ERICSSON

In partnership with

CDW

The IT leaders' guide to IoT and zero trust

Building scalable protection for distributed enterprise IoT environments

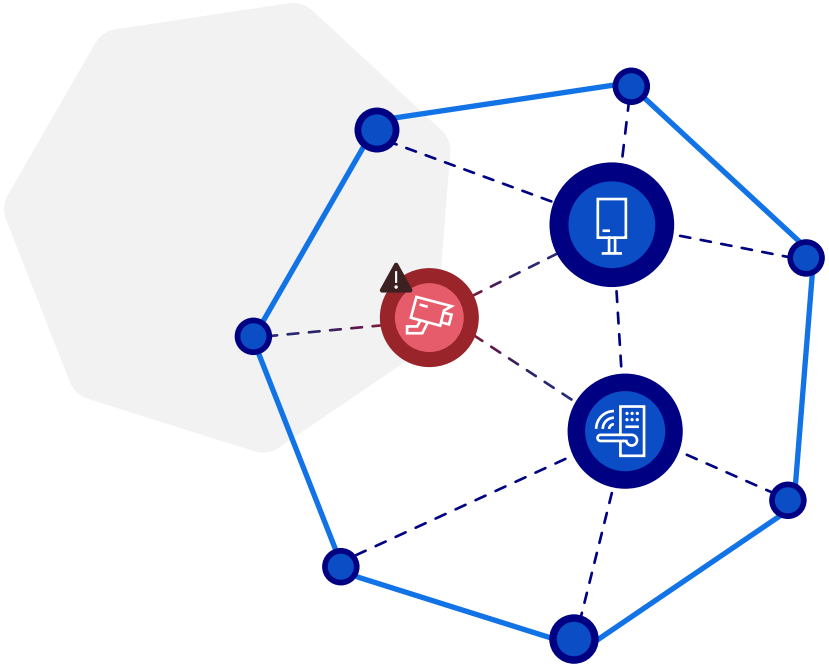
Image courtesy of Adobe Stock

IoT growth has redefined the network perimeter

Table of Contents

IoT is transforming enterprise operations, unlocking speed, efficiency, and insight. But the same innovations that deliver value across an organization are also expanding the attack surface and increasing exposure beyond what traditional tools can defend.

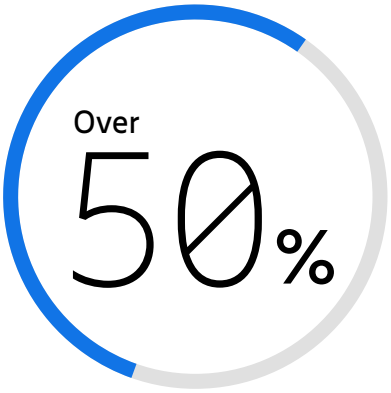
Even seasoned IT professionals encounter limited oversight when it comes to procurement and security, leaving significant gaps in IoT networks and the devices they connect. For IT leaders, this creates a dual imperative: they must extend protection to the edge without adding complexity. A zero trust foundation and cellular-first SASE strategy make both possible, without overhauling your architecture.



The business risk of IoT expansion

With nearly 18 billion devices already online and 25 billion expected by 2030, IoT is essential to business operations across industries. It's no longer just about "if" IoT is in your environment, it's how many, where, and whether they're secure.

According to research from San Diego State University, 84% of organizations already have IoT devices on their network. But over half still rely on little more than a password for protection. That gap between deployment and oversight introduces technical, operational, and financial risk.



of organizations don't employ security measures beyond default passwords

Often added by facilities teams, third parties, or "shadow IT," these devices typically lack patching, policy enforcement, and visibility, making even one seemingly minor device a potential entry point for attackers. When this happens, there's no one within the organization prepared to answer basic but essential questions, including:

- Who has access?
- What protections are in place?

IoT security gaps don't stay isolated, and neither do the impacts of a compromised device. In industrial and warehouse settings, for example, compromised devices or sensors can stall production or fulfillment, leading to costly operational downtime.

The business implications of IoT—compliance gaps, operational disruption, and reputational harm—are real. IT leaders must ask: How secure is the infrastructure I can't see?

