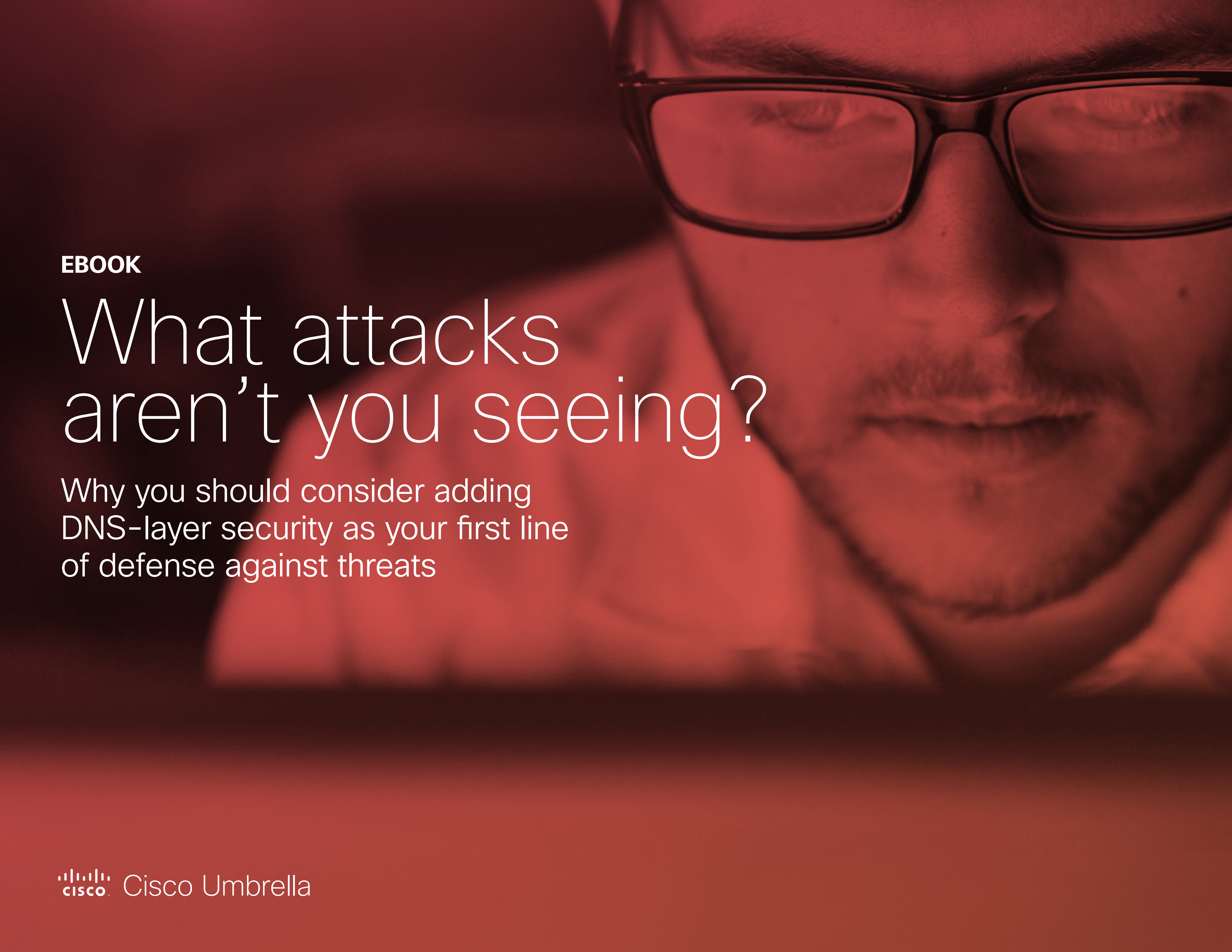


EBOOK

What attacks aren't you seeing?

