
SECURE YOUR EVERYTHING™

# CHECK POINT

# A Guide to Securing Software-Defined Wide Area Networks (SD-WAN)

# TABLE OF CONTENTS

The SD-WAN Revolution ..... 3

SDWAN: The New Paradigm for Branch Office Networking..... 5

Top Challenges to Securing Software Defined Wide Area Networks..... 6

Top 5 Recommendations for Securing SD-WAN ..... 7

1. Basic Next Generation Firewall Signature-based Inspection ..... 7
2. Enterprise-Grade Always Up to Date Threat Prevention Security..... 9
3. Unified Security Management, Security Policy and Threat Visibility..... 10
4. Flexible Deployment Options ..... 11
5. Best Security and Best Networking ..... 13

Summary ..... 14

# Introduction: The SD-WAN Revolution

Businesses are accelerating their digital transformation to cloud SaaS applications like Office 365 by adopting Software-Defined WAN technology. SD-WAN provides network innovation by enabling enterprises to connect branches directly to local Internet providers. This improves end user experience significantly by reducing latency caused by routing traffic through the data center. In addition, local Internet providers give enterprises more cost effective alternatives to using dedicated networking protocols, such as Multiprotocol Label Switching (MPLS) lines. Telecommunication providers have also adopted SD-WAN so they can offer SD-WAN as an alternative to the MPLS lines they already provide to enterprises.

SD-WAN adoption is starting to enter into the mainstream. Gartner estimates SD-WAN sales will grow at a 75% CAGR between 2017 and 2022[1]. However, connecting directly to the Internet using SD-WAN bypasses datacenter security and exposes branch offices to a range of cyber attacks from basic malware to sophisticated multi-vector attacks compromising privacy, data and intellectual property.

## HIGHLIGHTS

- SD-WAN solutions provide cloud connectivity closer to the edge removing latency for a better user experience and lowering costs.
- Connecting branch office SD-WANs to local internet providers bypasses datacenter security exposing branch offices to cyber attacks.
- SD-WAN Security solutions should prioritize threat prevention, flexible deployment options, and scalable management for security policy consistency.

This Guide to Securing Software-Defined Wide Area Networks will review why SD-WAN is popular and recommend how to solve the inherent security challenges.

## BACKGROUND: BRANCH NETWORKING MUST EVOLVE

Branch office locations play a crucial role in a wide variety of industries including financial services, retail and healthcare. The preference to interact with consumers directly for services like banking, insurance, retail and healthcare requires branch offices, clinics and stores to be distributed. In addition, the increase in "edge computing" (where data acquired in remote locations is processed locally) is becoming strategic in the drive for digital transformation.

---

1 Gartner: Market Guide for Managed SD-WAN Services, G00366593, 15 May, 2019

Traditionally, the network architecture to support branch offices was hub and spoke using MPLS, often with a Virtual Private Network (VPN) backup over broadband. This worked well enough when most processing was done in the data center, but that approach is no longer attractive for several reasons:

• According to Gartner, 50% of productivity apps will be moving to cloud by 2022[2] . This includes office productivity and collaboration applications like video conferencing.

• Traditional hub and spoke WAN architectures require the data to be routed through the data center before reaching the cloud. This adds latency leading to a poor cloud application user experience: SaaS or IaaS-based applications need high-speed, low latency direct Internet connections, with full application security and performance management.

