

Cisco Umbrella

**2019**

# Cybersecurity Trends

How emerging threats to remote user  
security are driving IT investments



# Security is on the move

It's no secret that the way people work has changed dramatically over the past few years. As highly distributed environments become the norm, security teams are scrambling to protect users, the growing number of device types they carry, and their data. Applications that previously resided on-premises are also on the move, as the volume of roaming workers continues to rise. Branch offices are adopting direct internet access, which is forcing a discussion on how to extend security to protect the edge.

With more users, devices, and applications connecting to the network, the number of risks and vulnerabilities is also increasing – triggering a total transformation in the security landscape.

In this research readout, we explore the complex factors that make remote and roaming user security a challenge, and the emerging solutions best positioned to meet the needs of today's increasingly distributed enterprise.



Remote workers. Branch offices.  
An ever-expanding perimeter.



SaaS apps.  
Unsanctioned downloads.



Malicious cryptomining and ransomware.  
More threats, more exposure, more risk.



Standalone security limitations.  
The frustration of disjointed point solutions.

# Keep an eye on these trends

Enterprise Strategy Group partnered with Cisco to validate market trends and understand customer perceptions and technology consumption patterns. What they found can help you create a security strategy that serves your needs now and in the future.

## 1. Trend:

A growing population of remote workers and branch offices need a new approach to security ➤

## 2. Trend:

Employees like to use unsanctioned apps – and they don't plan to stop ➤

## 3. Trend:

Threats are multiplying and becoming more sophisticated – targeting more branch offices and roaming users ➤

## 4. Trend:

More organizations are using a Secure Internet Gateway to provide secure access ➤

## 5. Solution:

Simplifying security with Cisco Umbrella ➤



## Trend:

A growing population of remote workers and branch offices need a new approach to security.

A thriving distributed workforce and an ever-expanding perimeter – securing this increasingly digital landscape is compounded by multiple layers of complexity.

---

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. This security readout provides a unique look at the trends impacting remote and roaming user security.

# Peeling back the layers on a complicated problem

Today's security teams face a common challenge: How to secure the growing universe of roaming users, devices, and SaaS apps without adding complexity or reducing end-user performance — while leveraging existing security investments.

Remote and branch offices need the same level of protection as central locations. IT must develop strategies to protect them from a variety of threats, including malware infections, command-and-control callbacks, phishing attacks, denial-of-service attacks, unauthorized access, and unacceptable use.

## Top remote and branch office cybersecurity challenges



34%

Internal applications, cloud-based workloads, and SaaS applications create new exposures.<sup>1</sup>



33%

Disparate ways of accessing the internet create a lack of visibility into remote and branch office/roaming activity.<sup>1</sup>



31%

Collaboration between security and network operations teams is a challenge for resource-limited teams.<sup>1</sup>

## Hackers know that roaming users are vulnerable – just how vulnerable might surprise you

Roaming users and devices are connecting directly to critical business resources with limited or no security. Why? Because centralized security policies are often no longer enforced, which increases the risk of a successful attack or compliance violation. Another reason is the massive shift to using applications to get work done. Internal applications, cloud-based workloads, and SaaS applications each have different policies, requirements, and vulnerabilities.

Another wrinkle: Within the next couple of years, organizations expect at least half of all users to be on the move, up from 40% today.<sup>1</sup>



68%

of respondents experienced targeted attacks in the last 12 months that compromised either a remote and branch office or roaming user.<sup>1</sup>



43%

of users are roaming – and were cited as the most vulnerable to a targeted attack.<sup>1</sup>

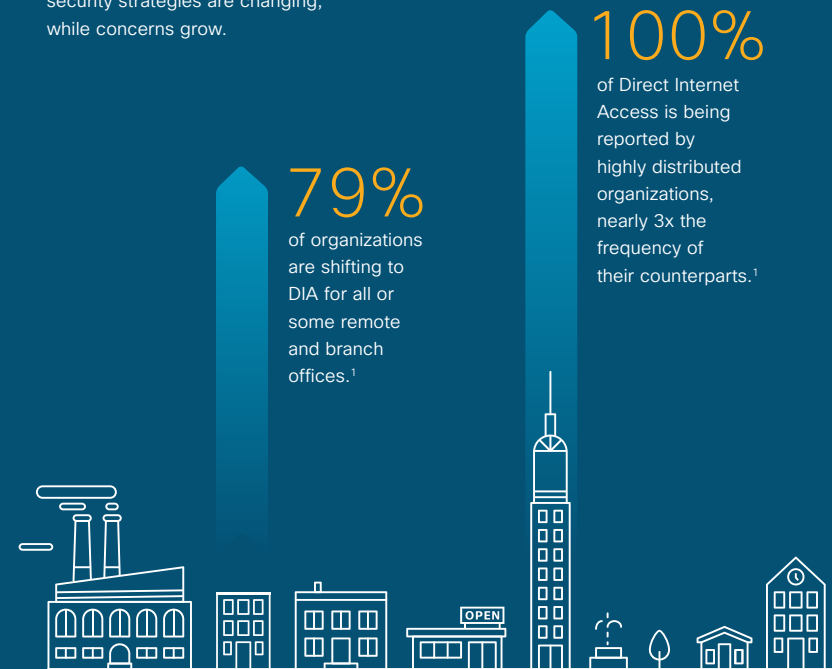
## More ways to access the internet. More potential exposures.