That question exposes a deeper flaw. The security tools most organizations rely on weren't built to handle this.

Why IoT devices are a security threat

Most IoT devices weren't built with enterprise-grade security in mind. They're lightweight machines designed for a single function. That simplicity creates significant security limitations:

Limited processing power

The majority of IoT devices can't run security agents, antivirus software, or modern endpoint security tools.

Nonstandard operating systems

These devices don't use standard operating systems, making it nearly impossible to deploy uniform security controls.

No browser support

Many IoT devices lack a web interface, so browser-based authentication or encryption isn't an option.

Image courtesy of Adobe Stock

This makes securing IoT at scale a fundamentally different challenge than securing laptops, phones, or servers.

IoT devices don't just lack defenses, they also introduce new risks into the network.

- Default passwords are rarely updated, making devices easy targets for brute-force attacks.
- Unpatched firmware leaves devices exposed to known exploits.
- Public IP broadcasting allows threat actors to discover devices using basic scanning tools.

But the real threat begins once a device is compromised. In a traditional VPN or flat network, that device often has broad access to other systems. Once in the door, attackers can move laterally, escalate privileges, and potentially access high-value data or operational systems.

Without zero trust protections, a single exposed device can become a gateway into the entire enterprise network.

The limits of legacy approaches for IoT

VPNs, firewalls, clients, and perimeter-based models have not kept pace with the evolution of today's IoT landscape. They assume a static environment with clear inside/outside boundaries. IoT breaks that assumption.

Traditional VPNs

These provide a certain level of security by encrypting the connection tunnel. However, once a device or user is connected, they have broad access, making it risky due to potential lateral movement. IoT devices don't require full network access, and VPNs often lack the granular controls needed to limit their reach.

Firewalls

They are designed to protect known perimeters. But in a modern IoT environment, those perimeters are blurry. Devices may sit outside the firewall entirely or route traffic in unpredictable ways.

Private APNs

These can offer an extra layer of protection, but they come with scaling challenges. They require upfront carrier coordination, don't address lateral movement risk, and can be challenging to manage across hundreds or thousands of endpoints.

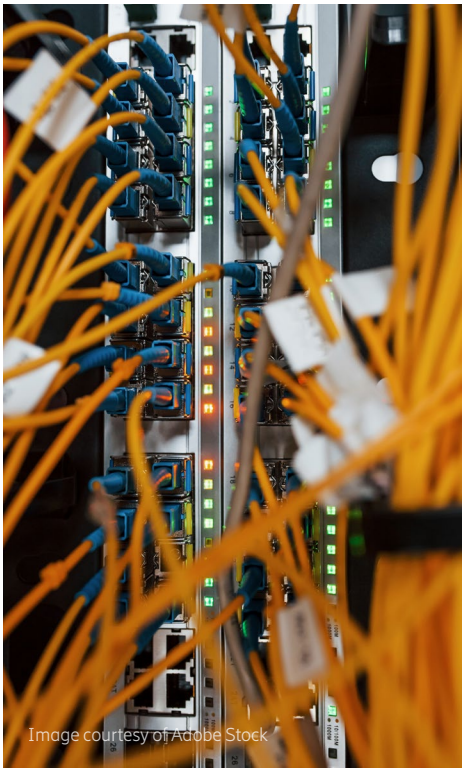


Image courtesy of Adobe Stock

Beyond security tool limitations, there's also a dangerous assumption at play that existing infrastructure covers IoT devices. But that assumption rarely holds. Attackers can gain entry via a single exposed device. Once inside, they're free to move laterally through the network to reach high-value systems.

While many assume bolting on layers of traditional security to protect IoT will help, it often backfires, leading to:

- Increased management responsibilities for IT teams that are already stretched thin.
- Vendor sprawl that fragments visibility and drives up cost.
- Inconsistent policy enforcement across environments.

