EBOOK

Network security made simple.

Secure every device, everywhere in less than 30 minutes.

cisco

Cisco Umbrella

Table of contents

In this ebook:

Taking the stress out of security

Security isn't for the faint of heart. The volume and sophistication of attacks are intensifying relentlessly — and it's clear that conventional defenses were not built for today's mobile workers, branch offices, and ever-expanding perimeter. Relying on on anti-virus products, firewalls, and closed systems that don't share data or intelligence is a dead-end strategy. With less budget, fewer resources, and more security alerts than ever, it's time to look for new ways to enhance your digital security without spending excessively or overburdening your staff.

In this ebook we'll look at the challenges facing today's security professionals and explore some simple actions you can take to reduce malware, simplify security and improve network performance.

The simplest decision you can make to improve your security.

New defenses for new threats

As the network changes, so does attack methodology. The speed and adaptability with which attackers spin up attack infrastructure creates new challenges for identifying and blocking malicious traffic for all businesses across all industries, including:

- Deceptive email spearphishing 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 signature and profiles are updated
- Low and slow attacks that evade network-based defensed and allow attackers to infiltrate infrastructure and take 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 their lack of technical skills

Staffing
3.5M cybersecurity positions to go unfilled by 2021[1]

Alerts
44% see more than 10K daily alerts[2]

Orchestration
79% struggle to orchestrate alerts across vendors[2]

1. Cybersecurity Ventures Cybersecurity Jobs Report | https://cybersecurityventures.com/cybersecurity-almanac-2019/
2. Cisco 2019 CISO Benchmark Survey | https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1963786/2019CISOBenchmarkReportCiscoCybersecuritySeries.pdf

DNS-layer security — a hidden goldmine

It's time to 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.

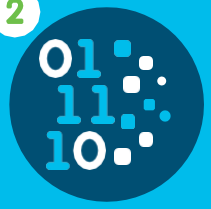
DNS is one of the most valuable sources of data within an organization. It should be mined regularly and cross-referenced against threat intelligence, to help security teams gain better accuracy and detection of compromised systems and improve visibility and network protection. IT security leaders should make proactive DNS-layer security a core component of their security strategies.

