NCR ATLEOS

How to embed security in modern enterprise networks

Exploring solutions to today's enterprise network challenges to secure the future

An NCR Atleos white paper

Contents

Introduction

In our increasingly digital world, the pressure on business leaders to deliver seamless, secure and efficient user experiences has never been greater. Traditional security models that patch on a firewall at the end of an IT project no longer cut it. Instead, a modern approach is emerging: one where security isn’t an afterthought but is embedded into the very fabric of your network. This secure-by-design strategy, underpinned by Zero Trust principles, embeds security into every layer of the network—from access networks like local area networks (LAN) and wireless local area networks (WLAN) through to cloud-optimized wide area networks (WAN) and software-defined wide area networks (SD-WAN), and cloud-delivered security like secure access service edge (SASE). This integrated approach not only fortifies your network against disruption but also drives tangible business outcomes.

In this document, we explore why modern networks require an embedded security strategy, what the core components of such an approach are and how organizations can successfully transition from legacy systems to a resilient, future-proof architecture.

A new era of connectivity and challenges

Over the last few decades, we have seen enterprise networks evolve dramatically. In the past, the focus was simply on connecting users in an office through LAN and WLAN. Today's digital ecosystem spans public clouds, software-as-a-service (SaaS) applications, branch offices connected via hybrid WANs, mobile workforces on 4G/5G and a growing sea of internet of things (IoT) sensors.

This flexibility powers innovation but also expands the attack surface: unsecured branch links and unmanaged devices become entry points for adversaries. Recent high-profile breaches—ranging from supply-chain compromises to artificial intelligence (AI)-assisted phishing campaigns—illustrate that reactive, siloed defenses leave critical gaps.

Global cybersecurity spending is projected to reach $212 billion in 2025—a 15% year-over-year jump from 2024—as organizations race to shore up defenses, according to Cybersecurity Dive.

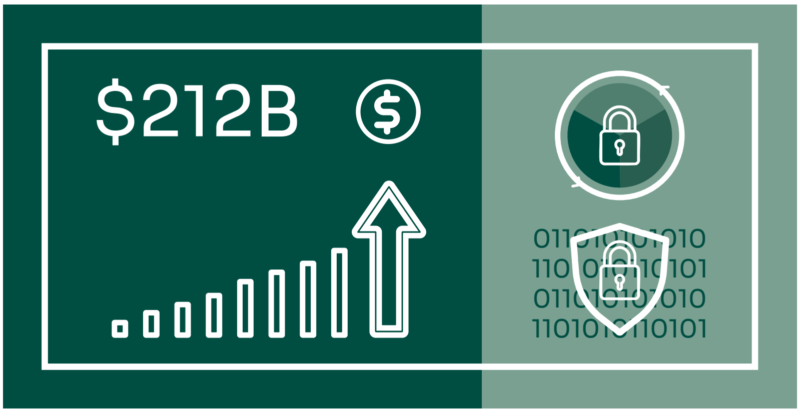


Figure 1. Global spending on security

However, investment alone doesn't guarantee resilience. Despite 94% of IT leaders expressing confidence in their resilience measures, the Splunk CISO Report 2025 paints a starkly different picture. The study found that 67% of organizations were compromised by social engineering and 57% by AI-driven phishing and deep-fake campaigns, yet fewer than half have modernized their strategies to meet these threats. This disconnect puts every organization at risk, because confidence without action leaves gaps that adversaries will exploit.

For any organization, the risk of downtime and data breaches is an unacceptable cost. These challenges call for a rethinking of traditional security strategies and an embrace of a proactive, integrated approach that places security at the heart of your network from day one.

