Cisco Umbrella

EBOOK

# Network Security for SD-WAN

Secure your cloud edge - from the network to satellite offices - with cloud security.

cisco

# Get informed, get started.

**The network**
What's driving network transformation?

**Customer challenges**
What changes are happening at remote offices?

**Risks**
What's driving the need for branch office security?

**The cloud edge**
Let's talk about the edge. The cloud edge.

**Advantages**
Security + networking: An integrated approach.

**Cisco's vision**
Secure branch and cloud edge architecture: The Cisco vision.

**Umbrella**
Secure the cloud edge with a secure internet gateway.

**Get started**
Where to begin?

# What's driving network transformation?

**Your branches are vital. They're also changing.**

In today's business environment, satellite offices are more important than ever. For the average enterprise, remote offices generate the vast majority of revenue – and 80% of users[1] are located there. But in most organizations, security at the branch office is limited, if it exists at all.

Historically, enterprises used a wide area network (WAN) to connect branches to a data center, backhauling all traffic through a central corporate network. But new business and IT demands are challenging that architecture. The use of software as a service (SaaS) and infrastructure as a service (IaaS) applications, via multiple clouds, has become central to business operations. And every year, workers use more connected devices at more locations. Users need every one of those devices to have fast, reliable access to the internet, so they can be as productive as possible.

## Four factors forcing distributed network transformation

**Complexity**

Manual operational processes combined with IT skills shortage leads to error

**Cost**

Existing WAN links are expensive and unable to handle increasing bandwidth demands

**Delays**

Slow, inconsistent app performance leads to reduced productivity

**Disruptions**

Lack of visibility and insights leads to slower decision making and increased vulnerability

# What changes are happening at remote offices?

**The problem(s) with the WAN.**

The WAN was built to give branch offices and roaming users access to IT resources within private data centers. But today, as networks become more decentralized and users connect directly to SaaS applications, backhauling traffic to apply security policies just isn't efficient. And that's not the only problem. Backhauling internet-bound traffic is expensive, and it adds latency.

The adoption of software-defined WAN represents the largest WAN transformation in recent history. Organizations are turning to SD-WAN to improve connectivity, reduce costs, and simplify management at their satellite office locations. In fact, a recent research study from the Enterprise Strategy Group (ESG) found that 4 out of 5 organizations report using SD-WAN in some capacity already. The research also indicated that 79 percent of organizations are shifting to direct internet access (DIA) for all or some remote and branch offices.[3] With DIA, enterprises can accelerate their digital transformation with faster access to cloud applications and workloads. While the benefits are clear, this also introduces new security challenges.

**WAN Transformation**

40% to 60% of enterprise data traffic is migrating from private WANs to the internet.[2]

**Branch Digitalization**

Organizations are adopting new digital business initiatives like IoT, digital signage, omnichannel experience, rich media content, and guest Wi-Fi.


68%
of recent attacks involved branch offices and roaming users as the source of compromise.[3]

# What's driving the need for branch office security?

**Changing architecture, increasing risks.**

Clearly, IT decision-makers have realized that they can accelerate growth, significantly decrease telecom costs, and improve network performance by allowing their branch offices and remote employees to connect directly to the internet. But as full or partial DIA increases, so do the risks – and not only because the attack surface has dramatically increased, although that's a central part of the problem:

By 2022, as a result of digital business projects, 75% of enterprise-generated data will be created and processed outside the traditional, centralized data center or cloud.[4]

## Today's evolved threats require a modern approach to security.

Along with IT architecture, today's threats have evolved, too; they're now more sophisticated than ever. Today's organizations must defend their branches against many threats, including malware infections, command-and-control callbacks, phishing attacks, denial-of-service attacks, unauthorized access, and unacceptable use.

