EBOOK

Top 5 Use Cases for Cisco Umbrella

Customers share the ways Umbrella protects their network like never before.

Cisco Umbrella

It's time to rise to the challenge.

The modern digital workplace has evolved, introducing a new and complex set of IT security, compliance, data protection, and regulations challenges. To keep your team and organization protected, you need a way to simplify your stack, while evolving it to meet today's needs and your unique challenges. That's where Cisco Umbrella can help.

Cisco Umbrella unifies secure web gateway, cloud-delivered firewall, DNS-layer security, and cloud access security broker (CASB) solutions into a single, easily deployed, cloud-based service — a secure on-ramp to the internet. Whether you're a security admin supporting a single location or an IT team securing a slew of branches and remote workers, Umbrella delivers the deep inspection and control you need to provide effective threat protection across a variety of use cases.

Tackle your toughest security challenges:

1. Sophisticated Threats
See how Axcess Financial proactively protects against complex malware.

2. Remote and Roaming Users
Learn how Cianbro keeps users safe, on or off network.

3. Direct Internet Access
Discover how Avril uses scaling security to protect branch offices.

4. Investigation and Response
Explore how Yelp addresses incidents, faster and easier than ever.

5. Risky Apps
Learn how Eurofins uncovers, assesses, and blocks shadow IT.

AXCESS FINANCIAL

Put sophisticated threats in their place.

66% of organizations have experienced or are currently combating targeted attacks[1] – but they've never faced threats like these before. More sophisticated and more prevalent, cyberattacks can strike anywhere – with every endpoint a potential point of weakness.

10x increase
in cryptomining traffic from January to September of 2019.[2]

11 seconds
The frequency with which a new organization will fall victim to ransomware by 2021.[3]

$6 trillion
The amount ransomware attacks will cost the global economy by 2021.[3]

Today's security leaders know that traditional controls alone just can't get the job done. Umbrella can help. By augmenting your existing security stack to amplify its effectiveness, and by protecting remote users and direct internet access breakouts, you can block threats before they become attacks, keeping your users and data safe.

Axcess Financial – a leading provider of payday loans – was looking to protect their team, their customers, and their critical data from complex threats. And, with an expanding network perimeter, Axcess needed more than the traditional on-premises security stack to see and protect every location and device.

AXCESS FINANCIAL

Introducing Cisco Umbrella into their stack along with Cisco Advanced Malware Protection (AMP) for Endpoints, Axcess has been able to dramatically reduce user exposure to malware – and improve their ability to detect, respond to, and remediate threats when necessary. Also, with Umbrella Investigate – interactive threat intelligence delivered via web console or API – security teams like those at Axcess can move away from simply reacting to incidents and begin proactively discovering and probing threats before they become attacks. Plus, by integrating with other security solutions (from both Cisco and third parties), security teams can stop switching between dashboards and chasing constant alerts – reducing issue prioritization, response, and mitigation time.

"Axcess's deployment of Umbrella and AMP for Endpoints has been a complete success story."

– Tony Hynes
Director of IT Security, Axcess Financial

With Umbrella, Axcess Financial was able to:

Reduce malware and ransomware by 75%

Reduce detection time from weeks (or months) to hours

Cut remediation time by 99%

CIANBRO

Provide protection without borders.

The modern workforce increasingly works outside the central office – and outside its protection. This shift presents new avenues where threats can strike – making remote and roaming users prime targets for attacks.

50%
of employees will work outside the central office within 2 years.[1]

78%
of cybersecurity experts believe roaming or remote users are most vulnerable to attack.[1]

68%
of businesses experienced attacks in the past year that compromised remote or roaming users.[1]

Securing remote and roaming workers presents a unique challenge to IT teams: How can you provide these users with the same level of security outside the network as in it – without increasing complexity or throttling performance? That's where Umbrella comes in.

Cianbro, one of the United States' largest construction companies, has a reputation for safety – and that includes the protection of its users, apps, devices, and data. An increasingly distributed workforce at job sites, fixed offices, and public hotspots was key to the company's success – but also created major vulnerabilities that threatened that safety.

CIANBRO

The Cianbro team needed to extend their protection beyond their network and VPN to better secure the entire organization from data breaches and malware.