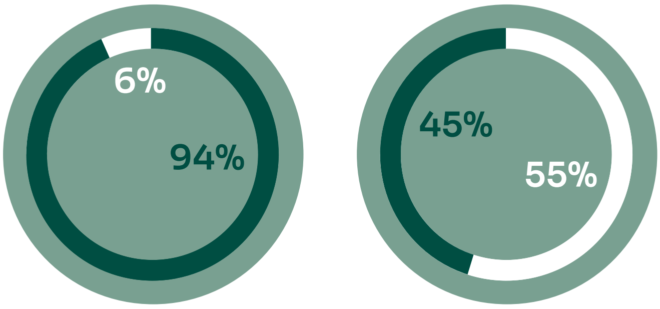


Figure 2. 94% believe they're secure yet only 45% are prepared for AI threats

The secure-by-design strategy

A holistic security strategy for modern enterprise networks addresses the “what” in terms of technology frameworks and business processes. It requires rearchitecting your network to integrate security controls at every layer rather than relying on add-on solutions after an incident occurs. The rise of AI-powered attacks, identity spoofing and remote workforces has made it clear: defending the edge is no longer enough. What’s needed now is not just more security, but smarter, context-aware security built into the very design of the network.

Zero Trust: Always verify, never assume
At the core of a secure-by-design strategy is the Zero Trust model—originally coined by Gartner. It’s more than just a buzzword; it represents a fundamental shift in the way organizations approach security. Instead of assuming that everything behind the corporate firewall is trustworthy, Zero Trust mandates that every request—whether from inside or outside the network—must be authenticated, authorized and continuously validated.

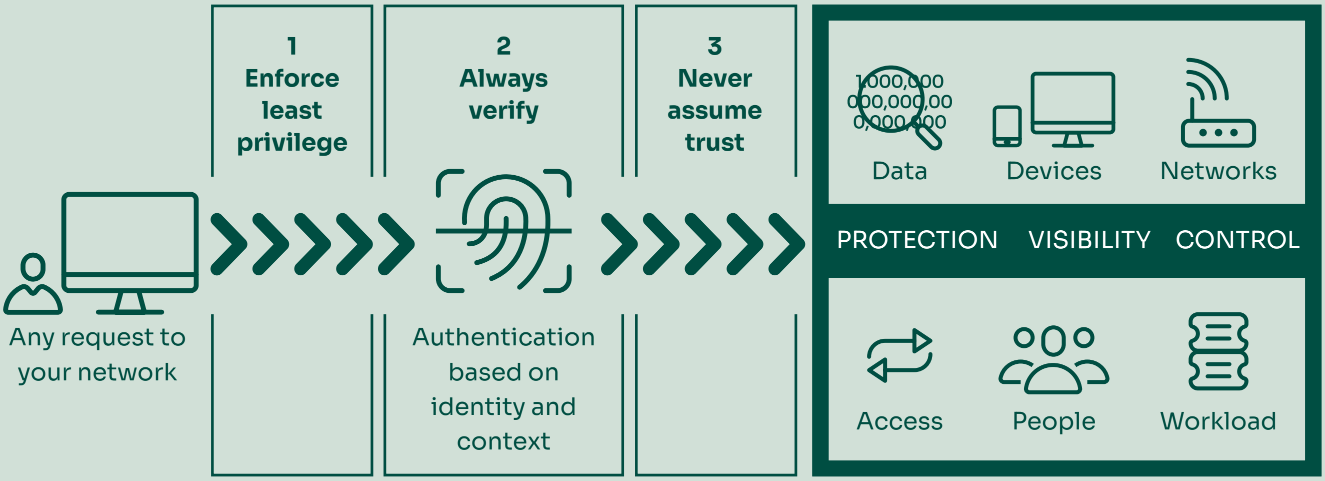
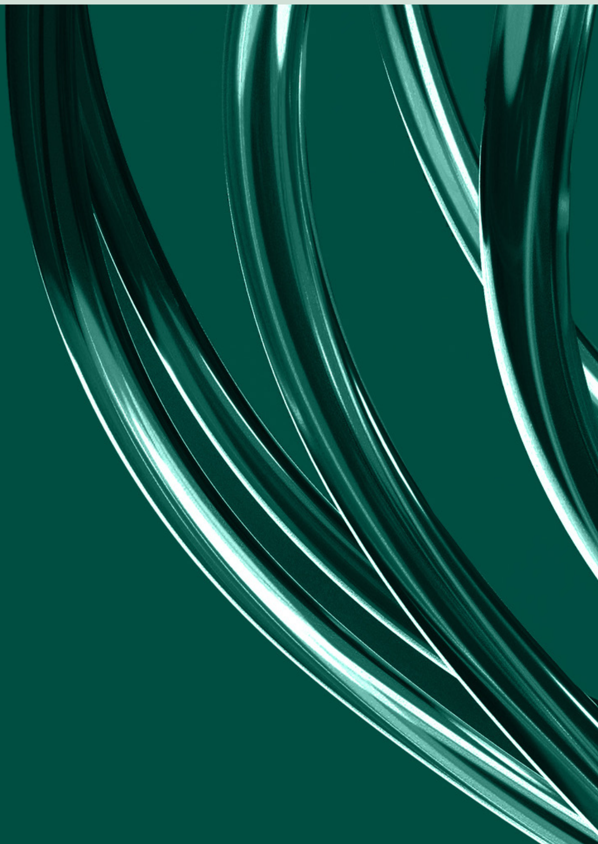


