White paper

The fastest, easiest way to secure your network

Why Cisco Umbrella is the simplest decision you can make to improve your company’s security.

You have to make some serious security decisions when you’re an IT leader. That’s because both the volume and sophistication of attacks are intensifying relentlessly — and it’s clear that conventional defenses alone are no longer adequate. More effective blocking of attackers is particularly important because under-the-radar attacks are wreaking havoc on businesses that rely on antivirus products, firewalls, and sandboxing alone.

Security in the DNS layer

Plus, no one has an unlimited security budget — so you must act quickly to enhance your digital security without spending excessively or overburdening your staff.

Given these realities, DNS-layer security offers extremely compelling value. With the right combination of internet infrastructure data and predictive intelligence, a DNS-layer solution can quickly identify malicious domains even before those domains and IPs are used to actually launch any type of attack. In fact, DNS-layer security is especially useful as your first line of defense, because DNS requests precede all internet activity.

This proactive DNS-based identification of malicious domains enables you to do the following:

Immediately block dangerous connections between your users and any potentially malicious domains

Stop command-and-control (C2) callbacks and data exfiltrations —
even if you haven’t yet noticed or pinpointed a compromised internal host

Dramatically reduce security incidents and alerts by proactively neutralizing them before they occur

New defenses for new threats

Innovation isn't restricted to legitimate businesses. Attackers also innovate aggressively. This innovation is in part motivated by necessity, since the security industry has a pretty good track record of developing policies, processes, and products to cope with each new wave of attacks.

In recent years, however, attacker innovation has also become even more motivated by the growing financial rewards that come with successful criminal activity. As people and organizations make greater use of digital technology, the volume and value of their data are increasing. Attacks can be highly profitable, whether they take the form of data theft and subsequent resale on the open market or the increasingly common ransomware attacks, which force an organization to pay for access to its own data.

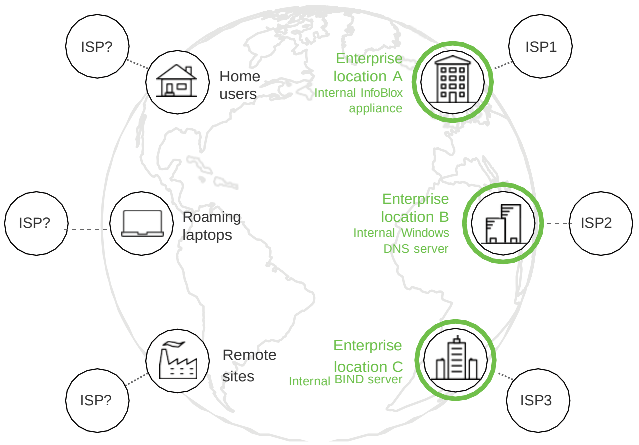
Several aspects of attack innovation have become particularly troubling to enterprise IT security leaders, including:

- **The sophistication of deceptive email spearphishing techniques** that enable attackers to bypass conventional defenses and successfully install ransomware and other malicious code
- **The ease with which attackers can now generate one-off malware packages** that can't readily be detected using conventional signature-based solutions — no matter how quickly those signatures and profiles are updated in response to attacks elsewhere
- **The trend toward "low and slow" attacks** that evade conventional network-based defenses and thereby allow attackers to infiltrate enterprise infrastructure and take data over extended periods of time without detection
- **The speed and adaptability with which attackers spin up attack infrastructure**, which creates new challenges when it comes to identifying and blocking potentially malicious traffic
- **The advent of malware kits and malware-as-a-service resources** that substantially increase threat volume by empowering individual bad actors and criminal organizations to engage in cyberattacks despite their personal lack of technical skill sets