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

1

Block dangerous connections between your users and malicious domains

2



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

3

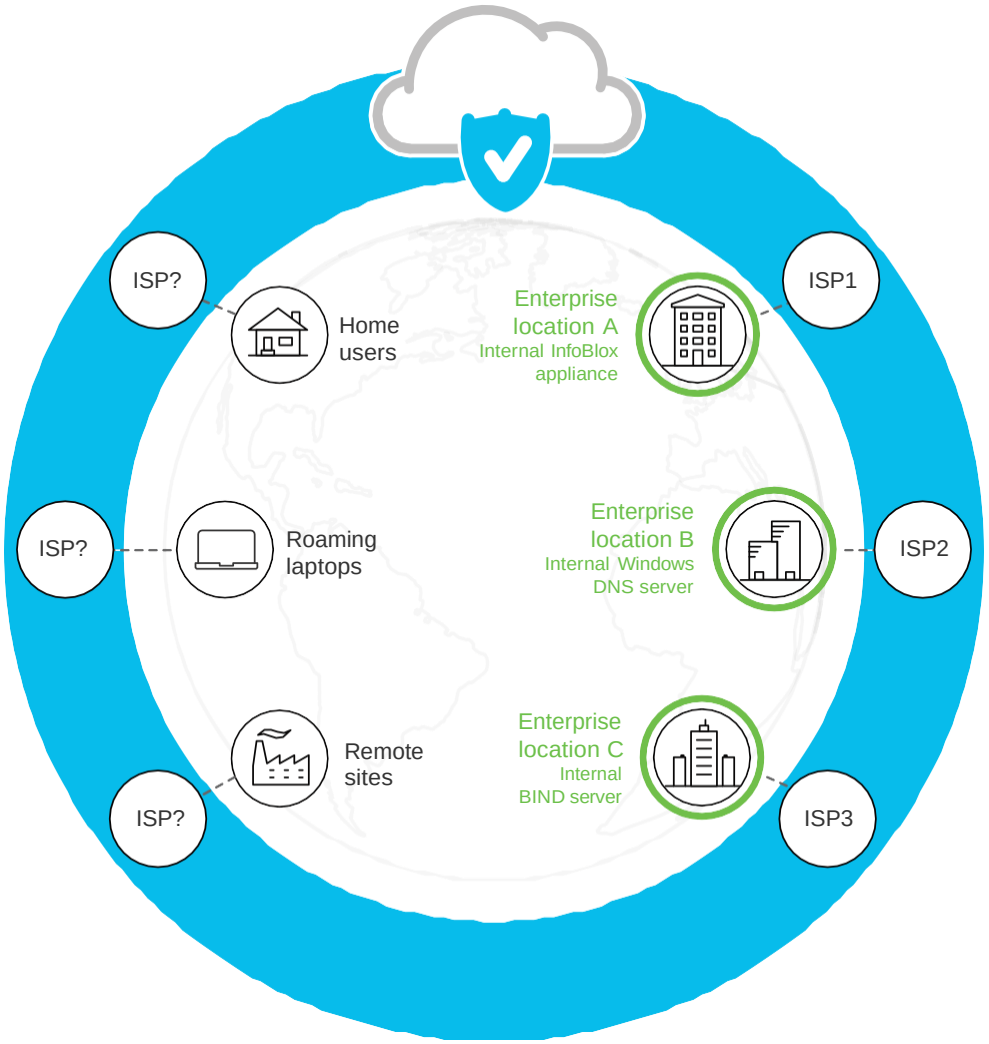
Reduce security incidents and alerts by neutralizing them before they occur

A better way to stop threats, faster

Increase visibility, decrease risk (and work!)

Most companies leave their DNS resolution up to their ISP. But as more organizations adopt direct internet connections and users bypass the VPN, this leads to a DNS blind spot. 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 provide better accuracy and detection of 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.



The indispensability of DNS-layer security

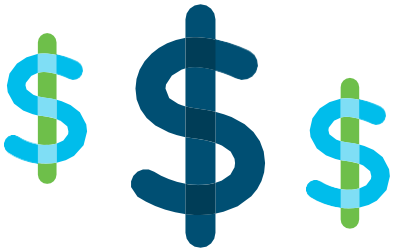
DNS-layer security operates on the simple principle that attacks — no matter how sophisticated or unique — must originate from somewhere. By pre-emptively blocking all requests over any port or protocol to any and all suspicious "somewheres," DNS-layer security can stop command-and-control exfiltration, 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 pre-emptively block requests for any domain or IP that might pose a threat to the business.

1 in 3

reported breaches could have been controlled by DNS[3]