Figure 3. Three key principles of Zero Trust



> Zero Trust: Always verify, never assume.”

Zero Trust principle	What it means	How it appears
Never assume trust	No user, device or application is implicitly trusted. Each access request starts with zero trust and must prove authenticity.	Network micro-segmentation isolates workloads and limits lateral movement. Even internal traffic is treated cautiously, reducing the potential impact of any breach.
Always verify	Access is continuously checked against authentication and authorization policies; if these checks fail—due to compromised credentials, device non-compliance or unusual behavior—the session is immediately terminated and the asset is isolated for investigation.	Contextual policies monitor identity, device posture and behavior in real time, revoking session tokens and placing non-compliant or risky devices into quarantine virtual local area networks (VLANs) or restricted segments, while generating alerts for security teams.
Enforce least privileges	Users and devices receive the minimal access rights needed for their tasks, and those rights are revoked immediately when no longer required.	Dynamic access controls adjust permissions in real time—granting only specific application or network segment access and reducing exposure.

These core principles are amplified by advanced capabilities that turn insights into action—detecting threats in real time and automating responses to keep your network secure by design. These supporting pillars are:

- Integrated threat intelligence: Aggregates data from network firewalls, endpoints and cloud services to detect anomalies and feed real-time insights into policy engines.

- Automation and orchestration: Automated playbooks codify incident response, policy updates and remediation—ensuring consistent, rapid actions across your entire environment.

By combining Zero Trust principles with live intelligence and automated enforcement, organizations shift from reactive defense to a proactive, adaptive security stance—anticipating threats and neutralizing them before they can escalate.

Built-in security across the network

Think of enterprise security as something that's purpose-built—not bolted on after the fact. It begins with how your LAN and WLAN are architected at each location, designed to verify every device and user that connects. It extends through an intelligently structured SD-WAN that interlinks offices and branches globally with policy-driven security baked into every route. And it culminates in cloud-delivered protection via SASE, where remote access and SaaS connectivity are safeguarded by continuous inspection and dynamic controls. This is a secure-by-design model, where Zero Trust isn't just a policy, it's an architectural foundation that hardens the entire network fabric from edge to cloud, ensuring performance, scalability and consistent risk mitigation at every layer.