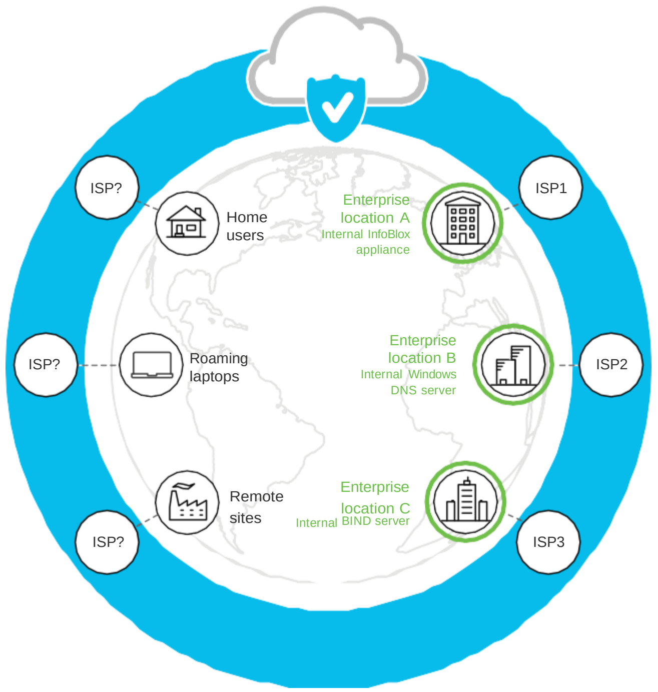
Innovation isn't restricted to legitimate businesses. Attackers also innovate aggressively, motivated by financial rewards.

Stop threats before they reach your network or endpoints

Multiple fragmented internet connections are difficult to secure.



With a cloud security platform, management of DNS requests can be unified and secured across all endpoints.



○ Recursive DNS for internet domains

○ Authoritative DNS for intranet domains

This multidimensional attack would itself be troubling enough for IT security leaders. However, the heightened risk caused by new kinds of attacks is exacerbated by changes taking place in the enterprise itself. These changes include an expanding threat surface, the growing tendency of mobile users to connect directly to cloud resoures via unsecured public Wi-Fi (rather than through secure VPN connections back to the enterprise), and an often overwhelming volume of security alerts generated by the multiple generations of “point” security solutions that IT has accumulated over time.

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.

Attacks never get a chance to carry out their malicious work, because they never touch the network, endpoints, or any protected remote user outside the corporate network.

There are two basic elements to DNS-layer security:

1. **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. This analysis entails more than merely blacklisting hosts in newly created domains. It also involves sophisticated analytical models that automate the detection of anomalies — such as detecting suspicious domain traffic spikes that are characteristic of attack activity and using natural language processing to flag domain names, including slightly obfuscated brand names that are typically created for use in spearphishing campaigns.
2. **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. Because this blocking is provided as a cloud service, its protection can be extended anywhere users go — including to roaming laptops outside the network perimeter, with no added latency.

Proactive protection against emerging threats. With predictive DNS-layer security, IT doesn't need to wait until an attack is launched and identified. Attacks can be stopped in their tracks before they ever come into contact with the IT environment, regardless of how well-camouflaged their malicious payloads or social engineering techniques may be.

DNS-layer security can stop attacks without first having to identify the specific natures of those attacks.

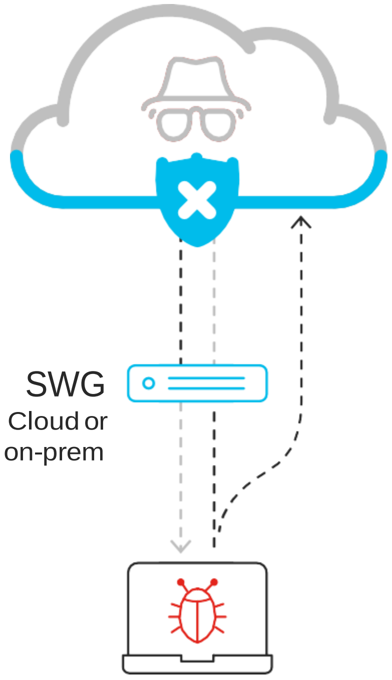
The Global Cyber Alliance, The Economic Value of DNS Security[1]

