

Ebook

Small businesses deserve big protection

A guide to solving your unique security challenges



SECURE
Partner



**INTERNETWORK
ENGINEERING**



In this ebook:

Small businesses deserve big protection >

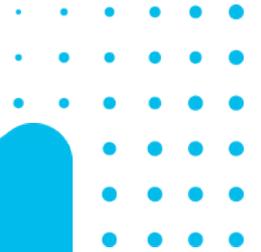
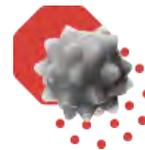
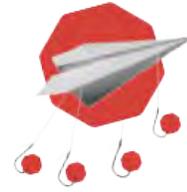
Security challenges for the small business >

Better protection starts with DNS >

Introducing Cisco Umbrella >

Why Cisco Umbrella is ideal for small businesses >

The next step to stronger security >



Small businesses deserve big protection

There are more than 30 million small businesses in the United States alone,¹ and each is a potential target for internet-based threats, attacks, and malicious actors.

You may think that, because of your size, your business can fly under the radar, but small businesses can be an even bigger target, as cybercriminals often see them as low-hanging fruit with a lower level of protection.

% of DNS queries related to threats²



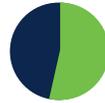
32.60%

Small businesses
(<1,000 employees)



13.64%

Mid-sized businesses
(1,000–9,999 employees)



54.09%

Large businesses
(>10,000 employees)

Today's small businesses face the same security challenges as larger organizations – along with their own unique concerns. They require protection just as effective as that of the enterprise, but which can also work within the confines of their limited budget and resources.

In this ebook, we'll take a closer look at the current state of small-business security, along with an introduction to the solutions that can help protect your organization.

66%

of small businesses have experienced a cyberattack.³

63%

have experienced a data breach.³

Security challenges for the small business

As technology continues to evolve, small businesses have the opportunity to pursue their goals in new and exciting ways. These changes shape the priorities of the small business, but also the challenges they're facing – particularly in these unprecedented and often uncertain times.

Business issues	IT priorities	IT challenges
Increasing profitability	Cloud	Cloud security
Increasing business growth	Mobility	Maintaining current IT infrastructure
Reducing operational costs	Collaboration	Budget constraints
Attracting and retaining new customers	Security	Managing data growth
Improving workforce productivity	Managed services	Mobile device security

You may be experiencing periods of rapid growth that require changes to your network – new locations or an expanded perimeter. Or you may need to deliver new and innovative services to better connect with customers. Regardless, you need to be able to adapt and evolve to ensure your business can operate the way both employees and customers need it to – with a strong mix of performance and security.

75%

of small businesses agree there should be more emphasis placed on security within their organization.⁴



What specific challenges are small businesses facing?

1. The rise of SaaS apps

Employees everywhere increasingly take advantage of cloud-based SaaS applications to work smarter, faster, and better. However, the majority of these apps are unsanctioned by the company's IT department. Unmonitored, this "shadow IT" often has security holes that can leave your business open to threats and cybercriminals.



54%

of small businesses report that the majority of their apps will be SaaS by 2021.⁵

41%

of cybersecurity experts worry about data breaches in SaaS apps.⁵

2. An increase in roaming, remote, and branch workers

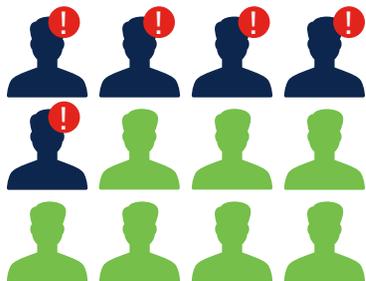
IT teams at small businesses are beginning to work with an ever-expanding network perimeter. Employees now work on the go, outside the office, and in various branch and remote locations, all of which still need to be secured from threats – no easy task using a traditional centralized security stack.

By 2021, 37% of small-business employees are expected to be roaming.⁵

i.e., working from a home office or on the road at least one day per week, using both corporate and personal devices, on and off the VPN.

79% of remote and branch officers are making the shift to direct internet access.⁵

i.e., connecting directly to the web instead of backhauling through the main office, to reduce latency and improve performance.

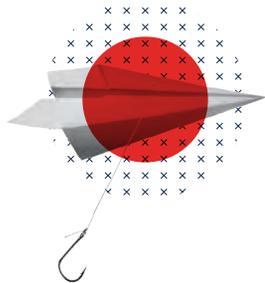


48%

of small businesses report that roaming, remote, and branch users have been compromised by targeted attacks.⁵

3. Increasingly outdated infrastructure

The threat landscape has vastly grown and evolved like never before, with more threats and more threat vectors increasing the strain on small-business security. These threats now include everything from phishing to ransomware to malicious cryptomining, each of which needs to be addressed with robust, up-to-date protection.



Phishing attacks
have doubled over
the past year.⁶

To try and keep up with these various threats, organizations often supplement dated security platforms with an ungainly stack of point solutions, which can be costly and difficult to deploy, manage, and maintain.