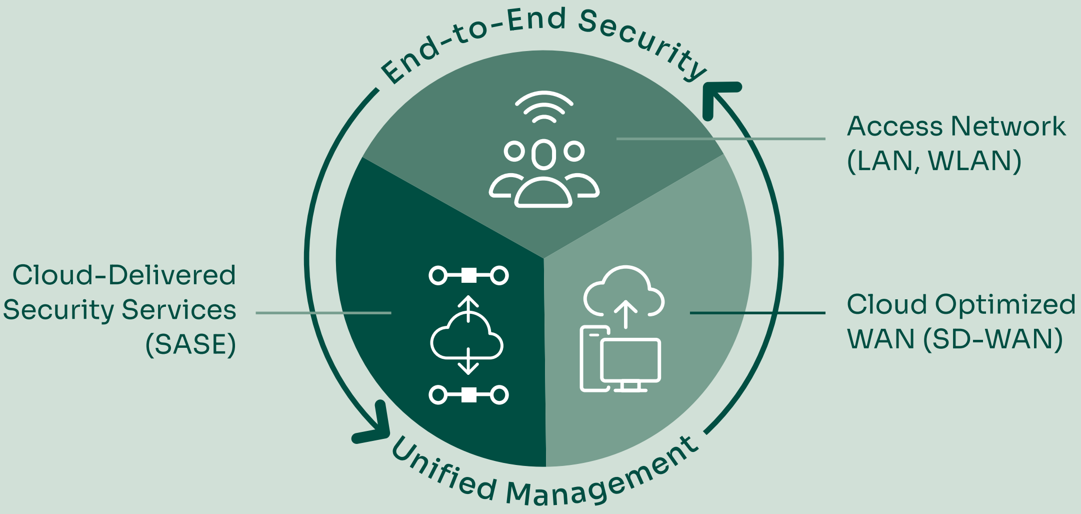


Figure 4. Security across access network, SD-WAN and cloud connectivity

1. Access network security (LAN, WLAN)

First, there's the access layer—comprising both LAN and WLAN—where employees connect as soon as they step into the office or log on from remote locations. Integrating security here means implementing identity-based access controls and network segmentation. The goal is simple: only trusted users and devices should gain entry and, once inside, their access is limited to only what they truly need. Leverage next-gen switches and wireless controllers with built-in network access control (NAC), device profiling and dynamic VLAN assignments. As soon as a user or device joins, network policies apply—identities are bound to specific micro-segments and egress rules. This stops malicious insiders or compromised endpoints from moving laterally.

2. Cloud-optimized WAN (SD-WAN) security

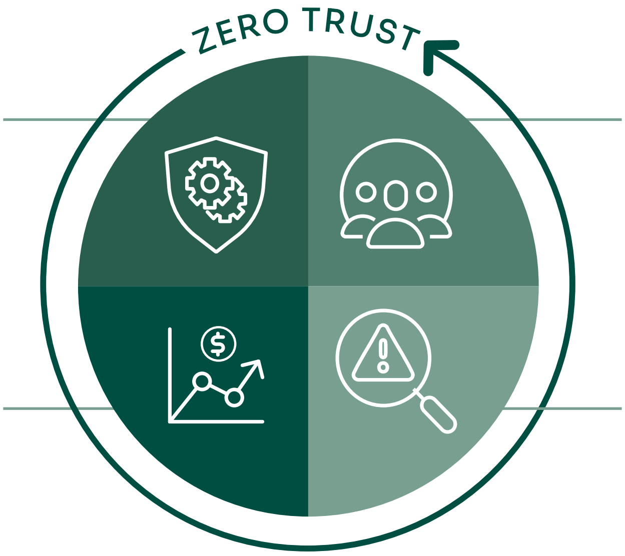
As connectivity extends beyond the office, SD-WAN solutions provide intelligent, dynamic routing across dispersed locations. Gone are the days of rigid legacy WANs that treat every connection the same. Modern SD-WAN appliances incorporate next-generation firewall (NGFW), intrusion prevention system (IPS) and domain name system (DNS) security within the same appliance that routes traffic. Policy-based orchestration ensures branch traffic destined for SaaS is routed through cloud security nodes, enforcing data loss prevention (DLP) and threat prevention without backhauling. This ensures that data moving between branches, data centers and clouds is both efficient and secure.

3. Cloud-delivered security services (SASE)

Cloud-delivered security—in the form of SASE—brings security functions like Zero Trust network access (ZTNA), cloud access security broker (CASB), secure web gateway (SWG) and firewall as a service (FWaaS) to the cloud, offering ZTNA, threat protection, data loss prevention and extended protection to the edge of the network. With the rise of remote work and cloud applications, delivering security from the cloud means that even when users are offsite, they receive the same level of protection without the hassle of backhauling traffic while reducing latency and ensuring secure access regardless of location.