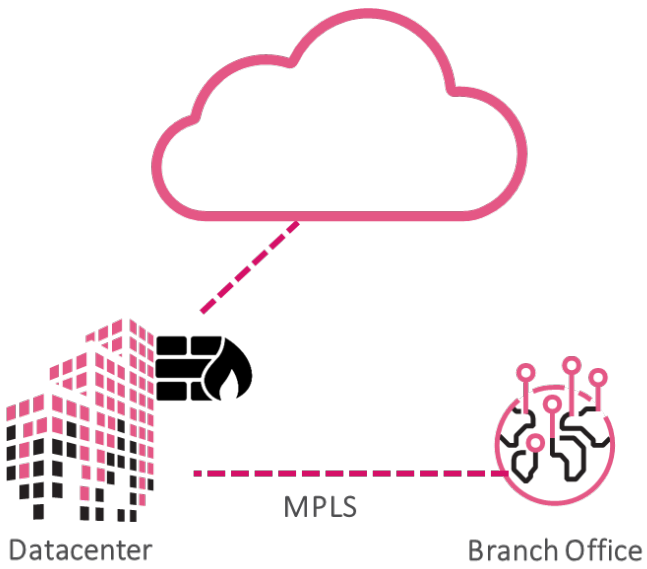
• The high cost per unit of bandwidth for MPLS lines that route traffic back to the datacenter

• A lack of flexibility in combining different types of network links and using them efficiently

• The delays associated with activating new or temporary branch office sites

• The need for specialized, expensive engineering and operational skills for router-based networks

These deficiencies have driven the search for a better approach for branch offices, and SD-WAN is the answer.

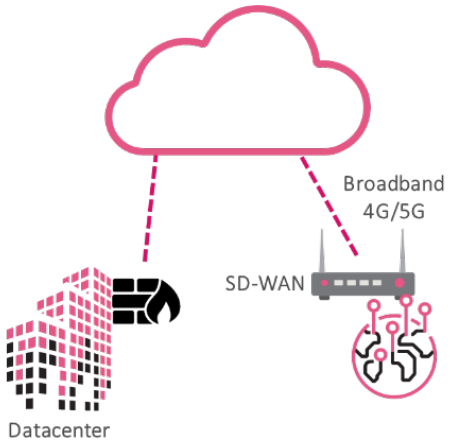



2 Gartner 2018 MQ for WAN Edge Infrastructure.

# SDWAN: The New Paradigm for Branch Office Networking

SD-WAN is revolutionary because it eliminates the key challenges of legacy networks and delivers lower costs, better flexibility, and a superior cloud user experience. It is no surprise that Gartner expects 90% of branches will use SD-WAN over traditional routers by 2023[3] .

SD-WAN replaces the hub and spoke router-based networks with software technology that provides these key capabilities:




| Feature | Capability |
|---|---|
| WAN optimization | • Monitor and optimize network Quality of Service (QOS)<br>• Route traffic based on Service Level Agreements (SLA) |
| Application-Aware Routing for Best User Experience | • Identifies applications and routes them through the network based on the bandwidth and service level needed<br>• Provides low latency high speed Internet connectivity needed for cloud applications including video. |
| Centralized network and security management | • Centralized network policy-based management<br>• Apply network policy applied once to multiple sites saving time and reduces errors |
| Centralized security management | • Integrate into unified policy and threat management system for simplified operations<br>• Better visibility into threat landscape to identify and quickly mitigate attacks |
| Zero Touch & Ease of use | • SD-WAN abstracts the underlying technology and presents a graphical, policy-based operational interface that is much simpler to understand.<br>• Zero-touch automated deployment of sites |
| Mixed Use of Internet Connectivity Options | • Supports mixed use of MPLS and multiple local broadband and wireless (LTE, 4G, 5G, Wi-Fi) internet connections<br>• Direct access to local Internet connections |
| Network-as-a-Service | • Cloud service or on-premises implementations<br>• Interconnecting cloud, datacenter and branch networking and security |

3 Google Transparency Report on HTTPS encryption on the web; transparencyreport.google.com

# Top Challenges to Securing Software Defined Wide Area Networks

Although SD-WAN has many networking benefits, it also creates serious considerations for security that must be addressed to avoid creating huge risks to the business. Security issues arise primarily because SD-WAN runs business traffic out of the branch locally, without backhauling it to the data center. Furthermore, built-in security from SD-WAN providers does not provide the next-generation threat prevention technologies needed to defend and protect against sophisticated multi-vector Gen V cyber attacks. The security issues that need to be addressed include:

• Inadequate Security Services: You can't rely on the data center security systems to enforce policy. The same level of enterprise security needs to be provided at the branch office to enable them to securely connect to local internet providers.