Traditionally, IT connected branches to a data center via a WAN, backhauling internet-bound traffic to apply security controls. But that approach is insufficient for modern branch offices and roaming users. Not only does it add latency, encouraging users to ditch authorized apps for personal ones, but it was also developed with desktops in mind.

As networks become decentralized, many organizations are migrating from WAN services and adopting more flexible SD-WAN technologies. With these changes comes the need for an easier, more effective way to secure users anywhere they access the internet or cloud applications.

### What's really going on inside

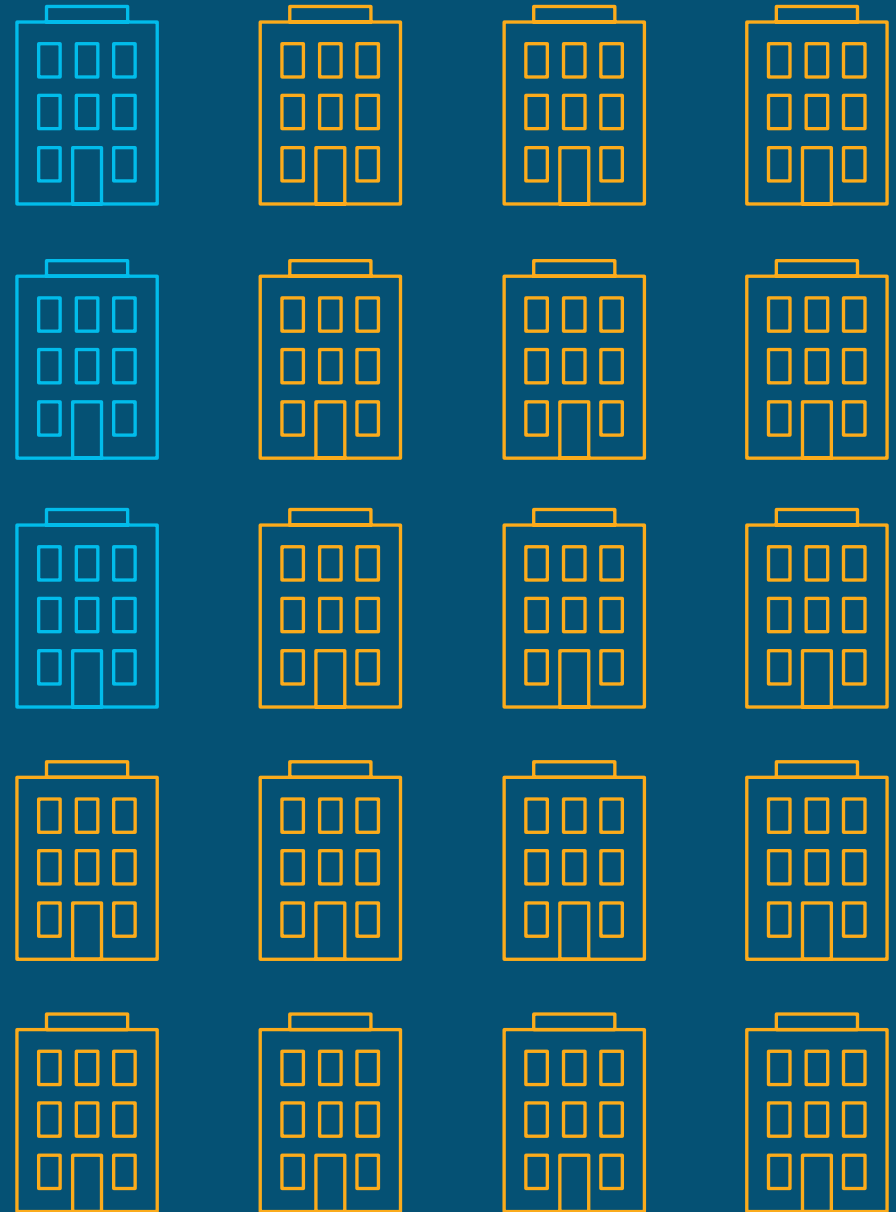
Survey results reveal that security strategies are changing, while concerns grow.



# 85%

of organizations think their users violate corporate VPN policies.<sup>1</sup>

Think a VPN will protect your users? Think again. Even if you have one that you trust, research shows that users regularly circumvent controls to access the applications or performance they need to get their jobs done. IT usually doesn't know about it until too late. This lack of visibility, and the increased vulnerability that comes from resulting gaps in protection, simply reinforce that a new approach is imperative.