$100 - 200B

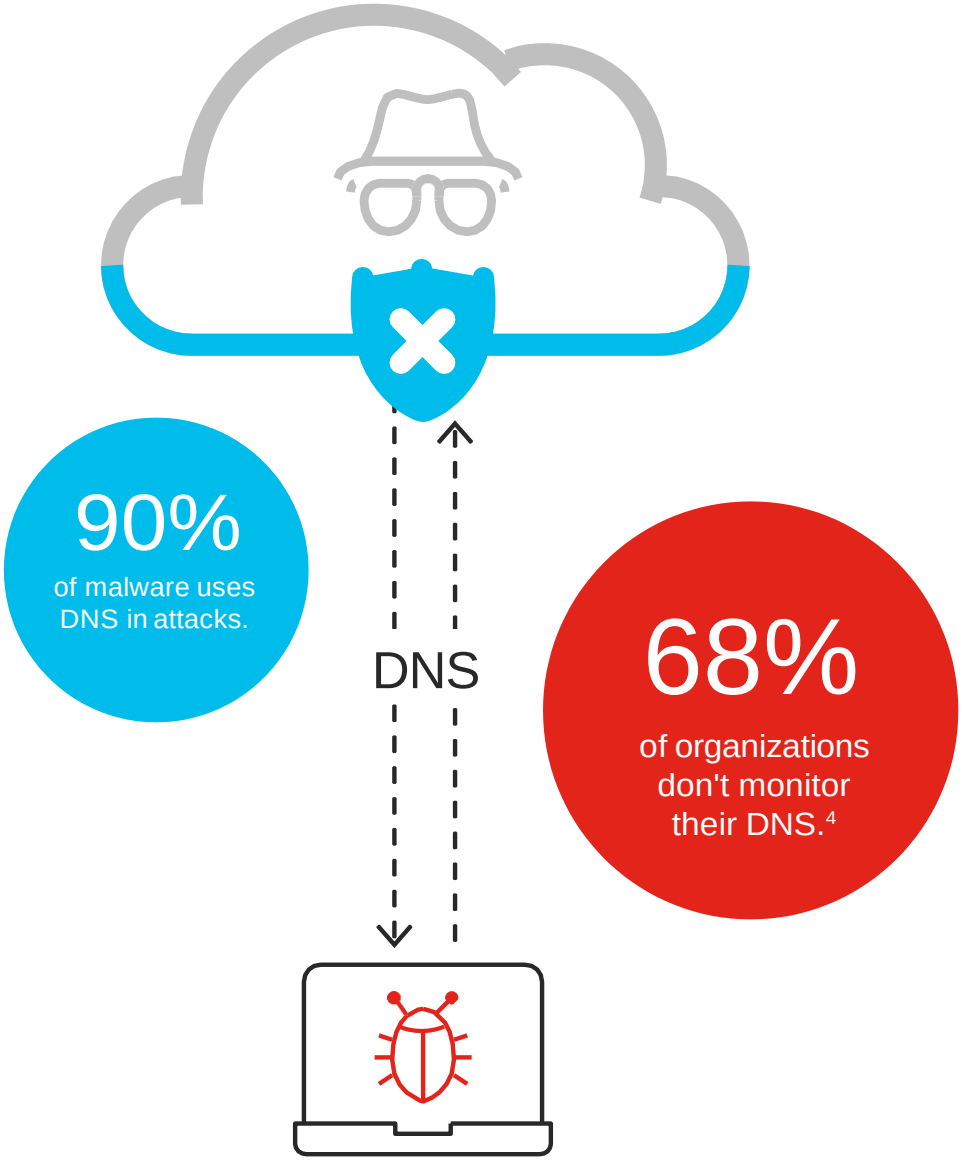
global losses could have been prevented by DNS[3]

3. The Economic Value of DNS Security," a new report published by the Global Cyber Alliance (GCA) https://www.darkreading.com/network-and-perimeter-security/dns-firewalls-could-save-companies-billions/d/d-id/1334965

DNS-layer security blocks threats others miss

By enforcing security at the DNS and IP layers, 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. Umbrella blocks direct IP connections from command and control callbacks for roaming users.

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



4. Cisco Security Research Report - https://umbrella.cisco.com/blog/2016/01/21/cisco-security-report-more-orgs-should-be-monitoring-dns/

Why Cisco Umbrella?

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.

- **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.
- **Unmatched DNS data volume and variety.** Cisco Umbrella possesses unmatched visibility into DNS activity worldwide. Umbrella processes 180 billion internet requests from over 100 million users across 160 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**.Umbrella boasts 100% uptime since 2006. Using Anycast routing, any of our 30 plus data centers across 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.** Umbrella unifies multiple security services in a single cloud platform to secure access to the internet and control cloud app usages 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 and Cisco ISR routers, Cisco Stealthwatch, and Cisco Advanced Malware Prevention.

