POINT OF VIEW

The Right SD-Branch Solution Solves Networking and Security Challenges

IoT Is One of Many Issues

Executive Summary

Distributed organizations are rapidly adopting the latest digital innovations. These include high-performance tools and a wide assortment of Internet-of-Things (IoT) devices. The explosion of these devices at the network edge has greatly expanded the attack surface of many organizations.

At the same time, increasing bandwidth and performance requirements are leading to changes to the branch WAN, often compromising security. Network engineering and operations leaders find it difficult to attain strong visibility and centralized policy management over their increasingly complicated and risk-prone branch infrastructures. A solution that converges networking and security functions is the best way to meet performance expectations and stop cyberattacks.

The number of IoT devices worldwide is forecast to almost double from 15.9 billion in 2023 to more than 32.1 billion IoT devices in 2030.[1]

Branch Networking and Security Challenges

Increased demand

The demand on networking infrastructures has exceeded the capacity of outdated WAN technologies. The traditional WAN relies on expensive MPLS connectivity and a hub-and-spoke architecture that backhauls all traffic through the corporate data center for centralized security checks. This approach creates bottlenecks that interfere with network performance and reliability. In addition to users demanding fast and reliable access to resources, IoT applications need reliable WAN connections to leverage cloud-based management and big data repositories.

Technologies like SD-WAN offer faster connectivity options to support digital innovation applications, but most solutions inherently lack security and advanced networking capabilities.

Complexity

Most branches have complex architectures with a variety of network devices that are not integrated and lack centralized administration, cohesive control of security policies, and visibility across all parts of the branch network. This is especially true for the access layer's wired switching and wireless access points. As a result, organizations often struggle to support critical functions like:

- Access control
- Traffic analysis
- Identification, tracking, and monitoring of networked devices
- Detection of advanced malware

Lack of visibility and centralized management ratchets up risk and increases inefficiencies for network engineering and operations leaders. The disaggregated networking and security products deployed across the branch infrastructure typically do not share threat intelligence or coordinate responses to cyber events, slowing down response times to security incidents. This disparate approach also makes it difficult to determine the causes of network issues. In turn, the chance that critical operations across the organization will be disrupted and that there will be a security breach is increased.

IoT exposure

To complicate matters further, IoT devices are being adopted in large numbers to facilitate business at the branch. IoT devices include everything from light switches to printers to medical devices. Cybercriminals frequently target these devices because they are some of the weakest points on the network.

These devices often lack built-in security, cannot be patched, and cause unique blind spots, presenting significant challenges to branch security. Traditional endpoint security solutions are too large or resource-intensive to run on most IoT devices. To make matters worse, many of these devices are added to the branch network without the knowledge of IT or security teams.

Cybersecurity threats such as malware attacks, phishing, and unauthorized access increasingly target IoT devices. These devices often act as entry points into broader networks, making them attractive targets for cybercriminals.[2]

Unfortunately, branch solutions typically lack key capabilities for addressing the lack of security and visibility that IoT devices present. Without comprehensive and centralized IoT device visibility, branches (and by extension, the broader organization) are vulnerable to attack. Network engineering and operations leaders need to be able to detect, classify, onboard, and secure every connected endpoint device on the branch network. However, outdated network access control solutions often lack advanced capabilities for managing IoT devices. For example, they do not automate policy-based threat response for a potentially compromised device, such as quarantine and detailed alerts. Unaddressed IoT device vulnerabilities at the branch also expose organizations to potential compliance violations, compounding the financial damage if a breach occurs.

Non-integrated branch architectures also lack the ability to share threat information in real time and adapt defenses to multiple points of attack in unison. This leaves organizations unable to defend themselves against a coordinated attack across multiple devices or parts of the distributed organization, such as IoT-targeting botnets. IoT devices with known vulnerabilities need to be automatically and immediately secured, in order to protect the organization.

Solving Today's Branch Challenges

As branches continue to evolve, the IT challenges become more complex. Security and IT leaders require a converged networking and security platform to solve increasing bandwidth and performance requirements, complexity, and unique IoT problems. Only by centralizing management and sharing information is it possible to reduce complexity, deliver visibility, and automate security.

To address the rise of IoT, an effective SD-Branch solution offers built-in tools to securely onboard headless IoT devices onto the network. It includes automated control features that proactively protect the wider network when these devices have known vulnerabilities and when they are compromised.

[1] Lionel Sujay Vailshery, Number of Internet of Things connections worldwide from 2022 to 2033, with forecasts from 2024 to 2030, Statista, June 12, 2024.

[2] What Are the Security Challenges of IoT? Nexus Group, March 28, 2024.

September 10, 2024 8:56 PM / 2856089-0-0-EN