

Secure Network

Current Offerings

28 June 2023

Contents

- 1 Description1
 - 1.1 Network scoping.....1
 - 1.2 Risk Assessment.....1
 - 1.3 Network architecture1
 - 1.4 Typical design.....2
 - 1.5 Network design.....2
 - 1.6 Site visit.....3
 - 1.7 Back-up and recovery testing3
- 2 Commercial Terms3
 - 2.1 Purchase Hardware3
 - 2.2 Networking Infrastructure3
 - 2.3 Monthly Subscription.....3
- 3 Service benefits4
- 4 Deploying and Operating the Service5
- 5 Supporting Documentation5
- 6 How Support Works5
- 7 What is not included.....6
- 8 How we may change the service from time to time.....6
- 9 Terminating our service6

1 Description

Our secure network service means we analyze with you your networking needs then design, deploy and monitor secure network devices to ensure that your network security is strong, that your network remains secure over time and that any attacks on your network are detected and reported so that any new threats can be addressed.

Our service is designed to be for organizations with simple networking requirements who do not have specialist networking staff yet where the network availability and performance is essential to the business.

1.1 Network scoping

Our service works as follows:

- a) You tell us what networking resources you currently have and where they are deployed:
 - i) Whether or not you currently have an internal corporate network.
 - ii) Details of your broadband providers, if any.
 - iii) The details of the network device deployed by your broadband provider connecting you to the internet.
 - iv) Any other networking equipment you are aware of that is currently deployed.
 - v) Whether any there is any existing network cabling deployed.
 - vi) How devices on your network are currently configured.
- b) We work with you to identify your needs for networking:
 - i) How many offices do you have that need to be connected to the network and where are they?
 - ii) Whether or not you have homeworkers and the extent that they need to connect in to your corporate network, for example to you file servers or any other server computers running on your network.
 - iii) How many computers and mobile phones do you need to connect to the network.
 - iv) The data transfer loaded expected to be required across your network.
 - v) The likely level of data to be sent or received across the internet.
 - vi) The different groups of users on your network and the extent to which you need to separate those groups onto individual networks for security or load.

1.2 Risk Assessment

We take you through a general security risk assessment process to help you understand the implications of security on your business and specifically factors that need to be covered when designing your network. Specifically, we consider with you the impact on your business if there was a network outage and the options available to ensure that there is always a backup that can be switched in to keep going if one item failed.

1.3 Network architecture

We then design with you a network architecture while taking into account the factors above as well as the physical security implications on your site:

- i) Whenever we can, we include your existing equipment in our design to minimize cost and waste.
- ii) Most small businesses have modest network needs and our solutions are typically quite simple in technology terms.
- iii) We prioritize into MUST, SHOULD and COULD the possible features of a design so that you can include more advanced protection which has a modest cost and a big impact improving your security, if that makes sense to you.

1.4 Typical design

A classic design for a small SME is:

- i) Deploying our advanced router in between your existing network and your current broadband device, ideally in a secure cabinet where your current broadband devices are located.
- ii) This router runs untangle enabling us to manage your router, the firewall protecting your network from the internet and your network.
- iii) Deployment at least one managed switch to provide greater control over your network.
- iv) Adding replacement high performance WIFI hubs often in a mesh configuration so that you can move anywhere in the building and remain connected to your WIFI network which appears to you as a single WIFI network.
- v) Configure a primary secure network integrating a WIFI network with your wired network for your computers that is not visible to the outside world.
- vi) A secondary WIFI network to which your staff can connect their mobile phones.
- vii) Configure a guest WIFI for any visitors, with a facility to give visitors limited connection time codes to connect to the network for the day.
- viii) Advanced configuration of the Firewall to detect the traffic on your network and only allow the traffic you authorize to pass across it.
- ix) Configuring the router to give priority to certain sorts of traffic, for example video so that staff are not interrupted if a large file transfer is taking place on the network.
- x) Integrating your new router with other systems such as for example your Windows Domain controller that manages your staff logging into the network.
- xi) Configuring a VPN so that our staff can connect into the office from home.

1.5 Network design

We can develop the network design significantly if required and some features might include:

- i) If you have multiple broadband suppliers connecting both to the router so you can maintain access if one provider fails by diverting all traffic from the failed provider.
- ii) Ensuring that your business computers always connect through a VPN but only communicate to the office for office communications, minimizing the load on the company broadband circuits.

