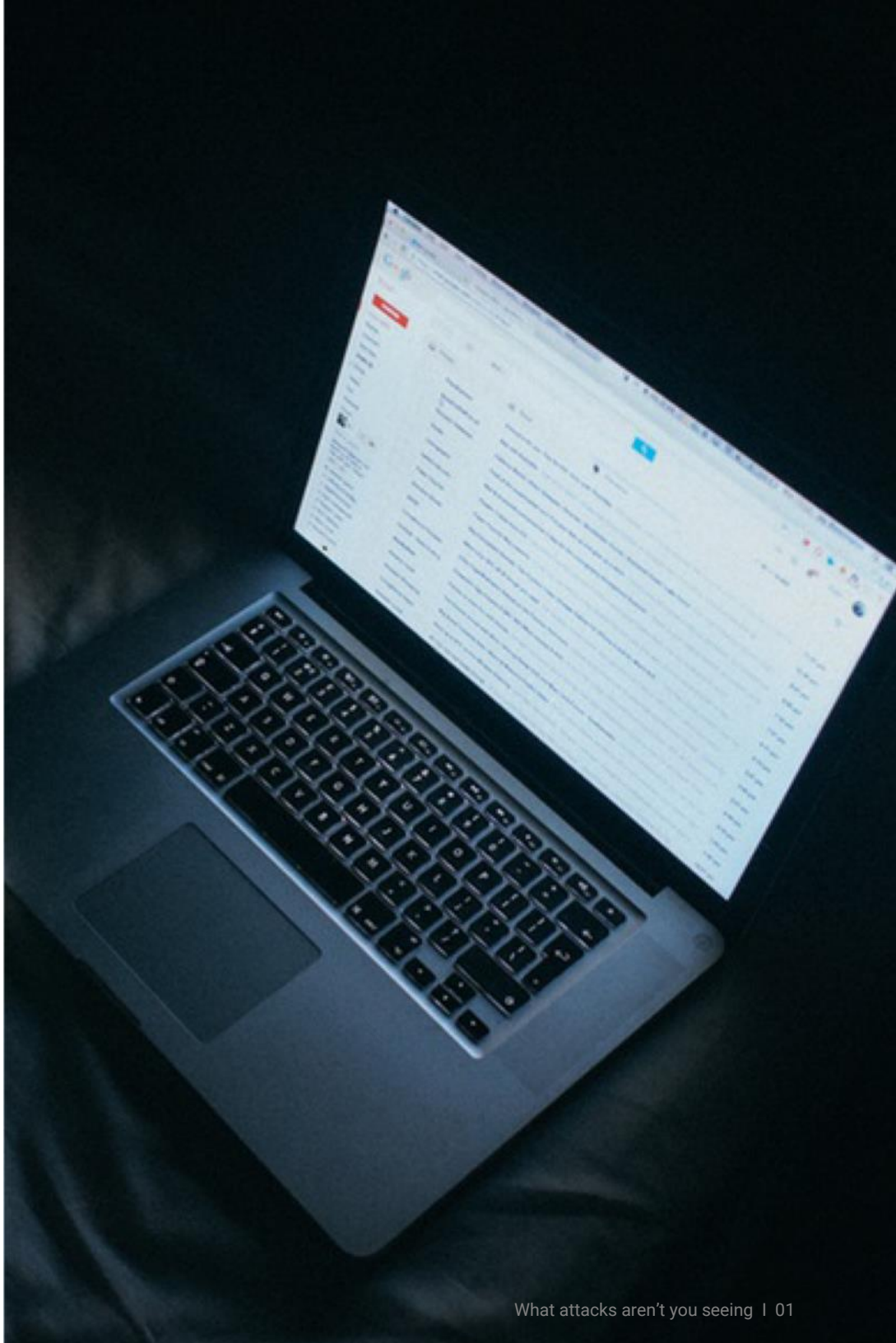
EBOOK

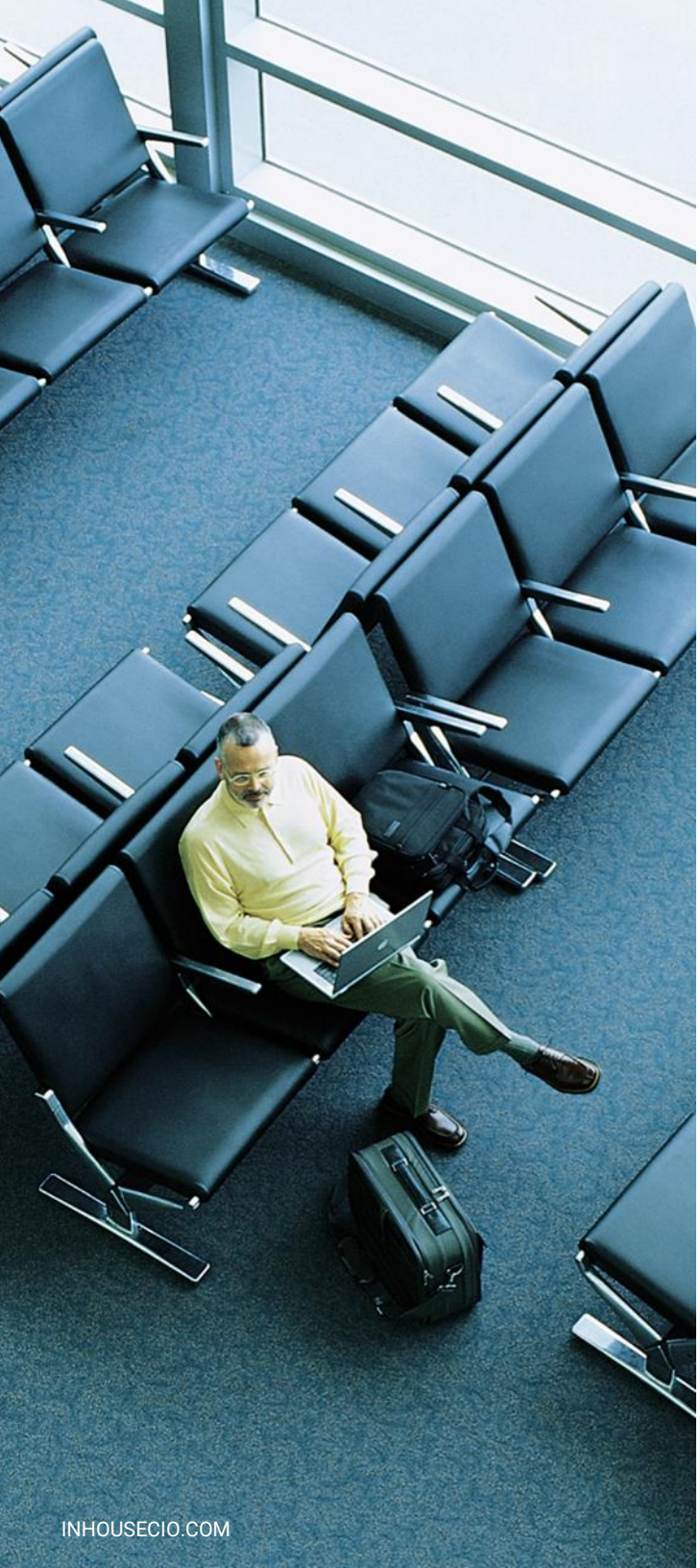
What attacks aren't you seeing?

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

InhouseCIO

In this Ebook





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 re-imagine and redefine their workdays.