The Umbrella Advantage

180B
billion daily DNS requests

100M
global daily active users

900+
partnerships with top ISPs and CDNs

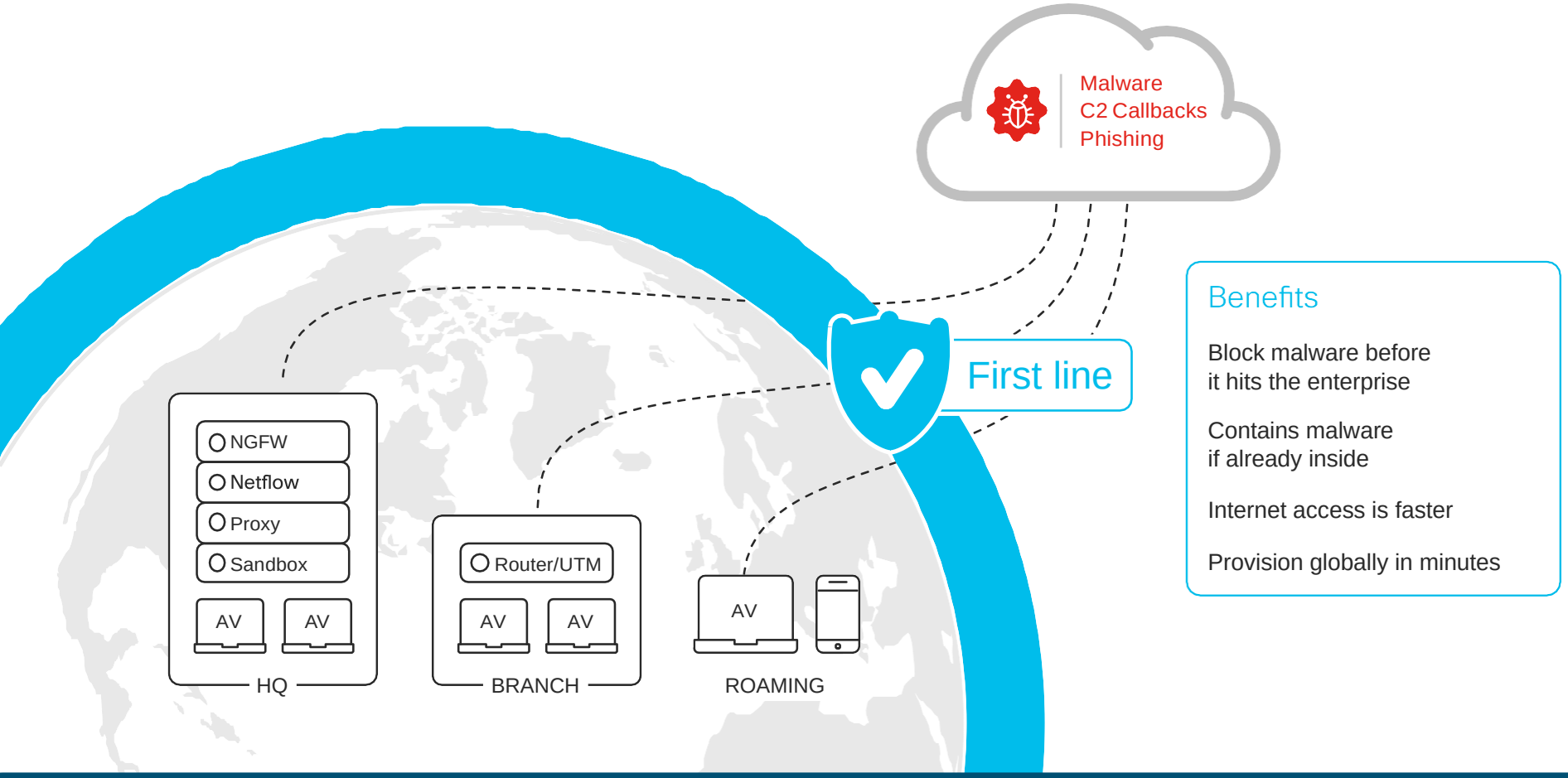
18.5K+
customers

30+
data centers across five continents

Where do you enforce security?

