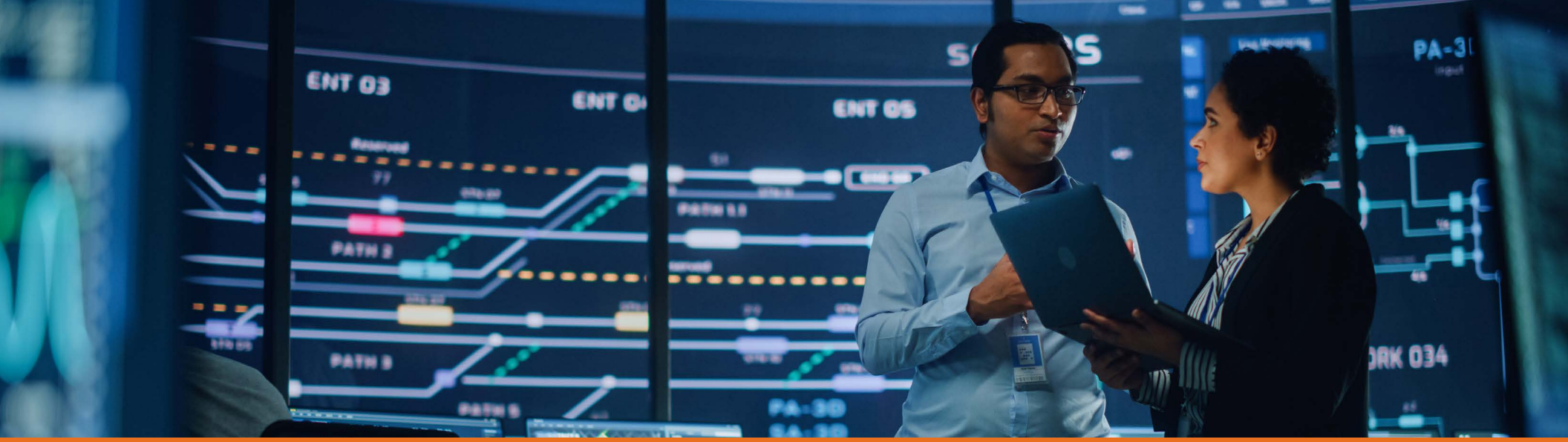
THE RISKS OF WAITING

WHAT LEGACY WI-FI® REALLY COSTS YOUR ORGANIZATION

RUCKUS® NETWORKS

Key takeaways

- **Many enterprise wireless networks can no longer keep pace with current user demands.** Device density has increased; wireless-first operations are now standard and AI-driven applications require reliable, low-latency connectivity. Legacy Wi-Fi wasn't designed for these conditions.
- **Deferring a Wi-Fi upgrade doesn't eliminate cost.** It shifts spending into daily operations, where reactive troubleshooting, longer resolution cycles and IT overhead continue to accumulate.
- **Legacy Wi-Fi infrastructure is a growing security risk**, with the average enterprise data breach costing approximately $4.4 million. Access points (APs) approaching end-of-support receive fewer updates, lack centralized visibility and increase exposure.
- **Wi-Fi 7 addresses performance, operational efficiency and security in a single upgrade cycle.** Organizations that plan ahead, control scope, timing and budget. Those that delay, are forced to upgrade under pressure, with compressed timelines and unplanned capital spend.
- **RUCKUS Networks® helps organizations modernize wireless infrastructure through readiness assessments, architecture planning and phased deployment.** Its Wi-Fi 7 APs, ICX switches and cloud-managed platforms deliver centralized visibility, policy control and AI-driven network intelligence, reducing operational complexity.



WHY DELAYING A WI-FI 7 UPGRADE COSTS MORE THAN YOU THINK

Have you ever sat in a conference room where half the team failed to connect to the network? Or watched a critical presentation break down because the Wi-Fi couldn't keep up? These are everyday occurrences for organizations still running legacy wireless infrastructure.

Most enterprise Wi-Fi networks don't fail at once. They fall behind, even as device counts climb and new applications demand more from the network. Yet for many IT teams, postponing a Wi-Fi 7 upgrade appears to keep operating expense (OpEx) flat, at least on paper. It doesn't. Instead, it shifts those costs into daily operations, where they're harder to see, forecast or contain.