• Visibility: Security starts with visibility, which is now much harder to attain because branch networking and security need to be distributed.

• Service Delivery: Remote branch office and retail locations have different networking and security requirements. Some industries like banking may need on-premises security for data location regulatory requirements. Other locations like retailers may not have the space or supporting staff to manage on-premises security equipment. A "one size fits all" approach to deploying security usually does not work.

• Inconsistent Policies: The key to effective security is enforcing a consistent policy across the network, but this is difficult if there are differences in security services and management.

• Scalable Management: Implementing security in dozens or even thousands of sites creates scalability, operations and management challenges.

• Separation of Duties: Networking and Security in most large enterprises are two different IT disciplines run by different teams. Effective separation of duties will be much harder if security and network services are unified in a single SD-WAN architecture and operational interface, but the teams are not.

## GLOBAL CHEMICAL MANUFACTURER GRACE SECURES CLOUD DIGITAL TRANSFORMATION WITH CHECK POINT CLOUDGUARD SOLUTIONS

*"In the new SD-WAN environment with CloudGuard Connect, we can deploy a site in five minutes or less—including getting a cup of coffee in the middle of the process. It is a phenomenal solution that is quick to deploy, built on a very secure platform that we're comfortable with."*

– David Antlitz, Global Manager, Security and Firewall Technologies, Grace

# Top Five Recommendations for Securing Software-Defined Wide Area Networks (SD-WAN)

What can be done to tackle the security challenges created by SD-WAN in branch offices?

Below are the Top Five Recommendations for securing SD-WAN networks.

## 1. BASIC NEXT GENERATION FIREWALL SIGNATURE-BASED INSPECTION

Basic Next Generation Firewall Signature-based inspection is part of a multi-layered defense and safely enables branch office employee access to the Internet. Multi-layered defense works best when it is fully integrated.

### Intrusion Prevention System (IPS)

Also known as intrusion detection prevention system (IDPS), monitors the network for any malicious attempts to exploit a known vulnerability. An Intrusion Prevention System's main function is to identify any suspicious activity and either detect and allow (IDS) or prevent (IPS) the threat. The attempt is logged and reported to the network managers or Security Operations Center (SOC) staff.

### URL and Web Filtering

Web access is a predominant route for attacks on enterprises. URL and Web Filtering controls access to millions of web sites by category, users, groups, and machines to protect users from malicious sites and enable safe use of the Internet. URL Filtering employs UserCheck technology, which educates users on web usage policy in real time.

### GRACE, GLOBAL CHEMICAL COMPANY, SECURES THEIR SD-WAN WITH CHECK POINT

**Grace has 18 manufacturing plants across 40 countries. They have 5000 employees working in office and manufacturing functions.**

#### Challenges

- Business has moved from on-premises to cloud-based services including Office 365, AWS and SalesForce, yet network traffic was still backhauled to a central data center for Internet access.
- Business demand had outgrown their network design; they needed flexibility, performance, and scalability, with the same security they had grown to trust.

#### Solution

- Grace implemented VMware SD-WAN and Check Point CloudGuard Connect for a secure, stable, better performing, and more efficient WAN solution.
- This solution met Grace's high cybersecurity and performance standards, providing them with the flexibility to adapt to changing business requirements.

### Application Control

Provides administrators with the ability to create granular web security policies based on users to identify, block or limit usage of web applications and widgets. This ensures that the data being used by and shared between applications is private and secure within an organization.

### Identity Awareness

Provides granular visibility of users, groups and machines, enabling application and access control through the creation of accurate, identity-based policies.