Driving tangible business outcomes

At this point, you might be asking, “What’s in it for my business?” The benefits of a secure-by-design approach stretch far beyond merely reducing the number of alerts or closing a few security gaps. They have real, tangible impacts on your bottom line and overall operations.



Operational continuity
Proactive security at every network layer minimizes disruptions and keeps critical operations running.

Enhanced user experience
Seamless protection keeps the network fast and reliable, delivering smooth user experiences without sacrificing security.

Cost optimization
Reducing breaches and downtime lowers response costs and frees resources for strategic growth.

Accelerated threat detection
Continuous connection validation detects threats in real time and prevents escalation.

Figure 5. Zero Trust: Aligning security with strategic business outcomes

Operational continuity

Operational continuity is mission-critical—especially in industries like banking, retail, healthcare and manufacturing, where even brief network disruptions can lead to financial loss, missed opportunities or compromised trust. By embedding security into every layer of the network, organizations can detect and contain threats before they impact operations. The result? Consistent performance, uninterrupted service delivery and teams that stay focused on innovation—not incident response.

Enhanced user experience

Security isn’t just an IT function—it’s what makes every transaction, interaction and process trustworthy. In banking, retail, healthcare or manufacturing, a secure, high-performing network keeps operations smooth and customers confident. When protection and performance align, you deliver dependable experiences for your users and your customers—and that’s real leadership in today’s digital world.

Accelerate threat detection

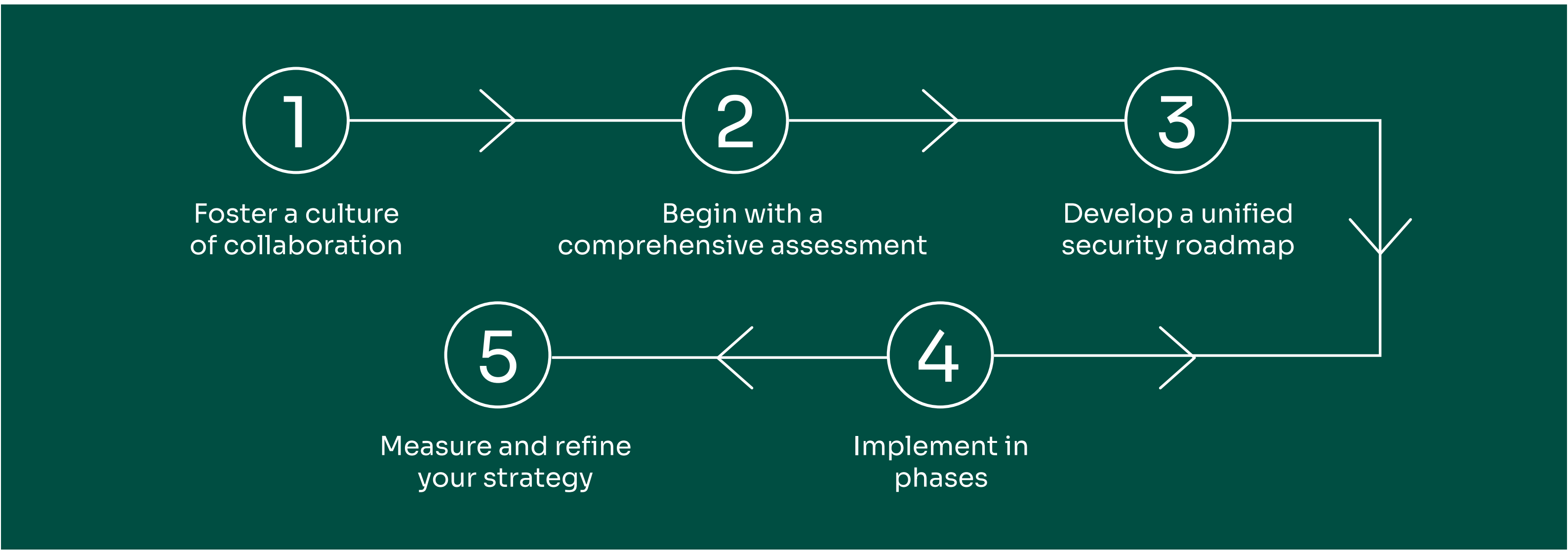
In cybersecurity, speed wins. When your defenses watch every connection in real time, you catch threats the moment they surface—before small sparks turn into raging fires. That rapid response not only keeps damage to a minimum but also saves the hours and resources you’d otherwise spend on cleanup. In the end, this real-time vigilance isn’t just about stopping attacks—it’s about keeping your team focused on moving the business forward, not fighting fires.