Why you should consider adding DNS-layer security as your first line of defense against threats

Cisco Umbrella

In this ebook

Introduction 03

Factors contributing to breaches 04

Beware the shape-shifting internet threat 05

Why firewalls are not enough 06

The network has changed 06

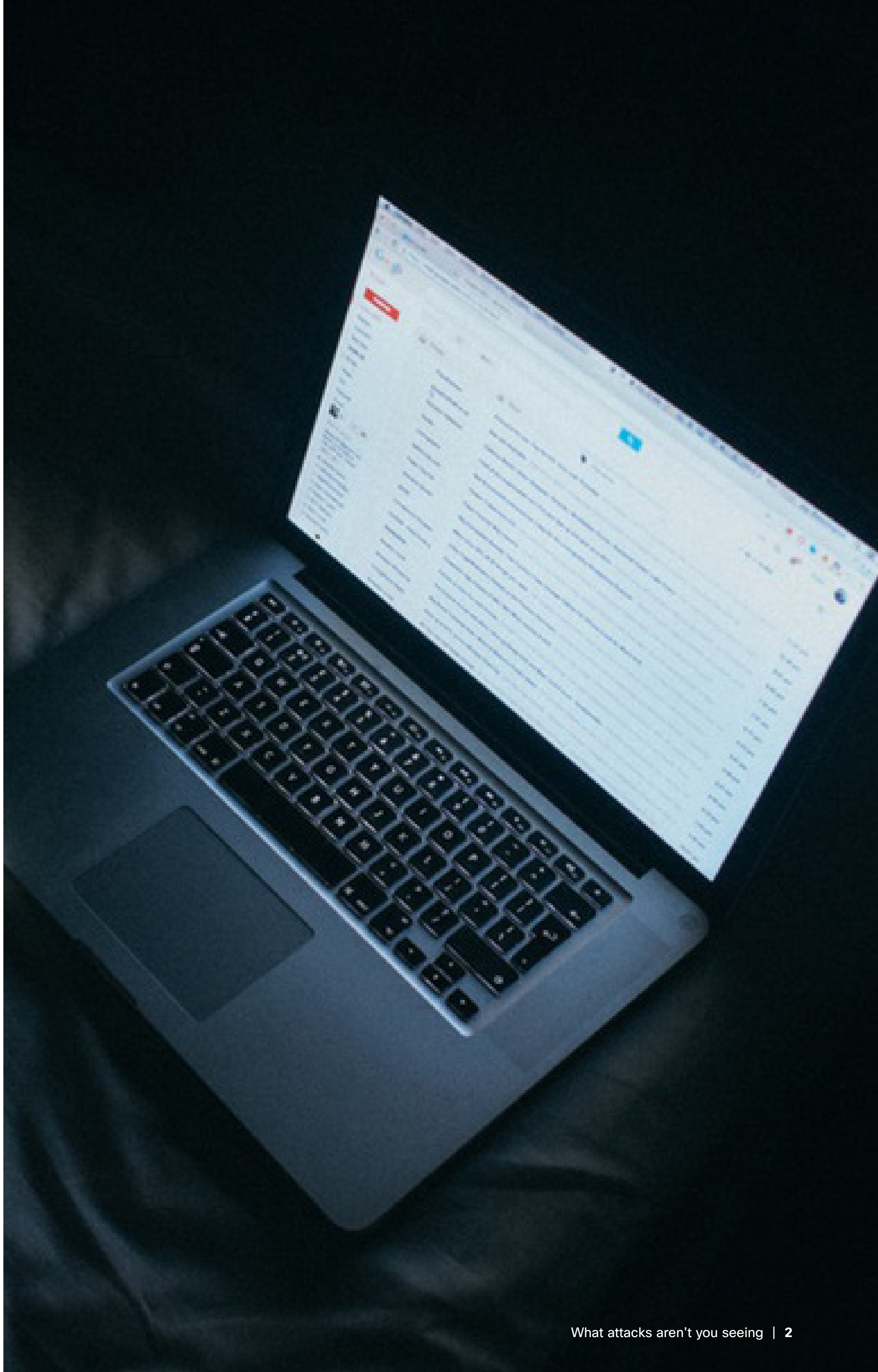
Traditional security is reactive 07

Employees want security to be invisible 08

Leveraging a secret weapon: DNS 08

Your first line of defense 09

Cisco Umbrella: Security beyond the firewall 10



Introduction

People work anywhere and everywhere now, from co-working spaces and coffee shops to airport lobbies, using innovative devices, apps, and cloud services to reimagine and redefine their workdays.

It's great for productivity and efficiency – but it's stretching network security to the breaking point, creating hidden gaps and vulnerabilities as employees move farther away from the traditional "office." With most security solutions still focused on protecting employees only while they're on the corporate network, organizations are increasingly at risk for cyberattacks.

