

Anywhere⁺ Frequently Asked Questions

Overview

What is Anywhere⁺?

Anywhere⁺ is the world's first SaaS security for roaming workers

Where does it work?

It works anywhere roaming employees connect to the Internet – at home, in a hotel room, at a client's premises, in a coffee shop or Wi-Fi hotspot.

What are the benefits of Anywhere⁺?

- Extend security to all roaming employees not just office workers
- Remove risk of infected laptops coming back to office LAN
- Move real-time scanning into the cloud
- Extend policy control to all employees
- Simplified management with no endpoint client hassle and updating
- Reduce network bandwidth congestion – no need to backhaul traffic via a VPN

What are the cost savings I can get from using Anywhere⁺?

No need to backhaul all data via a VPN, hence large bandwidth savings.

No large clean up bills when remote users get infected as you decided not to enforce backhaul via a VPN.

A potential customer says he is happy with his existing office security solution but would like to add Anywhere⁺ just for roaming users. Is that possible?

Yes, Anywhere⁺ can be sold separately. It is also very easy to add the remaining office workers at a later date.

How is it priced?

Customers pay for our regular office security services (Web malware scanning, Web filtering) PLUS an additional monthly per user fee for the number of outside users with the additional Anywhere⁺ security service.

Is Anywhere⁺ really unique? Aren't other companies offering the same thing?

Anywhere⁺ is the world's first SaaS security for roaming users. All other offerings in the marketplace work in the same way as the ScanSafe existing Virtual Connector.

How can my customers evaluate Anywhere⁺?

Customers can evaluate Anywhere⁺ in exactly the same way as any other ScanSafe service on a 30 day evaluation with no costs or obligation to buy.

Technical

What is split tunnelling?

Split tunnelling is a VPN term. This means that data that is bound for the corporate network is tunnelled back to the corporate gateway via the VPN, and all other traffic is routed to the internet in the normal way.

Does the VPN have to be in split or full tunnel mode?

Anywhere+ requires the customer to deploy the VPN in split tunnel mode.

All external Web traffic (both HTTP and HTTPS) should be allowed to go directly to the internet (where Anywhere+ will redirect it to the ScanSafe scanning infrastructure and apply the correct policies).

What VPNs does Anywhere+ work with?

Anywhere+ works with all major VPNs including:

- Aventail
- Cisco
- Checkpoint
- Juniper
- Microsoft
- Nortel
- Watchguard

What is the difference between Anywhere+ and Virtual connector?

The virtual connector is designed for stay-at-home workers. It is not suitable for roaming workers. It does not work through proxies (including transparent proxies) and also does not work through paid-for locations (e.g. hotspots) as the PAC file proxy direction will fail.

What happens when the user goes to a 3rd party client site?

Anywhere+ has been designed to work through third party proxies and transparent proxies, so it will work at 3rd party client sites with zero issues

Deployment

How is Anywhere+ deployed to end-users?

Anywhere+ is a single .MSI (Microsoft Standard Installer) file. It supports a silent installation and is supported by just about every software distribution mechanism including:

- Microsoft SMS
- GPO
- Login Script
- Big Fix

It is also possible to distribute the installer with a readily set up Anywhere+ config file.

How much memory does it require?

Less than 16mb. The installer itself is 4mb.

Can the user disable Anywhere+?

Anywhere+ is tamper-resistant. Without knowing the password for the service the user cannot disable or uninstall the product.

Can I deploy Anywhere+ just for my home users?

Yes, they can.

Now customers have Anywhere+, can they just get rid of their Desktop AV software?

No. ScanSafe's services protect unencrypted Web traffic only. Any other method of entry onto a laptop, for example by email, USB stick or network share are not protected, hence users still need local malware detection.