CHECK POINT™

Quantum
SD-WAN

MUST-HAVES FOR A SECURE SD-WAN SOLUTION

TABLE OF CONTENTS

INTRODUCTION:

CLOUD: CHANGING NETWORKS, STRATEGIES, AND SECURITY

The past several years have seen organizations accelerate their cloud journeys, moving more data, applications and workloads off-premises. Reducing operational costs and improving performance were two reasons why. Teams can reduce capital spend on premises-based infrastructure and pay for only the compute and storage capabilities they use. Cloud also enables organizations to become more agile—data and applications can be easily accessed via the cloud anywhere they're needed.

These factors are radically changing organizations' business and networking models. As a result, WAN, network and data center models are feeling the strain. To date, extending traditional MPLS WAN connectivity to branch locations has been expensive and complicated. Organizations have relied on private leased lines, where an MPLS Ethernet solution delivering 100Mbps capacity can easily cost $1,000 per site, per month. Not only is bandwidth insufficient for today's needs, but overheads can quickly add up, on top of the time it takes to secure circuits and deploy networking equipment.

The Move to SD-WAN

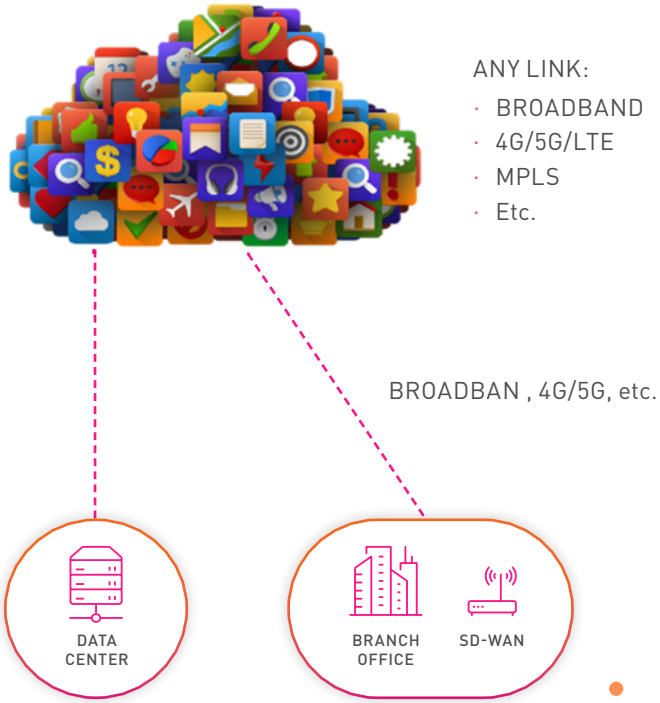
Organizations are turning to software-defined WANs (SD-WANs) to more easily connect branch locations to the cloud, to each other, to datacenters and their main campus.

Gartner predicts that by 2025, 65% of enterprises will have implemented SD-WAN—up from 30% in 2020 . Organizations have multiple goals.

To optimize budgets, organizations want the option of using multiple inexpensive links for more bandwidth and being able to route traffic based on cost, application or users. For example, they can prioritize bandwidth for latency-sensitive applications, such as web conferencing services (e.g. Zoom, Microsoft Teams) and remote help desk support, and give lower priority to non-business applications.

Improving performance, over an SD-WAN, branches can access cloud assets directly from local internet service provider links, without requiring network traffic to be backhauled to a data center first. With direct access, branch offices can connect to each other in an overlay network and to cloud assets via the internet with optimal speed and uptime.

In summary, an SD-WAN optimizes internet connectivity with better service levels and lower costs. For example, branches can implement two 1-Gbps broadband internet links at $80 each for $160 per month per site, and connect them both to an SD-WAN solution for $50 per month. All for a total of around $200 per month/site as compared to an MPLS solution of 100Mbps at $1,000-1,500 per month/site—immediately reducing costs by up to 80%. An organization can take advantage of multiple, inexpensive broadband connections and gain optimized connectivity everywhere it's needed, leveraging support for broadband, 4G/5G/LTE, and MPLS connections, to greatly simplify connectivity, with multiple links used in active/standby mode, or be used simultaneously for bandwidth aggregation.