By integrating Umbrella into their existing Cisco security architecture, Cianbro can now protect every user, everywhere, on every device. Proactively blocking attacks, Umbrella allows users to connect securely and confidently when working from laptops off the VPN, mobile devices, or on public Wi-Fi – all while ensuring performance at the same speeds workers have come to expect.

"Cisco Umbrella protects all of our production data, all of our mobile workforce, and all of our workstations – all of the time."

– Ryan Deppe
Network Operations Supervisor, Cianbro

With Umbrella, Cianbro was able to:

Reduce malware and ransomware by 75%

Reduce detection time from weeks (or months) to hours

Cut remediation time by 99%

Avril

Branch out your protection.

Today, direct internet access (DIA) allows branch offices to significantly improve network performance – eliminating latency by removing the need to traffic to the data center. But as a result, internet traffic from these locations isn't seen or protected by the centralized security stack, which can leave users and sensitive data exposed.

79%

of organizations are shifting to direct internet access.[1]

68%

of organizations experienced targeted attacks where branch offices and roaming users were the source of compromise.[1]

To embrace the increasing use of direct internet access, IT teams need a simplified, cloud-delivered service that unifies the power of multiple point security solutions in a single console. That solution is Cisco Umbrella.

Avril – a French agro-industrial group – was looking to provide branch offices with a reliable security solution that could continue to expand as Avril acquired new businesses and divisions. To secure these locations while still providing them with fast DIA, they needed a cloud-delivered security service that could work at the outer edges of the network, providing a front line of protection.

Avril

Using Cisco Umbrella's integrated network and security architecture, Avril is able to protect branch users, connected devices, and app usage at tens of thousands of direct internet access breakouts. Leveraging DNS-layer security to extend protection everywhere, Avril has been able to substantially reduce the risk of data exfiltration and malware across all ports and protocols. Simple to deploy and easy to manage from the cloud, Umbrella also allows Avril to keep expanding protection to keep up with new needs and new growth.

"Umbrella secured the whole company network in 10 minutes."

– Marc Tournier
Information Security and Compliance Manager (CISO), Avril

With Umbrella, the Avril Group was able to:

Reduce ransomware by 100%

Secure mobile users working off-network

Reduce security management time over previous solutions

yelp

Build your investigation reputation.

It's tough to get a complete picture of an attack. It's even tougher to handle it quickly and decisively when you're using tools from multiple vendors, each addressing only one piece of the puzzle! And don't forget all those alerts!

65%

of security teams say it isn't easy to determine the scope of a security compromise, contain it, and remediate it.[4]

79%

said it was challenging to orchestrate alerts from multiple vendor products.[4]

Investigating and responding to incidents requires a massive simplification and consolidation of security systems. Offering robust threat intelligence as both a web console and API, Cisco Umbrella Investigate helps incident response teams identify and respond to attacks, mitigate damage, and deliver proactive protection for the future by easily integrating with all of your other systems and Cisco security architecture. And, by introducing Cisco Threat Response to Umbrella, you can dramatically cut the time and effort needed to remediate incidents.

yelp

Yelp – a business directory service and review forum – is always looking for new ways to keep customers and employees safe. They wanted to speed the process by which they found and investigated threats, which meant dramatically simplifying the way they work with their security solutions. Using Umbrella, they were able to reduce the complexity, alerts, and noise from different security systems. Plus, by unifying a variety of security solutions in a single console, Umbrella also provided the Yelp team with centralized visibility.

"Cisco Umbrella gives us more confidence in our ability to proactively protect our customers and employees, and more efficiency in our incident response process."

– Vivek Raman
Head of Security, Yelp

With Umbrella, Yelp was able to:

Decrease incident response time from days to minutes

Reduce network security incidents and infected endpoints

eurofins

Shed light on shadow IT.

Workers are always seeking new ways to increase their productivity – and the right applications can make a big difference. Unfortunately, the vast majority of the time, these cloud-based apps are downloaded and used without being properly vetted by IT. Non-compliant with company security policies, much of this shadow IT has security vulnerabilities that can expose the network to attackers.