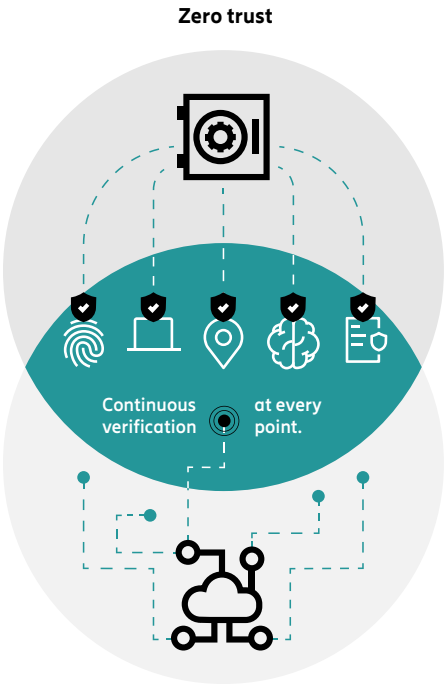
In this context, the attack surface grows exponentially, while security resources stay flat. The result is more operational overhead without improving security.

The smartest approach isn't to retrofit more security onto endpoints; it's to offload protection to the infrastructure around them, shifting from perimeter-based thinking to identity-based network access, distributed enforcement, and built-in controls that support scale without adding complexity.

In this hybrid architecture, routers enforce local policies, the cloud manages orchestration and inspection, and optional gateways add protection in complex environments. This offloads resource-intensive tasks such as segmentation and traffic inspection from the device to more capable infrastructure. Built-in zero trust features such as intrusion detection and prevention (IDS/IPS) strengthen protection even further without adding operational complexity.

Zero trust and SASE: A smarter way to secure IoT

A distributed architecture is robust on its own. But when combined with zero trust principles, it becomes transformative.



In a zero trust architecture, there's no assumed trust. Every connection is continuously verified based on identity, device type, location, behavior, and policy. Instead of open VPN tunnels, each connection becomes an isolated, encrypted tunnel with no lateral access or network discovery. Connections are isolated and temporary, resources are invisible by default, and most importantly, the blast radius if something goes wrong, stays small.

While zero trust gives you control, SASE gives you reach by combining networking and security. Together, they provide a unified, scalable way to secure a world that's always on and always moving.

How SASE unifies networking, security, and management

When you combine zero trust with cellular-first SD-WAN and SASE architecture, you get a powerful, coordinated approach to securing and managing distributed networks and IoT devices.

It starts with connectivity. Cellular networks remove the need for trenching or wired circuits, so sites or devices can be brought online quickly, anywhere, eliminating the need to wait for underground cables to be laid or internet providers to come online.

Then comes performance. The latest SD-WAN technology intelligently manages network traffic to keep critical applications running smoothly. It uses techniques such as link bonding to boost bandwidth and network slicing to prioritize high-value traffic streams.

Security is enforced at the network level. Ericsson NetCloud Secure Connect provides a zero trust alternative to VPNs, creating isolated, policy-controlled connections where IPs are hidden and lateral movement is blocked. Devices stay invisible to attackers, and access is limited by role, location, or behavior.

One platform replaces fragmented stacks and complex integrations. The result is stronger security and simplified operations, ideal for lean IT teams.

This unified model is powered by Ericsson NetCloud SASE, a tightly integrated platform purpose-built for secure, scalable IoT connectivity.

NetCloud SASE unifies networking and security into a single, AI-enhanced platform optimized for Wireless WAN with distributed IoT. Teams can manage security and connectivity directly through NetCloud Manager – without a separate management platform to learn.

Enforce

NetCloud Secure Connect – Replaces legacy VPNs with zero trust tunnels that cloak devices, restrict lateral movement, and enforce least-privilege access.

+

Protect

NetCloud ZTNA – Secure remote access through identity-based access to specific applications or resources via clientless or client-based connections.

+

Connect + Optimize

NetCloud SD-WAN – Delivers resilient, high-performance connectivity with cellular bonding, link steering, and network slicing.