An SD-WAN solution ***reduces monthly expenses by up to 80%*** *while delivering more resiliency, faster connectivity and routing that is optimized by user or application type.*

SD-WAN CHANGES THE SECURITY LANDSCAPE

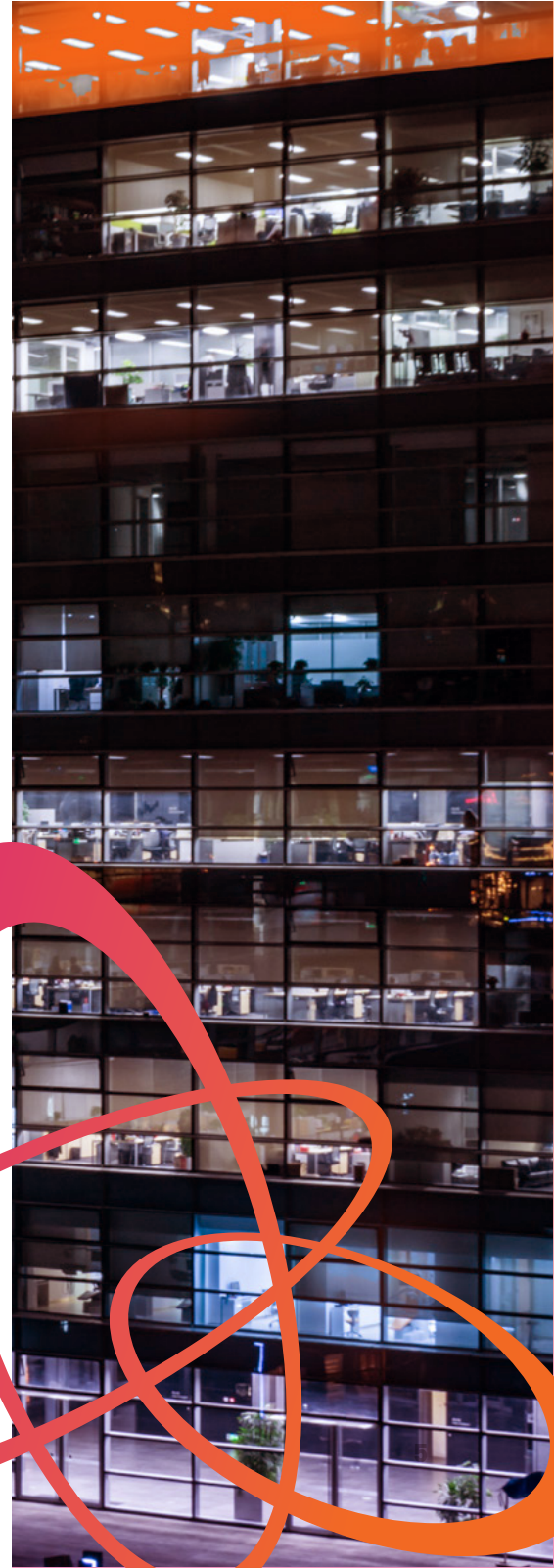
The benefits of SD-WAN are changing the networking landscape. However, the trade-off is security. Although traffic avoids backhaul to a centralized data center, it also bypasses centralized data center security measures, like firewalls, IPS, threat prevention and DLP, leaving branches unprotected. With an expanded footprint and local branches connected directly to the internet, an organization's attack surface and the risk of a cyber attack increase. Unprotected by centralized security defenses, users are more likely to download a malicious file, access a phishing site or inadvertently get infected with ransomware. Meanwhile, attackers or malicious insiders can exfiltrate sensitive information more easily with no mechanism to vet outgoing files, and prevent them from leaking to the web.

Making matters worse, IT and security teams have little or no visibility into suspicious activity at branch locations. Even though monitoring tools can increase security visibility, most lack the ability to investigate and troubleshoot locally with branch-level logging and event monitoring. Managing security policies across multiple locations also becomes more difficult. In a centralized security model, teams can apply consistent policy across the organization. In an SD-WAN environment, they now must apply policy to the primary campus and multiple smaller environments, making it difficult to ensure consistent protection. Not only does SD-WAN technology change the way organizations connect, it changes the way they must be secured.

Enter Integrated, Secure SD-WAN.

Naturally, as enterprises implement SD-WAN, they want to secure branches to protect incoming and outgoing connections with the latest security and threat prevention. A single solution that integrates security and optimized connectivity is becoming the preferred method of securing SD-WAN connections.