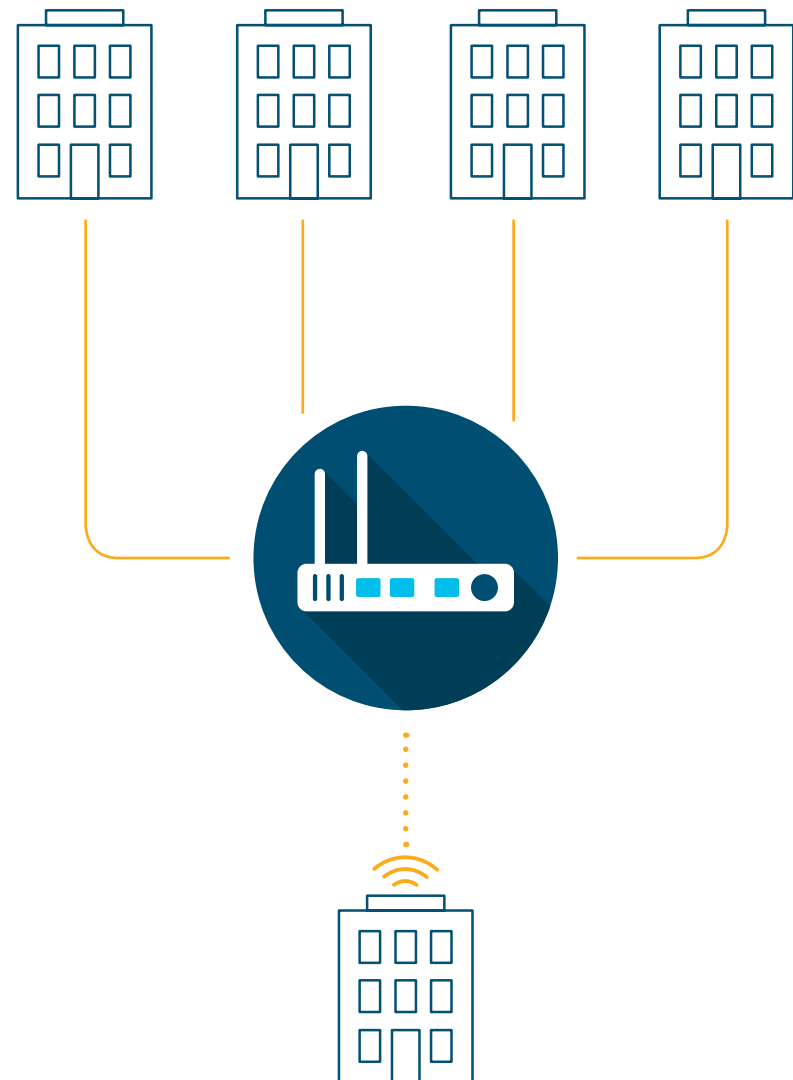


## Exit backhauling, enter DIA

IT decision makers are turning to the next obvious solution: Direct Internet Access (DIA). By allowing remote and branch offices and roaming users to make direct connections, organizations can accelerate growth, significantly decrease telecom costs, and improve network performance. The downside? Traffic from those locations isn't seen or protected by the traditional security stack, creating more ways for sensitive data to be exposed – either inadvertently or maliciously – in the cloud.

# 4 out of 5

organizations are shifting to DIA,  
and figuring out what to control is key.<sup>1</sup>



## How can you address those vulnerabilities? Hint: together.

As more remote and branch offices turn to DIA, IT needs a better way to improve visibility, secure users, simplify deployment, and scale with limited resources. The answer requires an integrated approach between unified systems and personnel.

Security and networking teams must work together to deploy a broad set of user protections across the network that not only strengthens security, but also reduces bandwidth costs for remote and branch offices.

Without strong collaborative processes and unified systems, remote and branch office and roaming users will continue to be susceptible to cyber attacks and system compromises.

“[Security and networking operations teams] have different goals. They’re measured in different ways. They use different tools. They may even have different languages. Making sure these two groups collaborate well, at all times, in real-time, especially in light of security threats that can change at a moment’s notice, is critically important.”

— **Jon Oltsik, Senior Principal Analyst & ESG Fellow**

## Securing roaming users is a team effort

Survey takers rated which teams are most instrumental in securing technologies that protect roaming users and remote and branch office infrastructure.<sup>1</sup>



44% Cybersecurity team

28% A general IT/IT operations team

18% Networking team

6% Application team

2% Endpoint team

1% Don't know

Source:  
1. ESG Research Publication, *Cisco Secure Internet Gateway Survey*, January 2019



## Trend:

Employees like to use unsanctioned apps – and don't plan to stop.

Employees at all levels are downloading popular apps to do their work faster, but their productivity gains come at a risk to the business. Attackers know that IT doesn't have visibility into many of these cloud-based apps, and are eager to exploit their vulnerabilities.

---

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. This security readout provides a unique look at the trends impacting remote and roaming user security.

# The new reality of Shadow IT

The image of employees using unauthorized apps often seems sinister. Are they sneaking in a game of Tetris, or sharing sensitive company data?

