How the Cisco Umbrella roaming client enables lightweight & transparent security everywhere.

We know everyone promises it. And we know you already have multiple clients on your endpoints. Our client’s footprint in memory and on disk is 4 times smaller than antivirus because enforcement happens in the cloud. More importantly, Cisco Umbrella prevents threats – unlike many clients that just detect them.

The Umbrella roaming client enables security at the DNS and IP layers, in the cloud, no matter where the endpoint is located. The client simply forwards DNS requests or tunnels suspect IP connections to the Umbrella global network. Something so simple is so powerful because it enables Umbrella to be a virtual “bump-in-the-wire” for every internet connection. We allow good requests. We redirect users to a block page for malicious requests. And we can even proxy the connection for deeper inspection, as needed.

Other endpoint protection or cloud service clients scan all system activity or redirect all data traffic, which increases the system footprint, network latency, and end user burdens.

Depending on your endpoint protection today, our customers are able to stop up to 98 percent more attacks when they deploy our roaming client – with the same endpoint impact as using instant messengers or downloading songs.

### Footprint in memory (during operation)

<table>
<thead>
<tr>
<th>Antivirus scanner (average of 6 vendors¹)</th>
<th>Virtual container (1 example vendor²)</th>
<th>Umbrella roaming client (3-4 running services³)</th>
<th>Instant messenger (1 example vendor⁴)</th>
</tr>
</thead>
<tbody>
<tr>
<td>185 MB (active)</td>
<td>153 MB (idle)</td>
<td>25-55MB* (active)</td>
<td>66 MB (max)</td>
</tr>
<tr>
<td>153 MB (idle)</td>
<td>~50 MB</td>
<td>26 MB (min)</td>
<td></td>
</tr>
<tr>
<td>153 MB (idle) (across of 6 vendors¹)</td>
<td>(1 example vendor²)</td>
<td>(3-4 running services³)</td>
<td>(1 example vendor⁴)</td>
</tr>
</tbody>
</table>

Data Sources

3. Umbrella engineers determined the footprint in memory by measuring and aggregating the private working set, which is the RAM that is not shared between system processes, for all running Umbrella Roaming Client services. User-initiated network activity was simulated by rapidly requesting websites, including domains like tmz.com, which has many browser redirects that generate hundreds of DNS requests. The system under test was running Windows 7 SP1 x64 and contained 4GB memory and an i3-4005U CPU (1.70GHz, 2 cores, 4 logical processors).
4. Third-party service tracked Yahoo Messenger (j.mp/YahooIM), which includes two services:ymsgr_tray.exe (j.mp/ymsgr_tray) and YahooMessenger.exe (j.mp/ymsgr_IM).
5. Third-party article (http://filecatalyst.com/todays-media-file-sizes-whats-average/)

*During stress tests, it consumes 45-55MB on Windows and 25-45 MB on Mac OS X. A fourth service (umbrella-ipsec.exe) runs on Mac OS X.

### Footprint on disk (after installation)

<table>
<thead>
<tr>
<th>Antivirus scanner (across of 6 vendors¹)</th>
<th>Virtual container (1 example vendor²)</th>
<th>Umbrella roaming client (all program files plus logs)</th>
<th>Average MP3 file²</th>
</tr>
</thead>
<tbody>
<tr>
<td>775 MB (average)</td>
<td>100 MB</td>
<td>6-16MB</td>
<td>3.5 MB</td>
</tr>
<tr>
<td>775 MB (average)</td>
<td></td>
<td>25-55MB* (active)</td>
<td></td>
</tr>
<tr>
<td>151 MB (smallest)</td>
<td></td>
<td>26 MB (min)</td>
<td></td>
</tr>
</tbody>
</table>

© 2016 Cisco and/or its affiliates. All rights reserved.
What does it mean to have a lightweight footprint?

**Memory and disk size are the most impactful metrics.**
(note: charts on page 1 are not to scale)

1. In memory, the collective footprint of several security clients can cause a memory shortage for office productivity and other business apps. The top culprit for an intrusive user experience is local system scans or application activity monitoring.

2. On disk, the distribution of large installation files or frequent security updates to thousands of endpoints can cripple the network. A common reason for unscaleable deployments is enforcing security locally on the endpoint, rather than in the cloud.

What does it mean to provide a transparent user experience?

**Security should work the way administrators and employees already work today.**

1. For administrators, new clients must be interoperable with the software provisioning systems, network infrastructure, and security clients that are already in use. Products that require system reboots or a manual registration process for immediate protection will delay an enterprise-wide rollout. Not with Umbrella!

2. For employees, new clients must not prompt them to take new actions. Common issues with some products is requiring a system reboot after a software update, or causing the browser to show a SSL certificate warning. Again, not with Umbrella!

What happens on the endpoint?

**The Umbrella roaming client services run in user space without any OS hooks.**

Unlike advanced threat defense clients that run in kernel space, our software does not risk crashing the system or stealing memory from OS processes. Standard software distribution practices will install the client on all endpoints, which runs three to four services:

1. **Dnscrypt-proxy.exe** — securely forwards DNS requests to the cloud

2. **ERCService.exe** (and on Mac, umbrella-ipsec.exe) — manages the OS’s built-in networking stack and its state to tunnel suspect IP connections to the cloud, and auto-updates software

3. **ERCInterface.exe** — a tray icon and interface is enabled by default, but you may opt to not install it via a flag in a command-line / distributed installation

What happens in the cloud?

**The Umbrella global network resolves DNS queries and routes IP connections without adding latency.**

1. Our service is more secure, ultra reliable, and speedy compared to ISPs or local DNS servers. And unlike cloud-based proxy or VPN gateways, Umbrella does not need to proxy or tunnel every connection.

2. For DNS queries, the domain request and IP response is compared against our security intelligence. If both are safe, the normal DNS response is returned. If not, a modified DNS response is returned to block or proxy the connection.

3. For IP connections, the destination is compared against our security intelligence. If it’s malicious, the connection is terminated. If it’s known to contain malicious content, the connection is proxied and only malicious URLs are blocked.

Want to learn even more?

Check out our roaming client feature briefs for Windows and Mac OSX.

Already use Cisco AnyConnect?

You’re in luck – no additional agents need to be installed! Simply upgrade to v4.3 or later and enable the roaming security module for the same protection wherever users go. Plus, it enables logging by username in addition to hostname.