The market for SD-WAN is expected to grow at a CAGR of 26%, growing from $2.8 billion in 2023 to $5 billion in 2026.



INTEGRATING SD-WAN SECURITY: WHY IT MATTERS

Securing a variety of locations, connections and applications that make up internal networks and the network edge can quickly become complicated. Most SD-WAN vendors include a level of basic security, leaving organizations to fill in gaps by deploying multiple solutions across their infrastructure. However, this "patchy integration" approach presents challenges:

Inadequate protection: Branches need the same enterprise-level security as the rest of the organization, especially with multiple internet connections that increase exposure to cyber risk.

Lack of visibility: SD-WAN routing can often bypass existing network monitoring tools in favor of the best available route. Without visibility into all traffic, it's difficult for teams to secure it.

Service delivery: Different branch locations have different security and networking requirements and exposure risks. Security must be tailored to each location's needs.

Inconsistent policies: When different security point products are deployed at different office locations, the result is disparate levels of security and threat prevention across branches.

Lack of scalability: Distributing security using different solutions across multiple sites and requirements quickly becomes hard to scale.

Management complexity: Combining networking and multiple independent security features makes it more difficult for IT and security to reconcile priorities and tasks.

A better approach is to integrate SD-WAN with industry-leading security protection. Look for an SD-WAN solution that integrates three critical capabilities:

Uncompromising branch security - Embed full, enterprise-grade security into the wide-area branch network for the best protection, and ensure protection for all types of threats.

Reliable, optimized connectivity: Ensure rich SD-WAN capabilities with sub-second failover and the ability to automatically optimize routing based on user group and application type, for example prioritizing web conferencing over file sharing services.

Single SASE solution: For central deployment and management of your security and networking needs, a single solution for security and internet access (SASE) ensures consistent threat prevention across branches with central management, monitoring and visibility across your organization, while providing branch-level granularity.

Look for a solution that integrates advanced threat prevention against and zero-day attacks, phishing, and ransomware threats.

INTEGRATE UNCOMPROMISING BRANCH SECURITY

Organizations should never have to choose between security and connectivity.

Prevention should be at the core of an integrated secure SD-WAN solution. It should provide industry-leading attack detection and fast blocking of attacks before they enter the network and do any damage. Look for a solution that integrates advanced threat prevention against zero-day, phishing, and ransomware threats. Today's 5th generation multi-vector attacks, can quickly move from their point of entry to other branches, applications and devices in your network, requiring advanced preventive capabilities.

Solutions today combine big-data global threat intelligence with AI engines to continuously catch known and unknown zero-day threats. Using deep learning, AI engines ensure that attacks for which no threat intelligence or indicators of compromise (IoCs) exist, are recognized and stopped with near-zero false positives—to minimize alerts and follow up by security teams.

Evaluate solutions for their ability to stop new threats for which no IoCs yet exist (zero-day threats), including new malware and phishing attacks.

The solution should include a full enterprise security stack for branches, including next-generation firewall, application control, URL filtering, antivirus, threat emulation and threat extraction (CDR), DLP and anti-bot features. In addition, SSL inspection delivers visibility into encrypted traffic.

LOOK FOR RELIABLE, OPTIMIZED CONNECTIVITY

Optimal application performance requires the ability to prioritize applications by bandwidth and latency requirements, users' roles, link costs, and other criteria. For example, online collaboration tools have become indispensable. Whether meeting in a web conference or troubleshooting a remote PC, the SD-WAN solution must be able to provide a reliable connection, without latency and jitter.

Optimize Routing for Applications and Users

With so many business and non-business applications competing for bandwidth, your SD-WAN needs a way to automatically prioritize available capacity. To this end, solutions feature autonomous steering of applications based on predefined categories. By distinguishing between latency-sensitive apps such as web conferencing and remote support connections, and other applications such as file sharing and consumer apps, traffic can be prioritized correctly and steered over the best available path.

Evaluate SD-WAN solutions for their ability to automate traffic steering based on application type, ideally with a built-in wizard for steering policy setup. It should be able to automatically identify applications from the very first packet, while accommodating specific policies per user or user groups (e.g. help desk group) to determine the best route and steer traffic accordingly.