### Antivirus

Protects computers and removes malicious software or code designed to damage computers or data. Today, malware is evolving so rapidly that some estimate a new malware instance is created nearly every second. Today's antivirus solutions combine global scanning, human expert threat analysis, industry collaboration, cloud integration, and alerting services.

### Anti-bot

A botnet is a network of malware-infected computers that can be controlled by a single command and control center operated by a threat actor. The network itself, which can be composed of thousands if not hundreds of thousands of computers, is then used to further spread the malware and increase the size of the network.

### Encrypted Traffic Inspection

A recent Google study showed that over 80% of web traffic generated by end-users using Chrome was encrypted[4] . Unfortunately at the same time, malware creators have learned to leverage Certification Authority (CA) automation initiatives like encryption to create phishing sites trusted by browsers. As encrypted traffic and threats proliferate, SD-WAN security solutions must be able to inspect encrypted traffic both to control access and prevent threats. It also must be sophisticated enough to support complex policies such as selective decryption so that certain traffic (e.g. employee on-line banking) can be excluded from decryption to avoid regulatory or liability issues.

---

4 https://transparencyreport.google.com/https/overview?hl=en

# 2. ENTERPRISE-GRADE ALWAYS UP TO DATE THREAT PREVENTION SECURITY

Don't compromise on branch office security services. Include the full set of enterprise grade security services that branches have come to expect from the datacenter. Branch security starts with protecting against both known and unknown threats with the same degree of efficacy.

SD-WAN security solutions need to go beyond Next Generation Firewalls to include advanced threat prevention:

### Threat Prevention versus Detection

Some security solutions focus on detection and response and not threat prevention. You need threat prevention to protect branch offices against the full range of threats from Zero Day to sophisticated multi-vector attacks. The SD-WAN security solution should include innovative technologies like threat emulation (sandboxing), threat extraction (Content Disarm and Reconstruction), CPU level inspection, and artificial intelligence.

### Cloud-based Threat Intelligence

Provides continuous, up-to-date protection against the latest cyber threats. Threat intelligence is the knowledge businesses have to prevent and/or mitigate the severity and frequency of cyber attacks. Real-time cloud-based threat intelligence sifts through mounds of data and uses contextual learning and knowledge to identify problems – intuitively separating false alarms from actual threats – so the proper solutions can be deployed to neutralize the attack.