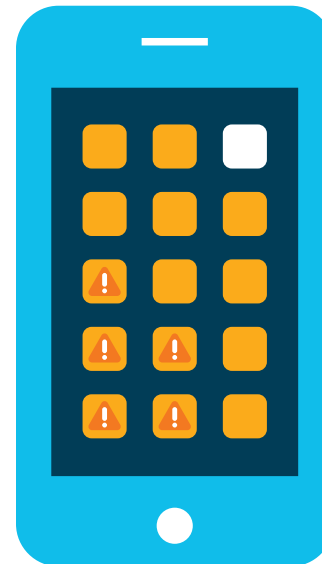
Most of the time, the answer is neither. They're just trying to do their jobs.

Startling new research shows that downloading apps on the sly isn't an occasional thing – it's happening everywhere, all the time. Which means that if your organization is like most, you've got a big problem on your hands – especially as more employees are working on the go.

**More apps. Less visibility. Greater risk.**

1200+

cloud services are used in the average large enterprise.<sup>1</sup>



98%

of those are shadow IT apps.<sup>2</sup>

27%

of discovered shadow IT apps are classified as high-risk.<sup>3</sup>

## Blame it on the... productivity?

The reason for this shift is one everyone can relate to: Cloud-based apps are simply easier and more convenient to use than most legacy, IT-approved apps. Whether it's file sharing, note-taking, or messaging, cloud applications make it easy to collaborate and increase productivity. No wonder they're being adopted without any involvement from IT or security teams.

Employees don't mean to create security problems when they use these apps, but they do. IT can't secure what it can't see, which means threats can creep in and cause damage before security teams know there's a problem. And the trend is expected to grow even bigger.



100's  
of apps

are being used without  
IT knowledge in a typical  
organization.<sup>4</sup>



60%

increase in SaaS usage  
is projected in the next  
two years, especially  
across highly distributed  
organizations.<sup>5</sup>

## The long reach of shadow IT

Whose job is it to keep a handle on how employees are using apps? Turns out, the responsibility falls on more than one person. Unsanctioned apps affect many people in the organization for different reasons.

### Improving communication across teams helps improve user enablement and keep security top of mind.



#### IT leaders

Must monitor cloud trends, understand usage patterns, and ensure business continuity.



#### Security leaders

Must verify app compliance and certifications, monitor usage levels, and secure data, apps, and users in the cloud.



#### Business leaders

Must ensure that investments are cost-effective and optimized across cloud services.

### Many unsanctioned apps add up to a big deal

Without a coordinated cloud strategy, your company might face new vulnerabilities that start out small, but develop into something big. Research shows that the use of unsanctioned apps can have surprising consequences, such as higher expenses, security risks, and morale and support issues.



45%

are concerned about the potential for sensitive data to be moved to SaaS applications without the proper controls or oversight.<sup>6</sup>



41%

are concerned about the risk of data loss from low-security apps, including those caused by user lapses or improper configuration.<sup>7</sup>

## Time to ramp up the damage control

Let's face it: There's no stopping the use of unsanctioned apps; they've now become integral to how work gets done. So how can you limit the potential damage and ensure that your users are protected, no matter where they're working?

The ideal solution is one that allows you to support employees and minimize risk to the business – exposing Shadow IT and its damaging side consequences for good.

### You need these three things:

- 1 Full visibility across distributed branch offices and endpoints**  
When you can see what everyone is doing, it's easier to monitor and control potential issues. You need the ability to gain a complete line of sight into sanctioned and unsanctioned activity across branches and endpoints. Once you have a clear view of the landscape, you can make better decisions about next steps.
- 2 A deep understanding of your exact exposures**  
Knowing specifics about the range, risks, patterns, and trends in your Shadow IT is crucial. When you know the extent of unsanctioned activity in your organization, you can identify high-risk apps, evaluate the risks they pose, and create a process for approving or denying access to those services.
- 3 The ability to manage and control future risks**  
Once you've gained visibility across environments and insight into the risks involved, you need the ability to take control. Ideally, you want to be able to view fine-grained details and block high-risk apps for individuals or groups.

Sources:

- 1, 2, 4. Cisco Blog, Gartner Report Says Shadow IT Will Result in 1/3 of Security Breaches
3. Help Net Security, 27% of cloud apps are high risk
- 5, 6, 7. ESG Research Publication, *Cisco Secure Internet Gateway Survey*, January 2019



## Trend:

# Threats are multiplying and becoming more sophisticated.

Despite all the buzz about security and staying prepared, malicious attackers are more audacious than ever. Today's threat landscape is expanding to include some threat vectors you're likely familiar with, and others you may have never seen before.

---

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. This security readout provides a unique look at the trends impacting remote and roaming user security.

# Threats... they keep on coming

Attackers are getting bolder and less discriminating. They're now targeting every kind of business, from every kind of business – small, medium, enterprise – in every location, from central headquarters to remote workers to branch offices. You can't stop them unless you know where they're coming from and what they want.