- iii) Including additional redundant equipment so there is no single point of failure on your network and in the event of a failure, fail over to the standby equipment is automatic.

1.6 Site visit

There may be a need for a site visit and if so, we charge for this in addition as a design service.

1.7 Back-up and recovery testing

On a regular basis, to an agreed calendar we will test backup and recovery procedures to ensure that the network can always be restarted following any failure.

Once the network is installed and configured, we then monitor all aspects of the network on your behalf to ensure that it remains operational.

You can see the facilities at <https://www.untangle.com/> available from untangle.

Carrying out additional professional services to add more equipment to the network or reconfigure the network or any devices on it is beyond the scope of this service. However, we are ideally placed to assist you through our Time and Materials Professional services to redesign the network, reconfigure any equipment or add new equipment to the network. If you engage us to carry out any such work, then we can include network support of those changes without additional cost other than the per device cost.

Note: we maintain control over all network equipment under our management.

2 Commercial Terms

2.1 Purchase Hardware

You pay for any hardware that we agree is required for the design.

2.2 Networking Infrastructure

There is also a charge for any works required to implement the network, for example to lay cable, to deploy the Wi-Fi hubs or to build a secure cabinet for your network equipment, though you may have a preferred supplier who can complete these works at your direction.

2.3 Monthly Subscription

You pay a single monthly subscription charge for each device you plan to have on the network. In the first year this includes an uplift to cover our initial design work, set up and configuration.

We review this charge on the anniversary of the service starting. Typically, the uplift would be removed if the level of support required by us during the year has been within the limits that we agree with you.

This charge is based on the standard protections we configure with you on the router as part of the design. If you need additional protection features from time to time then we can include them at a modest additional cost based on the underlying cost of adding the facility to the router.

You do not directly pay for own any underlying perpetual licenses or third-party subscriptions for our service. We manage all of the underlying technology.

When you take our service there is an initial 3-month commitment. You can terminate use of the service completely giving 30 days' notice on completion of the 3-month commitment.

If you terminate there is a small termination charge based on the period outstanding to the end of the anniversary of the contract because the router you own retains a dedicated untangle license to the end of that license period, and during that time while the full untangle license is active you will retain full functionality of the advanced router and firewall features.

If you terminate the service then we stop managing your network and have no further responsibilities to you. The equipment is yours and remains in place and we will provide you the appropriate details for you to manage it yourself.

Your charge is monthly in advance for payment within 15 days. We can take check or credit card but request you set up regular ACH payments to minimize administration and costs for both parties.

A small discount is available for increased long-term commitment or annual payments in advance provided payments are via ACH.

3 Service benefits

This provides our customer a number of significant benefits:

- Network protection is one of key elements of your cyber security protection. This approach gives you a low-cost path to advanced network security, which you can expand over time if the threat level you face increases.
- If your network is important to your business and you would be severely impacted by an outage, this service gives you the peace of mind that your network is being managed and can be restarted as promptly as possible following a network failure of any kind.
- Further, if you chose to invest in dual broadband providers then if one of them has an outage you know that your network connections will be automatically re-directed down the operational broadband channel.
- The router software automatically updates itself with its latest version so the risk of attacks directly against your router are minimized.
- Maintaining network security requires a small amount of regular attention from highly skilled and expensive network engineers. Instead of having to employ two such people (to ensure cover if one leaves), you can instead use our service which essentially means that once set up you only pay for the small amount of time required on your system from someone who is nevertheless fully focused on monitoring our customers networks.
- A traditional router can vary from a few hundred dollars to several thousand, or indeed tens of thousands of dollars, yet they have a planned lifetime, go out of support and must be replaced. By taking this service your router never goes out of service, because it's a software license subscription with the software being constantly updated. The underlying hardware is very low cost and can easily be replaced for a low charge if you expand and need a more powerful device or at its end of life and the license transferred. This flexibility and reduced cost mean that the overall total cost of ownership is significantly lower than most equivalent solutions.
- You will be provided with reports on traffic across the network which can provide valuable insights into the workload of staff and give early warning of a range of threats to your business which our service will alert you to.

Ultimately this service does the following for you:

- a) It delivers a reliable and available network for your business including WFH designed by an expert to minimize outages and maintain availability so that your business is not interrupted by network failures.