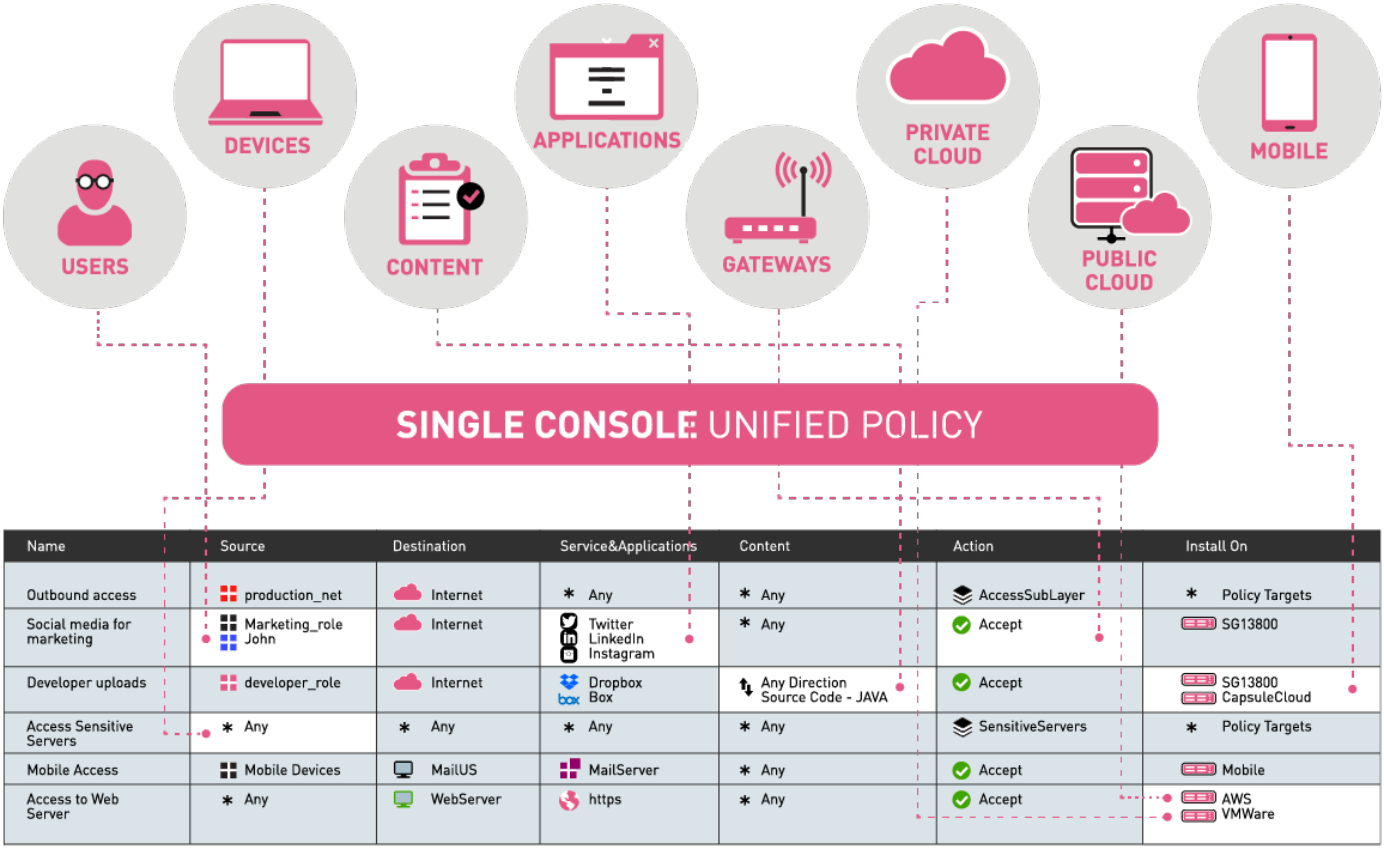
### Artificial Intelligence (AI) Security Engines

In addition to threat intelligence, you also need artificial intelligence security engines to mine the mountains of threat data received and to look for trends and anomalies. For example, Check Point's ThreatCloud intelligence system handles 86 billion security decisions a day. That is a lot of data to mine.

### Sandboxing

Sandboxing prevents the spread of cyber attacks by isolating applications or documents from the rest of the IT system. The security system can then inspect the files for unknown or known attacks before the files are distributed to a user. This provides an extra layer of security that prevents malware or harmful applications from getting distributed throughout the network before it is determined that they are harmful.

# 3. UNIFIED SECURITY MANAGEMENT, SECURITY POLICY AND THREAT VISIBILITY




| Name | Source | Destination | Service&Applications | Content | Action | Install On |
|---|---|---|---|---|---|---|
| Outbound access | production_net | Internet | Any | Any | AccessSubLayer | Policy Targets |
| Social media for marketing | Marketing_role John | Internet | Twitter LinkedIn Instagram | Any | Accept | SG13800 |
| Developer uploads | developer_role | Internet | Dropbox Box | Any Direction Source Code - JAVA | Accept | SG13800 CapsuleCloud |
| Access Sensitive Servers | Any | Any | Any | Any | SensitiveServers | Policy Targets |
| Mobile Access | Mobile Devices | MailUS | MailServer | Any | Accept | Mobile |
| Access to Web Server | Any | WebServer | https | Any | Accept | AWS VMWare |

Unified security policy and threat management will increase security and threat visibility, while reducing operating expenses up to 40%. Given the distributed nature of branch security, you need a simplified, unified security management platform that includes:

**Unified Security Policy and Threat Management**

It is essential that you have the same security policy options across the data center and remotes sites. This will allow you to drive policy consistency across the environment, but also to accommodate local variations easily. Key features of a unified security management system include:

- Unified Security Architecture across the datacenter, networks, branch, mobile, end point and IoT.
- Unified threat dashboard to assess attack risk across the enterprise.
- Real-time forensic threat analysis with quick mitigation and compliance.