Leveraging unmatched threat insights from Cisco Talos, one of the largest commercial threat intelligence teams in the world, Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being 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 Umbrella inarguably the best choice for small businesses without dedicated security professionals to multinational enterprises with complex environments, Umbrella provides more effective security protection and internet-wide visibility on and off your network.



Benefits

Block malware before it hits the enterprise

Contains malware if already inside

Internet access is faster

Provision globally in minutes

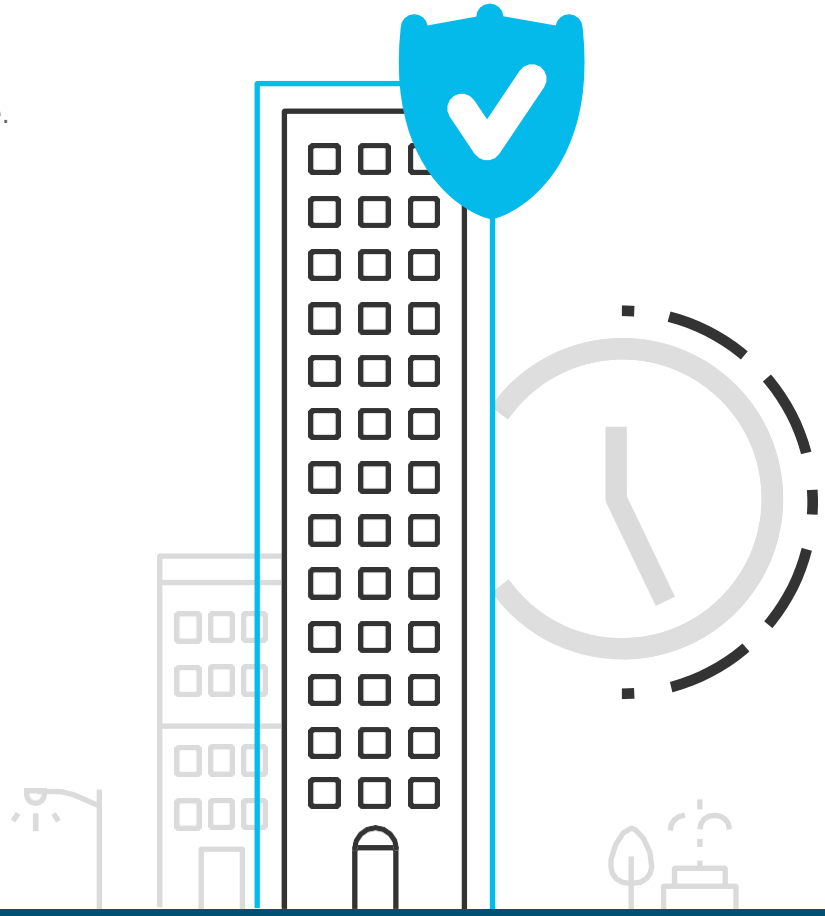
30 minutes to a safer enterprise

Umbrella customers reduce malware by 75%[5] and reduce remediation times by 50% or more[6].

Simplify security management

Umbrella is the fastest and easiest way to protect all of your users enterprise-wide in minutes, on and off the network, and reduces the number of infections and alerts you see from other security products by stopping threats at the earliest point. 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.



Interested to try out Umbrella for yourself?

Get worldwide threat protection in minutes. Try it out for 30 days.

Start a Free Trial

5. https://www.techvalidate.com/product-research/cisco-umbrella/facts/AF2-8E2-79D
6. https://www.techvalidate.com/product-research/cisco-umbrella/charts/F83-DB9-434

cisco

Cisco Umbrella