1. DNS Firewalls cold have mitigated one-third of the incidents we studied and could have prevented $10 billion in losses.
2. The DNS firewall is a relevant control against one-third of reported breaches.
3. Domain Name System (DNS) firewalls, also known as protective DNS, which are freely available and easy to install, could prevent 33% of cybersecurity data breaches from occurring.
4. It is rare to find a control with the combination of high impact and ease of deployment.
5. A DNS firewall could prevent between $19 and $37 billion in the US. or globally between $150 and $200 billion.

DNS-layer network security should block threats others miss.

91%

of C2 can be blocked at the DNS layer[2]



15%

of C2 bypasses web ports 80 & 443[3]

- **Early interdiction of command-and-control traffic.** In cases where an infiltration does occur, DNS-layer security can put a rapid end to C2 traffic and prevent data exfiltration. Communication with malicious domains is blocked because the domain is malicious, not because any exfiltration has to first be specifically identified.
- **Reduced security alert traffic.** Because DNS-layer security blocks such a high volume of malicious activity before it comes in contact with enterprise IT infrastructure, it can significantly reduce the volume of alerts that the security staff has to review and clear. This can represent a substantial cost savings and allow staff-hours to be reallocated to higher-value tasks.
- **Mitigation of contractor and partner vulnerabilities.** Many organizations have suffered security breaches because of lax practices by contractors and other third parties. By implementing DNS-layer security, businesses can better protect themselves against these vulnerabilities without placing excessive compliance burdens on their partners.

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 strategy.

Why Cisco Umbrella?

Umbrella is committed to delivering the best, most reliable, and fastest internet experience to every single one of our more than 100 million 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.

We are unique among security providers for several reasons, including:

- **More than a decade of DNS leadership**. Ten years of hands-on experience working with DNS technology and data gives Cisco Umbrella significant advantages when it comes to understanding how both legitimate and nonlegitimate parties register domains, provision infrastructure, and route IP traffic over the autonomous system life cycle.
- **Unmatched DNS data volume and variety.** The accuracy and completeness of any analytic outcome is largely contingent upon the quality, volume,and completeness of the data inputs. As a DNS provider, Cisco Umbrella processes 180 billion DNS requests for 100 million users and 18,500 businesses every day. By combining that data with third-party feeds, Cisco Umbrella possesses unmatched visibility into DNS activity worldwide.
- **Differentiated algorithms and analytics.** The statistical models required for truly effective and predictive DNS-layer security go far beyond simply spotting anomalies. In fact, the automated generation of malicious infrastructure by attackers has become so commonplace that it's not anomalous at all. That's why Cisco Umbrella has developed highly specialized models that block 7 million malicious destinations at any given time — and that often detect them before any other security provider on the planet.
- **Umbrella has a highly resilient cloud infrastructure that 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. As a result, your requests are sent transparently to the nearest, fastest data center, and failover is automatic. Umbrella peers with more than 900 of the world's top internet service providers (ISPs), content delivery networks (CDNs), and SaaS platforms to deliver superior speed and user satisfaction.
- **Sophisticated integrations from a trusted technology partner.** The security benefits don't stop at the DNS layer. As your network evolves, Umbrella can be extended to act as a full cloud-delivered secure internet gateway, with features including firewall, secure web gateway, threat intelligence, cloud app security, and more. 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.