**Internal Security Risks**

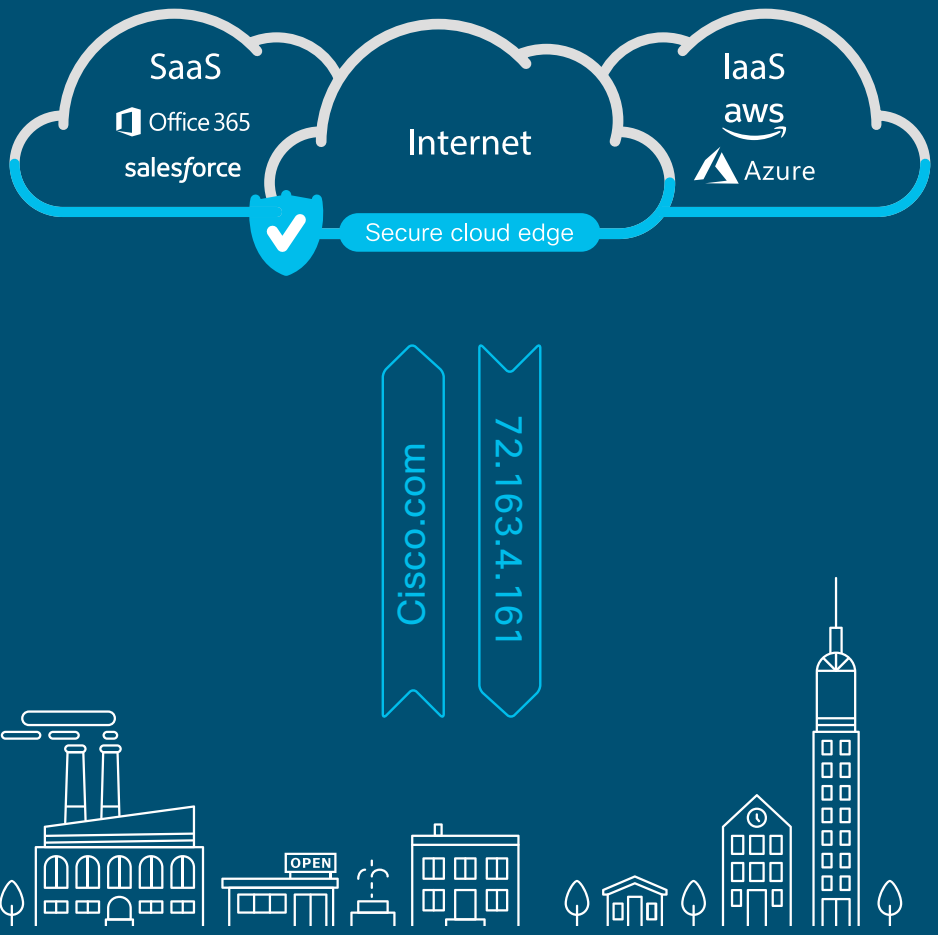
More nontraditional users and devices connecting exposes critical business resources.

**External Security Risks**

Direct internet access exposes users, connected devices, and applications.

# Let's talk about the edge. The cloud edge.

It is now essential to have security sitting in front of and protecting the internet, SaaS apps, and IaaS.




The focus used to be on securing the data center edge, because that's where the traditional security stack was built. But today, there's more than just a single edge; there are three types of locations – the data center, the cloud, and the branches. The WAN fabric provides paths connecting all of them.

Today, users and connected devices that were once managed by the organization are outside of corporate control, leading to gaps in visibility and coverage. And as more branch office locations connect directly to the internet, it's important to secure not just the data center edge but the cloud edge.

In other words, it is now essential to have security sitting in front of and protecting the internet, SaaS apps, and IaaS. By providing a secure cloud edge, you can reduce the risk of data exfiltration and block malware over all ports and protocols with no added latency.

# Security + networking: An integrated approach.

Security has to be top of mind as you transform your network with SD-WAN and move to DIA. Branch offices and roaming users are more vulnerable to attacks, and attackers can quickly exploit weaknesses. Scaling security at every location often means more appliances to ship and manage and more policies to separately maintain, which translates into more money and resources needed.

But it doesn't have to be that way. SD-WAN makes your networking simple, and that's the way that your security should be, too. At Cisco, we believe that branch-to-cloud-edge architecture can and should be integrated to provide better security and better networking.

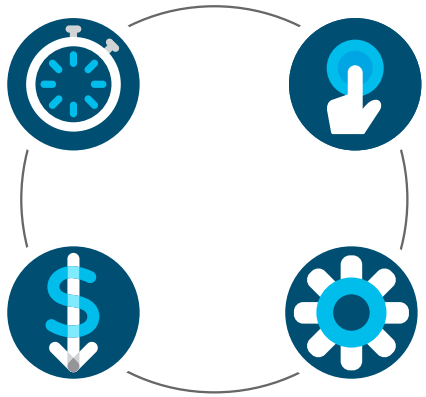
## The benefits of an integrated approach:

**Simpler, faster security.**

Simplify threat prevention with the shortest time-to-detection.