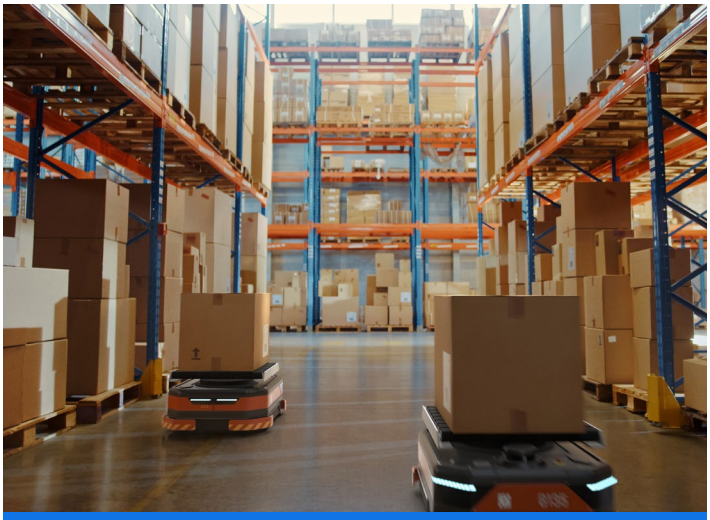
+

Manage + Scale

NetCloud Manager – Centralizes policy enforcement, diagnostics, and lifecycle orchestration across distributed deployments.

Real-world examples: IoT security in action

IoT security, when done right, does more than reduce risk. It also accelerates deployment, simplifies operations, and protects outcomes. Here's how zero trust architecture and cellular-first networking scale effectively across industries.



Warehousing

In large distribution centers, barcode scanners, sensors, robotics, and conveyor systems are becoming more prevalent. But managing security across dozens or hundreds of mobile endpoints is challenging.

With a cellular-first, zero trust approach:

- Devices connect to backend applications through encrypted, policy-based tunnels.
- Devices connected to Ericsson Cradlepoint routers are protected through the zero trust network, eliminating lateral movement.
- NetCloud ZTNA enforces role-specific access for both on-site and remote technicians and third-party contractors.
- SD-WAN features such as traffic steering and link bonding ensure high availability for critical systems.
- Devices are protected with the zero trust network, so they no longer broadcast their IP address, and lateral movement is eliminated.

This model supports rapid growth in throughput and automation without introducing new risks to the operational network.

Education

A growing number of school districts are upgrading HVAC systems, digital signage, and access control across campuses. These devices require centralized management and remote support while complying with privacy policies.

Zero trust networking delivers:

- Secure remote access for contractors and IT teams without a VPN client.
- Logical segmentation that isolates HVAC and badge systems from instructional networks, for example.
- Continuous monitoring and audit logs that support compliance and incident response.
- Security policies that isolate operational technology (OT) from other systems and limit exposure in case of a breach, reducing the risk of downtime, data loss, or compromised inventory.

Districts can standardize operations across sites without opening the door to risk or compromising student data.

Images courtesy of Adobe Stock

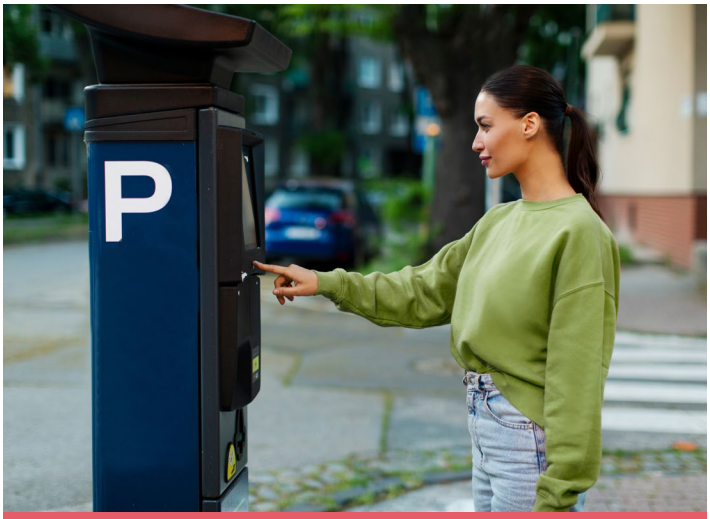
Healthcare

Hospitals increasingly rely on IoT for secure access, patient monitoring, and building controls. Many of these systems are managed by third-party vendors.

With zero trust security and wireless WAN:

- Each connected device or group of devices is segmented into its own secure zone.
- External vendors can monitor and maintain systems via clientless ZTNA portals with scoped permissions.
- Traffic is encrypted and logged, ensuring HIPAA-aligned access control and traceability.
- Lateral movement between systems is prohibited, which minimizes the blast radius of potential breaches and safeguards patient data, clinical workflows, and critical infrastructure

IoT helps healthcare facilities run more efficiently, and zero trust keeps those systems safe, resilient, and compliant.