Cost optimization

When you embed security from the start, you turn risk into a driver for cost optimization. Catching issues early means you avoid emergency fixes, surprise legal bills and hours lost to crisis management—expenses that quietly balloon when threats go unchecked. In practice, each dollar invested in built-in security shaves thousands off reactionary costs, streamlines operations and gives you the financial confidence to invest in tomorrow.

How to transform your network with integrated security

The “why” and “what” set the stage, but the real value comes in the “how.” How can you transition from outdated, siloed security measures to a future-proof, secure-by-design network? The answer is found in a structured, phased approach combined with collaboration across your organization.


1
Foster a culture of collaboration
2
Begin with a comprehensive assessment
3
Develop a unified security roadmap
4
Implement in phases
5
Measure and refine your strategy

1 **Foster a culture of collaboration**
Embedding security into your network touches every team—networking, security, IT operations and the business lines. Starting with leadership alignment, cross-functional workshops and clear executive sponsorship lays the foundation. Break down the silos between IT, network teams and business units. Encourage a collaborative mindset where all stakeholders have a shared understanding of the risks and opportunities. When everyone understands the “why” and owns the journey, each subsequent technical phase moves forward far more smoothly. In enterprise rollouts, sometimes pilot projects fail when teams aren’t on the same page. By front-loading the cultural dimension, you ensure technical efforts are embraced, not blocked, and that the shift to a secure-by-design architecture underpinned by a Zero Trust model becomes a shared success rather than a lone IT project.

2 **Begin with a comprehensive assessment**
Now that the right teams are engaged, start by taking an honest look at your current network and security infrastructure. Conduct an in-depth audit to identify gaps in your existing network—network topology, security controls and user workflows. This baseline assessment is essential for understanding where your legacy systems are falling short and what improvements are necessary to achieve a secure-by-design architecture.

3 **Develop a unified security roadmap**
Translate assessment findings into a strategic plan that aligns with broader business objectives, whether securing office LAN/WLAN environments or optimizing cloud access for remote users. The roadmap should clearly outline how to integrate Zero Trust principles into every layer of your network. Key actions include:

- Reassessing legacy systems: Identify outdated systems that are no longer sufficient to meet modern security requirements.

- Integrating continuous authentication: Ensure that every connection—whether on-premises or remote—is subject to real-time verification and authorization.

- Leveraging cloud-based security platforms: Incorporate solutions like SD-WAN and SASE that naturally support a Zero Trust model, ensuring secure communication and data access across your entire digital ecosystem.

4

Implement in phases

Network transformation does not have to be implemented all at once. Roll out changes in manageable stages—secure the access network layer first (LAN and WLAN), then the WAN edge and finally the cloud. Pilot and iterate to ensure stability before broad deployment. Consider a phased approach:

- **Phase 1: Secure the access networks (LAN and WLAN)**
  Begin by upgrading your LAN and WLAN security. Implement identity-based controls and segmentation to ensure that only verified users and devices are allowed to connect.

- **Phase 2: Transform WAN connectivity**
  Transition to SD-WAN solutions that inherently support security through encryption and smart, policy-driven routing. This phase connects your sites securely while ensuring optimal performance.

