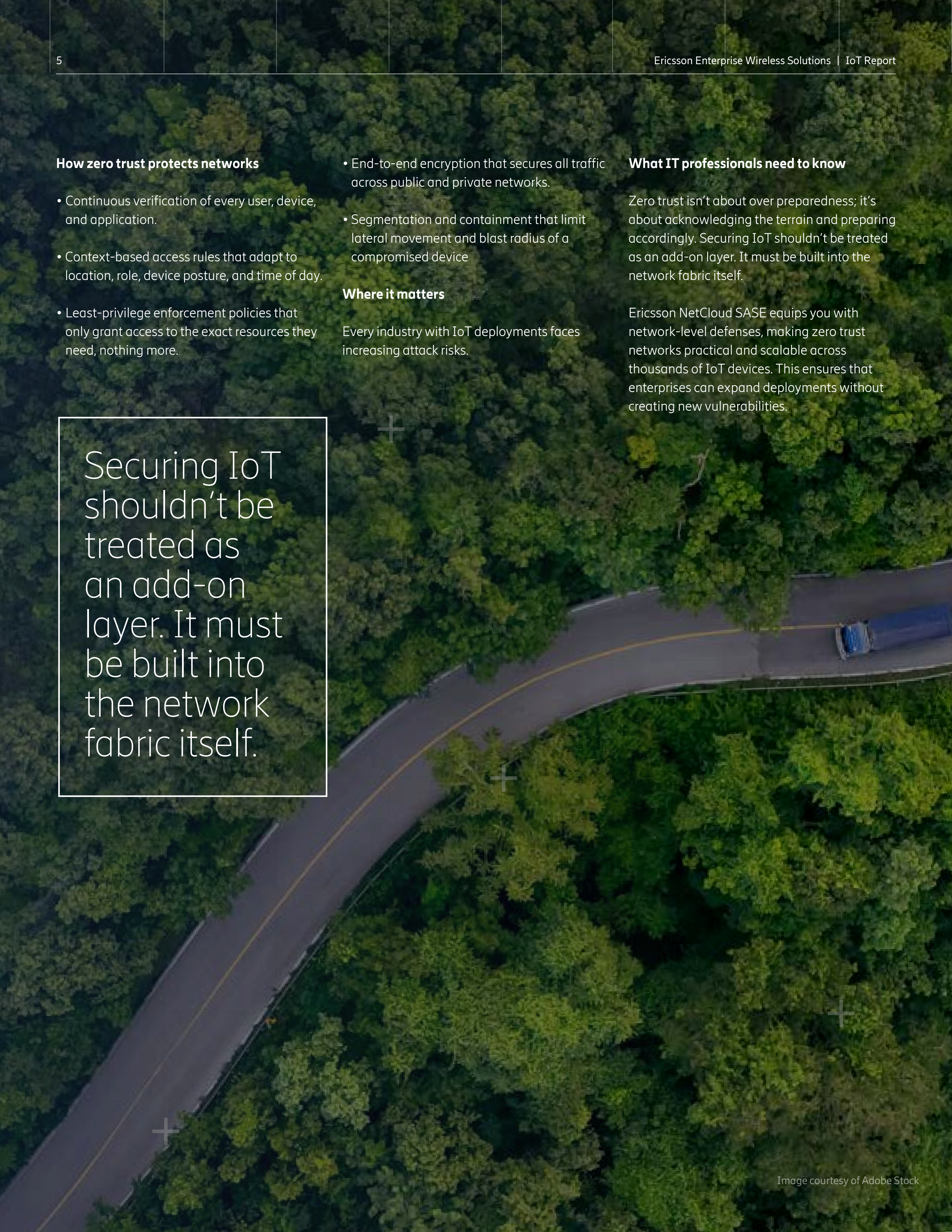


Image courtesy of Adobe Stock



How zero trust protects networks

- Continuous verification of every user, device, and application.
- Context-based access rules that adapt to location, role, device posture, and time of day.
- Least-privilege enforcement policies that only grant access to the exact resources they need, nothing more.
- End-to-end encryption that secures all traffic across public and private networks.
- Segmentation and containment that limit lateral movement and blast radius of a compromised device

Where it matters

Every industry with IoT deployments faces increasing attack risks.

> Securing IoT shouldn't be treated as an add-on layer. It must be built into the network fabric itself.

What IT professionals need to know

Zero trust isn't about over preparedness; it's about acknowledging the terrain and preparing accordingly. Securing IoT shouldn't be treated as an add-on layer. It must be built into the network fabric itself.