81%

of businesses find it challenging to manage security products from multiple vendors.⁷

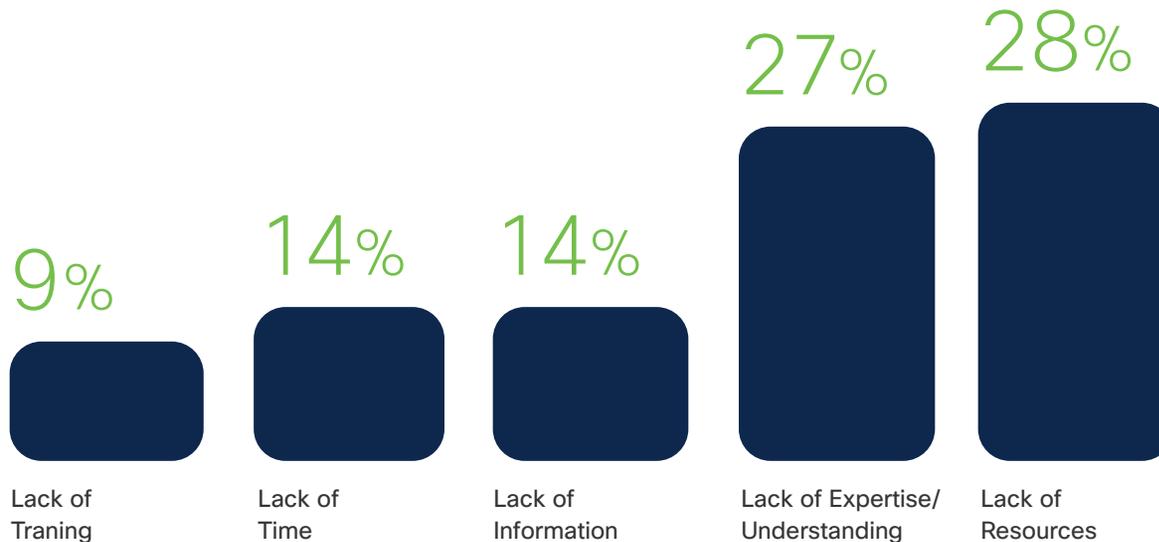
79%

say it's challenging to orchestrate alerts from multiple products.⁷

4. Limited budget and resources

Small businesses have the same security needs as larger enterprises, but often fewer means to deliver that security. It's difficult to make room in tight budgets for new security products – and for the well-staffed security team you need to monitor and remediate threats. Instead, all too often, security tasks fall to non-IT team members without the time or skills to keep up.

Common Challenges for Small-Business IT Teams⁸



In short, small businesses are facing the sort of challenges that require a wholly new type of security solution – one that's effective against enterprise-level threats, but also simple to use. This is where DNS-layer security can help.

81%

of small businesses don't have a dedicated IT person.⁹

46%

of organizations find it difficult to find and recruit qualified security personnel.⁵

Better protection starts with DNS

Most threats first attempt to infiltrate at the domain level. This makes the DNS layer, one of the foundations of the Internet, a real target – but also a real opportunity. Protect at the DNS level, and you can protect against the vast majority of attacks.

Blocking unwanted domains, IP addresses, and cloud applications over any port or protocol, DNS-layer security helps prevent threats at the earliest point of contact, while providing a single view of all internet activity across every location, device, and user.



90%

of malware uses DNS in attacks.⁶



68%

of orgs don't monitor their DNS.⁶

“DNS traffic is a critical dataset to analyze. Yet, most businesses do not have visibility into the billions of DNS lookups and resolutions that occur daily on a global basis.”

– Christina Richmond, Principal Analyst, Managed DNS Security Services

Introducing Cisco Umbrella

Cisco Umbrella is a cloud-delivered security service designed to protect businesses of all sizes from threats of all sizes. Delivering robust protection that starts at the DNS layer, Cisco Umbrella provides the first line of defense against web-based threats, helping small businesses see and block threats before a connection is ever established.

You have enough to do running the other parts of your small business. Cisco Umbrella takes the burden of security off your back, providing powerful, perimeter-wide protection that's easy to deploy and manage.

Cisco Umbrella unifies a variety of other security services for protection that goes even deeper than DNS. This includes a secure web gateway, cloud-delivered firewall, and CASB functionality.



Why is Cisco Umbrella the ideal security solution for your small business?

Simple to deploy and scale

Because Cisco Umbrella is built into the cloud, there's no hardware to install or software to maintain. Get up and running in minutes, with protection that grows with your business.