**Better user experience.**

Get the fastest and most reliable internet and multicloud access.



**Less costly, more agile networking.**

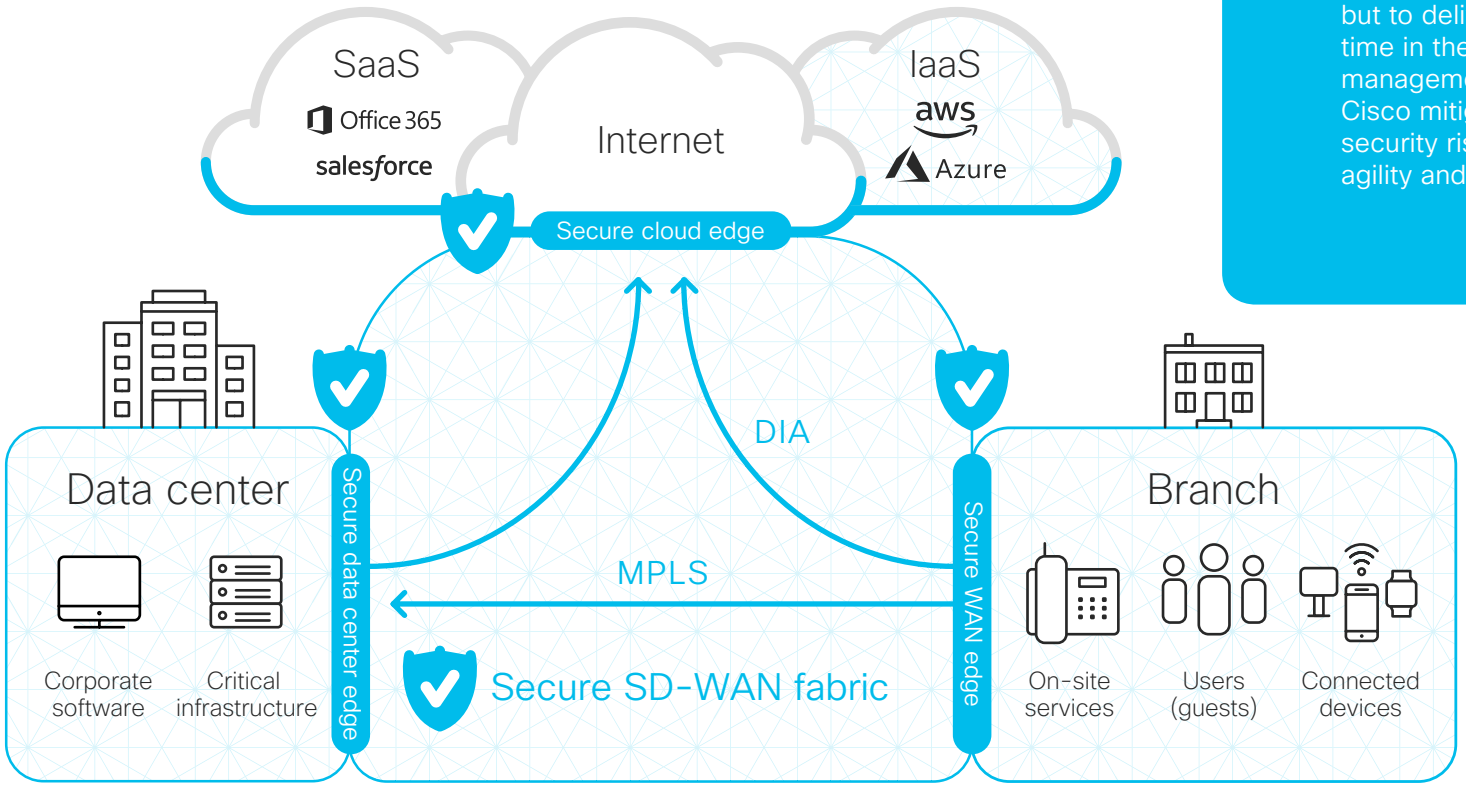
Minimize OpEx and CapEx while easily adding locations, devices, and apps to the WAN.

**Stronger business continuity.**

Use intent-based networking to automate app assurance and get better insights from your data.

# Secure branch to cloud edge architecture: The Cisco vision.

Cisco's solution enables secure branch transformation from the branch to cloud edge without gaps.