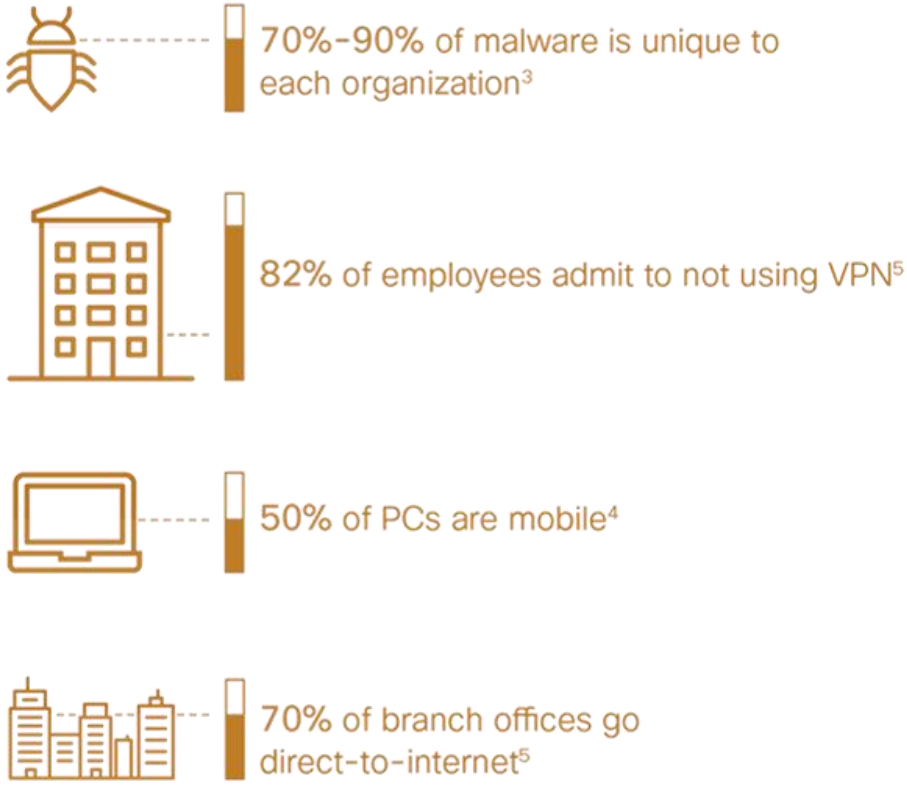
It's a great for productivity and efficiency—but its stretching network security to the breaking point, creating hidden gaps and vulnerabilities as employees move further away from the traditional "office." With most security solutions still focused on protecting employees only while they're on the corporate 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 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. So get ready, because end-of-year security reviews and surveys say attacks increased by 38% in 2015, and experts predict they'll continue to grow—in frequency, in number, and in sheer brute force. [1,2]

Factors contributing to breaches

There's a lot on the line

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? See why 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.



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 against unpleasant new relatives like ghostware, ransomware and targeted attacks on specific industries like banking. Phishing has evolved into spear phishing, which uses malicious emails that appear to come from someone the user knows and trusts. Older threats like the Heartbleed vulnerability are being worked into new attack schemes. Sheer volume and velocity are the weapons of choice in brute-force attacks that make multiple, repeated attempts to decrypt data or steal PINs, as well as indoors attacks that flood servers with incoming traffic in order to overwhelm them. [1,2]