## Growing threat trends

200x

Increase in cryptomining traffic  
in the last 9 months of 2018.<sup>1</sup>



11.5B

Is what ransomware is expected  
to cost businesses in 2019.<sup>2</sup>

# 76%

Of businesses reported being a victim of a phishing attack in the last year.<sup>3</sup>



## Three threats most likely to cause damage in 2019



### Malicious cryptomining

Hackers want to make money – and use your infrastructure to do it. As the infection spreads, it reduces system performance and raises costs across your organization by draining your computing power.



### Ransomware

It doesn't matter if the initial threat is to personal information or client data, if a machine is infected with ransomware, your entire organization could be at risk. Attacks can lie dormant for an undetermined length of time, making them even harder to spot and stop.



### Phishing

Attackers can easily obtain sensitive information such as usernames, passwords, banking data, or credit card details. If an employee opens a phishing email at work, or follows a malicious link, they could put the whole organization in jeopardy without realizing it.

## What's making security headlines?

As you develop a strategy to protect and defend your organization, here's what you need to know.

1.

### **Malicious cryptomining is a lucrative way to cash in.**

The most successful money-making scheme of 2018, cryptomining is still growing fast. System administrators often don't know it's happening, and if it spreads, it can spike power costs and slow down your users' devices.

2.

### **Email is still the most popular threat-delivery vehicle.**

91% of attacks start with a phishing email.<sup>1</sup> Last year, Emotet evolved from a banking Trojan to a significant threat that spreads via email, looking for access to personal devices.

3.

### **Ransomware may not be making headlines – but it's still dangerous.**

Malicious cryptomining has a better payout than ransomware, but the threat remains. GrandCrab and Ryuk both made their debut in 2018, using Emotet and Trickbot infections, so staying vigilant is key.<sup>2</sup>

4.

### **New threats are on the rise.**

Attackers are creative, and they're always working on something new. Whether it's digital extortion, Office 365 phishing, or an entirely new scheme, security teams must stay alert for emerging attacks.

5.

### **Security is moving to the cloud.**

In a recent Cisco study,<sup>3</sup> 93% of respondents said moving security to the cloud has increased efficiency, allowing security personnel to focus on other areas.

## Threat protection: It's complex

What makes the threat landscape such a difficult challenge to solve? According to the 2019 Chief Information Security Office (CISO) Benchmark Study,<sup>4</sup> here's what's keeping them up at night.

---

### Employee preparedness

People are the front-line defense for organizations, yet individual users are often cited as the weakest link in security. What gives?

Only 51%

Rated themselves as doing an excellent job of managing human resources on security via comprehensive employee onboarding and appropriate processes for handling employee transfers and departures.

---

### The big unknown

Not having visibility into the scope and extent of emerging threats is a key challenge for today's security teams. It's difficult to defend against threats you can't see.

Only 35%

Were able to confirm that it is easy to determine the scope of a compromise, contain it, and remediate from exploits.

---

### Too many alerts

When teams piece together security solutions from multiple vendors that aren't integrated, it often leads to alert overload – which doesn't help.

79%

Said it was somewhat or very challenging to orchestrate alerts from multiple vendor products.

## What's working for other security teams?

With highly distributed environments the norm, SaaS usage on the rise, and more roaming users under attack, security leaders are looking for a better way to tackle threats and secure their networks.

### To take back control of your security program, you need to:

- 1 Align security budgets with desired outcomes.** Identify the measurable results you want to achieve with security initiatives, and the practical strategies that will get you there. Use cyber insurance and risk assessments to guide your procurement, strategy, and management decisions.
- 2 Collaborate across siloes.** Bring people together across IT, Networking, Security, and Compliance groups to gain a holistic understanding of security needs.
- 3 Use proven processes to reduce exposures and limit the extent of breaches.** Prepare with drills, employ rigorous investigative methods, and know the most expedient methods of recovery.

While the threat landscape is always evolving, and nothing stays the same for long, one thing is clear: if you take a vigilant approach to security, you can get the upper hand.

- 4 Invest in automation technologies.** Leverage the reach and speed of machine learning, artificial intelligence, and other automation tech to boost security efforts exponentially.
- 5 Build a Security Operations Center (SOC).** A focused team can manage breach response in organizations of all sizes.
- 6 Deploy cloud security to help with the unknown.** 91% of survey respondents agreed that utilizing cloud security increased visibility into the network.

Sources:

1. Cofense, Why Can't We Solve Phishing?
- 2-5. Cisco, CISO 2019 Benchmark Study

## Trend:

# More organizations are using a Secure Internet Gateway for secure access.

What if you could provide workers with safe access to the internet – no matter what device they're using or where they're located, even if they aren't on the VPN? A Secure Internet Gateway (SIG) provides just that. No wonder it's gaining traction.

---

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. This security readout provides a unique look at the trends impacting remote and roaming user security.



# How secure is your onramp to the internet?

In the face of expanding threats and growing numbers of remote workers, many IT professionals turn to more security tools, hoping it will all add up to better protection.

But that standalone, siloed approach is no longer effective at helping burdened security teams dig themselves out from constant alerts, and prioritize remediation efforts across distributed networks and branch offices.

