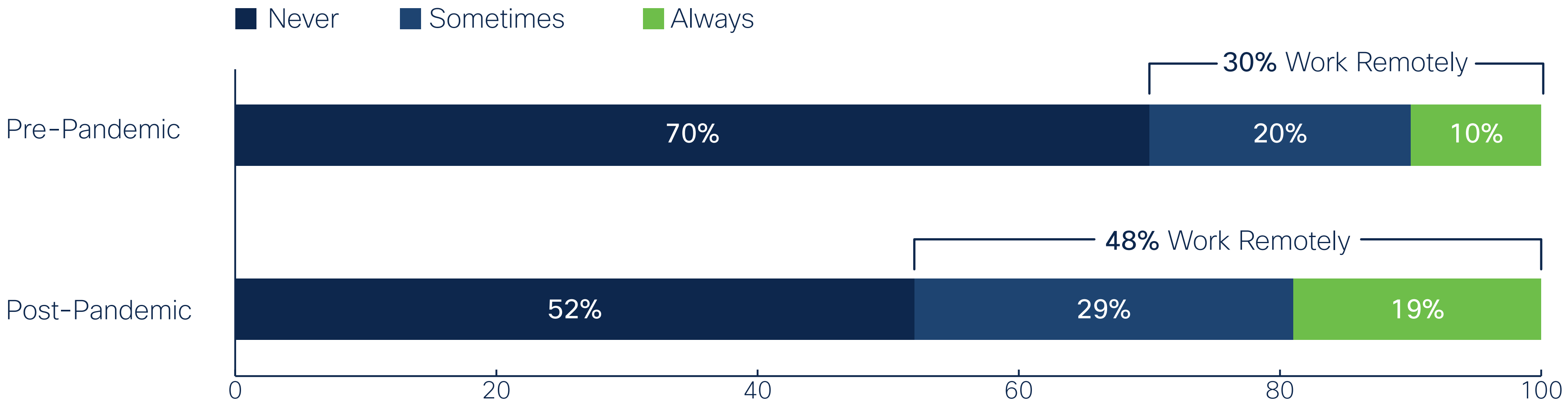
Cisco Umbrella

Ebook
Cisco Public

Cybersecurity for remote workers

How to secure every device, everywhere

In this ebook:



Percentage of employees working remotely, pre- and post-pandemic (Projected)

Protection in the post-pandemic workplace

The COVID-19 pandemic has had a profound impact on the way we work, creating change that will last well into the future – with some changes that may well be permanent. As businesses begin to develop their strategies for operating in a post-pandemic world, one of their biggest challenges will be addressing their evolving cybersecurity needs as remote work becomes a de facto aspect of the modern workplace.

In 2019, Gartner predicted that by 2030, the demand for remote work would increase by up to 30%. The COVID-19 pandemic, of course, massively accelerated this trend, with many organizations making the move to remote work for most or all of their workforce. Now, having gotten used to remote life, many employees are looking to stay that way – and CFOs are seeing the cost advantages in doing so. As a result, it's predicted that, post-pandemic, 48% of employees at large enterprises will work remotely at least some of the time. And they're going to need protection.[1]

Conventional defenses weren't built for the post-pandemic worker – users who may be working remote, in the office, or some hybrid combination of both. Relying on anti-virus products, firewalls, and isolated security solutions that don't share intelligence just won't do the trick. It's time to look for new ways to enhance your cybersecurity and ensure your organization is ready to come out of the pandemic with the protection you need, wherever your users are working.

68% of branch offices and roaming users were the source of compromise in recent attacks.[2]

In this ebook, we'll look at the challenges facing today's security professionals and explore simple actions you can take to reduce malware, simplify security, and protect your growing population of remote and roaming workers.

A multi-function, cloud-based security solution is the simplest way to secure employees and students working remotely in the post-COVID world. Delivering protection that starts at the DNS layer, this solution should unify a variety of other security services – a firewall, a secure web gateway, CASB – to help businesses see and stop threats before they can do damage.

New defenses for new threats

As the network changes, so does attack methodology – and this certainly includes the move to remote work. Attackers spin up new attack infrastructure with incredible speed and adaptability, making it challenging to identify and block malicious traffic as it crops up in new areas and in more evasive and nefarious variations. Some of the latest threats include:

- Deceptive email spear phishing techniques that enable attackers to bypass conventional defenses and install ransomware and malicious code
- One-off malware packages that can't be readily detected using signature-based solutions – regardless of how quickly those signatures and profiles are updated
- Low-and-slow attacks that evade network-based defenses and allow attackers to infiltrate infrastructure and exfiltrate data, undetected, over extended periods of time
- Malware kits and malware-as-a-service resources that increase threat volume by empowering bad actors and criminal organizations to engage in cyberattacks like malicious cryptomining, despite a lack of technical skills

Staffing

1.8M cybersecurity positions to go unfilled by 2022[3]

Orchestration

79% struggle to orchestrate alerts across vendors[4]