• A unified threat dashboard makes it far easier to see the complete picture of possible attacks and risks across the enterprise. This can control security events with real-time forensic and event investigation, compliance and reporting, enabling you to respond to security incidents immediately and reducing the time spent remediating incidents.

• Consistent policy and threat management will not only drive greatly improved security and threat visibility, but will also reduce operating expenses.

**Scalable Distributed Network**

Ensure your management systems and operational model support the level of scale required for highly distributed security. Many solutions work well when you have a handful of devices and administrators, but collapse at scale. Time to manually configure a device x increases linearly for every device managed. This includes several dimensions:

• Number of devices

• Number and variation of policies, including identity and application awareness

• Number of simultaneous administrators

A unified threat dashboard makes it far easier to see the complete picture of possible attacks and risks across the enterprise. Consistent policy and threat management will not only drive greatly improved security and threat visibility, but will also reduce operating expenses.

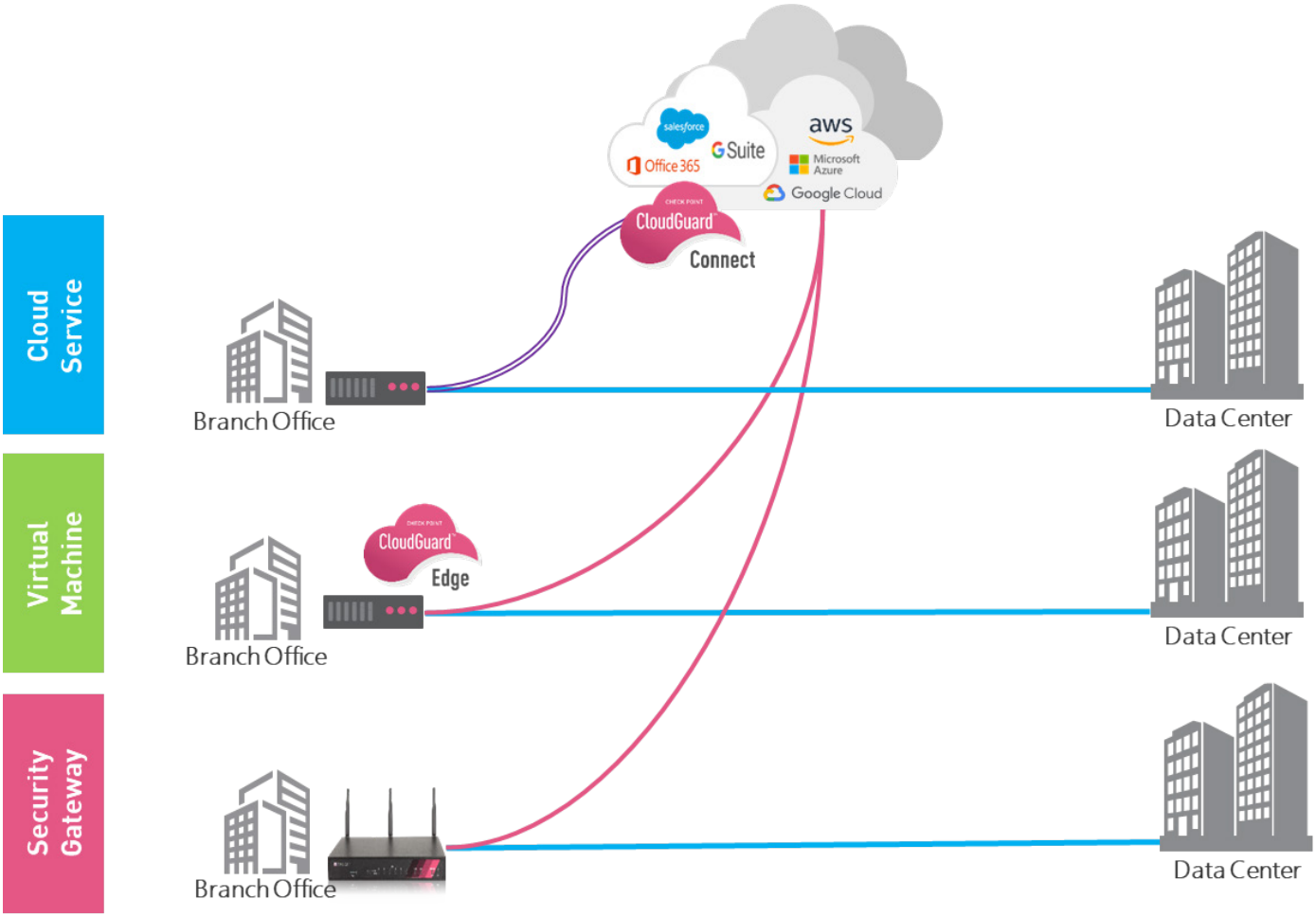
## 4. FLEXIBLE DEPLOYMENT OPTIONS

Remote branch offices are not homogeneous, and can have completely different requirements. For example, financial services, retail and healthcare locations, have different communication and security requirements and IT staff support. It is important to select a vendor that has the ability to provide a variety of SD-WAN security solutions that can meet the needs of any branch office. A complete SD-WAN security solution includes these three options:

1. Cloud Network Security as a service. Does not require any on-premises hardware or IT support, e.g. Check Point CloudGuard Connect.

2. Software Virtual Network Function (VNF): On-premises virtual network function (VNF) security gateway. Can be run in an SD-WAN device or branch office server, e.g. Check Point CloudGuard Edge.

3. Security Gateway Appliance: on-premises security gateway that secures network traffic coming into and out of the branch office. e.g. Check Point Quantum Security Gateways.