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 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. Gartner anticipates worldwide enterprise security spending to total $96 billion in 2018, with organizations spending more on security as a result of regulations, shifting buyer mindset and the evolution to a digital business strategy.[1]

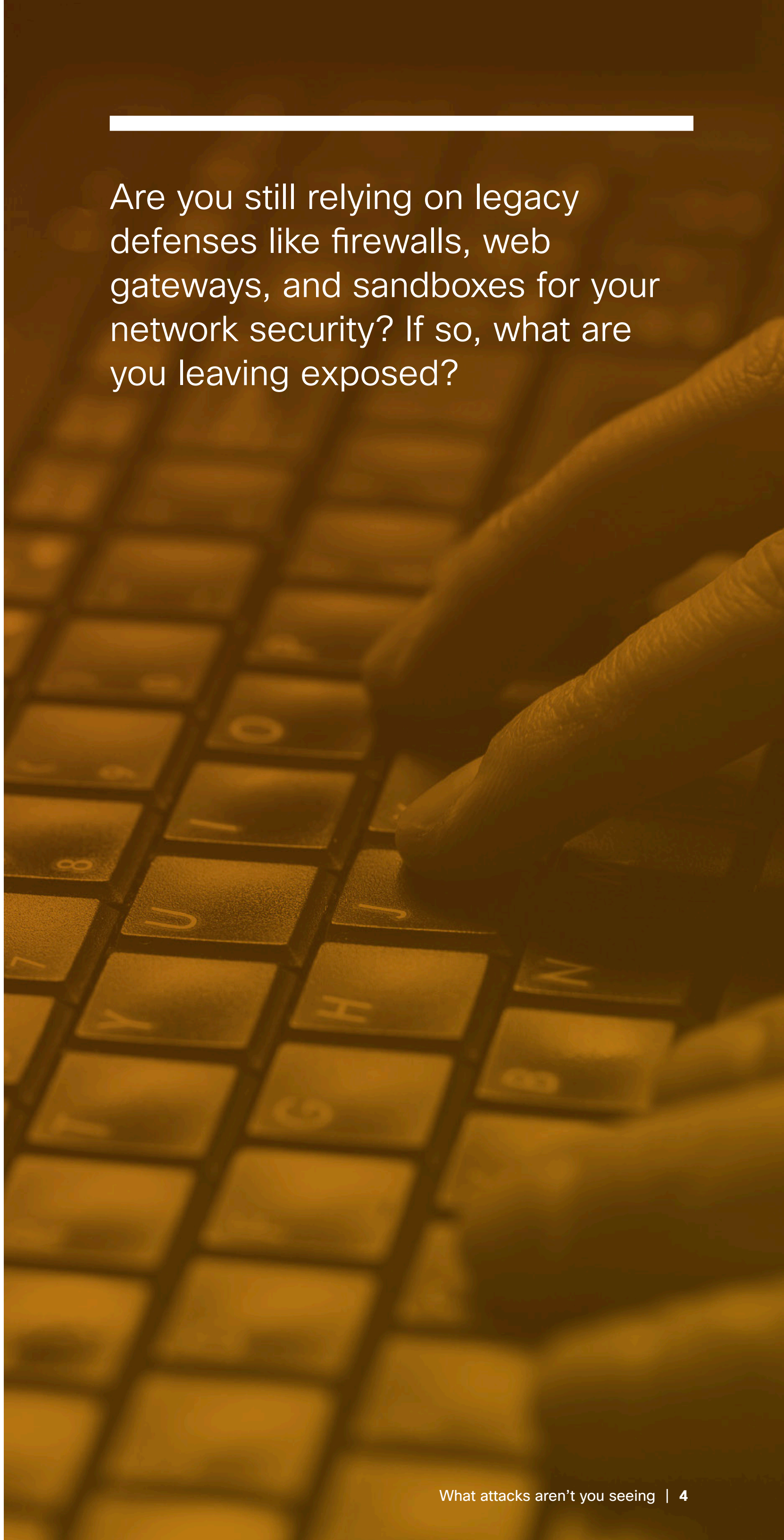
Factors contributing to breaches

What's your organization doing to block the threat of a breach? Are you still relying on legacy defenses like firewalls, web gateways, and sandboxes for network security? If so, what are you leaving exposed? According to the Cisco 2018 Security Capabilities Benchmark Study, there was a sharp increase in security breaches affecting more than 50% of systems last year.[2] Consequently, both 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 they face and the tools they're using to create security that can follow workers wherever they go.