Alerts

44% of cybersecurity experts see more than 10K daily alerts[4]

Reporting

300% increase in reported cybercrimes[5]

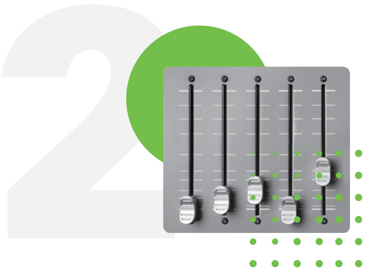
DNS-layer security – secure remote employees, easily

To protect users on and off network in the post-pandemic world, use the internet to your security advantage. 91% of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic. But when internet requests are resolved by a recursive DNS service, they become the perfect place to check for and block malicious or inappropriate domains and IPs. Security teams that are not monitoring DNS for indications of compromise are missing an important opportunity.

DNS is one of the most valuable sources of data within an organization. It should be mined regularly and cross-referenced against threat intelligence to help security teams more accurately detect compromised systems and improve visibility and network protection. IT security leaders should make proactive DNS-layer security a core component of their security strategies. It's a great first line of defense against threats targeting remote employees.

Proactive DNS-layer security, as easy as 1, 2, 3

Block dangerous connections between your users and malicious domains



Stop command-and-control (C2) callbacks and data exfiltrations easily

Reduce security incidents and alerts by neutralizing them before they occur

A better way to stop threats, faster

Increase visibility, decrease risk (and work!)

Most companies leave their DNS resolution up to their ISP. But with the rise in remote work, organizations are increasingly adopting direct internet connections, and more and more users are bypassing the VPN. This leads to DNS blind spots. DNS requests precede the IP connection, which enables DNS resolvers to log requested domains regardless of the connection's protocol or port. Monitoring DNS requests (as well as subsequent IP connections) is an easy way to more accurately detect compromised systems, which improves security visibility and network protection.

The bottom line: IT security leaders are looking for more effective security strategies that don't add complexity to their security operations. And DNS-layer security can help.

The indispensability of DNS-layer security

DNS-layer security operates on the simple principle that attacks – no matter how sophisticated or unique – must originate from somewhere. By preemptively blocking all requests over any port or protocol to any and all suspicious "somewheres," DNS-layer security can stop command-and-control exfiltration, malicious cryptomining, ransomware, and other attacks without the burden of first having to identify the specific nature of those attacks. Bad domains are blocked because they are quickly and accurately identified as bad domains.

DNS-layer security delivers:

- Predictive identification of malicious hosts. By aggregating and analyzing DNS-related data—including tens of billions of daily DNS requests, WHOIS records, and Border Gateway Protocol routing information—it's possible to identify suspicious domains with a very high degree of accuracy.
- DNS request blocking as a cloud service. Armed with a constantly updated list of suspect domains, a cloud service provider can preemptively block requests for any domain or IP that might pose a threat to the business.

1 in 3

companies reported breaches that could have been controlled by DNS[6]

$100 – 200B

global losses could have been prevented by DNS[6]

DNS-layer security blocks threats others miss

By enforcing security at the DNS and IP layers, Cisco Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints, with no added latency. Cisco Umbrella also blocks direct IP connections from command-and-control callbacks for roaming users. Together, this allows you to protect anywhere and everywhere – ideal for the post-pandemic world of users working both on and off network.

Cisco Umbrella categorizes and retains all internet activity to simplify the process of investigating threats and attacks. Using the Umbrella Investigate console and on-demand enrichment API, it provides the context to prioritize incidents and speed up incident response, so you can more quickly detect and remediate threats with Cisco Threat Response.

AV-TEST conducted a threat detection test for leading DNS-layer security solutions, and Cisco Umbrella performed significantly better than other vendors, with a 70% detection rate when utilizing a selective proxy. That's more than 17% more effective than other solutions on the market.

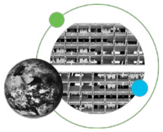
AV-TEST: DNS-layer protection security efficacy test results[7]

Vendor	Detection rate | Number of test cases 3,572
Cisco Umbrella (DNS-layer with selective proxy)	70.7%
Akamai Enterprise Threat Protector	53.6%
Infoblox BloxOne Threat Defense	36.3%

The Cisco Umbrella global network advantage

620B daily DNS requests

500M global daily active users



900+ partnerships with top ISPs and CDNs

20K+ Customers

35+ data centers across 5 continents

Why Cisco Umbrella?

Cisco Umbrella is committed to delivering the best, most reliable, and fastest internet experience to every single one of our users. We are the leading provider of network security and DNS services, enabling the world to connect to the internet with confidence on any device. As we move towards a post-pandemic world, you can rest assured that Cisco Umbrella has the background and the technology to protect your remote, roaming, and in-office workers.

