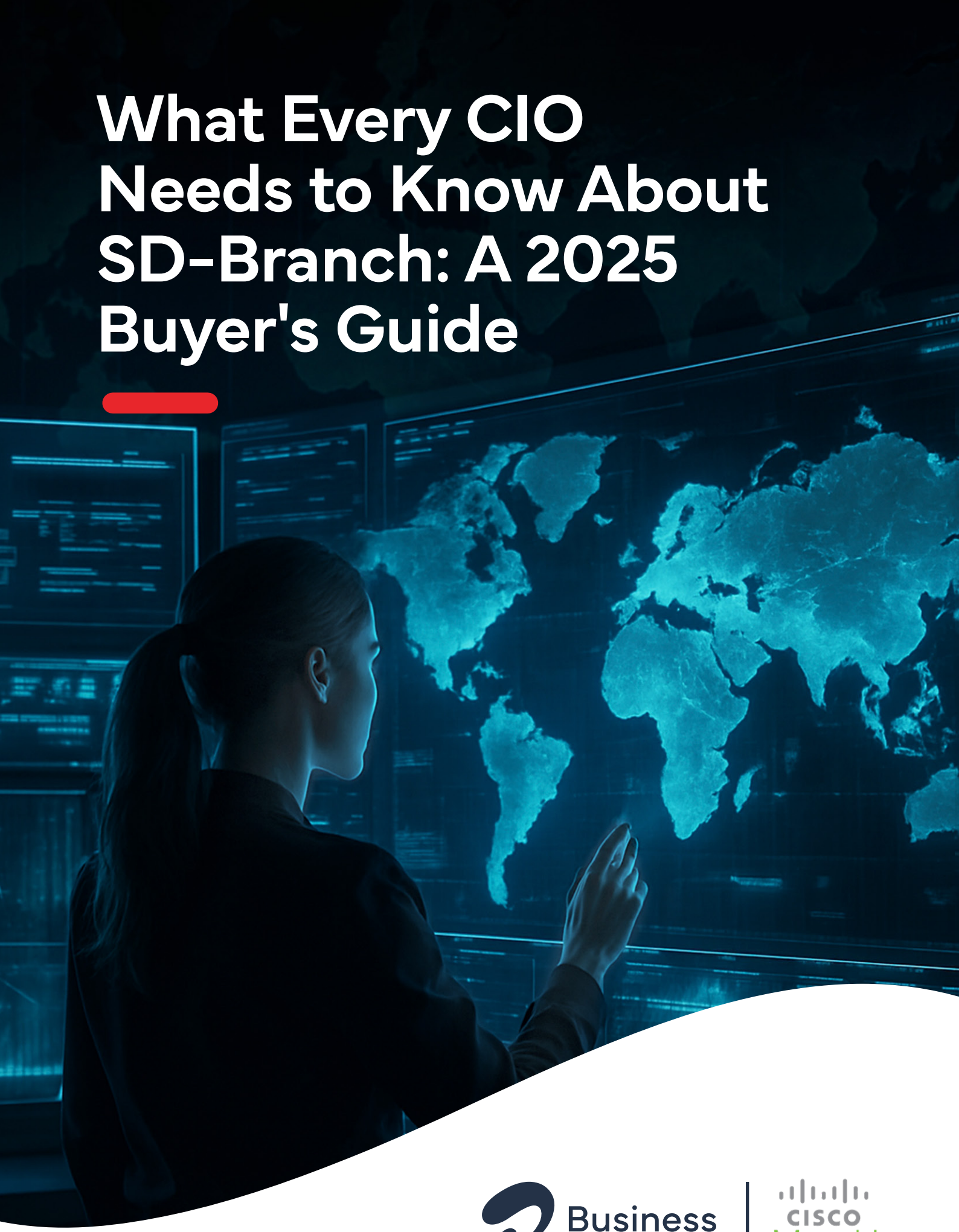
What Every CIO Needs to Know About SD-Branch: A 2025 Buyer's Guide



Business | cisco Meraki

Introduction and Context

As businesses expand across geographies, managing multiple branch networks has become increasingly complex. Traditional WAN architectures no longer meet the demands of modern cloud-first operations. Airtel SD-Branch, powered by Cisco Meraki, offers a secure, scalable, cloud-managed solution to simplify and optimize branch networking.

