# SECURING THE NEXT PHASE OF REMOTE WORK:

## THE ABC'S OF SDWAN + SASE + ZTNA

SDWAN (software-defined wide area networks) has been a very hot topic in my conversations with partners lately, and here's why: While SDWAN may have sounded like a costly and inaccessible alternative to traditional MPLS network connectivity just a few years ago, IT executives are quickly recognizing the productivity, scalability, and security benefits of next-gen WAN solutions to support remote workers and multi-location operations in today's post-pandemic world. Consider this: Due in large part to the increased need for mobility and cloud services, the global SDWAN market size is expected to grow from $3.4 billion in 2022 to $13.7 billion by 2027 – that's a 31.9% compound annual growth rate (CAGR).

As a technology advisor, you can win big with IT decision makers by supporting their digital transformation needs with a complete SDWAN plan that also protects their business from growing cyber threats. SDWAN layered with SASE and ZTNA will be a powerful differentiator for partners looking to grow their cybersecurity business. Let's break down this alphabet soup and take a look at what opportunities lie ahead for you and your SMB customers in 2023.
Why SD-WAN? Because businesses don't live in castles anymore.
Your customers likely have some data sitting in a cloud infrastructure, while other data lives on-premise or in a separate data center. Perhaps a third-party server like Microsoft handles email. And the security team probably works out of a satellite office. Managing all of these endpoints via a traditional WAN where information is programmed directly into each device is near impossible in today's remote and hybrid workplace. Enter SDWAN.

SDWAN is a response to the evolution from the data center to the cloud, allowing businesses to connect their end-users in a safe and reliable way to their third-party cloud platforms and SaaS applications.
SDWAN can intelligently route traffic around congestion based on the type of content being transferred, the endpoint, the time of day, the application's security needs, latency sensitivity, or bandwidth costs. IT teams can manage potentially thousands of network switches from a centralized controller over the internet, cloud topologies, and more. This gives them the ability to scale the network as needed, optimize performance, and make more efficient use of resources.

### Meet SASE & ZTNA: Critical security layers for the digal workplace

Secure access service edge (SASE, pronounced “sassy”) is a framework for network architecture that brings cloud native security technologies together with SDWAN capabilities to securely connect users, systems, and endpoints to applications and services anywhere. Gartner forecasts worldwide spending on SASE will reach $9.2 billion in 2023, a 39 percent increase from 2022. SDWAN + SASE allows IT teams to bring critical security implementations to the remotest edge of their network to address the changing needs of a remote workforce. It also ensures cloud-destined traffic isn’t backhauled to the on-premises data center but transits seamlessly from the user to the cloud without delay or performance impact.

But wait, there’s more! No secure network would be complete without the additional layer of zero trust network access (ZTNA). ZTNA is based on a Zero Trust security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and validated before being granted access to any company data or devices. According to Gartner, Zero Trust is “based on the belief that trust is a vulnerability, and therefore, security must be defined by the strategy, ‘Never trust, always verify.’” So, users only have access to what they need, and everything else is locked down (kind of like how a key card works in a hotel elevator), resulting in better compliance and threat mitigation. Gartner predicts that by 2025 ZTNA will phase out VPN, and will make up at least 70% of new remote access deployments.

### Gartner Predictions

- By 2025, 50% of new SDWAN purchases will be part of a single-vendor SASE offering, up from 10% in 2022
- SASE purchases will reach $9.2 billion in 2023, a 39% increase from 2022
- Zero Trust will replace VPN by 2025, making up 70% of new deployments

### Where AI and ML fit into the mix

Today SASE + ZTNA platforms use AI and ML to determine risk, severity of risk and automatically remediate malicious anomalies—all of which can help IT teams more proactively address network issues and accelerate resolution. SDWAN + SASE is also hooking in all aspects of AI-assisted IT telemetry into a single management orchestration so administrators will no longer need multiple tools with multiple portals to collect and analyze data. Telarus will be continuously updating our partners on the latest AI developments across our supplier portfolio throughout the year.

### Making the business case for the complete SDWAN package

If your customers are hesitant to future-proof their business with new SDWAN solutions, it’s likely because of perceived cost and complexity barriers. Fortunately, these are easy to address. One of the big advantages is the solutions can be acquired as a software-as-a-service (SaaS) with little up-front spend. Once adopted, cost savings continue through improved network utilization and productivity. Plus, consider the burden that SDWAN removes from time-strapped engineers because it automates the complexity of managing highly dynamic cloud and remote office environments.

With the shift to the remote and hybrid workforce, the opportunity to introduce the productivity and cost-savings benefits of a secure, complete SDWAN package to your customers has never been better. As a Telarus partner, you have access to best-in-class suppliers who are now offering SDWAN with critical security layers like SASE and ZTNA all in a single-vendor solution, which translates to less administrative overhead and integration challenges compared to multiple solutions. If you haven’t already done so, be sure to check out our SolutionVue™ Cybersecurity Quick Solution Assessment (QSA) tool — it’s a game-changer for taking the guesswork out of creating and walking your customers through a specific action that includes supplier recommendations, education, and quantified business risk.

By: Jason Stein, VP of Cybersecurity, Telarus