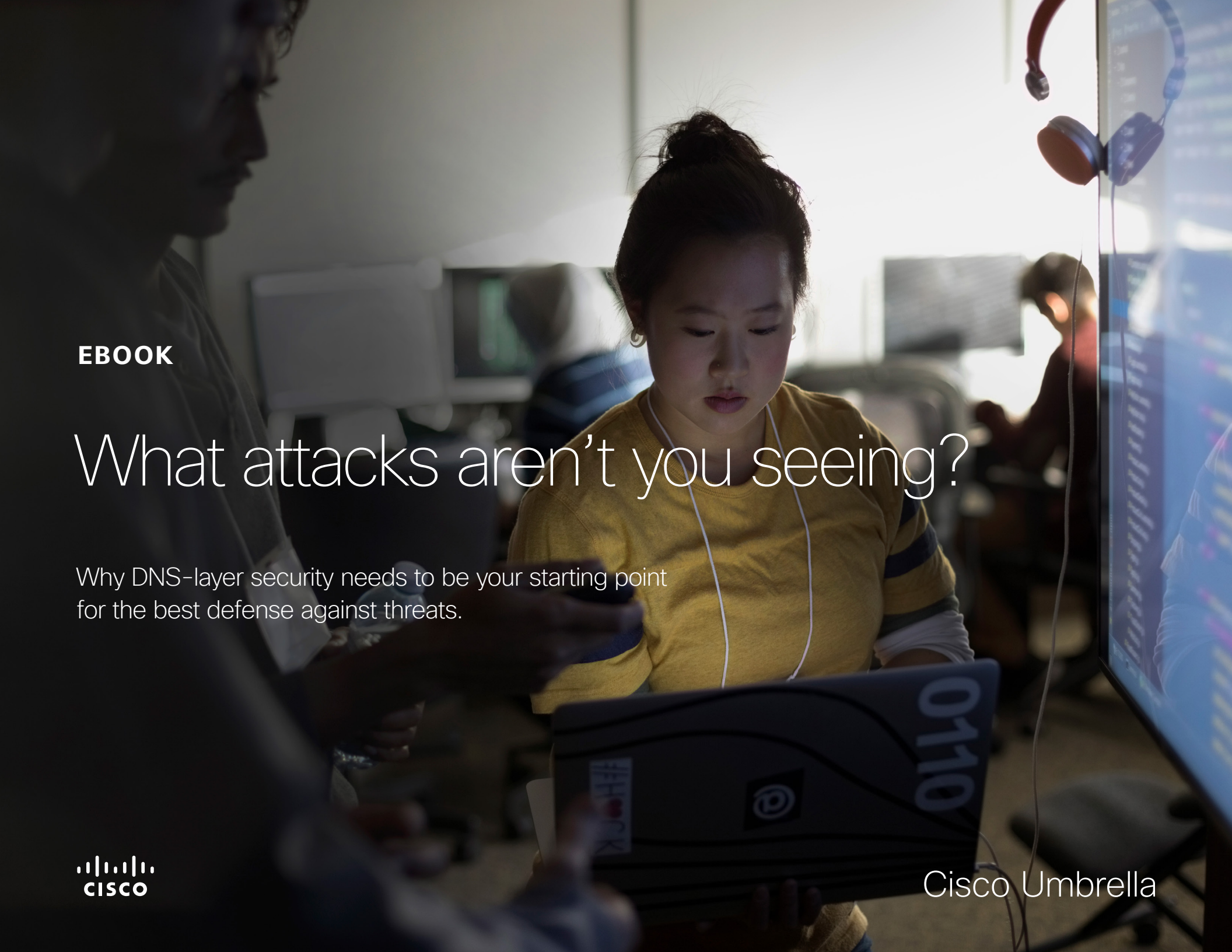


EBOOK

What attacks aren't you seeing?

Why DNS-layer security needs to be your starting point for the best defense against threats.

cisco

Cisco Umbrella

Table of contents

In this ebook:

93% are moving security to the cloud for increased efficiency, allowing security professionals to be more effective and more proactive[1].

Security is shifting

People work anywhere and everywhere now, from co-working spaces and coffee shops to airport lobbies, using connected devices and cloud apps to re-imagine and redefine their workdays. It's great for productivity and efficiency – but it's stretching network security to the breaking point, creating gaps and vulnerabilities as employees move further away from the traditional "office." With 79% of organizations embracing direct internet access (DIA) and SaaS adoption increasing to 60% in the next two years[2], organizations are realizing that the old approach works for the way we used to work, not for today's new network. Security professionals need an easier, more reliable way to improve visibility and security for distributed environments and users, both on and off-network.