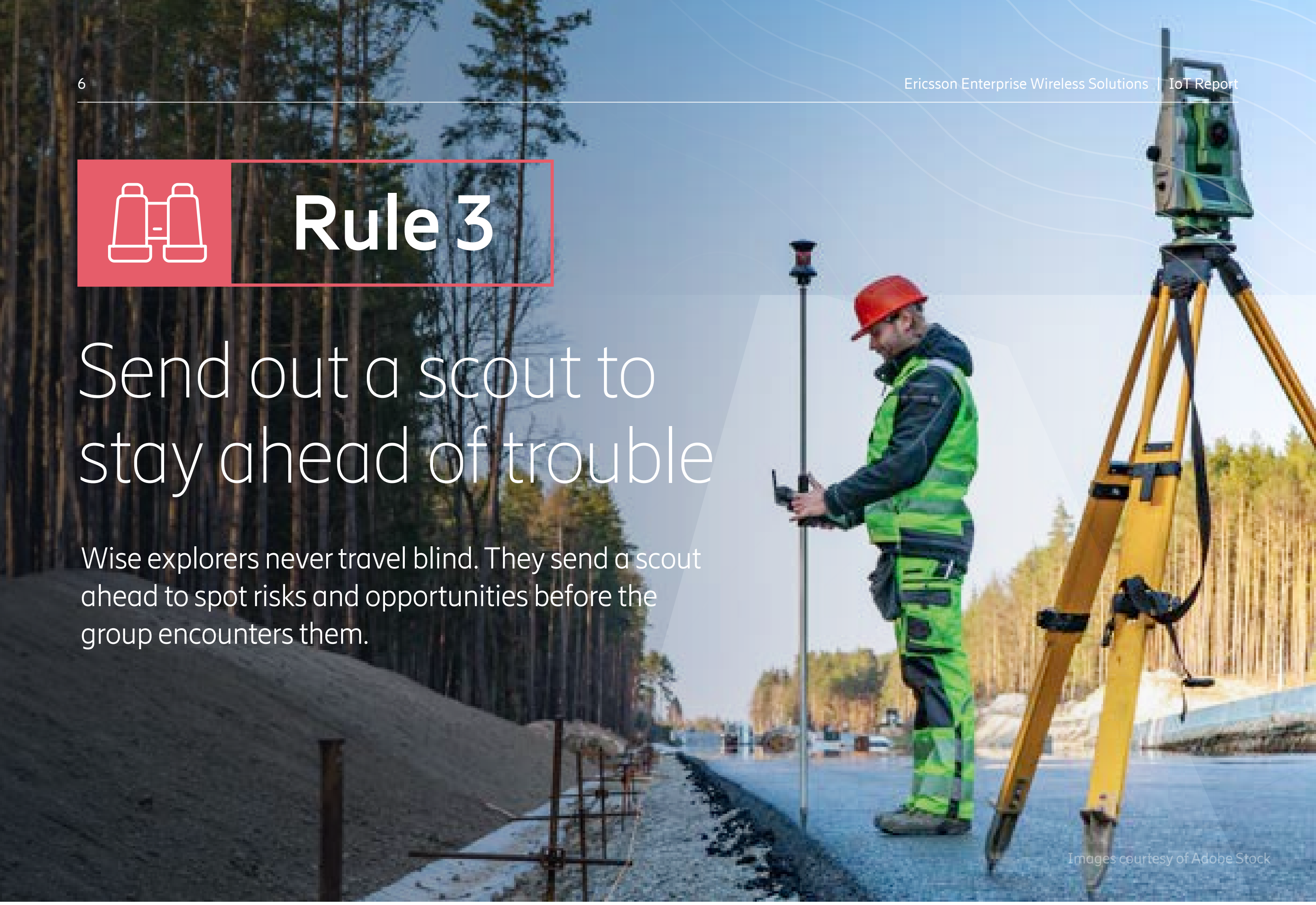
Ericsson NetCloud SASE equips you with network-level defenses, making zero trust networks practical and scalable across thousands of IoT devices. This ensures that enterprises can expand deployments without creating new vulnerabilities.

Image courtesy of Adobe Stock

Rule 3

Send out a scout to stay ahead of trouble

Wise explorers never travel blind. They send a scout ahead to spot risks and opportunities before the group encounters them.