Today, security leaders need to find ways to give users back their freedom while still protecting sensitive data. A Secure Internet Gateway (SIG) is a cloud-based security platform that delivers performance, flexibility, and security for users anywhere they access the internet or cloud apps.

## **What is a Secure Internet Gateway (SIG)?**

A Secure Internet Gateway (SIG) acts as a secure onramp to the internet, providing safe access anywhere users go, even off the VPN. Before a user connects to any destination, a SIG delivers the first line of defense and inspection. Its policies can be tuned to specific devices, users, and locations, to protect and proxy communication between a user and any service – whether they are at the branch office, headquarters or roaming. Plus, it integrates with your existing security stack to extend protection beyond the perimeter.

## Why SIG, and why now?

Hackers don't discriminate across industries or geographies. A startling 66% of organizations have experienced or are currently battling targeted attacks.<sup>1</sup> Every company is at risk – and security leaders know that traditional controls simply aren't working anymore.

Enter the Secure Internet Gateway. It protects against threats before they ever reach your network or endpoints. Instead of chasing attacks that are already inside the system, a SIG prevents them from getting in.

A SIG enables better protection, central management, and operational efficiency. 87% of organizations agree that SIG platforms would protect remote and branch offices and roaming users effectively<sup>2</sup> – something every business wants.

### What's driving SIG adoption?

The need for a Secure Internet Gateway is driven by the growing need for better security efficacy, operational efficiency, and improved performance.



31%  
to mitigate risk & improve security posture.<sup>3</sup>



26%  
to enable policy management, configuration management, and reporting for security across all remote offices/branch offices and roaming users.<sup>4</sup>



25%  
to achieve better performance and end-user satisfaction.<sup>5</sup>

## A SIG keeps users safe anytime, anywhere

Networks are becoming decentralized. More people are using cloud-based apps and services to work on proprietary documents and data. That's why a SIG is particularly effective – it goes where IT can't, without restricting user access or freedom.

For distributed enterprises with remote workers and branch offices, a SIG is a huge asset. When workers are off the company network, logged into a personal or new device, or simply subverting the VPN, SIG still keeps them safe.

### SIG and Remote and branch office: Better together

- 1 Helps you discover and control SaaS apps**  
Shadow IT – when employees use personal or unauthorized apps – is less scary when you have full visibility. Use a SIG that offers cloud application and blocking, like Cloud Access Security Brokers capabilities, to protect the use of data and applications in the cloud. Visibility gives you the power to intelligently manage cloud usage and make decisions rooted in data to optimize productivity, minimize expenses, and reduce risk.
- 2 Integrates security functions for better management**  
With a SIG, you reduce complexity, security alerts, and noise from multiple disparate systems to better secure users, devices, and apps across the business. By unifying your security stack across functions (SWG, firewall, CASB, DNS-layer) you gain centralized visibility. This makes SIG platforms ideal for organizations with large populations of branch offices and remote workers that need more effective protection, for all users and all networks, against malware.
- 3 Doesn't interrupt users or their workflow**  
A SIG doesn't stand in the way of worker productivity – in fact, it's just the opposite. It works automatically, so remote employees can get their jobs done, wherever they are, without worrying about slow or broken connections or performance issues. If implemented correctly, it should improve network performance and feel seamless to the end user.

# 5 things you need in a Security Internet Gateway solution

The benefits of a SIG are undeniable, but it's not enough to invest in just any solution. As you're evaluating options, make sure to choose one that will deliver on everything you need.

## Look for these components

A Secure Internet Gateway should provide a combination of DNS-layer security plus web gateway, firewall, and CASB functionality – all in a unified platform. It should deliver the flexibility, integrations, threat intelligence, and speed required to secure internet use in any distributed organization.

With a SIG, you can deliver that secure onramp to the internet for your employees wherever they are, while gaining visibility, control, and protection – all the must-have's for modern security teams.

## Make sure it provides these 5 things:

- 1 Advanced visibility and enforcement.** Get a complete view into internet activity, no matter where your users are located, and block threats before they become attacks. This will help your users stay safe on any network, anytime, on any device.
- 2 Centralized management.** With centralized management, strained resources are better able to manage policies, see trends, and defend against threats.
- 3 Comprehensive threat protection.** Protect your users with comprehensive coverage over every protocol and port. No matter what threats are lurking, SIG keeps everyone safer.
- 4 Proxy-based web traffic and file inspection.** A cloud-delivered full proxy deeply inspects and scans all web traffic for greater transparency, control, and protection from malware and other threats. Advanced content filtering helps with policy enforcement and compliance challenges.
- 5 An open platform for integration with your existing stack.** The right SIG is built as an open platform that seamlessly integrates and shares intelligence with other systems, reducing overhead and improving incident investigations and remediation tasks. Organizations need a highly reliable solution when integrating key functions to prevent a choke point.