- **Phase 3: Extend protection to the cloud**
  Roll out SASE or similar cloud-delivered security services to protect remote and cloud-based environments. This extends the Zero Trust model to every digital edge and supports modern, hybrid work models.

For each phase, pilot deployments can help you fine-tune the integration process and ensure that the transition is seamless. Regularly reviewing and adjusting your plan based on real-world performance is essential, as it keeps your network adaptive and resilient to changing threats.

5

Measure and refine your strategy

Track operational, security, user-experience and financial metrics. Use these insights to continuously improve, keeping your network agile and resilient. Implement clear metrics to track your progress over time:

- Operational metrics: Monitor uptime, incident response times and system availability.

- User experience indicators: Employ user satisfaction surveys and performance benchmarks to gauge how well your network is serving its users.

- Security effectiveness: Track the number of incidents, the speed of threat detection and the efficiency of responses.

- Cost savings: Analyze reductions in operating expenses and compare them against your initial investments.

These measurements will not only demonstrate the impact of your transformation but also help continuously refine your strategy as you adapt to evolving challenges.

Critical considerations for enterprise leaders

For today's enterprise leaders, rethinking your network security posture is vital to business resilience and long-term viability. Security must be embedded across all layers of your infrastructure—from the data center to the network edge, from branch connectivity to user access.

As you assess your organization's readiness, consider these five key questions:

1. If your network were breached tomorrow, how long would it take before business operations—and your customers' trust—begin to unravel?

2. In a world where cyber threats evolve faster than strategies, how sure are you that your security architecture isn't quietly becoming your biggest competitive liability?

3. How many of your teams are still firefighting fragmented network and security controls instead of focusing on improving performance, uptime or user experience?

4. How much are you spending on reactive fixes, licensing overlaps or unmanaged risks that go undetected?

5. When systems span cloud, edge and hybrid work, how confident are you that your network security is working as a cohesive defense—not just a patchwork of tools?

As the cyber landscape grows more challenging, a secure-by-design strategy becomes a strategic necessity. It's not just an IT issue but a leadership priority. Are you prepared to lead your enterprise into a secure future?

Conclusion

In today's digital-first world, siloed and legacy security models can't keep pace with modern threats or growing network complexity. By embedding security into every layer—from the access network (LAN/WLAN) to the WAN edge with SD-WAN, and secure, policy-driven access to cloud applications through SASE—you ensure continuity, enhance user experiences, detect threats faster and reduce costs.

As businesses become more distributed and cloud-reliant, the risk of sticking with outdated network infrastructure grows. Forward-thinking leaders are now reimagining their networks—not just to connect, but to protect. If you're planning a transformation or facing challenges modernizing your network, our experts are here to help. Schedule a complimentary consultation to assess your readiness and define a path forward. Let's build a future-ready network with security at its core.

To learn more about how NCR Atleos Managed Network Services can help your operation, email NCRAtleos.TelecomandTechnology@ncratleos.com.

NCR Atleos Telecom & Technology team is your global end-to-end service partner for enterprise network infrastructure. We embrace innovation to optimize customer experience while maintaining the highest levels of service delivery, efficiency, and quality - no matter which part of the world you or your customers are.

Contact us at NCRAtleos.com today

Why NCR?

NCR Atleos (NYSE: NATL) is a leader in facilitating banks and retailers to deliver best-in-class self-service banking experiences for consumers. NCR Atleos helps customers expand their reach, provide greater financial access for customers and reduce operational complexity through industry-leading technologies, unmatched global services capabilities, the largest surcharge-free network and expertise in running ATM networks. NCR Atleos is headquartered in Atlanta, Georgia, with 20,000 employees globally.

NCR ATLEOS

NCR Atleos continually improves products as new technologies and components become available. NCR Atleos, therefore, reserves the right to change specifications without prior notice.

All features, functions and operations described herein may not be marketed by NCR in all parts of the world. Consult your NCR Atleos representative or NCR Atleos office for the latest information.

Patents Pending   SECNETF-0625   ncratleos.com