**On-Premises Requirements**

Companies in regulated industries like financial services may have data location or privacy requirements that don't allow them to put their data in the cloud. For example, there may be legal requirements to keep certain classes of data within national boundaries. There may be applications hosted in the branch that require users to connect to the branch to access resources. Security monitoring of incoming network traffic to the branch is not normally supported by a cloud security service. Cloud services focus on securing branch connections to the cloud.

For companies who have these types of requirements, either of these two options that we discussed above will meet your requirements.

- Software VNF: On-premises virtual network function (VNF) security gateway. Can be run in an SD-WAN device or branch office server, e.g. Check Point CloudGuard Edge.
- Security Gateway Appliance: on-premises security gateway that secures network traffic coming into and out of the branch office, e.g. Check Point Quantum Security Gateways.

The recommended option between the two depends on your performance requirements. A dedicated security gateway appliance should typically provide better threat prevention performance than a software VNF running inside a SD-WAN device or branch server.

### Cloud Network Security as a Service

On the other hand, cloud-based security services are easy to scale and support, and eliminate CapEx costs. They can provide security in branches with little or no IT support like retail locations. Look for a cloud network security service with:

- A cloud native architecture that is low latency, elastic, scalable, with 99.999% uptime
- Always up to date with advanced NSS top-rated threat prevention
- Maintenance-free security service that can be delivered to branch offices in minutes

## 5. BEST SECURITY AND BEST NETWORKING

Look for solutions that combine leading SD-WAN providers like VMware, Silver Peak, Cisco, Citrix, Aruba and Aryaka with the top security providers like Check Point. This is a no-compromise approach that gives you the best of both worlds. Below we have outlined the key security and SD-WAN features that will deliver the Best SD-WAN Security and Best SD-WAN Networking.

