Cisco Umbrella

CITYNET

Cisco Premier Partner

Big threats to small business

How you can start securing your organization in a matter of minutes

With threats on the rise, how can you protect your valuable assets?

The increasing shift to remote and roaming work has left businesses of all sizes more vulnerable to threats and attacks, with employees working off-network, from the cloud, and with technology and apps that aren't necessarily sanctioned (or protected) by the home office.

Unfortunately, just because you're a small business doesn't mean you won't be a target for attackers. In fact, small businesses can often be seen as particularly vulnerable because they lack the security resources of larger businesses.

And these attacks do real damage – small businesses spend an average of $955,000 per attack to restore normal operations; 60% of victims actually go out of business within 6 months of an attack.[1]

As time goes on, threats are becoming more numerous and complex, with orchestrated, multi-staged, evasive attacks becoming the norm.[2] In this new normal, it's not enough to throw more bodies and more effort at the problem. To keep up with growing threats, it may be time to upgrade your security technology to something stronger.

With so much to defend and so much to defend against, where should you start? Let's find out.

54%

of small businesses think they're too small for a cyberattack, but...

43%

of all attacks target small businesses.

47%

of small businesses say they have no understanding of how to protect themselves against cyberattacks.[1]

cisco Cisco Umbrella

CITYNET

cisco Premier Partner

DNS: the perfect place to protect

The domain name system (DNS) is one of the foundational components of the Internet – the first point at which a connection is made, and often the first place where threats attempt to infiltrate.

But that's actually a golden opportunity: protect at the DNS level, and you're protecting at the frontline – the earliest point of contact – to stop threats before they can gain access to your network.

"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

Not only is DNS-layer security powerful; it's also the easiest and fastest way to protect your small business, with the ability to deliver visibility and security – across every location, user, and device – in a matter of minutes.

91%

of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic.[3]

The power of DNS-layer security with Cisco Umbrella

Cisco Umbrella is a multi-function, cloud-native service made up of a variety of unified security solutions. At its heart, though, is DNS-layer security, which can provide a number of unique benefits to your small business.

In addition to DNS-layer security, Cisco Umbrella offers a secure web gateway (SWG), cloud access security broker (CASB), and firewall-as-a-service (FWaaS) for even more robust protection.

CITYNET

Premier Partner

Rapid deployment

The modern business is a complex entity, with team members working from a variety of devices and locations, both on and off the corporate network. Introducing traditional centralized on-premises security would be slow and cumbersome – and, in the case of off-network protection – all but impossible to deliver.

One major benefit of DNS-layer security is that it's a quick and easy win for your small business. Because Cisco Umbrella is cloud-native, there's no hardware to install or software to maintain. With Cisco Umbrella, you can get powerful protection up and running in minutes, for immediate time to value.

"It took less than 10 minutes for us to point our DNS traffic to the Cisco Umbrella Global Network. We could protect our remote offices around the world in less than an hour and a half."

Director of Information Security, Small Business Computer Software Company

Protection anywhere and everywhere

Today, threats are more complex and plentiful than ever, but by enforcing security at the DNS and IP layers, Cisco Umbrella stops them all – malware, ransomware, phishing, and botnets – before a connection is ever established, blocking threats over any port or protocol before they reach your network or endpoints.

And, because Cisco Umbrella works from the DNS layer, you can see and protect all your users, on all their devices, no matter where they're working – including roaming laptops, Android, and iOS devices – without impacting performance.

"Umbrella has reduced infections and malware to near zero, saving hours of staff time and lost productivity."

IT Director, Small Business Medical Company

Wi-Fi protection with Cisco Umbrella

With so many teams working remotely and roaming, you want to ensure users have fast and secure Wi-Fi access. However, relying solely on traditional solutions like proxies can slow or stall internet performance. And complications with root certificates and non-browser web apps can prevent users from viewing SSL-encrypted sites; to get around this, many organizations allow traffic to bypass the proxy, which can lead to gaps in visibility and protection.

Because Cisco Umbrella works from the DNS layer, the software adds zero latency, for zero impact on performance. And because DNS requests precede IP connections, there are no issues with root certificates and non-web apps. When a Wi-Fi user tries to access a malicious site (or a site that violates your content filtering policies), Cisco Umbrella sends them to a customizable block page instead.

CITYNET®

Cisco Premier Partner

Visibility into internet activity and cloud applications

It's not just protection with Cisco Umbrella – Umbrella also provides a single view of all internet activity across every location, device, and user. Cisco Umbrella then categorizes and retains this key information to help speed investigation and incident response times. Access reports and quickly view trends across your deployment, then use that insight to get a complete picture of risks – and take action when necessary.

This visibility also extends to the SaaS applications employees use across your business. Small business teams love cloud-based applications for their go-anywhere flexibility, but staying on top of unsanctioned (and often vulnerable) apps can be a real challenge for IT. With Cisco Umbrella, you can see exactly which apps are being used, understand the risk they pose to your organization, and then approve, deny, or block those apps.

You can detect and remediate threats even faster by automating integrations across Cisco security products and third-party threat feeds.

"With Umbrella, we have gained increased visibility into our DNS traffic, which provides greater actionable information for handling security incidents."

Administrator, Small Business Transportation Services Company

Reliability and performance

Downtime and performance issues are small business owners' worst nightmare, with far-reaching and expensive implications including loss of business and loss of customer loyalty.

Cisco Umbrella delivers a fast, secure, and reliable internet experience to more than 100 million users, with a unique infrastructure that improves performance, reduces latency, and keeps small businesses up and running. As a truly cloud-native service, we deliver high capacity and throughput, solid reliability, and agile infrastructure. Cisco Umbrella has a highly resilient global cloud architecture. Since 2006, Cisco's DNS security service has maintained 100% business uptime. And in a recent performance test, Cisco Umbrella demonstrated a 73% reduction in latency compared to an ISP.[4]

40%

of small businesses experienced eight or more hours of downtime due to a cyber breach, accounting for an average of $1.56 million in losses.[1]

"By allowing us to concentrate on doing business without interruptions from incidents, Umbrella has made us more effective in providing our customers the products and services they need."

Engineer, Small Business Insurance Company

Cisco Umbrella

CITYNET

Premier Partner

Big protection on a small business budget

One major challenge for the small business is making the most of what you have. Small businesses face just as many threats as larger organizations, but they often have fewer resources – in terms of time, budget, and staff.

Cisco Umbrella can fill in the gaps for your small business cybersecurity team. A single unified security service reduces the complexity of monitoring and managing threats and alerts, so your team can do more with less. Plus, Umbrella provides the extra support you need to make the most of your solution. Fewer infections overall mean less remediation time, less downtime, and fewer of the costs associated with each.

"What I like most about Cisco Umbrella is the ease of use. I also appreciate their support."

Senior IT Architect, Small Business Health Company

For small businesses, threats are never going to stop coming. But with simple deployment and powerful protection, visibility, and performance, Cisco Umbrella can provide the big win you need.

75%

of small businesses say they don't have the personnel to address IT security.

83%

of small businesses haven't put cash aside for dealing with a cyberattack.[1]

Ready to see how Cisco Umbrella can help your small business improve security?

Watch a live demo of Cisco Umbrella in action.

View demo

Sources:

1. Maddie Shepherd, **30 Surprising Small Business Cyber Security Statistics**, Fundera, 2021.
2. **The Modern Cybersecurity Landscape: Scaling for Threats in Motion**, Cisco, November 2020.
3. Owen Lystrup, **Cisco Security Report: Majority of Orgs Do Not Monitor DNS**, Cisco, August 2020.
4. Miercom Independent Testing Labs, miercom.com