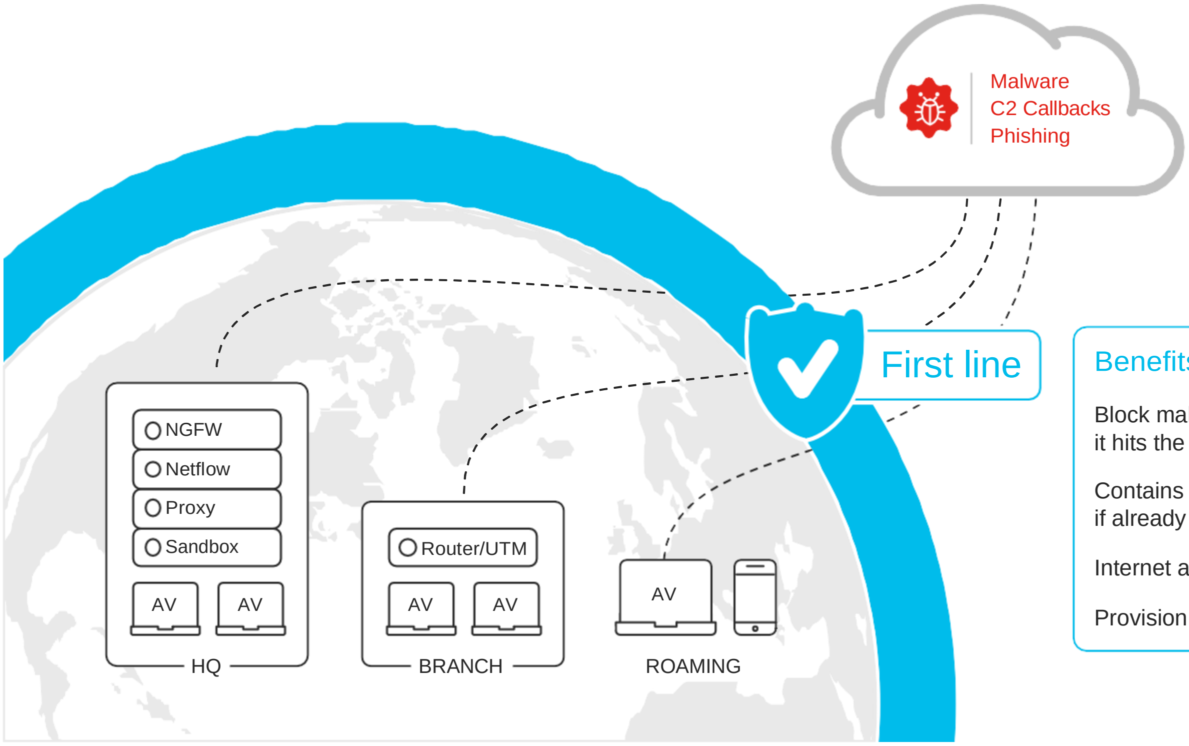
Cisco Umbrella is the leading provider of network security and DNS services, letting you connect to the internet with confidence.

> "Umbrella is the single most effective product we own in our security arsenal."
>
> IT Director,
> Higher Education

After deploying Umbrella, 85% of respondents saw value within a week.

Source: TechValidate survey of users of Cisco Umbrella

Where do you enforce security?



Benefits

Block malware before it hits the enterprise

Contains malware if already inside

Internet access is faster

Provision globally in minutes

- **30-minute deployment.** Umbrella is the fastest and easiest way to protect all of your users enterprise-wide in minutes, 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.

  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.

30 minutes to a safer enterprise

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? Explore the Umbrella guided demo to see how you can block threats, reduce malware and protect your users and devices, anywhere they access the internet.

NOTE: Chrome or Firefox browser is required and you will be asked to install a third-party plug-in, WalkMe.

The Cisco Umbrella Advantage

100M+ **daily active users**

13+ **Over a decade of hands-on experience**

180B+ **DNS requests**

18,500+ **businesses**

7M+ **malicious destinations blocked**

900 **of the world's leading ISPs and CDNs**

[1] https://www.globalcyberalliance.org/dns-economic-value-report/

[2] Cisco. "Cisco 2016 Annual Security Report." January 2016.

[3] Lancope Research. "Visual Investigations of Botnet Command and Control Behavior." 2013