Images courtesy of Adobe Stock

The complexity of IoT deployments is escalating with an increasing number of devices, more data, and higher demands on already lean IT teams. AI is the quintessential scout, scanning ahead, lightening the load, and pointing teams toward the safest, fastest path forward.

How AI acts as the reliable scout

- Predictive foresight detects anomalies and forecasts failures before they escalate into outages, reducing downtime and costs.
- Automated routines handle provisioning, firmware upgrades, and compliance at scale, freeing IT staff to focus on higher-value work.
- Natural language interfaces allow teams to "ask the network" directly, lowering training requirements and enabling faster troubleshooting.
- Edge intelligence processes data locally (e.g., compressing 4K/8K video, enabling autonomous robotics) so operations continue even if WAN connectivity is disrupted.

Where it matters

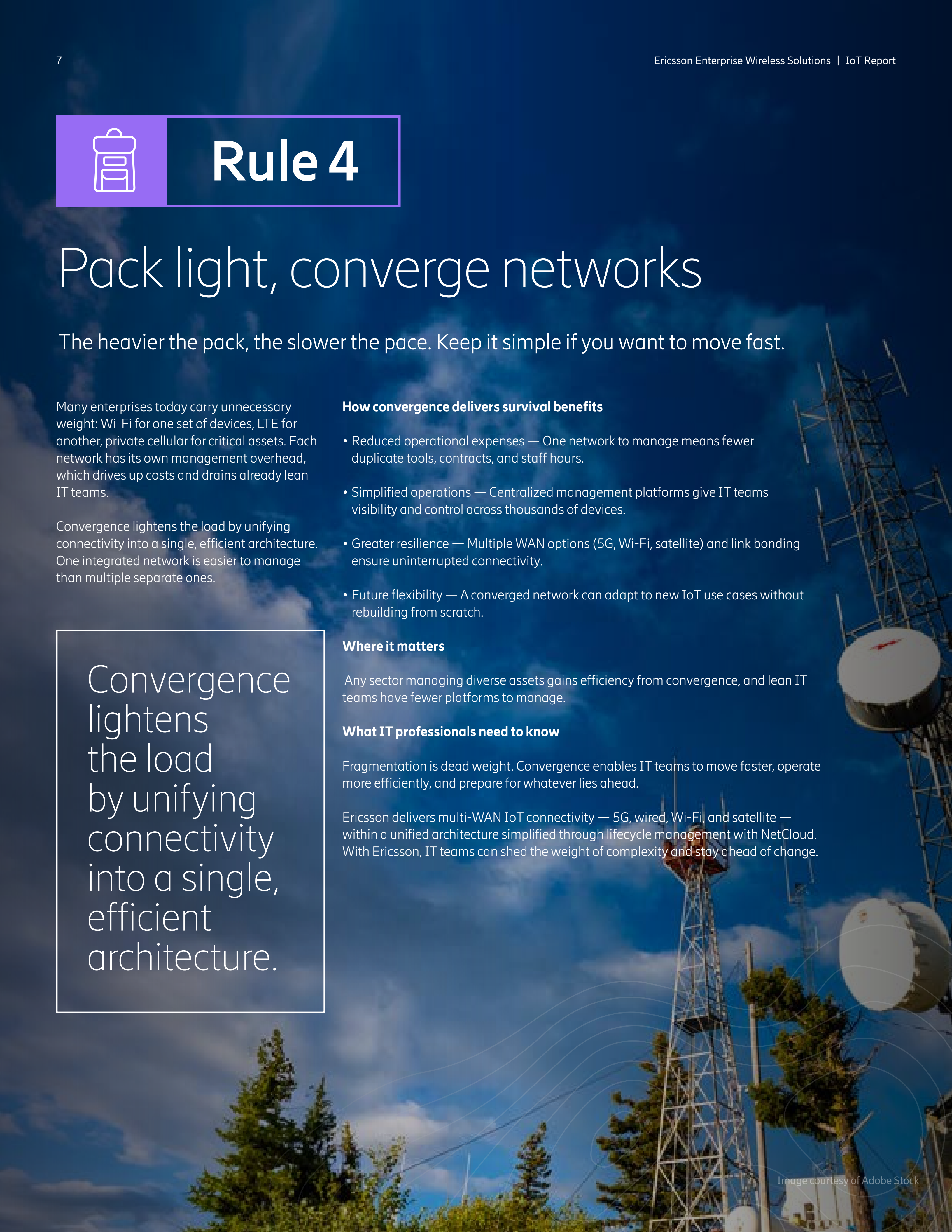
Any environment where uptime is critical benefits from a scout that never sleeps.