- b) It forms a key part of your cyber security defence.
- c) It is a cost-effective solution that you can expand as your needs grow.

4 Deploying and Operating the Service

Setup requires equipment to be installed in an appropriate environment.

Once configured, this should be transparent to the people in your organization in most respects.

We will provide you with regular reports and alert you to any activity of interest for which management action might be required.

5 Supporting Documentation

As the operation of this service is transparent to your organization, there is no requirement for extensive documentation on the service itself.

We provide a short operations manual describing:

- a) Our understanding of your environment.
- b) Your responsibilities to inform us in good time of any changes that might impact our management of your network.
- c) Mechanisms for requesting reports and the meaning of the reports we deliver to you.
- d) The operation of our support system, how you can track any issue that has arisen and the SLAs and KPIs by which you can measure our performance.

We also provide an operations manual describing how to carry out critical onsite tasks to replace items of hardware to restart a device to that you can undertake basic functions for us as we work remotely.

6 How Support Works

The following is a brief description of our support mechanism. This is explained fully in our support manual:

- When an issue occurs on your network that is automatically reported to us then we document then triage that problem.
- A new issue is then raised in our service desk environment, on behalf of the nominated user associated with the item of equipment concerned.
- We may merge incidents reported for many devices if they are fundamentally the same problem, and particularly if you took another of our services that would report problems with the network.
- You may raise a support issue directly for any item of equipment we are managing by using the Company's icon on your machine. As soon as this appears on our service desk environment, you can then add further comments or information related to the problem.

- All information related to the issue should be entered via service desk, but we will accept calls to escalate urgent/serious issues by email or phone.
- Once an issue is raised, you can then track the issue through to resolution.
- We access your router where that is required via a VPN so need you to authorize and provision accounts for us on your network and authorize us to access the router via the VPN.

Support is provided during the working day between 0800 and 1800. Optionally you can purchase extended support for out of hours or 24 x 7.

Onsite support is not included as part of this service: we work with your onsite representative. However, we are able to provide onsite support as part of our Equipment Managed service offering.

At the end of each month, you are provided with a report describing our performance against agreed KPIs.

Our service desk is available at the following URL

<https://cysure.atlassian.net/servicedesk/customer/portal/2>

7 What is not included

This service does not include onsite maintenance. We can work with your staff to provide operational procedures describing tasks that require onsite work. We provide a full lifecycle support of equipment as a separate service.

8 How we may change the service from time to time

Our service is based on purchasing software licenses and subscriptions which we then use to deliver the service. From time to time the technology vendors of these products increase their prices and we need to similarly increase our prices.

We will publish any revised prices on our website and will notify you of any price rises giving you 3 months' notice of such price rises. By taking this service you agree to accept any such price rises. You may terminate the service if you wish.

We may change the product we use to provide this service at any time. It is then our responsibility to ensure that the change of product has no impact for you. Note:

- a) the most likely reason for a change would be that an alternative product either provides significantly more functionality at a comparable price or is more cost effective for the capability delivered.
- b) As we would bear to cost of any transition, this is not something we would do lightly!

9 Terminating our service

If you decide to terminate our service, then for this service you must provide us 30 days' notice of termination.

If you terminate this service, there is a small termination charge calculated based on the outstanding period of the underlying annual untangle license which will continue to

run on your router until the completion of the license term. We will calculate this and invoice you once you give notice.

On termination we will no longer monitor your untangle router or any aspect of your networks. We will also disconnect your WIFI extenders from our management hub. Until you configure them using an alternative support facility you will no longer be able to issue GUEST WIFI tickets.

On termination and provided we have received payment in full on all outstanding invoices, we will provide to you details of all passwords and other confidential information related to your network hardware so that you can continue to manage the network yourself.

After one month or sooner if you request, we will remove details of the devices from our management platform and then remove all details of your organization from the platform.

It is your responsibility to archive any reports important to you before you terminate because once we remove your organization from the platform all historic data is deleted.

If you require any assistance from us when terminating, for example to transfer to an in-house solution or to an alternative vendor, then as a responsible supplier we will assist you in this process if requested and charge you at our standard professional services rates on a time and materials basis.

If you request to purchase our network training package, we can deliver this training and show you how to manage your network. We encourage you to during this period to prove that you have full access based on the passwords or other details we have provided.