Sources:  
1-5. ESG Research Publication, *Cisco Secure Internet Gateway Survey*, January 2019

**Solution:**

# Cisco Umbrella

As your perimeter expands with more roaming employees and branch offices, so does your attack surface. Cisco Umbrella offers effective protection for your users, no matter where they are working. Now you can give your employees the freedom to work wherever and whenever they want without putting your business at risk.

---

Cisco and ESG surveyed 450 cybersecurity professionals to understand technology consumption patterns and validate market trends. Combined with exclusive threat data made available through Cisco Talos Intelligence Group, this security readout provides a unique look at the trends impacting remote and roaming user security.

# When it comes to security, Umbrella has you covered

Cisco Umbrella is a cloud security platform that provides the first line of defense against virtual threats, wherever users go. Because it's built into the foundation of the internet, Umbrella delivers complete visibility into internet activity across all locations, devices, and users. It allows you to take a proactive stance against attackers, instead of chasing them down once they're already inside your system.

“Umbrella enables us to allow branches to access the internet locally and securely instead of being backhauled to the datacenter.”

— **IT Director, Medium Enterprise Professional Services Company**

Umbrella uses the internet's infrastructure to deliver complete visibility into internet activity across all locations, devices, and users. It can help you see and block threats before they ever reach your network or endpoints, reducing the number of malware infections your team needs to review and respond to.

## With Cisco Umbrella, you get 5 big advantages:



### **Complete visibility, complete threat protection.**

See and protect on-the-go users, on all devices, in every location.  
Proactively block connections to malicious destinations at the DNS and IP layers.



### **Superior, predictive intelligence.**

Uncover attacks before they infiltrate your system, with live threat intelligence, statistical and machine learning models, and human intelligence.



### **Smart integration.**

Pair Umbrella with your existing security tools to make the most out of your investments. With an open platform and APIs, sharing data and extending protection is simplified.



### **Easy, quick deployment.**

Since Cisco Umbrella is built in the cloud, there's no hardware to install, and no software to maintain. Now you can leverage your existing Cisco footprint – Cisco AnyConnect, Cisco routers, Meraki, SD-WAN and more – to provision thousands of network devices and laptops in minutes.



### **Fast, reliable infrastructure.**

With Anycast routing, requests are transparently sent to the fastest datacenter available with automated failover. And with more than 800 peering partnerships with ISPs and CDNs, we resolve requests faster, boosting network performance.

“Umbrella gives us a consistent user experience across all locations globally. We have 40+ locations and users get the same experience regardless of location.”

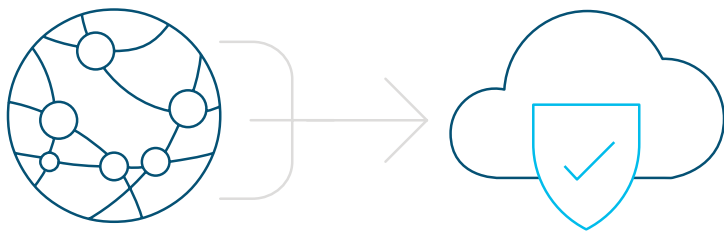
– Senior IT Manager,  
Large Enterprise Industrial Manufacturing Company

# Protection that's as seamless and flexible as today's work environments

## Better security and performance for branch & remote workers

With the increasing adoption of SD-WAN, more and more offices and remote workers are connecting directly to the internet – creating a huge security risk. Cisco Umbrella enables you to secure your SD-WAN in minutes, protecting all devices, locations, and users, even if they're off VPN.

Simply point your DNS to the Umbrella global network to protect any device that joins your network. No added latency, and no hassle for your employees. You no longer have to worry when users roam, because your network will stay secure.



## Expose Shadow IT once and for all

When you can see what's happening across your organization, you can take steps to protect it. Umbrella allows you to discover which SaaS apps are being used, who's using them, and what risks they pose to your organization. You'll gain full visibility into Shadow IT activity – and the ability to block apps and secure users, even when they're roaming.

“I think Cisco Umbrella's biggest strength is providing clarity on what applications and services our clients are trying to connect with – and making it a simple process to approve or deny access to those services.”

– Nick Currie, Network Administrator, ABN Group (VIC) PTY LTD



## A new approach means no more playing defense

### Don't wait for threats to strike first

As threat risks continue to escalate, Cisco Umbrella turns you into a proactive defender. It maps internet activity patterns and learns from past behavior, actively processing and enforcing more than 7 million unique malicious domains and IPs concurrently at the DNS layer. Every day, it adds 60,000+ new destinations to its block list. With this massive reach and volume, Umbrella allows you to identify, understand, and block threats even faster.

“With Umbrella, the risk of security breaches is less likely and mitigated across our user base. The solution allowed us to utilize broadband internet local at the branch which improved internet access speeds without compromising security.”

– IT Director, Medium Enterprise Professional Services Company

# 7 million

unique malicious domains and  
IPs blocked daily.