Hackers are paying attention, and they're matching today's technology innovations with maddening creativity of their own. They've graduated from attacks designed to steal data to extortion hacks that instead lock people out of their data unless a ransom is paid. They manipulate files and sabotage software and appliances in order to affect stock value or deface websites. They exploit zero-day vulnerabilities, intercept split-second online credit card transactions and hack connected devices ranging from security cameras to smart watches, skateboards and even cars.

1. Cisco 2019 Benchmark study
2. https://learn-umbrella.cisco.com/analyst-reports/research-insights-report-executive-summary-the-future-of-remote-workers-and-branch-offices

Factors contributing to breaches

What's your organization doing to block the threat of a breach? Are you still relying on legacy defenses that focus on trying to secure endpoints behind an eroding perimeter? According to the Cisco Cybersecurity special report, 53% of midmarket businesses have experienced a security breach! Yet midmarket companies investigate only 56% of security alerts. But it's not just the midmarket that's struggling[3]. Fortune 50 enterprises and small businesses are turning to cloud-delivered security services to shore up these defenses and get in front of attacks as they increase in sophistication. This ebook takes a look at the challenges caused by reliance on closed security systems that don't integrate, share intelligence, or help understaffed security teams operate effectively. It's time for a new, proactive approach to secure users and their devices anywhere they choose to go.

1 in 4

organizations are at risk for a major breach in the next 24 months[6]

2019 trends on cyber attacks:

75%	of enterprise-generated data will be created and processed outside the traditional, centralized data center or cloud by 2022, as a result of digital business projects[4].
83%	of senior information technology practitioners surveyed predict unsecured IOT devices will likely cause a data breach in their organization[5].
85%	of organizations say that users violate their mandate to use a VPN[2].
41%	worry about data breaches in SaaS apps[2].

$3.92M

In 2019, the average cost of a breach has grown to $3.92M[6]

2. https://learn-umbrella.cisco.com/analyst-reports/research-insights-report-executive-summary-the-future-of-remote-workers-and-branch-offices
3. https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf
4. Gartner, "Start Moving Data Management Capabilities Toward the Edge,"Ted Friedman, 2017.
5 "2018 Study on Global Megatrends in Cybersecurity," Ponemon Institute, 2018.
6. Ponemon 2019 Cost of a Data Breach Study

Beware the shape-shifting internet threat

Cybercriminals know that businesses are working overtime to secure endpoints and end users against threats, and they're working just as hard to beat them to the punch – and to find new gaps to exploit.

Today's IT professionals must guard not only against known threats like ransomware, but also unpleasant new relatives like Emotet, malicious cryptomining, and targeted attacks on specific industries like financial services, manufacturing, and education. The value of cryptocurrencies has fluctuated wildly, but the value is still high enough to garner a lot of attention, both legitimate and malicious.

Over the past year, the Cisco Umbrella Global Network has seen a seismic shift in the threat landscape with the explosive growth of malicious cryptomining. This threat is spreading across the internet like wildfire and is being delivered through multiple vectors, including email, web, and active exploitation. In fact, energy/utilities are targeted by cryptomining 15 times more often than other industries.

Hackers are constantly refining and recombining attack techniques to exploit vulnerabilities. It's one reason the manufacturing industry is targeted by malware 30x more than other sectors. These organizations are typically slower to update software on machines for fear of downtime, making them an easier target.

16%

Manufacturing[7]

14%

SLED[7]

8%

Financial Services[7]

8%

Professional Services[7]

4%

Energy/Utilities[7]

7. Cisco Umbrella Global Network

Networking and security must work together

The market consideration and 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 branch locations. But what about security? IT professionals are relying on traditional network defenses to guard against emergent threats that have been designed specifically to skirt them.

The network has changed

Consider the inherent vulnerabilities of today's corporate network, which now extends beyond the physical office to branch offices, data centers, and roaming devices. Second, it's more distributed. Corporate data is stored on third-party servers through cloud-delivered solutions like Google Apps or Salesforce and accessed from third-party networks over Wi-Fi access points and through wireless carriers. Much of this activity happens on BYOD laptops, tablets, and mobile devices that IT can't monitor. It also includes the growing array of connected devices that make up the Internet of Things. Traditional appliance-based network security measures simply weren't designed to defend a perimeter this large or variable.