This is often accomplished with steering behavior objects, which let you apply similar policies to similar use cases, either automatically or manually when customization is needed. Steering objects allow setting routing preferences based on performance thresholds, link costs or other attributes.
For example, an organization may prioritize links from one or two service providers over a third wireless internet provider, or vice versa.

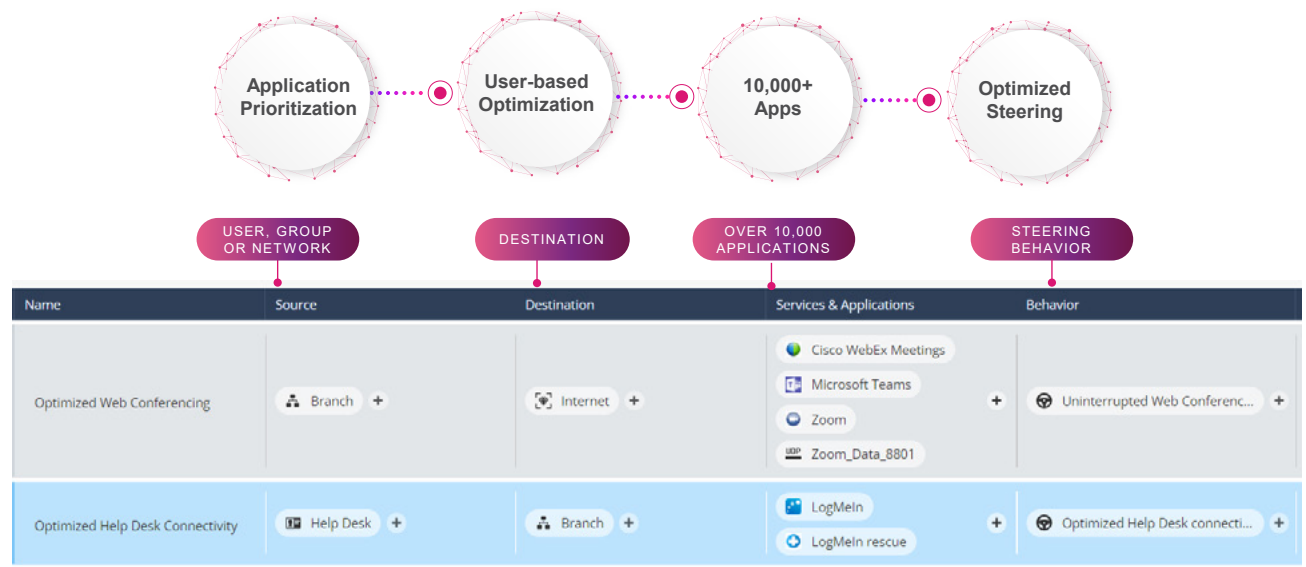


Figure 1: Ensure optimized routing per application or user group

Monitor Link Health

Look for a solution with continuous monitoring to detect unstable connections, burnouts or failures at the application-level in the overlay or local breakout networks and the ability to dynamically select the next best path in real time. Traffic should be monitored for latency, jitter or packet loss to enable automated link swapping, switching from one link to another when defined traffic thresholds are exceeded.