### Best SD-WAN Security

| THREAT PREVENTION | UNIFIED MANAGEMENT | FLEXIBLE SECURITY OPTIONS |
|---|---|---|
| Threat Emulation (Sandboxing) | Unified Security Policy | Network SaaS |
| CPU Level Inspection | Unified Threat Dashboard | Virtual Network Function |
| AI & Threat Intelligence | Real-time Forensics | Security Appliances |

### Best SD-WAN Networking

| APPLICATION BASED ROUTING | CENTRALIZED MANAGEMENT AND CONFIGURATION | WAN OPTIMIZATION |
|---|---|---|
| Identifying apps in the network and routing accordingly | Large scale, profile based central management | QOS, monitoring and improve SLA. Route selection based on SLA |
| **ZERO TOUCH & EASE OF USE** | **EDGE APPLIANCE** | **NETWORK-AS-A-SERVICE** |
| Zero-touch and automating deployment | Providing multiple ISP Wi-fi, 4G/LTE Capabilities | Interconnecting cloud, Datacenter and Branches |

In addition, despite the SD-WAN paradigm change, security and networking remain different disciplines in many IT organizations. Therefore, ensure that your architecture allows complete separation of duties, so that security and network policies can be decoupled operationally. This will decrease the friction associated with SD-WAN adoption, and will ease the burden of meeting compliance requirements.

# Summary

Software-Defined WAN (SD-WAN) is indeed a revolution in network architectures enabling businesses to accelerate their digital transformation to cloud SaaS applications like Office365. Enterprises can now leverage a variety of less expensive local Internet providers without sacrificing cloud application performance. This also enables companies to still use MPLS lines when dedicated bandwidth is required. Because SD-WAN improves the cloud application user experience while also reducing communication costs, we expect SD-WAN to become ubiquitous over the next several years.

Although SD-WAN has many virtues, it also creates serious considerations for security that must be addressed to avoid creating huge risks to the business. The security issues arise because SD-WAN enables branches to connect to local internet providers bypassing datacenter security and exposing them to cyber attacks. Furthermore, built-in security from SD-WAN providers does not provide the next-generation threat prevention technologies needed to defend and protect against sophisticated multi-vector Gen V cyber attacks.

To mitigate these challenges, Check Point recommends that branches implement the same enterprise-grade security delivered by the datacenter. SD-WAN security solutions need to go beyond Next Generation Firewalls to include the following:

- Enterprise-Grade Always Up to Date Threat Prevention Security
- Unified and Scalable Security Management with unified policy and threat visibility
- Flexible Deployment Options on-premises and in the cloud including a:
    - o Cloud network security as a service
    - o Virtual security appliance (VNF) that runs on a SD-WAN device or branch server
    - o Security appliance
- Demand the Best Security and Best Networking. Look for solutions that combine leading SD-WAN providers like VMware, Silver Peak, Cisco, Citrix, Aryaka and Aruba with the top security providers like Check Point. This is a no-compromise approach that gives you the best of both worlds.

If you are considering moving to SD-WAN, seriously consider implementing Check Point CloudGuard Connect service, CloudGuard Edge VNF, or a branch security appliance. These three SD-WAN solutions secure connections to the cloud with top-rated threat prevention, quick and easy deployment, and unified security management and threat visibility saving enterprises up to 40% in operating expenses.

For more information, go to

https://www.checkpoint.com/solutions/sd-wan-security

https://www.checkpoint.com/products/branch-cloud-security/

https://www.checkpoint.com/products/branch-virtual-security-gateway/

https://www.checkpoint.com/products/branch-office-security/

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

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070, USA | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117

**www.checkpoint.com**