Across industries, organizations still operate wireless infrastructure built for an earlier era when device density was lower, traffic patterns were predictable and applications were less sensitive to latency. Client devices now generate three to four times more traffic,[1] and AI-driven workflows increasingly require reliable, low-latency connectivity.

Delaying an upgrade doesn't eliminate operational burden. Over time, small inefficiencies compound, adding business and operational risk that affects productivity, service delivery and overall user experience.

[1] "Traffic Growth in Mobile Networks Driven by 5G," Ericsson Mobility Report. Ericsson. Accessed March 26, 2026.

YOUR WIRELESS INFRASTRUCTURE IS ALREADY BEHIND

To understand why, let's look at how the wireless environment has changed. Many enterprise workspaces were designed to support a mix of wired and wireless connectivity. Today, organizations increasingly operate in a wireless-first model as Ethernet ports disappear from laptops, hybrid work reduces permanently assigned desks and devices connect across conference rooms, open office areas and shared collaboration spaces.

At the same time, the number of connected devices per user continues to increase. In educational environments, teachers, students and administrative staff routinely connect 3–5 devices.[2] In hospitality, a single guest room typically supports 10–15 active connections, including smartphones, tablets, laptops, streaming devices and wearables. Similarly, a single multi-dwelling unit (MDU) may support 20 or more simultaneous connections.

In high-density venues and event spaces, APs routinely handle 50 or more simultaneous clients and must absorb unpredictable demand spikes as users arrive, connect and shift locations. Manufacturing and logistics environments add another layer of complexity, with mobile scanners, tablets, cameras and automation systems operating continuously on the same wireless fabric.

The performance gap keeps widening. Older wireless architectures weren't designed for sustained high-density traffic, frequent small data transmissions from Internet of Things (IoT) devices, wearables and edge endpoints. Persistent background cloud synchronization and unpredictable demand spikes add to network loads.

[2] "Rethinking Campus Connectivity," EDUCAUSE Review, May 2025.

MORE DEVICES, MORE PRESSURE: WHY EVERY INDUSTRY FEELS THE PAIN

Whether you manage a hotel, hospital, warehouse or university campus, the pattern is the same.

In hospitality, Wi-Fi is part of the brand promise. Most modern devices display the Wi-Fi standard in use, giving guests immediate visibility into network quality and raising expectations in premium properties. Guests demand seamless connectivity across rooms, public areas and conference spaces. As device density increases, unreliable Wi-Fi directly affects satisfaction scores and repeat bookings. At high-profile conferences and events, intermittent connectivity can trigger six-figure penalties.

Connectivity is a key MDU amenity, particularly in high-end apartment communities and new residential developments with smart appliances. Residents expect reliable, high-speed Wi-Fi for remote work, streaming, gaming and smart home devices. Inconsistent service drives up helpdesk calls and weakens competitive positioning in crowded rental and real estate markets.

In educational facilities, digital curriculum, collaboration tools and safety systems depend on uninterrupted wireless access. Small IT teams throughout K–12 districts must manage dense classroom device deployments and standardized testing windows with limited margin for disruption. For colleges and universities, latency-sensitive AI-driven research, campus-wide mobility, competitive esports programs and high-definition media streaming further raise the Wi-Fi performance bar as device counts continue to climb.

At high-profile events, intermittent connectivity can trigger six figure penalties.

The consequences of unreliable Wi-Fi extend to manufacturing and logistics operations. Nowadays, Wi-Fi connects smart building sensors, IP cameras, inventory management systems and medical equipment, all of which demand consistent, low-latency connectivity. Connected vehicle fleets introduce high-bandwidth, low-latency demands of their own. Many offload tens of gigabytes of sensor and mapping data per vehicle each day, with autonomous vehicles generating significantly more.

Beyond connected vehicles, bandwidth-intensive, time-sensitive applications like augmented reality training, 4K/8K video conferencing and real-time AI-driven collaboration tools place increasing demands on legacy networks.