What IT professionals need to know

A scout doesn't replace leadership; it informs it. AI still requires human oversight and proper training for use cases, but it dramatically increases resilience and speed in uncertain terrain.

Ericsson equips you with AI-ready networks, edge compute support, and embedded assistants such as Ericsson's NetCloud Assistant, ANA, that turn sprawling IoT deployments into manageable, forward-looking systems. With Ericsson, IT teams always have a scout on point.

> AI is the quintessential scout, scanning ahead, lightening the load, and pointing teams toward the safest, fastest path forward.



Rule 4

Pack light, converge networks

The heavier the pack, the slower the pace. Keep it simple if you want to move fast.

Many enterprises today carry unnecessary weight: Wi-Fi for one set of devices, LTE for another, private cellular for critical assets. Each network has its own management overhead, which drives up costs and drains already lean IT teams.

Convergence lightens the load by unifying connectivity into a single, efficient architecture. One integrated network is easier to manage than multiple separate ones.

> Convergence lightens the load by unifying connectivity into a single, efficient architecture.

How convergence delivers survival benefits

- Reduced operational expenses — One network to manage means fewer duplicate tools, contracts, and staff hours.
- Simplified operations — Centralized management platforms give IT teams visibility and control across thousands of devices.
- Greater resilience — Multiple WAN options (5G, Wi-Fi, satellite) and link bonding ensure uninterrupted connectivity.
- Future flexibility — A converged network can adapt to new IoT use cases without rebuilding from scratch.

Where it matters

Any sector managing diverse assets gains efficiency from convergence, and lean IT teams have fewer platforms to manage.

What IT professionals need to know

Fragmentation is dead weight. Convergence enables IT teams to move faster, operate more efficiently, and prepare for whatever lies ahead.

Ericsson delivers multi-WAN IoT connectivity — 5G, wired, Wi-Fi, and satellite — within a unified architecture simplified through lifecycle management with NetCloud. With Ericsson, IT teams can shed the weight of complexity and stay ahead of change.

Image courtesy of Adobe Stock

Survival isn’t luck: it’s preparation

Image courtesy of Adobe Stock

The IoT wilderness of 2026 is not for the unprepared. LTE sunsets, AI-driven cyberthreats, exploding device counts, and leaner IT teams are converging into a new landscape that demands resilience. For IT leaders, the stakes are high. Choose the wrong path, and you risk stranded devices, costly outages, or vulnerabilities that compromise the entire enterprise.

> Survival is never about luck. It’s about having the right skills, the right plan, and the right partner at your side.

But survival is never about luck. It’s about having the right skills, the right plan, and the right partner at your side. Enterprises that build on the four survival rules—finding reliable shelter with RedCap, embedding zero trust security to protect your camp, deploying AI scouts, and converging networks to balance the load—will not just endure the expedition. They’ll emerge stronger, more agile, and more competitive.

Success comes more easily with a single vendor to equip your journey

IoT success doesn’t come from piecing together siloed solutions. It comes from having an outfitter that can supply the complete survival kit.

Look for a single vendor who delivers:

- Connectivity — LTE, 5G, RedCap, Wi-Fi, and hybrid WAN options, along with SD-WAN features such as link bonding and application-aware traffic steering for mission-critical and high-performance applications.
- Security — Zero trust, secure remote access, encryption, and SASE built into the network fabric.
- Intelligence — Embedded AI and edge compute to guide teams, automate tasks, and unlock real-time decision-making.
- Management —Lifecycle management tools such as NetCloud that simplify operations across thousands of devices.

Ericsson is your outfitter for the next IoT frontier

Ericsson brings it all together. With deep expertise in networking infrastructure and IoT connectivity, we provide enterprises with comprehensive, end-to-end solutions designed for 2026 and beyond. Enterprises trust Ericsson because:

- Our **product reliability** reduces costly site visits and downtime.
- Our **embedded AI** lightens the load for lean IT teams.
- Our **integrated approach** delivers security, performance, and scale from the edge to the cloud.

Ericsson isn't just another gear supplier. We're the outfitter that equips IT teams with everything they need to navigate new frontiers and own the map.

The new environment is coming fast. The question isn't whether enterprises will face these challenges; it's whether they'll be ready. With Ericsson, IT leaders don't just survive 2026. They lead the expedition.

Learn more about enterprise wireless solutions

Image courtesy of Adobe Stock