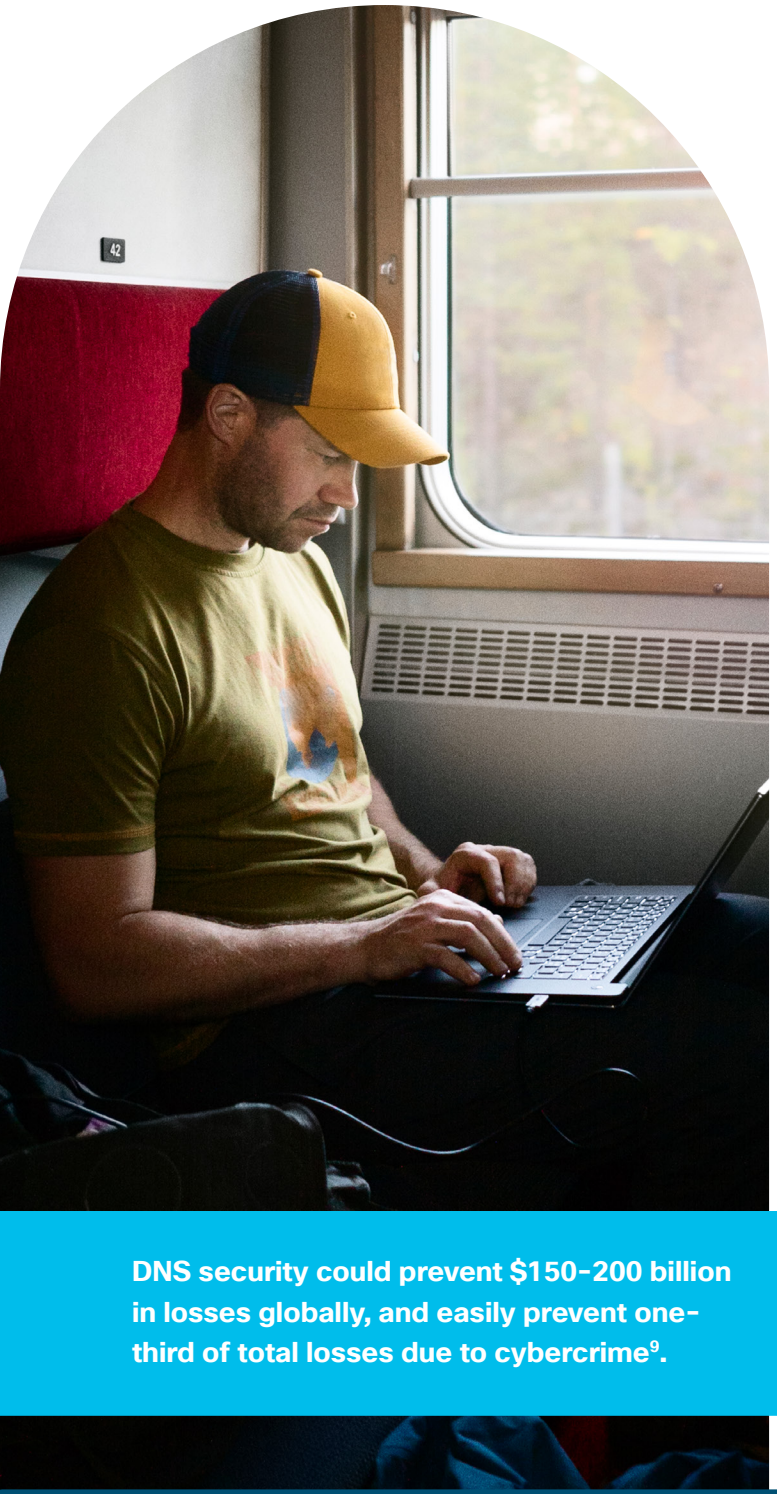
Leveraging a secret weapon: DNS

Since the existing security stack does a good job of protecting against known threats when users are on the corporate network, any additional protection within that stack must be able to extend protection off-premises to employees working anywhere. And it needs to be port- and protocol-agnostic so it can block any kind of threat.

Organizations must move beyond local, reactive intelligence to predictive intelligence based on Internet-wide visibility across all geographies, markets, and protocols. Why? Because hackers use the Internet to develop, stage, and refine their attacks – and in doing so, they leave behind traces like domain names and callbacks that can be analyzed.