Figure 2: Monitor link health against target thresholds

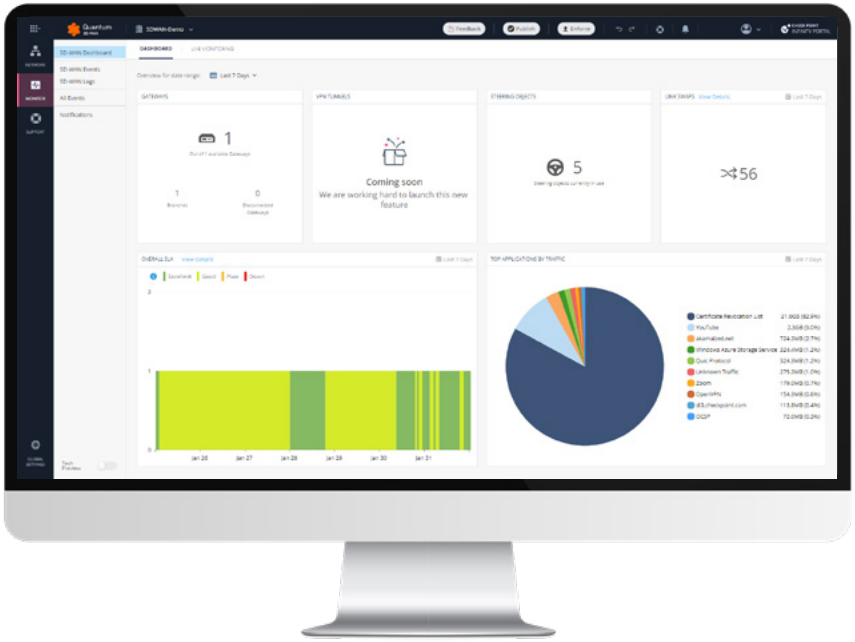


Figure 3: Look for branch-level visiblity with central management

Look for Adanced Analytics

Advanced real-time monitoring and analytics should be easily available on a dedicated dashboard. Look for live monitoring of link SLAs, analytics on link swaps and overall network health. This provides both an at-a-glance overview with the ability to drill down for more detail, if needed, to maintain branch connectivity.

Ensure Sub-second failover

Traffic steering needs may change quickly. The ability to optimize routing for enterprise applications and users is critical to ensuring good user experiences, especially for web conferencing, remote support and other latency-sensitive applications. Unstable connections, link burnouts or outages mean that the SD-WAN and its security must adapt on the fly. Look for a solution with sub-second failover for smooth, seamless handoffs when needed, so changing connections from one service provider to another remains virtually unnoticeable.

Support Multiple Links

Multiple links make it possible to use more bandwidth and choose the most efficient path for traffic based on application, performance, link cost or other attributes. While some solutions support all connection or link types, others support only some. For wireless connections, such as 4G, 5G and LTE and 5G some integrated secure SD-WAN appliances already contain SIM card slots. Ensure the solution can support any link you plan to use, which may include DSL (copper phone lines), cable (aka coaxial cables) and fiber-optic cables.

Aggregate Bandwidth

Ensure the ability to aggregate link capacity utilizing links from multiple service providers. Bandwidth aggregation eliminates the need to designate redundant tunnels that sit idle in active/standby mode until needed. Link aggregation also maximizes bandwidth utilization using local breakout and overlay connectivity.

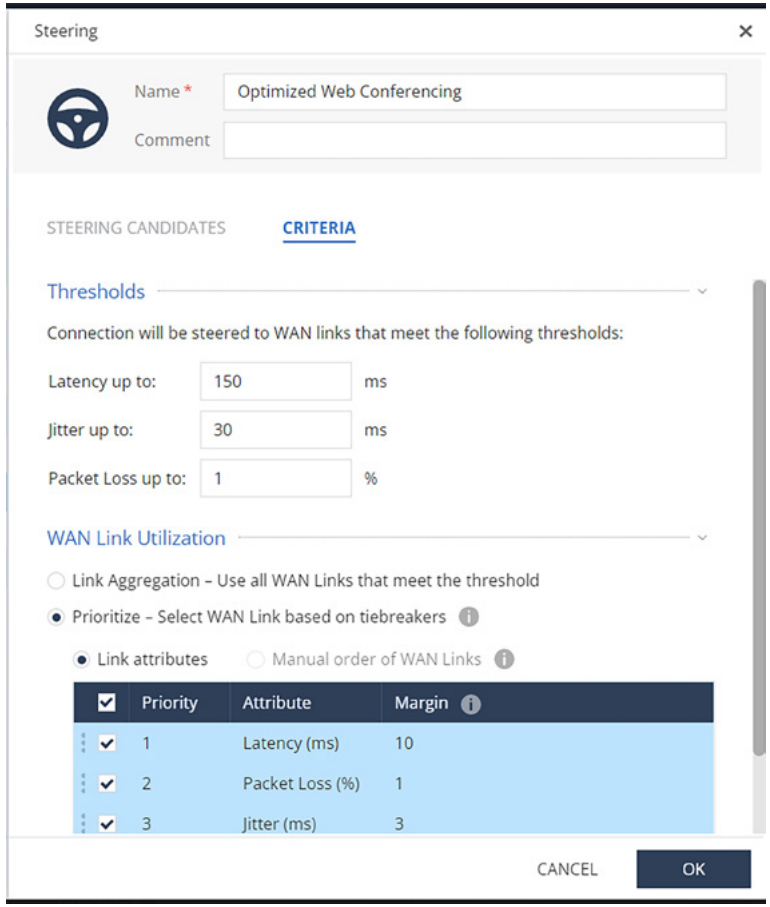
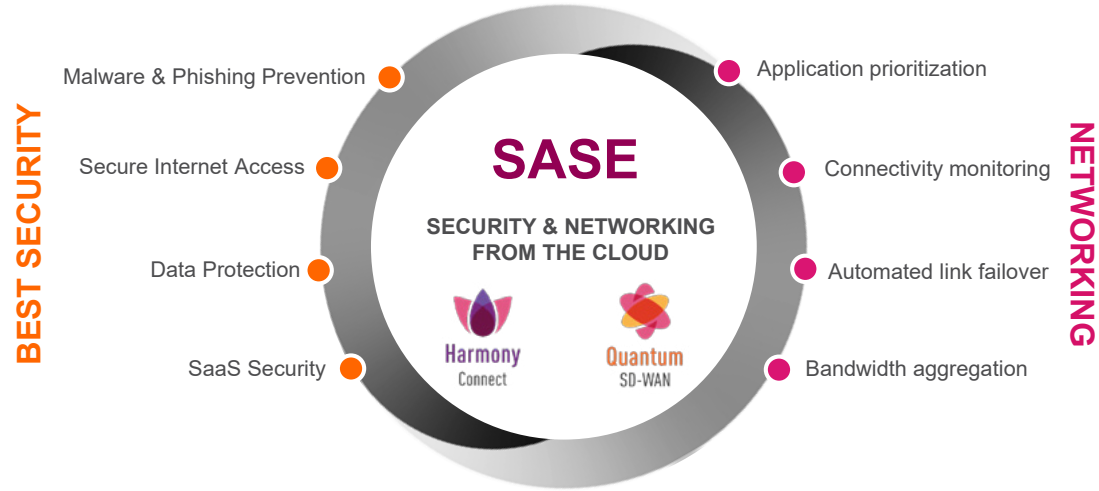