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

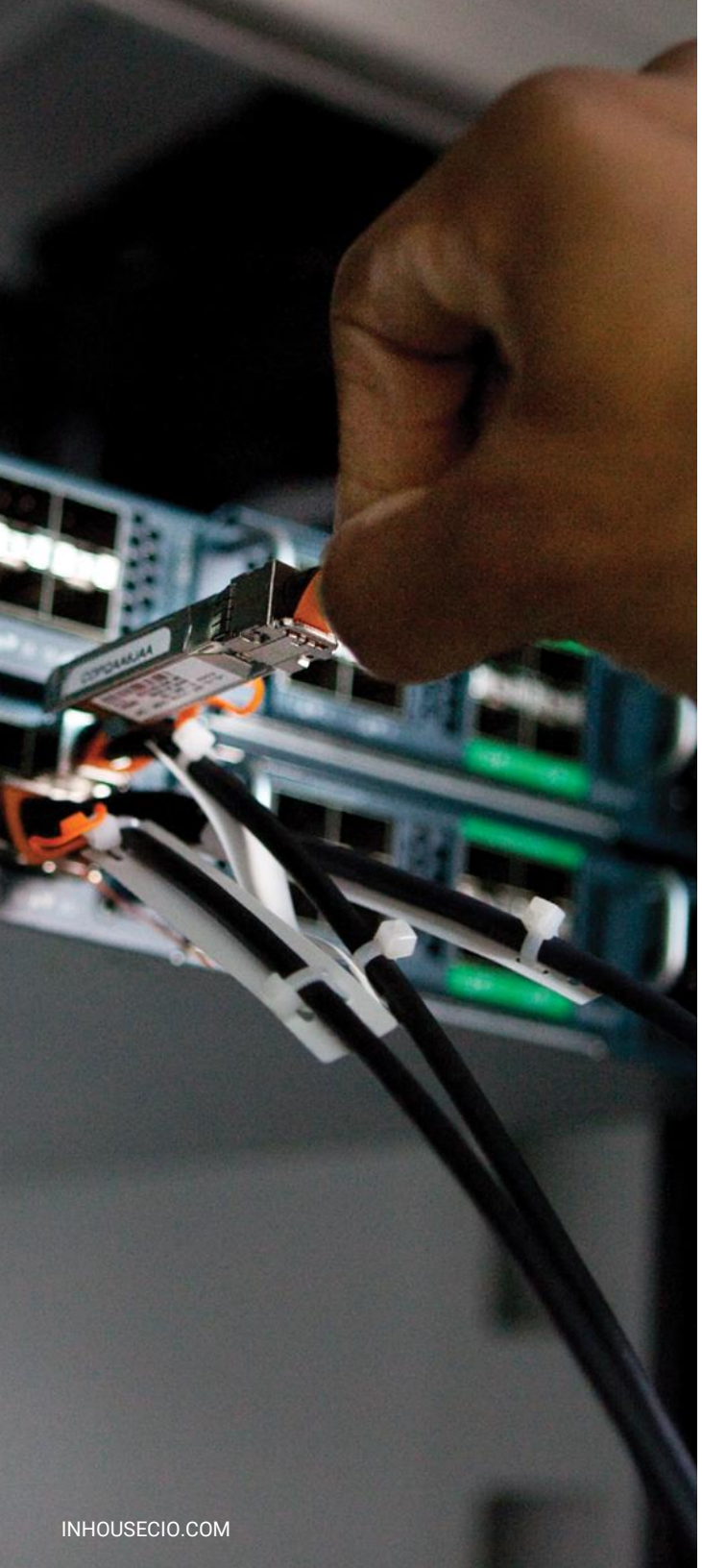
The fact of the matter is that organizations won't be able to come to grips with cybercriminals unless they adopt a more forward-looking approach.

Why firewalls are not enough

The basic problem IT professionals face is they're still relying on traditional network defences 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

The traditional security approach hasn't changed much, and in some ways, that's not a bad thing. Every piece of malware ever created is still out there, and signature-based solutions such as antivirus are still important in preventing most known threats from infecting your systems. More than 90% of attacks are found at the DNS layer – this should be every company's first layer of support.[6]

The problem is that traditional approaches can't extend protection to mobile users or handle exponential increases in internet traffic—or deal with the velocity and volume of new attack tools and techniques. These approaches are also inherently reactive: they can only protect against malware, phishing, and other attacks after they're detected. Similarly, no matter how quickly vendors react to a new threat, it still takes a little time to design patches and security updates, and even this brief delay leaves networks vulnerable.

IT needs to keep security simple

IT needs security to be as seamless and automated as possible. Consider that each time IT deploys a new security appliance, they may also be adding the need to log into a separate console to manage reports and update policies. This is not ideal.