By pointing DNS requests from all devices to a cloud-delivered security service, you can become part of a massive community that offers up a cross section of Internet activity for that service to analyze. This enables the service to detect patterns forming between domains and IPs, IPs and ASNs, domains and co-occurring domains, or domains.

8. Cisco Security Research Report



DNS security could prevent $150-200 billion in losses globally, and easily prevent one-third of total losses due to cybercrime[9].

Use the internet to your security advantage

If you're relying only on traditional security, you're vulnerable in a number of ways. When users leave the network, they're creating blind spots you need to defend, but can't.

With traditional security, intelligence is derived from static reputation scores issued after threats have been detected. Plus, if you're relying solely on hardware, appliance-processing power will limit what you can accomplish. If you're using a number of different security products from multiple vendors, you're left to reconcile, synthesize, and prioritize alerts from what are likely siloed systems.

SaaS apps, while effective for productivity, provide little visibility into user activity. This enables company, employee, or customer data to be exposed without your IT team knowing about it.

Monitoring DNS requests can be an easy way to reduce blind spots and provide better accuracy and detection of compromised systems, improving network protection.

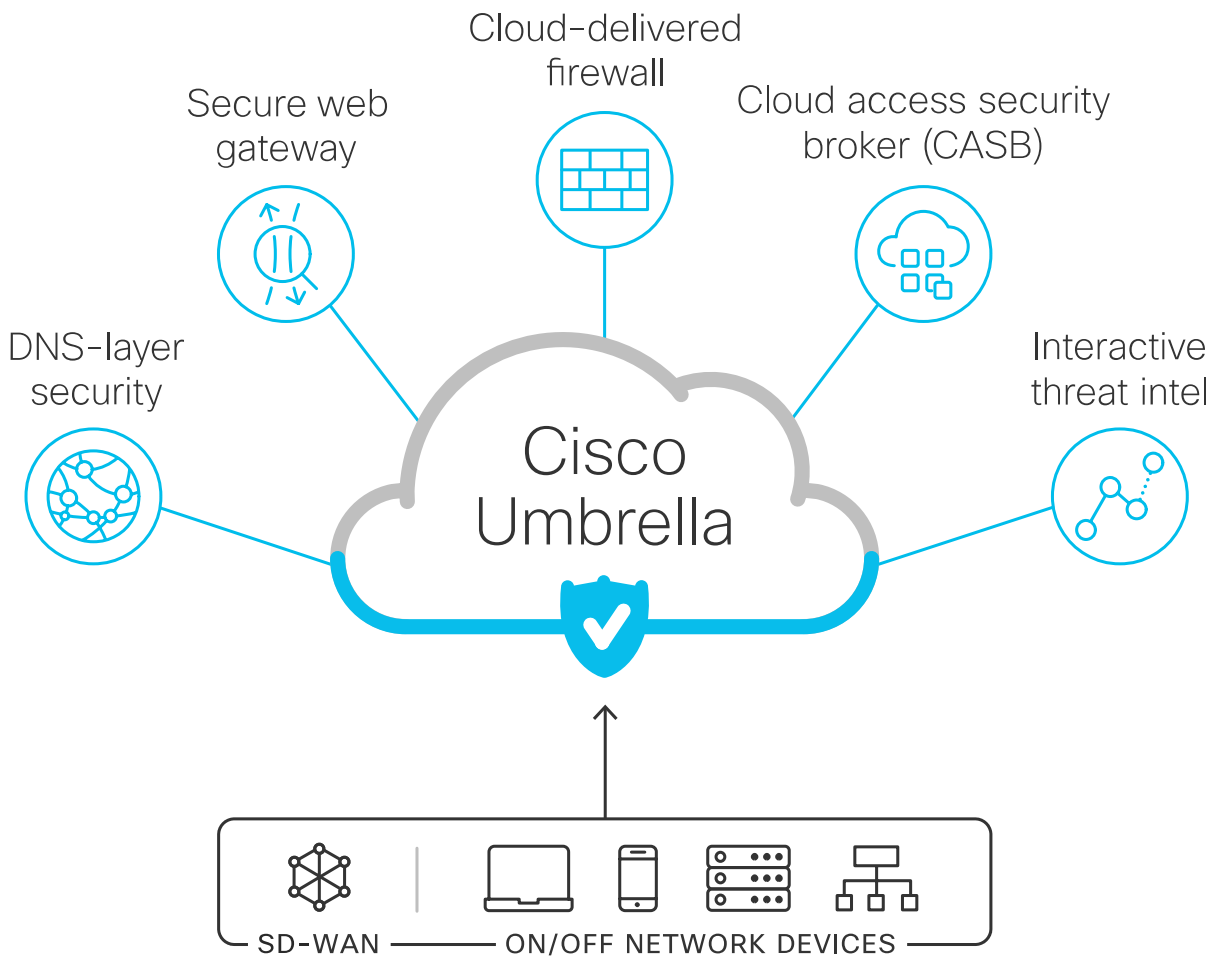
9. Global Cyber Alliance (CGA) https://www.globalcyberalliance.org/use-of-dns-firewalls-could-reduce-33-of-all-cybersecurity-breaches/