Figure 4: Support multiple links with customizable failover thresholds

GAIN A UNIFIED SASE SOLUTION

To simplify administration, improve visibility and enforce consistent policies, look for a complete security and internet access solution, also called a secure access service edge (SASE). Ideally, a single intuitive cloud-based platform should be used to centrally manage branch-level connectivity (SD-WAN) and branch-level security.



Unified Management from Check Point Infinity

Ensure Consistency Everywhere

Unified management features are non-negotiable. With unified management, teams have complete visibility across everything—data centers, branch offices, remote users, internet connections, cloud assets and SaaS apps. Customizing policy should be easy and intuitive. Teams should have fine-grained visibility into links and applications for defining link thresholds and steering behavior. Centralized visibility ensures that security defenses and policy enforcement are consistent everywhere.

Easy Customization

The solution should enable teams to set steering policy for applications, users and networks on the overlay and local breakout networks. Look for the capacity to steer traffic for thousands of applications and services. Customization should be as simple as defining the source (users, groups, devices or networks) and assigning the relevant steering behavior. For example, VOIP traffic will be routed to any available low-latency link while the company's sales application traffic can be routed over other links.

Planning for a single Secure Access Service Edge

SASE combines wide-area networking with scalable security services into a single solution. It enables teams to secure branch connections and remote user access for any application, anywhere, without the complexities of multiple point security products, disparate management consoles and separate logs. As organizations become more distributed, ensuring visibility and consistency become key to securing an every growing attack surface without compromising on the speed of your connectivity.