Interference in congested 2.4 GHz and 5 GHz bands can affect the functionality of these systems and devices, particularly in high-density deployments. Newer wireless generations introduce access to the 6 GHz spectrum, expanding capacity and reducing contention.

Yet performance isn't the only concern. Aging infrastructure is also a growing security risk.

AGING INFRASTRUCTURE ISN'T JUST OUTDATED. IT'S A LIABILITY.

When did your oldest access point last receive a firmware update? If you're not sure, you're not alone. For many organizations, the answer reveals an infrastructure gap that carries real security risks. Industry research estimates the average cost of an enterprise data breach at approximately $4.4 million.[3]

While not all breaches originate at the wireless layer, infrastructure life cycle has a direct impact on security. Unsupported systems leave organizations increasingly vulnerable. As APs and controllers age, they reach end-of-support status. Software updates slow, and vendors may no longer deliver security patches.

Newer Wi-Fi APs support stronger encryption and authentication standards, including Wi-Fi Protected Access 3 (WPA3) in the 6 GHz band. Modern cloud-managed platforms further reduce operational risk through centralized policy enforcement, automated software updates and continuous monitoring. While these capabilities don't eliminate threats like social engineering or ransomware, they directly improve visibility, accelerate response and support disciplined life-cycle management.

However, the impact of aging infrastructure doesn't stop at the security layer. It drives a persistent operational burden that accumulates quietly, day after day.

Industry research estimates the average cost of an enterprise data breach at approximately $4.4 million.

[3] Cost of a Data Breach Report 2025. IBM and Ponemon Institute, 2025.

LEGACY WI-FI GENERATES HIDDEN COSTS THAT COMPOUND DAILY

Has your IT team ever spent an afternoon chasing a wireless complaint that turned out to be a coverage gap no one documented? On legacy networks, this kind of reactive troubleshooting is the norm, not the exception.

In many organizations, aging wireless environments drive a significant increase in time spent on reactive support and issue resolution. And that time has a price. Helpdesk tickets increase incrementally, resolution cycles lengthen and intermittent issues are harder to diagnose. Three out of four organizations report delays in deployment and troubleshooting directly attributed to legacy infrastructure.

In lean IT environments, the impact is more noticeable. Small teams in K–12 districts, mid-market enterprises and multi-site organizations are often overwhelmed, lacking dedicated or advanced wireless expertise. As network performance grows less predictable under load, strategic initiatives give way to firefighting, further constraining already limited resources.

Older systems, particularly those approaching end-of-support status, often lack centralized visibility and shared diagnostic capability, resulting in slower, more labor-intensive resolution. In contrast, modern cloud-managed Wi-Fi environments demonstrate measurable reductions in mean time to resolution (MTTR), with troubleshooting efficiency improving by 50–70%[4] compared to legacy, siloed management models. AI-driven platforms go further, delivering continuous network assurance that identifies and addresses potential issues before they affect users.

Three out of four organizations report delays in deployment and troubleshooting directly attributed to legacy infrastructure.

Time spent resolving wireless performance issues prevents IT departments from deploying new services, advancing digital initiatives and improving user experience. Over time, this operational tax outweighs the apparent savings of a deferred refresh. The only question is, will you modernize on your own terms or during a crisis?

[4] RUCKUS Networks. "Managed Service Providers." Accessed March 26, 2026.

WI-FI 7: BUILT FOR THE DEMANDS LEGACY NETWORKS CAN'T MEET

Are you upgrading to Wi-Fi 7 to better handle device density, address AI-driven performance demands or shore up vulnerable infrastructure? You're not alone.

Most enterprises upgrade their wireless networks for multiple reasons: increased device density, support for emerging low-latency applications, improved operational efficiency through AI, stronger security posture and evolving user expectations. Wi-Fi 7 addresses all these simultaneously, improving latency, reliability and spectrum efficiency.

Features such as multi-link operation (MLO) enable devices to use multiple frequency bands at once, maintaining performance consistency under load. Access to the 6 GHz band introduces cleaner spectrum, reducing interference and congestion. AI-driven network management continuously optimizes channel selection, band steering and load balancing to deliver performance as demand grows.