Employees want security to be visible

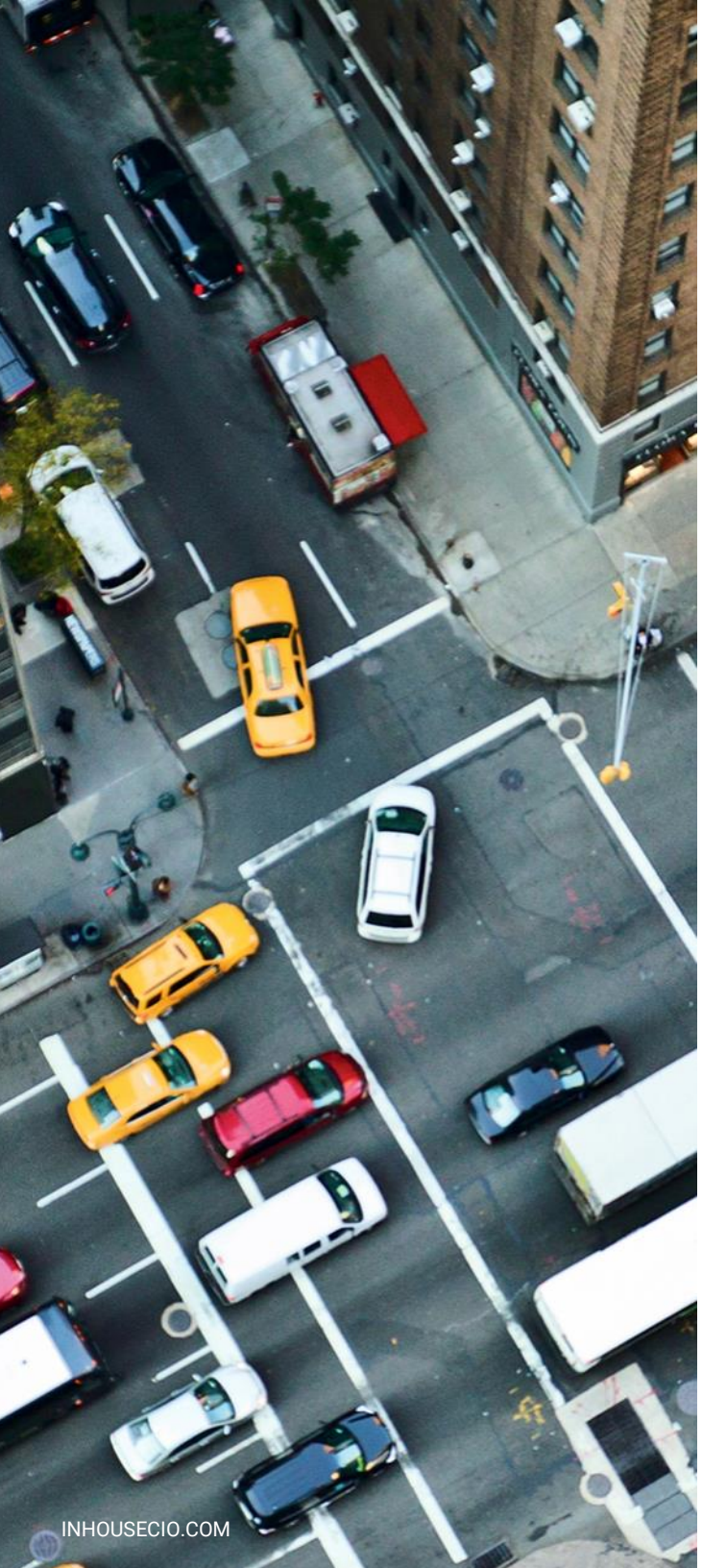
Finally, IT professionals are under pressure to manage security in ways that don't also sacrifice performance and productivity. While it might be possible to secure internet traffic by backhauling every connection through proxy or VPN gateways, doing so is intensely complicated and can add significant 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 user 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 Umbrella—use cases