HOW CHECK POINT QUANTUM SD-WAN CAN HELP

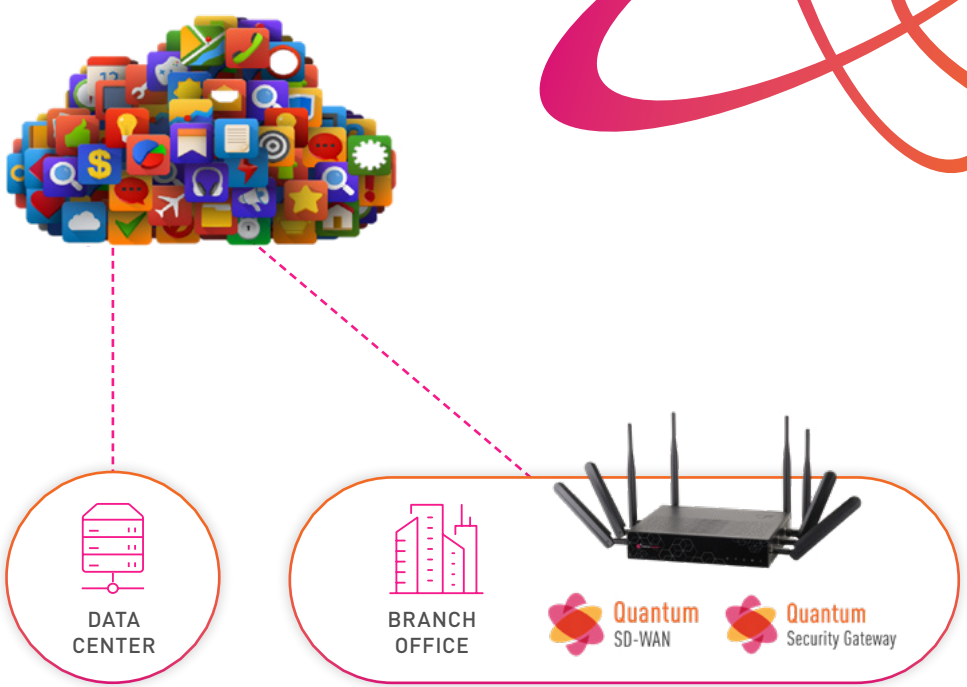
Quantum SD-WAN unifies the Best Security with Optimized Connectivity

Quantum SD-WAN is a software blade in Quantum Gateways that unifies the best security with optimized internet and network connectivity.

Deployed at the branch level, it provides comprehensive prevention against zero-day, phishing, and ransomware attacks, while optimizing routing for users and over 10,000 applications with rich SD-WAN capabilities.

To ensure uninterrupted web conferencing, the solution monitors internet connectivity for latency, jitter, and packet loss, performing sub-second failover for unstable connections.

And for consistent protection and connectivity across users and branch offices, Quantum SD-WAN and Harmony Connect (SSE) combine to deliver a complete security and internet access solution (SASE) managed from the Check Point Infinity cloud platform.



Get an All-in-One Solution

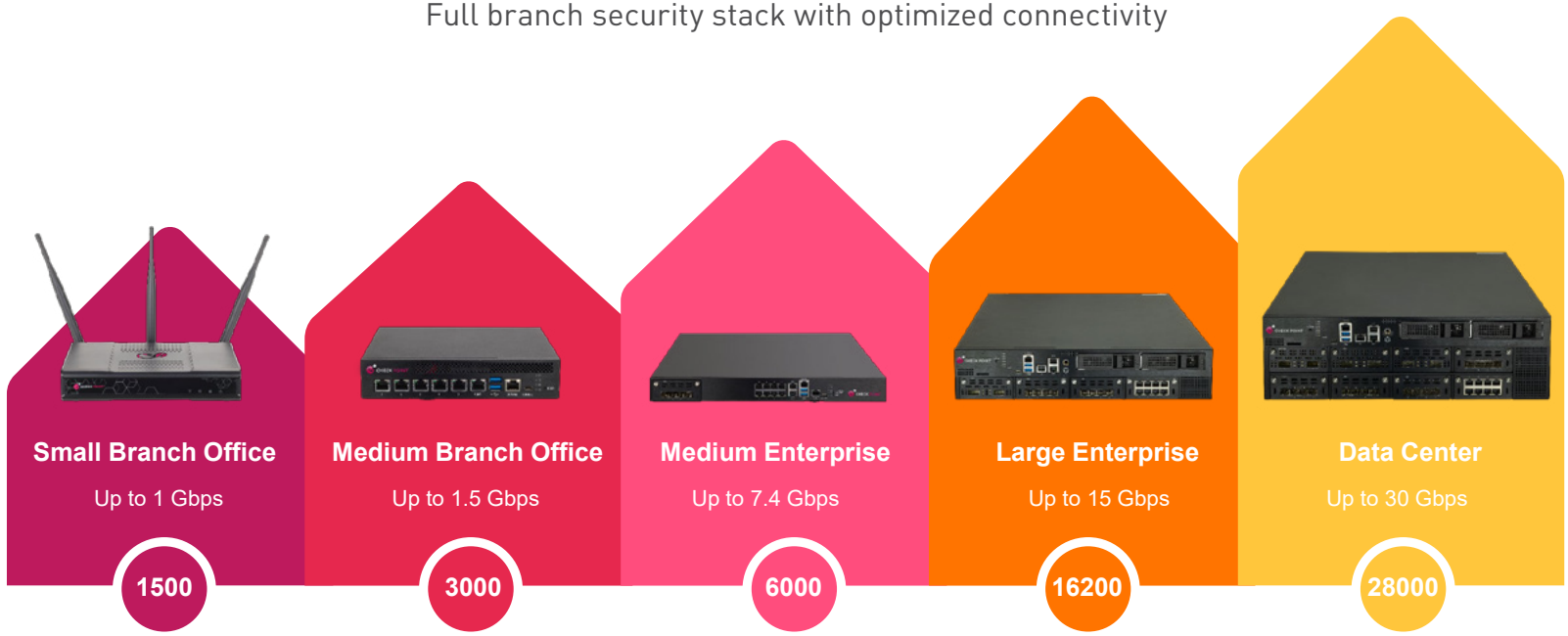
Check Point Quantum SD-WAN embeds rich SD-WAN capabilities into Quantum Security Gateways' industry-leading threat prevention for a lower total cost of operation (TCO) with a single appliance.

