Cisco Umbrella

SOLUTION BRIEF

The only off-network security for law firms & legal services.

Your need: always-on network security

It's quite simple: the more your associates and partners collaborate with clients, the faster the firm grows. But access to your client's data makes your firm a prime target for attacks, so you've implemented a security stack with best-practices. You've stacked multiple security solutions (e.g. firewall, proxy, antivirus) for "defense-in-depth". And yet, you're still re-imaging laptops and flooded by security alerts.

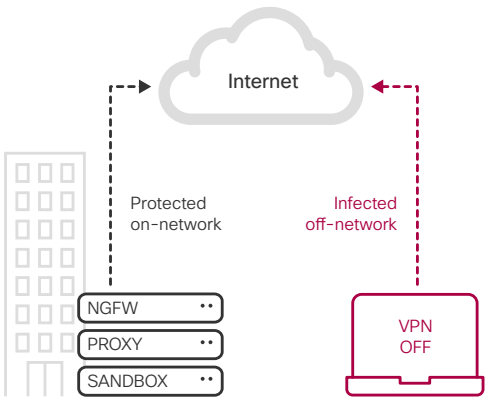
First dilemma: too much malware reaches you

Your security stack must wait until malicious traffic reaches your perimeter or endpoints. Then, your firewall, proxy, and antivirus can detect and prevent the threat. If you use a SIEM, it receives too many alerts for every attack that reaches each of these security layers. Your CISO is asking, "Would a better firewall or proxy or antivirus result in more effective security, OR do we need something new?"

Second dilemma: perimeter security is often blind

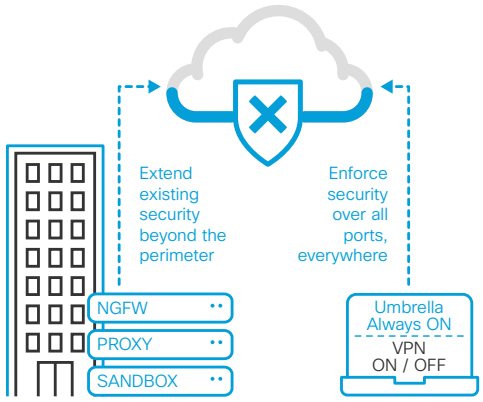
Whether you're using new cloud-based law practice management apps or every-day cloud apps such as Office 365 and DocuSign, the data your partners and associates need to access is no longer on-premises. As remote users work directly via the cloud, perimeter security appliances and VPNs are no longer always going to protect your devices and client data. And most of your security stack loses control and visibility of the malware reaching your endpoints. Your CISO now wonders, "How can we enable the firm to work from anywhere, yet, ensure consistent always-on security?"

You cannot rely on the VPN



Remote access to the corporate network is no longer required to get work done.

You need off-network security



Enable your firm to embrace the cloud and work from anywhere.

The bottom line

The VPN is not always-on despite "best practice" or "locked down" policies. And your firewall, proxy, and AV are not enough to protect your mobile workforce.

The reality today

Gartner

"By 2018, Gartner estimates that 25% of corporate data traffic will bypass perimeter security and flow directly from mobile devices to the cloud."

Our solution: Cisco Umbrella as the first line of defense

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. Because it's built into the foundation of the internet, Umbrella blocks threats over any port or protocol before they ever reach your network or endpoints. Plus, it delivers complete visibility into internet activity across all locations, devices, and users. Our service is transparent to your employees and devices because it leverages existing internet infrastructure, VPN agents, and OS components.

By analyzing and learning from internet activity patterns, Umbrella automatically identifies current attacks and uncovers internet infrastructure staged for emerging threats. Then it proactively blocks requests to malicious destinations before a connection is even established.

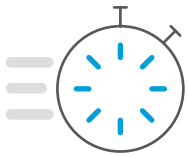
With Umbrella, you can stop phishing and malware infections earlier, identify infected devices faster, and prevent data exfiltration. And because it's delivered from the cloud with an open API, Cisco Umbrella provides an effective security platform that is simple to use and automated. It's the fastest and easiest way to protect all of your users in minutes.

Over 150 leading law firms already rely on Umbrella for always-on network security

Why law firms choose Umbrella to improve security

The easiest and fastest security you'll ever deploy.

- There is no hardware to install or software to manually update.
- For the first time, adding security won't add any latency.
- Our endpoint footprint is one-quarter the size of antivirus because everything happens in the cloud, and when a new version is available, it automatically updates without reboots.



The largest reduction in security noise and break-fix busy work.

- Noise from your security stack's alerts can hide the most damaging attacks from your incident response team.
- Prevent both garden-variety and advanced threats before an IP connection is ever attempted or a file is ever downloaded, so there are far fewer alerts to triage and prioritize.
- Simply put: AV, firewalls, and proxies are not enough.

The best way to extend protection beyond the perimeter .

- Convert your local threat detection into global threat prevention using our API-based cloud service.
- Many turnkey integrations are available – go to cs.co/fireeyeintegration to learn more about our most popular integration.
- Using our API, easily extend and immediately block any malicious domains detected by your existing security stack.