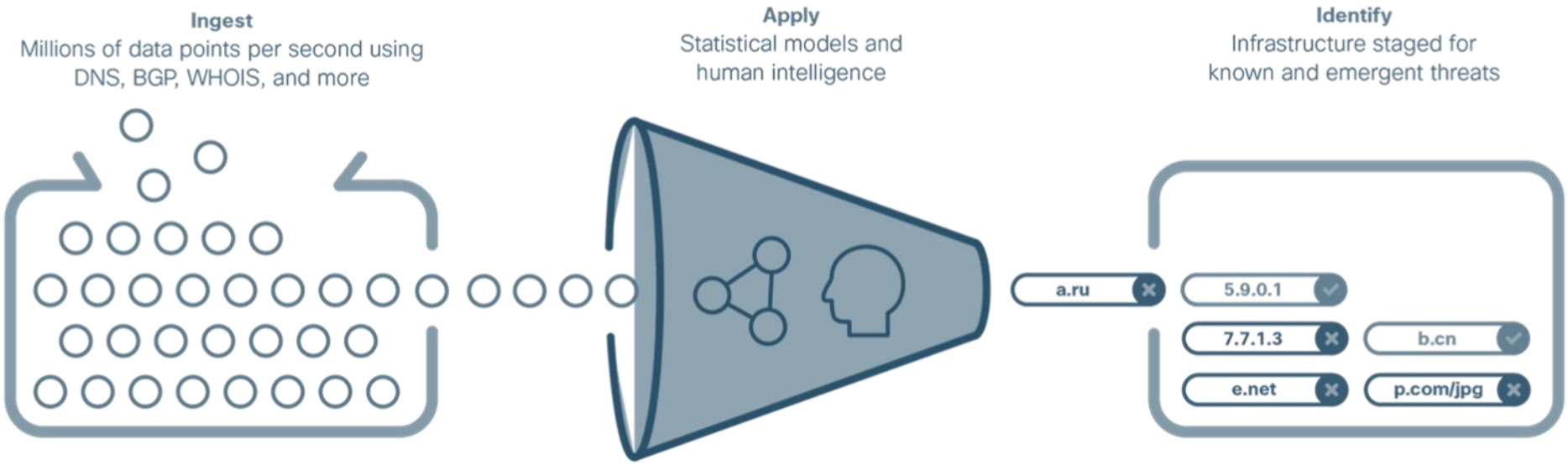
- Prevent web & non-web C2 callbacks from compromised systems
- Prevent malware drive-bys or phishing attempts from malicious or fraudulent websites
- Enforce and comply with acceptable use policies using 60 content categories and your own lists
- Pinpoint compromised systems using real-time security activity
- Speed up investigations
- Prioritize investigations and response
- Stay ahead of attacks
- Enrich security systems with real-time data

InhouseCIO uses Cisco Umbrella: Security beyond the firewall

The Umbrella cloud security compliments 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 refining and recombining attack techniques to breach corporate and governmental networks. Fortunately, InhouseCIO with Umbrella can help.



About Cisco Umbrella

Cisco Umbrella is a cloud security platform that 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 65 million active users across 160+ countries point their DNS traffic to Umbrella, giving them visibility into 80 billion daily requests, as well as Border Gateway Protocol (BGP) route information exchanged with more than 500 partners. 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 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 and effective security platform that is open, automated, and simple to use.

Let InhouseCIO help you make Cisco Umbrella work for you.

EMAIL US

SALES@INHOUSECIO.COM

CALL US

(773) 239-8378

VISIT US

INHOUSECIO.COM

References

1 "The biggest security threats we'll face in 2016" Wired, January 2016.

2 "The Global State of Information Security Survey 2016" PWC, 2015-2016

3 "2015 Data Breach Investigations Report" Verizon 2015

4 "forecast: PCs, Ultramobiles and Mobile Phones, Worldwide, 2011-2018, 4Q14 Update" Gartner, December 2014

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

6 "Cisco 2015 Annual Security Report" Cisco, 2016

Cover image Designed by katemangostar / Freepik
Page 4,8 images Designed by Pressfoto / Freepik