- **More than a decade of DNS leadership**. Thirteen years of hands-on experience working with DNS technology and data gives Cisco Umbrella significant advantages when it comes to understanding and blocking attacker infrastructure.
- **Unparalleled DNS data volume and variety.** Cisco Umbrella possesses unmatched visibility into DNS activity worldwide. The Cisco Umbrella global network processes 620 billion internet requests from over 500 million users across 190 countries worldwide.
- **Predictive intelligence and statistical models**. Cisco Umbrella has developed highly specialized models that block 7 million malicious destinations at any given time – and detects them before any other security provider on the planet.
- **Highly resilient cloud infrastructure.** Cisco Umbrella boasts 100% uptime since 2006. Using Anycast routing, any of our 35+ data centers around the globe are available using the same single IP address. Requests are sent transparently to the nearest, fastest data center, and failover is automatic.
- **Integrations that amplify investments.** Cisco Umbrella unifies multiple security services in a single cloud platform to secure access to the internet and control cloud app usage anywhere users go. Users can manage security policies and enforcement across their entire infrastructure from a single dashboard, through integrations with Cisco SD-WAN architecture, Cisco Meraki MR, Cisco Meraki MX and Cisco ISR routers, Cisco Secure Network Analytics (Stealthwatch), and Cisco Secure Endpoint (Advanced Malware Protection).

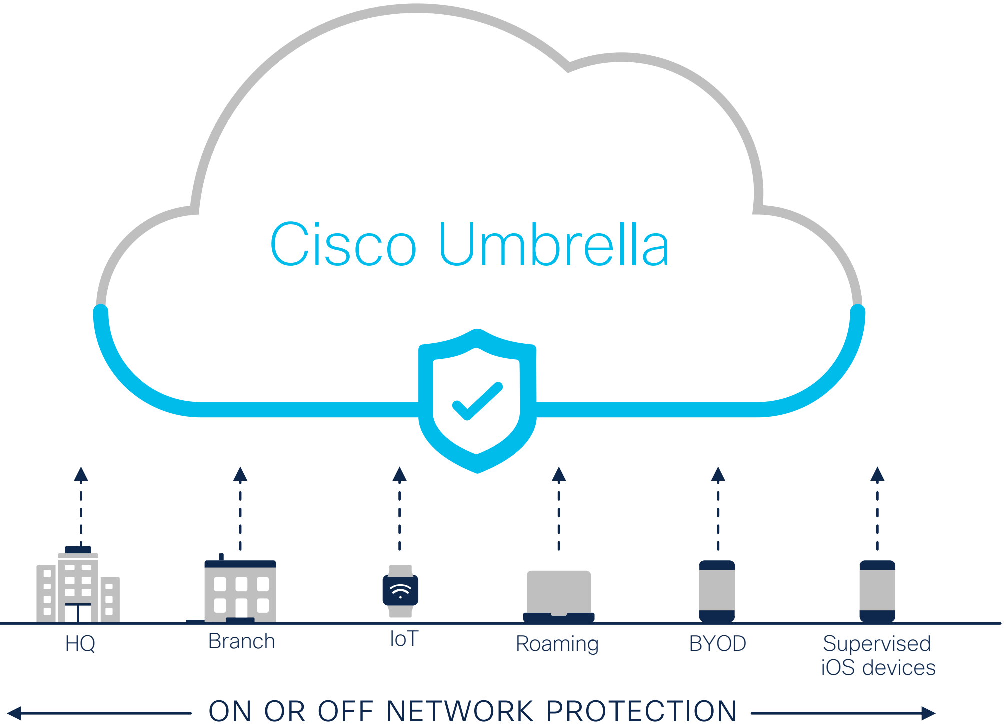
Security enforcement for HQ, branch, and remote offices

Leveraging unmatched threat insights from Cisco Talos, one of the largest commercial threat intelligence teams in the world, Cisco Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files used in attacks. We also feed huge volumes of global internet activity into a combination of statistical and machine learning models to identify new attacks being staged on the internet.

These distinctive attributes make Cisco Umbrella the ideal choice for securing organizations of all sizes in the post-pandemic era – from small businesses without dedicated security professionals, to multinational enterprises with complex environments. Cisco Umbrella provides more effective protection and internet-wide visibility both on and off your network – ensuring all your workers, remote or not, are secure.

A versatile first line of defense

- See all Internet traffic
- Block attacks earlier
- Contain malware if already inside
- Easily enforce content web filtering
- Discover, manage, or block cloud apps
- Gain context for faster investigation



30 minutes to secure workers anywhere

Simplify security for remote employees in the post-COVID world

As the pandemic pushes us to a more flexible form of workplace, Cisco Umbrella is the fastest and easiest way to protect all of your employees, whether they work from home, the office, or on the road. With no hardware to install and no software to manually update, ongoing management is simple. You simply redirect your DNS to Cisco Umbrella. That's it. Then you can leverage your existing Cisco footprint – Cisco AnyConnect, Cisco routers (ISR 1K and 4K series), Cisco Wireless LAN Controllers, and Meraki MR/ MX – to provision thousands of network devices and laptops in minutes. Protecting remote users really is that simple.

Interested in trying Cisco Umbrella for yourself?

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