Buyer Challenges and Pain Points

Organizations encounter mounting complexity in managing their branch networks. Legacy WAN architectures, fragmented LAN setups, inconsistent security controls, and limited visibility can significantly hinder performance, user experience, and operational efficiency. IT teams are stretched thin trying to maintain uptime, enforce policies, and support growing digital demands — often with tools that weren't built for distributed, cloud-first environments.

Below are the most common challenges enterprises face, grouped by core areas of branch networking:

WAN (Wide Area Network) Challenges

- Frequent outages or performance degradation affecting cloud apps, VoIP, and customer-facing systems
- Single-line dependency leads to branch downtime during failures
- High cost of legacy MPLS circuits across multiple branches
- No application-aware traffic routing or prioritization. Business-critical apps (e.g., POS, ERP) compete with recreational traffic.
- Long provisioning cycles for new site connectivity

LAN (Local Area Network) Challenges

- IT burden and higher error rates during rollouts or updates
- No segmentation between employee, guest, and IoT devices
- Guest devices and internal users may share the same broadcast domain—security and compliance risk
- Lack of visibility into switch port health or client associations
- No real-time visibility or alerting on LAN device status or port activity

Security Challenges

- Each location may have different policies or versions, increasing attack surface
- No branch-level intrusion detection or malware prevention
- Inability to enforce content filtering or usage policies. No control over user behavior, opening risks of phishing, shadow IT, or non-compliance.
- Manual VPN setup between branches and HQ — error-prone and hard to scale
- No protection against lateral threats once inside the branch LAN

Insights & Analytics Challenges

- IT lacks awareness of application usage, device status, bandwidth consumption at each branch
- No centralized logs or telemetry. Difficult to troubleshoot or audit past issues
- No insight into which users are accessing risky content or hogging bandwidth
- Threats or unusual behavior often go undetected until damage is done

Management & Operations Challenges

- Each branch managed independently — increases admin overhead, delays in rollout or response
- High chance of misconfiguration; hard to maintain consistent policy enforcement
- Delayed patching introduces risk and instability
- Limited ability to segment control across teams (e.g., Wi-Fi vs WAN vs security teams)
- IT teams rely on site visits or VPNs to debug, increasing downtime and costs

Self-Assessment Checklist

Use this worksheet to assess your current network capabilities. Mark each item with:

- Fully in place - Score 1 ☐
- Partially implemented - Score 0.5 ☐
- Not in place - Score 0 ☐

WAN Challenges

- Reliable dual-WAN connectivity at all branches ☐
- Automatic WAN failover in case of link failure ☐
- Application-level traffic steering based on performance ☐
- Cost-efficient WAN with optimized use of broadband/LTE over MPLS ☐
- Rapid provisioning of WAN links for new branches ☐

LAN Challenges

- Consistent Wi-Fi coverage across all branch zones ☐
- Segmentation of employee, guest, and IoT traffic using VLANs or SSIDs ☐
- Cloud-managed switches and access points ☐
- Remote, real-time troubleshooting capabilities ☐

Security Challenges

- Consistent firewall policies across all branches ☐
- Deployment of intrusion prevention and malware protection at branch level ☐
- Ability to block access to malicious and inappropriate websites ☐
- Scalable, automated VPNs between branches and HQ ☐

Insights & Analytics Challenges

- Real-time visibility into network usage at every branch ☐
- Bandwidth tracking per user, application, and device ☐
- Centralized storage of logs and analytics for auditing and forensics ☐
- Automated detection of anomalies and security threats ☐

Management & Operations Challenges

- Centralized management of the entire branch network ☐
- Automated provisioning, patching, and configuration updates ☐
- Use of policy templates for consistent deployment ☐
- Role-based access control for multi-team or regional ☐

Score Yourself

- **22–20 :** You're in great shape-consider Airtel SD-Branch to simplify and scale ☐
- **19–13 :** Partial readiness-time to modernize with cloud-managed automation ☐
- **12 or less :** You're exposed to inefficiencies and risks-a strong case for SD-Branch transformation ☐