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.[3]

83% of senior information technology practitioners surveyed predict unsecured IOT devices will likely cause a data breach in their organization.[4]

80% of breaches originate inside the business and not through the perimeter.[5]



Are you still relying on legacy defenses like firewalls, web gateways, and sandboxes for your network security? If so, what are you leaving exposed?

Beware the shape-shifting internet threat

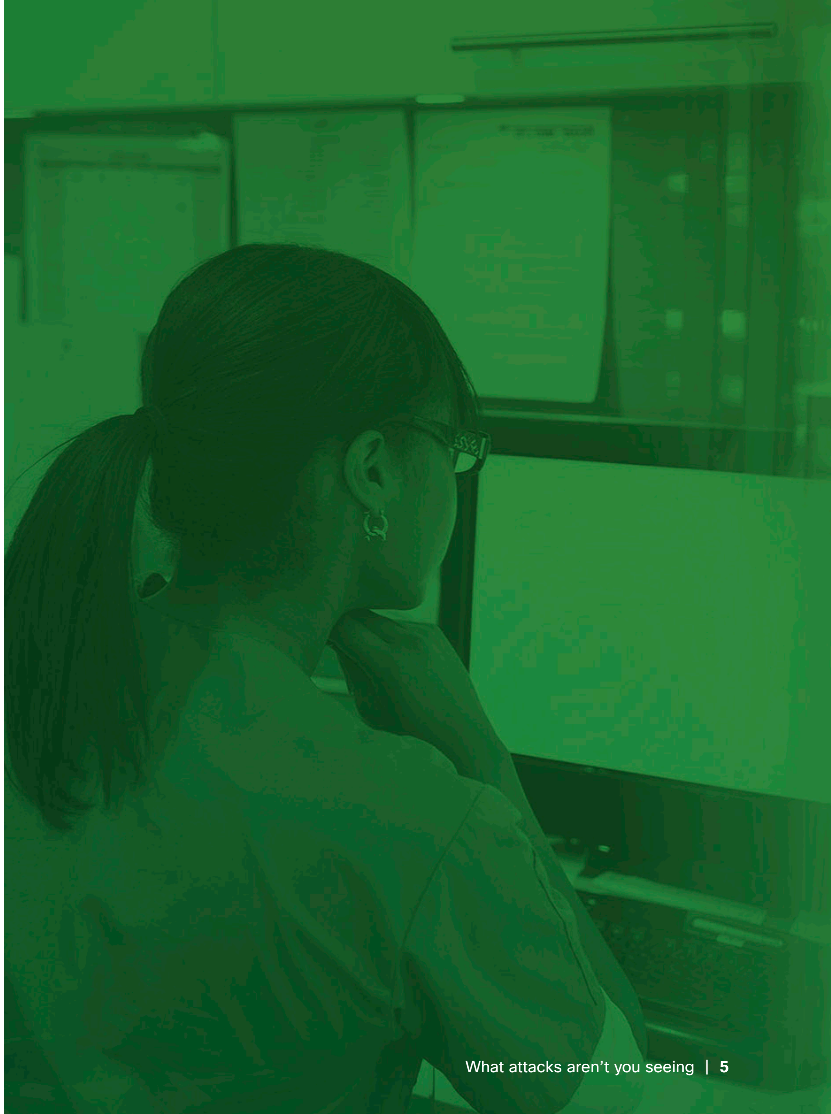
Cybercriminals know that businesses are working overtime to secure endpoints and end users against threats, and they’re working just as hard to beat them to the punch–and to find new gaps to exploit.

Today’s IT professionals must guard not only against known threats like malware, but also unpleasant new relatives like ghostware, ransomware, and targeted attacks on specific industries like banking and healthcare. Phishing has evolved into spear phishing, which uses malicious emails that appear to come from someone the user knows and trusts. 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, Cisco has seen a seismic shift in the threat landscape with the explosive growth of malicious cryptocurrency mining. This threat is spreading across the internet like wildfire and is being delivered through multiple vectors, including email, web, and active exploitation.

Hackers are constantly refining and recombining attack techniques to breach corporate and government networks. The result is technological evolution at its most malevolent.

The fact of the matter is that organizations won’t be able to come to grips with cybercriminals unless they adopt a more forward-looking approach.