In a recent survey

---

More than half of respondents saw a reduction in malware infections by

75%



or more<sup>1</sup>

---

More than 2/3 of respondents stated that Umbrella helped to improve protection for remote workers and branch offices by

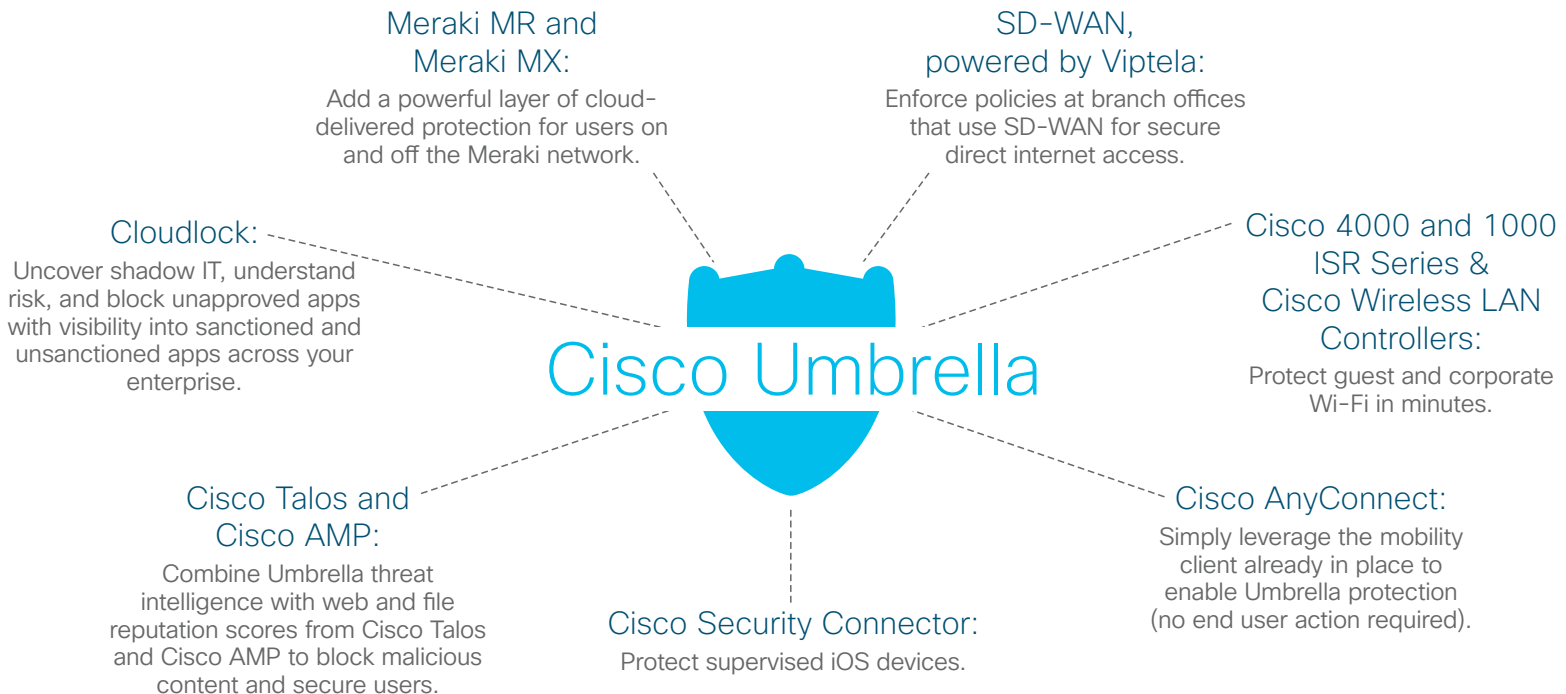
75%<sup>1</sup>



# Discover the industry's first Secure Internet Gateway

Cisco Umbrella provides a comprehensive SIG solution that protects every device on your network, whether managed or unmanaged – including mobile and Internet of Things (IoT) devices. Umbrella offers more effective protection for all of your office locations from a single platform, reducing the time, money, and resources previously required for deployment, configuration, and integration tasks.

## Take advantage of the Cisco Security ecosystem.



Source:  
1. TechValidate survey of 195 users of Cisco Umbrella

# Cisco Umbrella

Multiple, disparate tools with glitchy integrations. Siloed data. Hundreds of security alerts and thousands of incidents to investigate. As resources remain squeezed and the security skills gap widens, you need to prioritize your team's efforts. Where to begin?

If you're using traditional security tools and expecting them to scale across your SD-WAN, you'll likely run into trouble. The best approach is an integrated one that works with your stack, not against it.

Cisco Umbrella amplifies your existing investments with a bi-directional API that easily integrates with other systems and your Cisco security architecture. And it starts working in minutes. Simply point your DNS to Umbrella – and start protecting against malware, ransomware, DNS tunneling, and more.

[Learn more about the top security trends](#)

See full report [▶](#)

## The Umbrella Advantage

180B

daily DNS requests  
(over all ports and protocols)

800

partnerships with top ISPs and CDNs

90M

global daily active users

3,900

peering sessions

31

data centers across five continents

**Don't take our word for it.  
Try our world-class threat protection for 14 days.**

[Start free trial](#)