The best branch office protection comes from an integrated network and security architecture that deploys quickly and improves security efficacy, user experience, network agility, and business continuity.

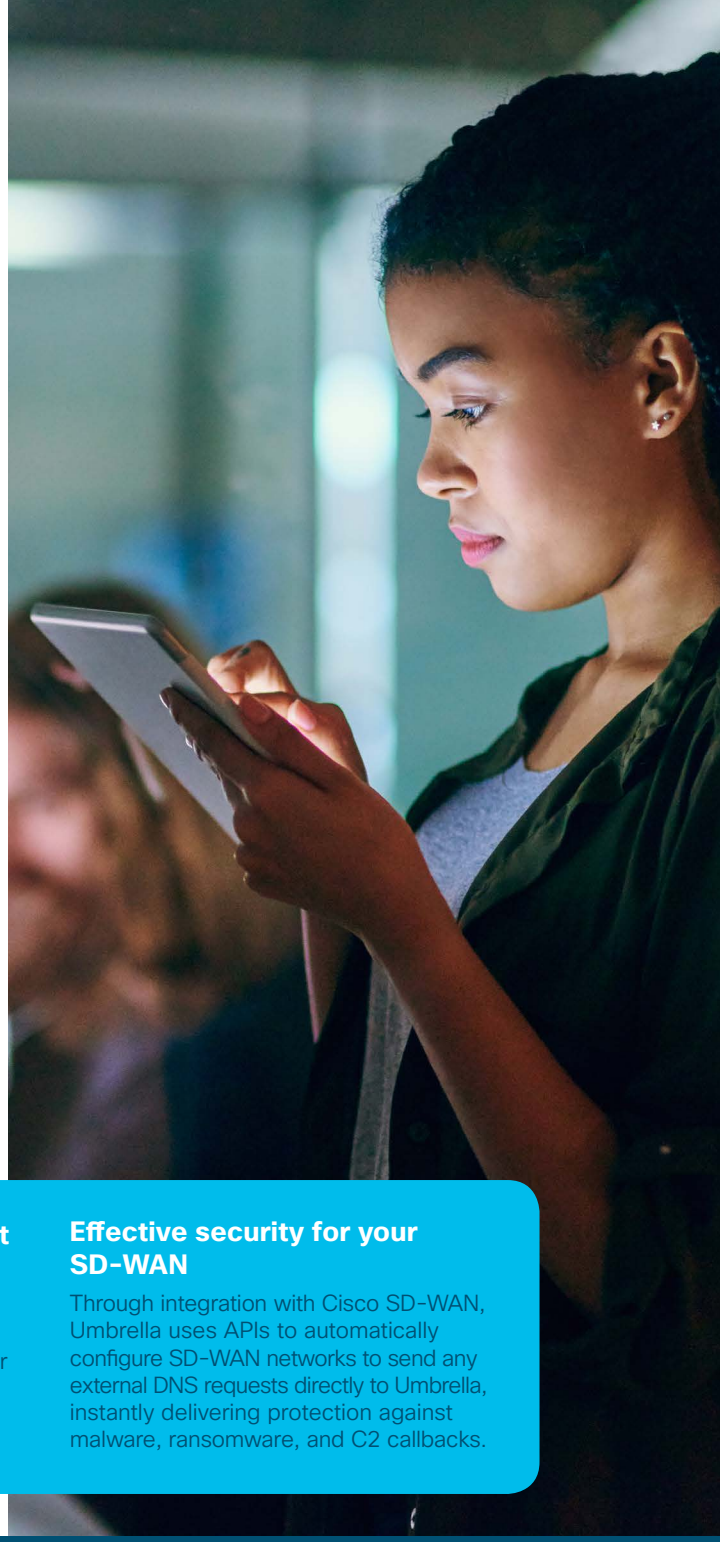
Cisco's integrated approach protects branch users, connected devices, and application usage at tens of thousands of DIA breakouts. Backed by Cisco Talos security intelligence, our cloud-delivered and intent-based solutions constantly learn, adapt, and protect, to not only see where attacks are staged, but to deliver the shortest threat detection time in the industry. With simplified cloud management and zero-touch provisioning, Cisco mitigates both external and internal security risks to the branch, improving network agility and business continuity.