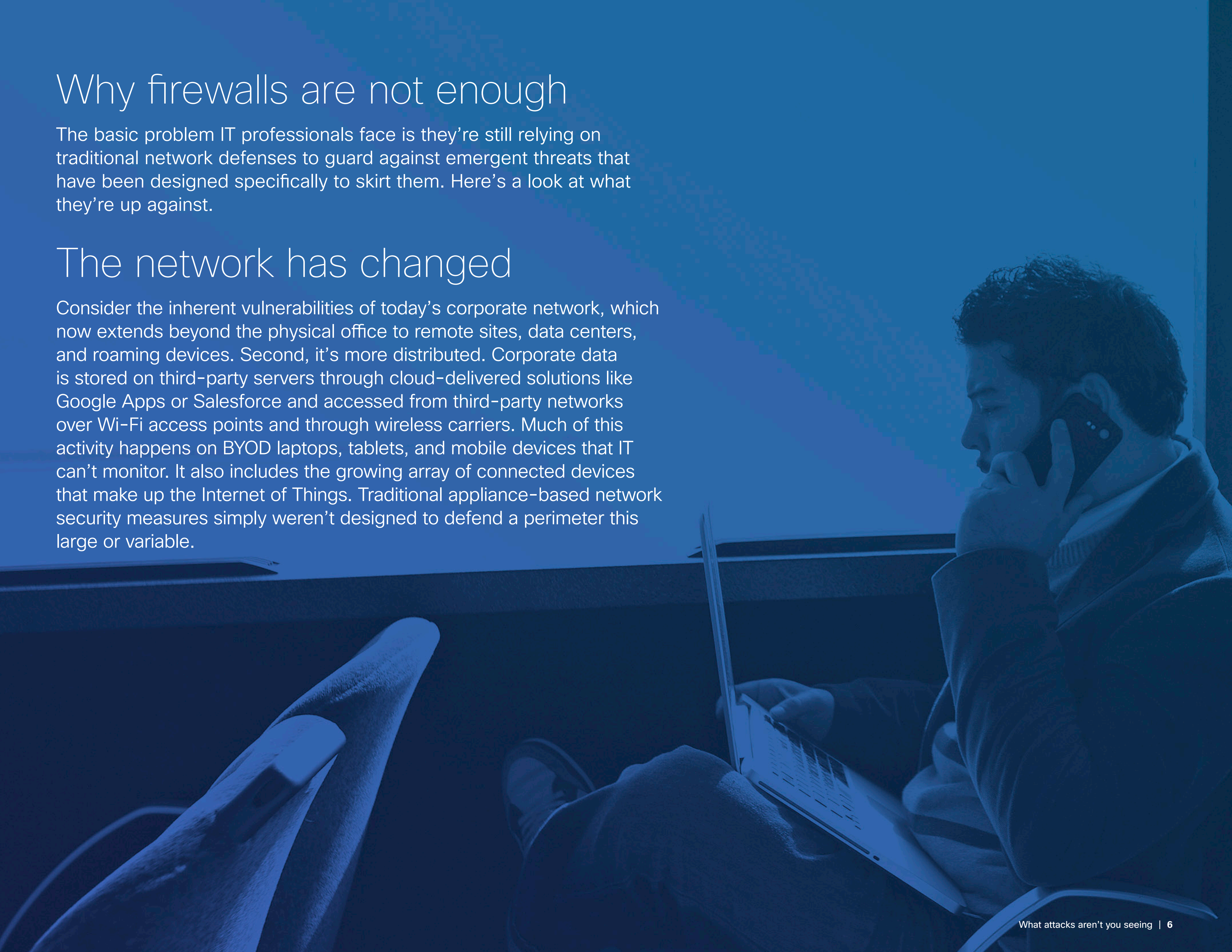


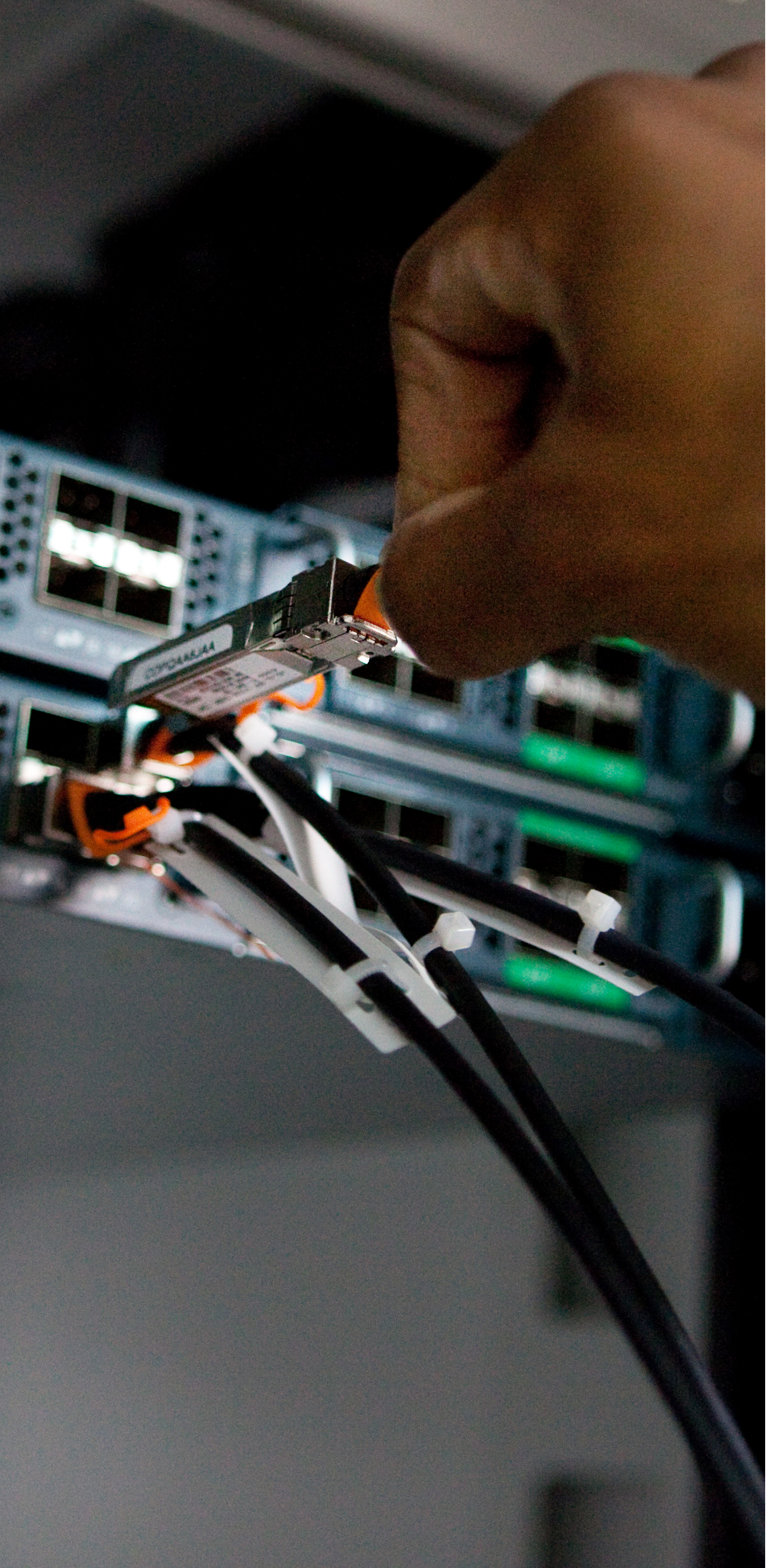
Why firewalls are not enough

The basic problem IT professionals face is they’re still relying on traditional network defenses to guard against emergent threats that have been designed specifically to skirt them. Here’s a look at what they’re up against.

The network has changed

Consider the inherent vulnerabilities of today’s corporate network, which now extends beyond the physical office to remote sites, 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.





Traditional security is reactive

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.

Then, there’s the problem of staying ahead. 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.

Traditional solutions limit integration, too. So 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.

And finally, the SaaS apps that are so effective from a productivity standpoint provide little visibility into user activity, so sensitive company, employee, or customer data can be uploaded to, and shared in, the cloud without your IT team knowing about it.

With more than 90% of attacks found at the DNS layer, this should be every company’s first layer of support.[6]

Employees want security to be invisible

Finally, IT professionals are under pressure to manage security in ways that don't also sacrifice performance and productivity. While it might be possible to secure Internet traffic by backhauling every connection through proxy or VPN gateways, doing so is intensely complicated and can add significant latency to the system. Also, creating an extra hoop for employees to jump through might prompt busy workers to sidestep security protocols and open themselves to attack.