Leverage your current Infrastructure

If Check Point Quantum Security Gateways are already deployed, the SD-WAN software blade can be activated with a software upgrade of the current appliance, with no additional hardware required.

Supported in a broad range of Quantum Gateways

Full branch security stack with optimized connectivity



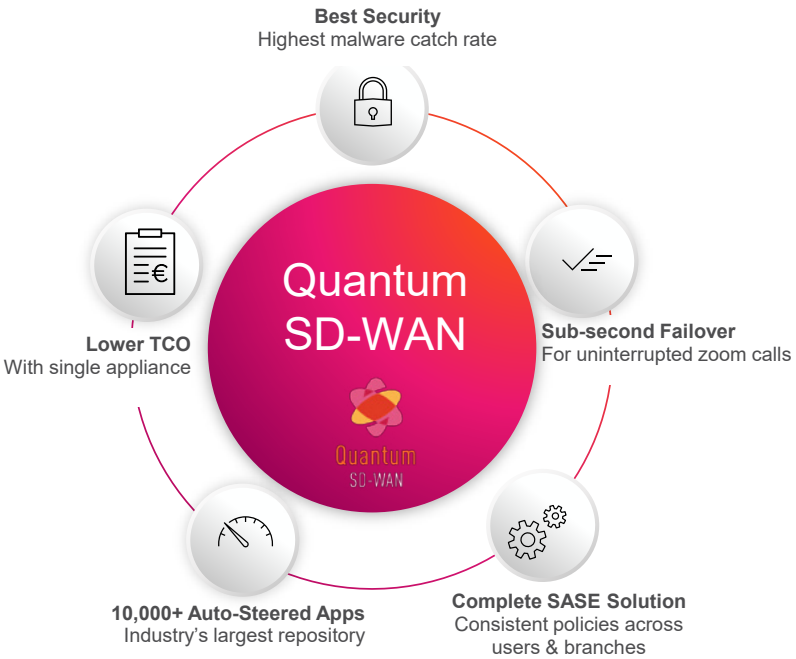
THREAT PREVENTION + SD-WAN* THROUGHPUT

*estimated

Part of the Infinity Architecture

Quantum SD-WAN is part of Check Point Infinity, the only fully consolidated cyber security architecture that protects businesses and IT infrastructures against Gen V multi-vector cyber-attacks across networks, IoT devices, endpoint, cloud and mobile. Check Point Infinity delivers unprecedented protection against current and potential attacks—today and in the future.

For more information, visit:
www.checkpoint.com/quantum/sd-wan/



CHECK POINT™

About
Check Point Software Tchnologies Ltd.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

To learn more about us, visit: www.checkpoint.com

CHECK POINT™

Contact us

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv
67897, Israel
Tel: 972-3-753-4555
Fax: 972-3-624-1100
Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300,
San Carlos, CA 94070
Tel: 800-429-439 / 650-628-2000
Fax: 650-654-4233