Smart cities

When a city expands its network of traffic cameras, environmental sensors, or digital kiosks, running fiber to each location isn't always efficient or practical. Instead, cities can deploy cellular networking that can be installed and brought online the same day.

Using zero trust controls:

- Devices are cloaked behind name-based routing, eliminating public IP exposure.
- Default access is blocked entirely, so only approved users and systems can connect.
- Remote access is tightly segmented by role and function, reducing the risk of lateral movement.
- Sensitive systems like public safety infrastructure stay protected even in widely distributed, high-traffic environments.

The result is a secure, scalable infrastructure that doesn't require digging up streets.

Images courtesy of Adobe Stock

A practical starting point for zero trust IoT security

Getting started

Adopting zero trust in an IoT environment doesn't have to be all-or-nothing. Enterprises can begin modernizing IoT security and reducing the attack surface with small, strategic steps. Here's how to get started.

1. **Audit your IoT security.** Review basic security IoT policies, procedures (update passwords, regular patches, turn off IP broadcasting).
2. **Replace default credentials and apply patches.** IoT devices are often the weakest link, but this simple step sharply reduces exposure.
3. **Implement a zero trust foundation** with NetCloud Secure Connect to replace legacy VPNs.
4. **Move to zero trust incrementally.** Start with high-risk or high-value assets, then expand to wider device groups.
5. **Simplify remote access with ZTNA.** Give vendors and employees the access they need and nothing more.
6. **Consolidate platforms.** Use unified tools such as NetCloud SASE to reduce training burdens, cut costs, and ease management.

Image courtesy of Adobe Stock

Secure IoT deployment checklist

As more devices connect to your network, this checklist will help ensure your deployment is secure, reliable, and ready to scale.

Before you deploy

Set clear goals

- ○ Have we defined what success looks like for this IoT rollout?
- ○ Are the right teams (IT, operations, facilities, vendors) involved and aligned?

Understand what the devices need

- ○ Do we know how much bandwidth and how little delay these devices require?
- ○ Have we checked cellular coverage and data plans for each site?
- ○ Do we know how data will flow from the devices to the cloud or data center?

Plan for growth and security

- ○ Have we thought through how this setup will scale over time?
- ○ Can we manage device updates and settings remotely?
- ○ Have we thoroughly considered what could go wrong and planned for how we'd handle it?

Deployment readiness

Make sure devices and connections are ready

- ○ Can our routers support future needs like traffic steering or link bonding?
- ○ Do we have a secure way to access these devices remotely if something breaks?
- ○ Are the devices designed to handle the weather or rough environments?
- ○ What is the backup connection (cellular, wired, or satellite) if the main link goes down?

Set up smart, secure operations

- ○ Are we isolating devices so they don't talk to parts of the network they shouldn't?
- ○ Are we planning to use zero trust instead of traditional VPNs or private APNs?
- ○ Do we have a backup plan if we lose access to a remote device?
- ○ Can we monitor for unusual activity and enforce security rules?

Coordinate across teams

- ○ Can we see and manage all our devices from one place?
- ○ Do we have secure options for giving third parties or contractors remote access?
- ○ Are we using AI or smart tools to help troubleshoot or spot problems?
- ○ Have our teams been trained on setup, security, and support?

IoT security that scales with you

IoT is not going away; neither are the risks it introduces. In a world where billions of devices are coming online, securing your IoT infrastructure is not a technical decision; it's a business imperative.

The attack surface is expanding as bad actors continue to evolve. A zero trust framework combines cellular-first networking and management within a SASE platform, empowering enterprise leaders to safeguard their assets, support their teams, and scale with confidence.

With the right foundation, IoT can deliver efficiency, insight and speed without compromising security. The solution lies in building security into the fabric of the system, not just layering it on top of connectivity. That's what makes it scalable, even at the edge.

The next era of connectivity demands more than just tools; it demands architecture that scales with innovation. The best IoT structure helps small teams achieve big things, securely.

Learn more about enterprise wireless solutions


Image courtesy of Adobe Stock