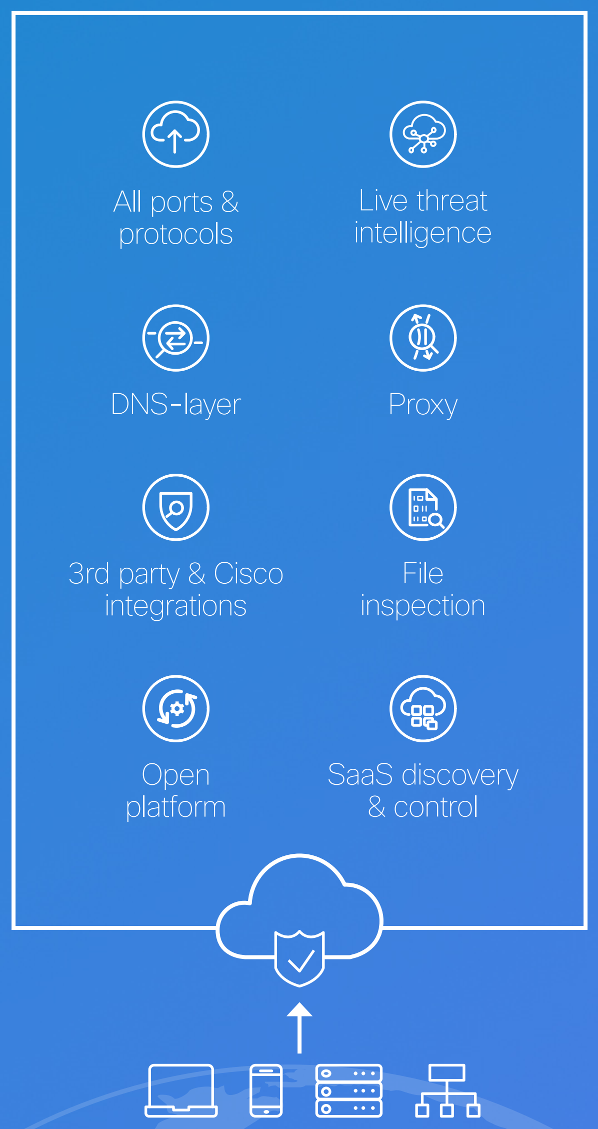
Leveraging a secret weapon: DNS

Given these challenges, what's the solution? Since the existing security stack does a good job of protecting the network against known threats, any additional protection within that stack must be able to extend protection off-premises to employees working anywhere. It needs to integrate with all the other layers. And it needs to be port–and protocol–agnostic so it can block any kind of threat.

This takes care of known types of attacks. But what about new ones that you can't see coming? To handle these, 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.

If security analytics capabilities seem out of reach, what if you learned you already had a secret weapon that could help you take advantage of predictive intelligence? You do: the domain name system (DNS), sometimes called the Internet's phonebook. 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 and related domains. It does so via WHOIS records or malicious files.

Cisco's secure internet gateway



All ports & protocols

Live threat intelligence

DNS-layer

Proxy

3rd party & Cisco integrations

File inspection

Open platform

SaaS discovery & control

On and off-network coverage

Your first line of defense

Cisco Umbrella is your first line of defense against threats. Anytime and anywhere your users access the Internet, traffic goes through Umbrella first. Umbrella blocks connections to sites hosting malware or phishing campaigns, and blocks threats before they reach endpoints. If infected devices join your network, Umbrella contains command-and-control callbacks to stop data exfiltration. Umbrella provides:

