Use Case: Cisco Umbrella

Five deployment scenarios that will benefit from a new first line of defence

For further details visit ccsmedia.com

The difficulty many organisations face is the number of locations and devices they're now expected to protect. The corporate network no longer represents a conventional perimeter as the workplace transcends company premises, and thanks to mobile computing extends to practically any location wherein an Internet connection can be obtained. Consequently, a rising volume of roaming users and a lack of visibility over their activity means that an ever-increasing and complex attack surface is being created. Unfortunately, the centralised control you were once used to and the perimeter security measures you typically rely on no longer stand up to the new threats these trends represent. And cybercriminals are smart – they know this and use your new vulnerabilities to their advantage.

For that reason, it's not enough to simply respond to security issues as they arise. Instead, a far more proactive approach to managing threats is helping organisations of all sizes to achieve powerful and effective protection on and off-network.

What is it?

Cisco Umbrella is the first line of defence for the corporate network. Aptly named, it provides a virtual 'umbrella' of protection against threats on the Internet by recognising patterns and identifying suspicious behaviour to uncover and block attacker infrastructure before it can even make its move. Umbrella is the world's first Secure Internet Gateway (SIG) in the cloud; a global solution depended on by over 12,000 enterprises and 65 million daily active users worldwide. Delivering security at the Domain Name Server (DNS) and Internet Protocol (IP) layers, Umbrella sits at the very edge of the network and processes billions of requests each day to predict and prevent attacks earlier. By learning from Internet activity patterns, Umbrella automatically uncovers current and emerging threats to offer better protection. Thanks to its cloud-based origin, it is far more effective, economical, and scalable than traditional DNS security, in addition to being simple to deploy and control. Importantly, it requires no specialist security skills to run, and offers instant protection from the moment of activation, ensuring that no time is unnecessarily wasted on upkeep or fears over inadequate protection.

Why use it?

1. Replace legacy DNS

It's easy to overlook and underestimate the vulnerabilities tied into your Domain Name Servers (DNS). They are responsible for the translation of the domain names we use to search for websites into IP addresses that the computer can read. Due to the sheer amount of information they exchange and retain every day while processing countless translations, this makes them an attractive target for cybercriminals who inject them with malicious code to redirect traffic and intercept data.
Cisco Umbrella replaces your on-site DNS. As an entirely cloud-based solution, not only does that mean high availability and more resilient security, it also removes the need for any further hardware when replacing the DNS – it is software through and through, which could result in huge cost savings for your business and a predictable recurring cost for managing this dimension of your security. This doesn't mean you're exchanging the challenges of hardware for a never-ending routine of manual updates either; once Umbrella is installed, this is all done automatically, safeguarding the time and resources of your IT team. Importantly, Umbrella is also designed to be compatible with any existing security infrastructure, so seamlessly integrates with your environment, regardless of the protection you already have in place. And with no added latency, employees will not know notice any change in performance.

2. Made for the mobile workforce

The flexibility made possible by remote and mobile working is not a 'nice-to-have' but an expectation from a new generation of workers shaping tomorrow's workforce. They want the freedom of staying productive on-the-go, anywhere at any time, using the tools and technology that they're most familiar with. What this requires, however, is the assurance that no matter where they're working, the critical data they have access to always remains secure.
Likewise, it's not uncommon for employees to also seek out unauthorised third-party cloud-based applications to help them do their jobs better. 'Shadow IT' can present significant security risks, particularly when apps are used outside of the corporate network and there is risk of corporate data being exchanged with them.
Used hand in hand with Cisco Meraki, Cisco Umbrella protects everything, everywhere. It can be applied to all company devices, protecting them whether they're on or off the corporate VPN. Its single, unified interface was purpose-built for proactive threat management, allowing any detected malware to be recognised and blocked instantly across all networks, on any device, whether the user is at company HQ or the local coffee shop. Critically, any data passed through Umbrella is automatically encrypted too, so in the unlikely event that it is intercepted it's useless to a hacker. Finally, permissions for cloud-based apps are also easily applied by administrators, who control access to their domain names, essentially black listing undesirable services. All of this is achieved while users enjoy the freedom to work securely wherever they want, using whichever devices they prefer.

3. Branch Internet Services

Integrating branch offices into traditional MPLS circuits is costly and complex. However, the rise in ultra-fast broadband offers both compelling bandwidth and commercials to connect new premises to corporate networks over the public Internet. While it's an exciting opportunity, this presents new security risks, not least because of the exposure of corporate data outside of conventional networks. Using Cisco Umbrella these locations, the users working at them, and all of their devices can instantly be protected. It's incredibly easy to deploy, and can literally be implemented in minutes, so there aren't any delays in waiting for software to be installed and absolutely no hardware to worry about either. It is a ready-to-go, out-of-the-box configuration that is already compatible with the other security measures you're using.

4. Your GDPR strategy

The General Data Protection Regulation (GDPR) is a hot topic for many businesses at the moment, and all efforts are being put into becoming, and remaining, data compliant. Umbrella protects your data everywhere, its proactive approach massively reducing the likelihood of a data breach. In fact, over 50% of Umbrella customers have reported a 100% reduction in malware attacks since integrating the service into their environment. And because it's entirely in the cloud, you gain the added benefit of Cisco's global threat intelligence from the word 'go' and the flexibility to extend coverage as your business grows.

5. Overcoming the security skills gap

Many IT teams lack the specialist skills to properly deploy and operate sophisticated security measures as they are so complex. Unlike these solutions, Cisco Umbrella was designed

For further details visit ccsmedia.com
Let's talk Call 01246 200 200

CCS Media Ltd, Old Birdholme House, Derby Road, Chesterfield, Derbyshire, S40 2EX

to be easy to use and provides a critical first layer of protection without the costly burden of specialist security expertise. As a cloud service you'll draw on all the expertise of Cisco and enjoy a solution that just works, all of the time, and is simple to install and manage. It means even without your own security experts you can take a proactive stance on security instead of remediating after the fact. All you need to do is locate the device serving DNS, update the server's settings to point to Umbrella, flush the DNS cache, and you're away. It really is that straightforward. And so is the interface. It offers visibility over the whole of your infrastructure from a single, user-friendly pane of glass. This provides comprehensive intelligence and real-time reporting on the threats it has stopped, the current state of your network traffic, and even allows policies to be enforced. Combined with reliable 100% uptime, this quick and low-touch console means there is next-to-no-management overhead whatsoever.

CCS Media has been a trusted Cisco partner for over 20 years, and during that time we've developed an impressive track record surrounding the orchestration and integration of their security, including the implementation of Cisco Umbrella to many different enterprises. While the five scenarios outlined above are mainstream use cases, Umbrella has the potential to support a whole host of more specialist requirements, from big data to the Internet of Things. We're fully aware that both budget and speed are highly important factors in the delivery of security, particularly across increasingly diverse user environments, which is why Umbrella makes for an ideal match, if only due to its incredible flexibility and the sheer ease of its deployment. Cisco, too, speaks for its own value, as a worldwide leader in IT that is shaping the future of security. Their proven heritage and expertise in cloud-based security solutions is difficult to rival, ensuring that any interoperability challenges are minimised and investment in their technology is maximised.

If you'd like to know more about Cisco Umbrella, we are offering a 21-day free trial. If you're not quite ready for a full trial, we're more than happy to offer demonstrations of what Umbrella is capable of, so contact us to book one in.

For further details visit ccsmedia.com
Let's talk Call 01246 200 200

CCS MEDIA

CCS Media Ltd, Old Birdholme House, Derby Road, Chesterfield, Derbyshire, S40 2EX