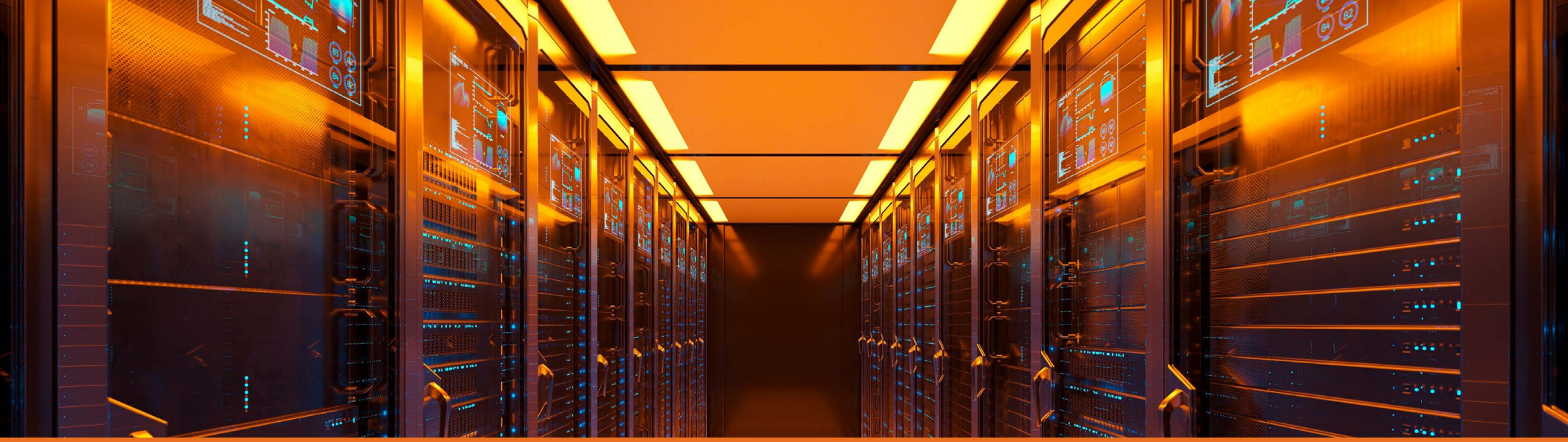
Even older client devices benefit from Wi-Fi 7, with newer APs improving legacy client performance by 15–25%[5] through more efficient radio design, data packet processing and network traffic management.

For organizations planning network infrastructure on a five- to seven-year horizon, upgrading to Wi-Fi 7 is a strategic decision.

As AI-driven applications reshape traffic patterns, quality of service (QoS) matters as much as available bandwidth. Upstream demand is growing particularly fast, as organizations push more data to the cloud for AI processing and analytics. Real-time translation, analytics and continuous data synchronization require predictable latency.

For organizations planning network infrastructure over the next five to seven years, upgrading to Wi-Fi 7 isn't an incremental update. It's a strategic decision.

[5] "New Test Results from Intel Show Significant Wi-Fi 7 Performance Improvements over Wi-Fi 6, Even with Legacy Equipment," Wi-Fi NOW, January 2026.



UPGRADE ON YOUR TERMS OR UNDER PRESSURE

No IT leader plans to upgrade their network in the middle of a crisis. But that's exactly how it happens to many organizations. Unfortunately, crisis-driven upgrades compress timelines, limit vendor evaluation and force unplanned capital expense (CapEx).

Proactively upgrading to Wi-Fi 7 allows organizations to control scope, timing and budget. Phased rollouts, pilot deployments and readiness assessments give IT teams the flexibility to plan strategically for:

- Device density trends over the next three to five years
- Application latency and reliability requirements
- Infrastructure life-cycle status
- Operational burden on IT teams
- Total cost of ownership (TCO) across the refresh cycle