Your first line of defense

Cisco Umbrella is a cloud-native solution that protects users anywhere they work. Umbrella delivers the most effective defense against threats for decentralized networks. By integrating critical security functions into a single cloud-delivered platform, Umbrella helps to accelerate threat detection, improve performance, and centralize management across all locations and roaming users.

With Umbrella, you can simplify daily management, embrace DIA, and gain the following benefits:

- End gaps in visibility and control
- Unite multiple, disparate systems
- Gain consistent policy enforcement
- Support and scale limited security resources



Cisco Umbrella: unmatched threat intelligence

Leveraging insights from from Cisco Talos, one of the world's largest commercial threat intelligence teams with more than 300 researchers, 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.

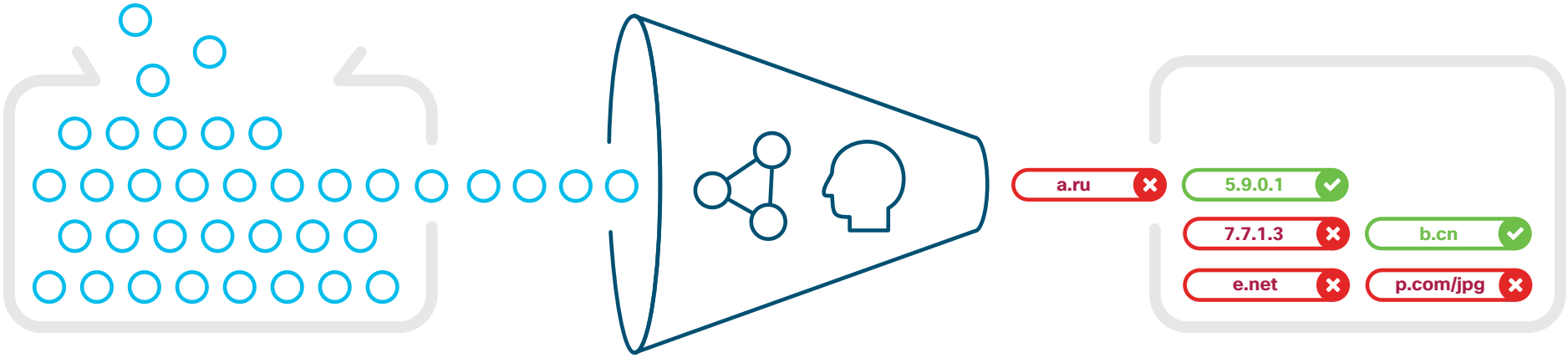
This gives you the power to stop advanced threats earlier and extend your network perimeter to protect employees and devices anywhere your users go.

By enforcing security at the DNS and IP layers, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established – before they reach your network or endpoints. The cloud-based full proxy logs and inspects all web traffic for greater transparency, control, and protection. The cloud-delivered firewall helps to log and block traffic using IP, port, and protocol rules for consistent enforcement throughout your environment.

Ingest
Millions of data points per second using DNS, BGP, WHOIS, and more

Apply
Statistical models and human intelligence

Identify
Infrastructure staged for known and emergent threats



About Cisco Umbrella

Cisco Umbrella is a cloud-native platform that delivers the fastest, most reliable, and most secure internet experience to more than 100 million users daily. Unlike disparate point products, Umbrella unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single platform to help businesses of all sizes secure their networks. Umbrella makes it easy to extend protection to roaming users and branch offices.

With Cisco Umbrella, you can stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration. And because it's delivered from the cloud, Cisco Umbrella provides effective security that is open, automated, and simple to use.

Start a Cisco Umbrella free trial

Umbrella is simple to deploy and easy to manage. Give Umbrella a try and you can start blocking in minutes.

Start a Free Trial

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

cisco

Cisco Umbrella