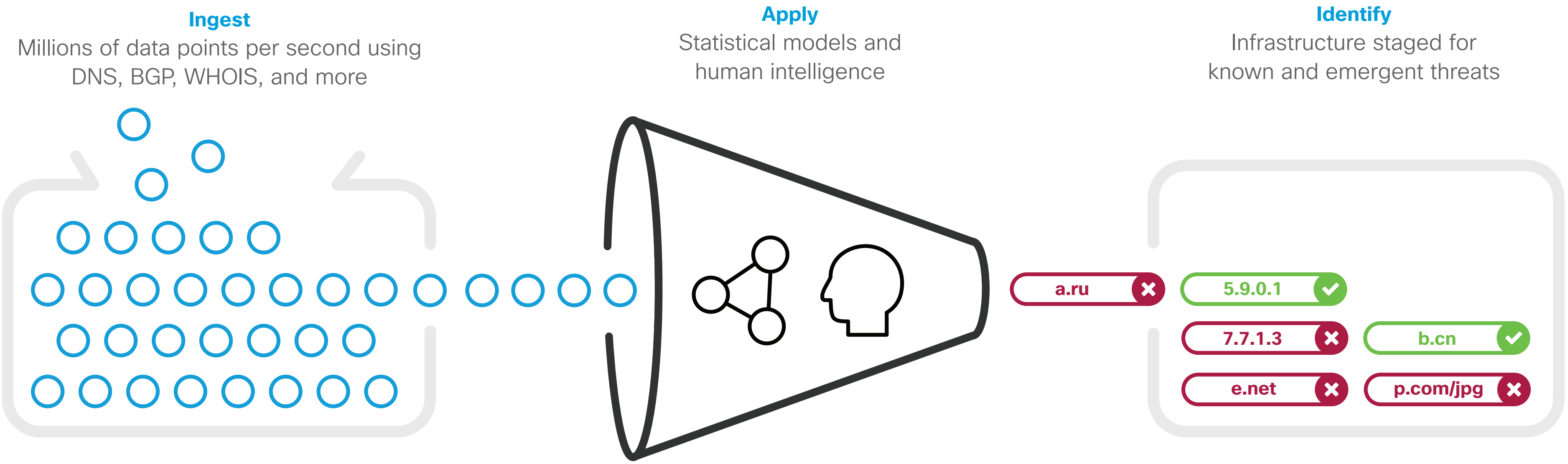
- Malware and breach protection for users, on- and off-network
- Visibility and protection to see all network devices, locations and roaming users, and risky or inappropriate applications
- Intelligence to predict and stop attacks before they launch
- Discovery and control of sensitive data across sanctioned and unsanctioned SaaS apps
- An open platform for easily extending threat protection beyond the perimeter to secure remote, branch, and mobile users

Cisco Umbrella: security beyond the firewall

Cisco Umbrella, a secure Internet gateway, complements your existing security measures by providing insight into the connections and relationships between networks on the internet—and enforces this insight at the DNS layer.

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

Even though the news about cybercrime often seems full of unpleasant surprises, the good guys can share predictive threat intelligence via the cloud to turn hackers' own activities against them. Security implemented at the DNS layer provides the power to uncover and block connections to malicious domains and IPs inside and outside the network perimeter, providing security that moves with employees. And the data gathered in the process can be used to outpace emerging threats across the globe. This means IT teams and employees get to focus on their real work: making their business a success. It's true: Hackers are constantly both refining and recombining attack techniques to breach corporate and governmental networks. Fortunately, Umbrella can help.


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
a.ru ✗
5.9.0.1 ✓
7.7.1.3 ✗
b.cn ✓
e.net ✗
p.com/jpg ✗

About Cisco Umbrella

Since 2006, Cisco Umbrella has delivered 100% reliability. The secret is Anycast routing, which always connects you to the fastest data center at any moment. Umbrella is the only solution that blankets security and boosts performance. We've established 3,900 peering sessions and partner with more than 700 top internet service providers (ISPs) and content delivery networks (CDNs) to shorten the routes between every network in the world and our data centers, making your internet access even faster.

Umbrella protects any device over any port or protocol to prevent command-and-control callbacks, malware and phishing from exfiltrating data, and compromising systems. By enforcing security in the cloud, Umbrella is easy to manage, with no hardware to install or software to maintain, and zero added latency. Cisco Umbrella offers the most complete view of internet domains, IP addresses, and autonomous systems to pinpoint attackers' infrastructures and predict future threats before they can cause damage. More than 90 million active users across 160+ countries point their DNS traffic to Umbrella, giving us visibility into 150 billion daily requests. The resulting data set gives us a view of the internet like no other.

By analyzing and learning from internet activity patterns, Cisco Umbrella automatically uncovers attacker infrastructure staged for current and emerging threats, and proactively blocks requests to malicious destinations before a connection is even established.

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.

Cisco Umbrella

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 FREE TRIAL

References

1 "Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017," December 7, 2017.

2 "Cisco 2018 Annual Cybersecurity Report," 2018.

3 Gartner, "Start Moving Data Management Capabilities Toward the Edge," Ted Friedman, 2017.

4 "2018 Study on Global Megatrends in Cybersecurity," Ponemon Institute, 2018.

5 "Evolve the Network into a Security Sensor and Enforcer to Improve Business Security," ZK Research, April 2016.

6 "Securing Direct-to-Internet Branch Offices: Cloud-Based Security Offers Flexibility And Control," Forrester (commissioned by OpenDNS), July 2015.