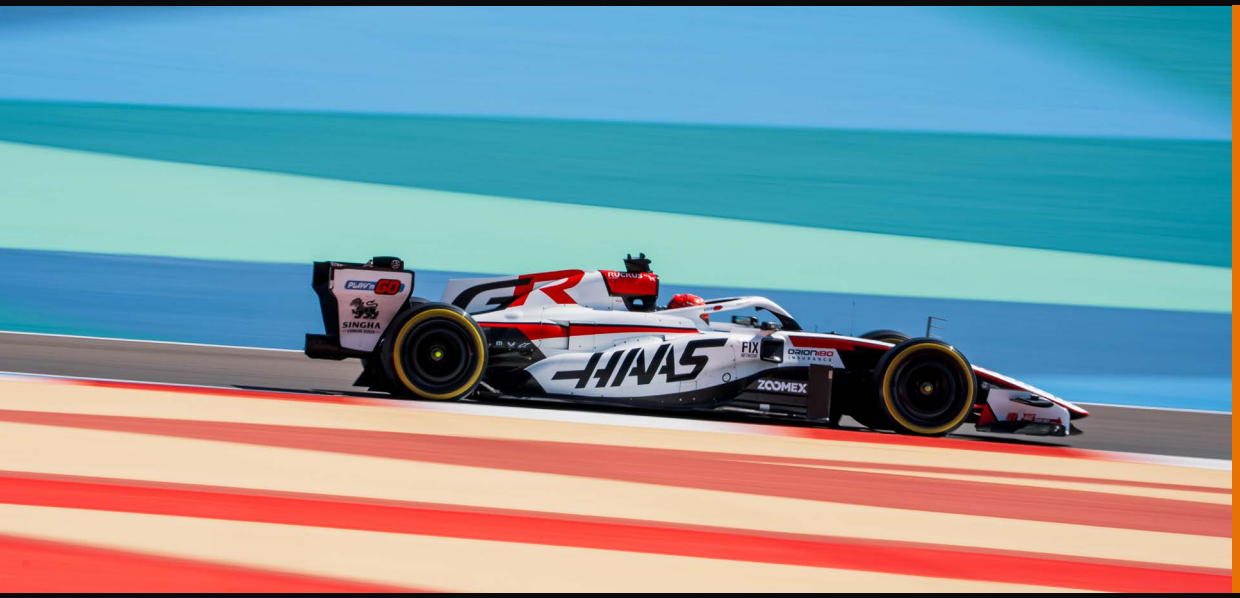
Planning ahead transforms modernization from a reactive expense into a controlled, strategic investment. Modernization doesn't need to be disruptive. It can begin with a structured readiness assessment, performance benchmarking or a targeted pilot in high-density environments. With cloud-managed platforms, AI-driven network intelligence and disciplined migration planning, organizations can modernize incrementally while maintaining service continuity.

> Crisis-driven upgrades compress timelines, limit vendor evaluation and forced unplanned CapEx.

YOUR WI-FI 7 ROADMAP STARTS HERE

RUCKUS Networks and its partners guide organizations through end-to-end upgrade initiatives, from security assessments and readiness reviews to architecture planning and phased deployment across complex, distributed environments. RUCKUS One® provides centralized visibility, AI-driven network intelligence and automated policy management, while RUCKUS Wi-Fi 7 APs and RUCKUS switches deliver the performance and density support modern environments demand. RUCKUS Professional Services help organizations migrate efficiently at every stage.

If you're evaluating your wireless road map, now is the time to assess infrastructure readiness and define a Wi-Fi 7 modernization strategy that supports future growth. With Wi-Fi 7 devices projected to represent most new client connections by 2027, that window is closing.



"Formula 1 is about speed, efficiency, and reliability, and partnering with RUCKUS Networks allows us to showcase how our networking solutions perform in one of the most data-intensive environments in the world."

Ayao Komatsu
Team Principal of TGR Haas F1 Team[6]

[6] RUCKUS Networks. "RUCKUS Networks Announces Official Partnership with TGR Haas F1 Team." January 21, 2026.

* Wi-Fi and Wi-Fi 7 are trademarks of the Wi-Fi Alliance.

About RUCKUS: RUCKUS® Networks builds and delivers purpose-driven networks that perform in the tough, unique environments of the industries we serve. Leveraging network assurance and enterprise-wide automation driven by AI and machine learning (ML), we empower our customers to deliver exceptional experiences for every employee, guest, customer, student and resident who counts on those networks to connect with their digital lives. Discover more at ruckusnetworks.com.

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

EB-300111-EN (04/26)