1,200+
cloud services are used in the average large enterprise.[5]

98%
these cloud services are unsanctioned shadow IT apps.[5]

27%
of discovered shadow IT apps are classified as high-risk.[6]

Employees are going to keep using applications with or without approval, so IT teams need a new way to monitor the apps being used – and block the risky ones that shouldn't be. Cisco Umbrella provides the needed visibility to see what's happening across your organization, so you can take steps to protect it.

eurofins

Eurofins – a life sciences testing company – needed a secure way to protect their sensitive customer data. Traditional approaches like VPN could no longer meet security requirements for an increasingly mobile workforce, which relies on cloud-based applications to stay productive when working off-network.

Eurofins chose Cisco Umbrella to help them efficiently and reliably secure users, protect data, and ensure that potentially perilous apps could not slip in under the radar. With complete visibility across the company's network, devices, and apps, the Eurofins team was able to identify thousands of apps in use by employees. Associating each of these apps with a risk score, Umbrella gave Eurofins the ability to drill down further into granular details like site registration and the location from which DNS requests were triggered.

"In the past, it's been hard for us to keep track of all the apps running on our systems. Now, we can use this list from Umbrella to put together a complete list of approved apps – and block the riskier ones."

– Romain Dawidski
Network Architect, Eurofins

With Umbrella, Eurofins was able to:

Discover and evaluate 6,500 applications across the business

Block 220,000 malicious requests in the first month of use

Protect remote employees and laptops 100% of the time without a VPN

Challenge accepted.

Cisco Umbrella is the only solution that can address all of the unique security challenges your organization is facing. Umbrella unifies secure web gateway, cloud-delivered firewall, DNS-layer security, and cloud access security broker (CASB) capabilities into one powerful, versatile solution for securing internet access and controlling cloud app usage. Uniting your entire security stack, Umbrella simplifies these point solutions into a single interface that's easy to deploy, configure, and manage – saving you time and resources. And, by delivering all of this from the cloud, with 100% uptime, Umbrella offers the visibility and enforcement to protect your users anywhere and everywhere.

With Umbrella, your team has access to the centralized management, consistent policies, and flexible levels of enforcement they need to more efficiently and effectively secure your organization.

Cisco Umbrella plays well with others to provide even more powerful protection.

Cisco Meraki

Umbrella quickly and easily integrates with Cisco Meraki to provide additional visibility and control across your network. Complementing Meraki's built-in content filtering, Umbrella blocks malicious destinations before Meraki learns of them and before a connection is even made.

Cisco SD-WAN

Cisco Umbrella integrates with Cisco SD-WAN in just a few clicks, instantly deploying powerful protection across hundreds of users and devices. Combined, SD-WAN and Umbrella allow you to secure your users wherever they access the internet, while providing a streamlined user experience and simplified security management.

Cisco Advanced Malware Protection (AMP) for Endpoints

Working in harmony, Cisco AMP for Endpoints and Umbrella can provide even greater protection from breaches – Umbrella preventing connections to malicious domains and IPs while AMP inspects and blocks malicious files. Together, these solutions help organizations protect against blended threats that use both email and web, and other sophisticated techniques.

Cisco Duo Security

Duo's multi-factor authentication lets you verify the identity of all users before granting them access to corporate apps. Working together, Umbrella and Duo enable you to uncover shadow IT, ensure the sanctioned use of cloud apps, and offer powerful protection against compromised credentials, phishing, and other threats – anywhere your users work.

Cisco Email Security

Operating in tandem, Cisco Email Security and Cisco Umbrella help prevent malicious links and files from propagating into full-blown attacks. With Email Security guarding against spam, fraudulent senders, infected files, and risky URLs, and Umbrella preventing links from connecting to malware and attacker infrastructure, these solutions provide your organization with even stronger protection from phishing and other threats.

Umbrella's simple, powerful integrations across the Cisco ecosystem enable you to quickly protect your users wherever they access the internet, ensure consistent policy enforcement on or off network, and gain sharper visibility across your entire organization – all from a single cloud console.

Cisco Umbrella

To learn more about how Umbrella can address your unique security challenges, contact a Cisco representative – or explore which package is right for you.

Explore Umbrella packages

Sources:

1. Cybercrime Magazine, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021
2. Enterprise Strategy Group, *Market Dynamics Impacting Remote and Roaming User Security Requirements*, January 2019
3. Cisco Umbrella Global Network
4. Cisco, CISO 2019 Benchmark Study
5. Cisco Blog, Gartner Report Says Shadow IT Will Result in 1/3 of Security Breaches
6. Help Net Security, 27% of Cloud Apps Are High Risk