# Secure the cloud edge with a secure internet gateway.

Cisco Umbrella is a secure internet gateway (SIG) that provides the first line of defense against threats on the internet wherever users go, starting with DNS-layer enforcement. Just point your DNS to Umbrella, and deploy a layer of protection to stop threats before malware can ever reach your network or endpoints. Beyond the DNS layer, Umbrella delivers a secure web gateway, cloud-delivered firewall, cloud access security broker, and interactive threat intelligence in a single, integrated cloud platform.

Umbrella learns from internet activity to automatically identify attacker infrastructure staged for current and emergent threats. We capture and understand relationships among malware, domains, IPs, and networks across the internet. With Umbrella, you can mitigate remediation costs and breach damage, reduce the time to detect and contain threats, and increase visibility into internet activity and cloud apps across all locations and users. Plus, Umbrella is the simplest security you'll ever deploy to protect branch offices. There is no hardware to install or software to manually update, and the browser-based interface provides quick setup and ongoing management.

By delivering security from the cloud, Umbrella not only saves you money, but provides your organization with more effective protection against malware, phishing, command-and-control callbacks, and unacceptable requests. Here's how:



**Simple, flexible, and efficient**

Umbrella deploys in minutes, and manages security policies for all locations and user groups from one console. Reduce the hassle of hardware installs and ongoing maintenance with cloud-delivered security.

**Unmatched visibility and threat protection**

Backed by Cisco Talos, one of the largest threat intelligence teams in the world, Umbrella uncovers malicious attacks through analysis of global internet activity.

**Reduced complexity and cost for direct internet access**

Umbrella delivers reliable, secure direct internet connections for branch offices with 100% uptime and superior performance for end users.

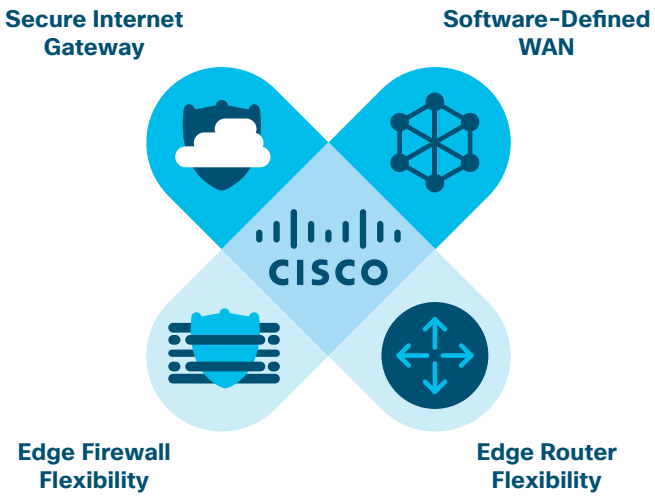
**Effective security for your SD-WAN**

Through integration with Cisco SD-WAN, Umbrella uses APIs to automatically configure SD-WAN networks to send any external DNS requests directly to Umbrella, instantly delivering protection against malware, ransomware, and C2 callbacks.

# See what other security solutions miss.

When you analyze more than 180 billion internet requests a day, that gives you insight like no other. As you transform your branch network through adoption of SD-WAN technology, or if you offer guest Wi-Fi to your customers, Umbrella provides a simple, effective way to protect users who connect directly to the internet.

And with the Cisco SD-WAN and Umbrella integration, you can deploy Umbrella across your network to hundreds of devices in minutes and instantly gain web and DNS-layer protection against threats such as malware, ransomware, and C2 callbacks.




**180B**
Internet requests

**100M**
Daily active users

**18K**
Enterprise customers

**160**
Countries worldwide

Cisco Umbrella

# Where to begin?
# Start by securing your cloud edge.

Visibility and protection on and off network

Your first line of defense against threats

Gain visibility and control into shadow IT with application discovery and blocking

Intelligence to uncover threats earlier

Broadest coverage of malicious destinations and files

Gain web and DNS-layer protection for users at direct internet access locations

Most open, simplest cloud security platform

Get worldwide threat protection in minutes. Try it free for 14 days.

**Start your Umbrella free trial**


Sources:

1. "It's not your dad's branch office," Nojitter.com, 2016
2. "Network Evolution and Market Outlook," IDC, 2017
3. Enterprise Strategy Group, 2019
4. Gartner, "Start Moving Data Management Capabilities Toward the Edge," Ted Friedman, 2017