Full visibility into SaaS app usage

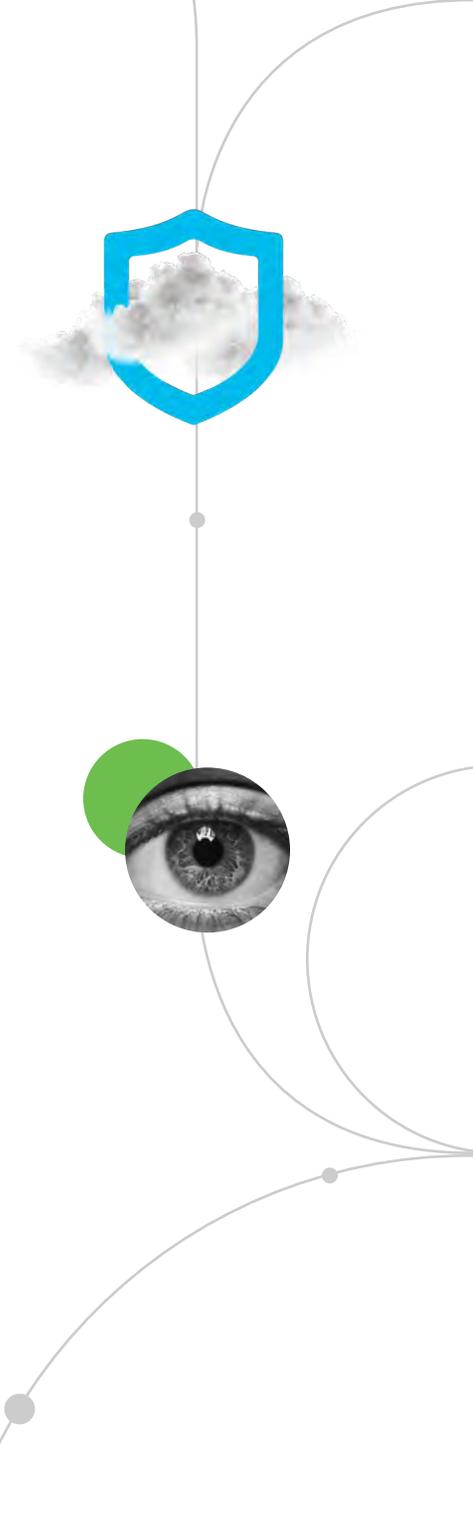
See which apps are being used and what risk they pose to your organization. Approve, deny, and block these apps, so users are secure – even outside your perimeter.

Effective against threats everywhere

Because Cisco Umbrella works from the DNS layer, you can see and protect all your users, on all their devices, in every location – without impacting performance.

Cost-effective

A single unified security service reduces the complexity of monitoring and managing threats and alerts, so your team can do more with less. Plus, fewer infections overall mean less remediation time, less downtime, and less of the costs associated with each.



Cisco Umbrella delivers 2x the protection of competitors

Not all DNS-layer protection is created equal. According to a recent security efficacy test by AV-TEST, Cisco Umbrella is #1 in threat detection.¹⁰



72.6%



Cisco Umbrella (DNS-layer with selective proxy)

35.3%



Infoblox BloxOne

26.5%



Akamai Enterprise Threat Protector

13.7%



Palo Alto Networks Next-Generation Firewall

Cisco Umbrella, powered by Talos Threat Intelligence

One of the largest and most trusted security research organizations, Talos continually scans the globe for new attacks, dangerous URLs, malware, and spoofs. Delivering rapid, actionable intelligence that's shared across every Cisco product, Talos ensures Cisco Umbrella instantly has access to the latest info, so it can identify and block threats faster and better.

The next step to stronger security



SECURE
Partner



Small businesses face the same security challenges as their larger brethren, along with a variety of obstacles all their own. You deserve a solution that provides powerful overall protection, while reducing overall cost and complexity.

Cisco Umbrella addresses the unique IT challenges and priorities of the small business, providing robust DNS-layer security that can protect all the data, users, devices, and locations across your organization.

Try Cisco Umbrella for yourself or get in touch with a Cisco managed service provider for IT services that include Umbrella – we're here to help.

Get started with some free trials

220B+
daily DNS requests
(over all ports and protocols)

30+
data centers across
five continents

100M+
global daily active consumer
and enterprise users

1000+
partnerships with
top ISPs and CDNs

Sources:

1. U.S. Small Business Administration, 2019 Small Business Profile.
2. Cisco Umbrella, *Know Your Enemy: Protecting Against the Top Threats of 2020*, March 2020.
3. Ponemon Institute, *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses*.
4. Vanson Bourne, *Underserved and Unprepared: The State of SMB Cyber Security in 2019*.
5. Enterprise Strategy Group, *Market Dynamics Impacting Remote and Roaming User Security Requirements*, 2019.
6. Cisco Umbrella Threat Research
7. Cisco CISO Benchmark Cybersecurity Series, February 2020.
8. Verizon Data Breach Investigation Report
9. T-Mobile, *No IT Person? No Prob. Meet T-Mobile for Business Help Desk: Small Biz Support for All Things IT*, November 2018.
10. AV-TEST, *DNS-Layer Protection & Secure Web Gateway Security Efficacy Test*, February 2020.