



# Remote Monitoring

## Current Offerings

19 October 2022

## Contents

1	Description.....	1
2	Commercial Terms .....	2
2.1	Monthly subscription .....	2
2.2	Anti-malware .....	2
2.3	Back up service.....	2
2.4	Payment .....	2
3	Service benefits .....	2
4	Deploying and Operating the Service.....	3
5	Supporting Documentation .....	4
6	How Support Works.....	5
7	What is not included .....	5
8	How we may change the service from time to time.....	6
9	Terminating our service .....	6

## 1 Description

Our remote monitoring product is based on Ninja RMM and a full description of their capability can be seen at <https://www.ninjarmm.com/>

The following describes the service we provide:

- a) We install the Ninja agent on every device you nominate. Generally, this is every Windows or MacOS machine in your estate. It can in addition be installed on the following devices:
  - i) CentOS, RedHat, Debian, and Ubuntu Linux
  - ii) VMWare
  - iii) Hypervisor-V
- b) The installed agent monitors the health of the device on which it is installed and tells us if there is an issue or problem with that device. When a problem is encountered, we are sent an email and can then login to the console and investigate the issue.
- c) From our operations center we are able to remotely download scripts to run on each device, or issue local commands to each device so that we can correct issues and maintain the health and performance of each device.
- d) Examples of the types of issues that we can detect and resolve include:
  - i) Ensure Windows updates are installed.
  - ii) Ensure basic Backups of data in defined directories are successfully completed.
  - iii) Verify anti-virus software is up to date.
  - iv) The status of the fan and the internal temperature of the machine.
  - v) Whether USB access is enabled or disabled.
  - vi) If disks are encrypted using bitlocker.
  - vii) Warnings of potential failures such as disk errors.
  - viii) Catalogue the software installed on a machine
  - ix) Add, update or remove software as appropriate from the machine including drivers.
- e) Reports are available to provide point in time evidence for the business, for example for audit purposes. They can be generated and emailed automatically on a timed basis if required.
- f) Essential to our service is the provision of a support facility through which:
  - i) All incidents that occur can be viewed by you.
  - ii) You can view our SLAs and monitor our performance responding to any issue.
  - iii) Overall KPIs governing our service.
  - iv) Our service is intended to cover all the equipment in your estate as a key element of protecting your estate from Cyber-attack.
- g) The remote monitoring solution also comes with Teamviewer host for remote access

- h) We optionally offer Webroot Antivirus for customers who do not currently have an adequate anti-malware solution available.
- i) We have an additional backup and recovery solution which is an extra service but can only be taken if you are already taking this service. This service is described in our Business Continuity Service description.

## 2 Commercial Terms

### 2.1 Monthly subscription

You pay a single monthly subscription charge for each device we manage. You do not pay for any underlying perpetual licenses or third-party subscriptions for our service. We manage all of the underlying technology and carry the risk of you terminating.

When you take our service there is an initial 3-month commitment. After that our subscription charge is elastic. You may expand the scope of service at any time paying an initial pro-rata amount to align to the next normal billing date. You can reduce the amount of equipment under management and the associated device price giving 30 days' notice after the initial 3-month commitment is completed.

You can terminate use of the service completely giving 30 days' notice on completion of the 3-month commitment.

### 2.2 Anti-malware

The core service does not include anti-malware so you do not have to pay if you have an alternative and the additional price for adding WebRoot is in our product pricing schedule display on our website.

### 2.3 Back up service

Our basic backup service is included in this Service but our full business continuity and disaster recover service is not and is priced separately based on your detailed requirements.

If you terminate the service then we remove the agents so you have nothing to do.

### 2.4 Payment

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:

- a) Ensures that all your equipment configuration complies with your security policy optimizing your defense against cyber-attacks in a cost effective, coherent and consistent manner.

- b) In the event that an issue arises, we are informed promptly and can in most cases take immediate action to resolve the issue before you are aware of a problem.
- c) We get early warning of a potential machine failure. This means we can:
  - i) Ensure a backup is taken immediately so that no data is lost.
  - ii) Carry out scheduled preventative maintenance or swap out and replace a component out of hours and before a total failure occurs.
  - iii) Minimize the risk of a failure during a critical business activity
- d) Maintain a current and accurate register of all equipment in real time so you know where all your equipment is and enabling you to manage how you replace equipment over time, possibly re-using equipment for less strenuous activity as it ages.
- e) Automate tasks such as disk clean up and defragmentation to maintain optimal performance.
- f) Maintaining a software inventory ensures that you comply with your software license obligations by not installing software beyond your license limits, and allowing you identify the location of deployed licenses so that you can remove them and re-assign them to prevent unnecessary purchase of licenses.
- g) We can be alerted if a machine that should be permanently on-line becomes inaccessible potentially triggering an investigation into the theft of equipment.
- h) In the event of the loss of a machine, once a replacement has been connected to the network and the Ninja agent installed, we can supervise the recovery of the computer from a backup.
- i) If any unexpected event occurs, which is not covered by any of our automatic or scripted tools, and providing the machine remains on the network, we can connect remotely, investigate the problem and hopefully resolve it.
- j) The reporting engine means that we can create custom reports on your estate to meet your needs. Generally custom reports would attract an additional minimal charge.
- k) All our services are provided as a single aggregated invoice with a detailed breakdown of individual charges so that you have only one invoice to pay each month for the range of technologies underpinning our service, yet you have full visibility of how the charge is made up.
- l) We can deploy the technology underpinning our service at a lower cost than if you bought all components individually because of our buying power operating at scale, and we share the savings with you.

Ultimately this service does two things:

- a) It gives you peace of mind that your estate is being effectively managed.
- b) It forms a key part of your cyber security defense.

## 4 Deploying and Operating the Service

Provision of this service assumes that your device can be connected to a broadband network of sufficient performance to support the backup of data from all devices in accordance with a daily backup schedule.

The agent is easily installed onto each computer by downloading from a secure source which may be our website, any secure shared data area in your environment or from a secure installation device such as an encrypted USB provided by us with the password.

We will automatically apply operating system patches to monitored devices when patches are published by the vendor. If you have any concerns that operating system patches may impact other software installed on the device you must tell us and we will instead alert you that there are updates available so that you can test the overall platform and then apply the patches yourself.

The monitoring services should identify a problem on a device and allow us to remotely login to the device and resolve the issue. By taking this service you authorize us to connect in this way.

If you identify a problem with a device before we do, you have an obligation to use the agent on that device to log an error through our support system alerting us to the issue you are observing through our support system, so that the issue is attended to as promptly as possible.

Every time a major change is made to your configuration, an image backup will be taken of the relevant device so that it is possible to restore from this backup in the future if necessary. Otherwise, incremental backups will be taken daily of each device.

**Commented [ND1]:** Need to talk through this.

If the volume of data increases you will pay for the charge associated with backing up that data. We will alert you to unexpected increases in your use of storage so that you can choose to purge any data that is building up and which you do not need to backup.

**Commented [ND2]:** Addition.

## 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) Key details of the service such as installation of the agent
- b) Mechanisms for requesting reports and the meaning of the reports we deliver to you.
- c) 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 computer or where we have taken on support for non-standard devices of yours that require specific instructions.

## 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 any of your equipment our service detects the problem.
- We 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.
- You may raise a support issue directly for any item of equipment we are managing by using the Cysure 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.

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 can work with a member of your staff who is on site to undertake any tasks which require an onsite presence. We can be available to come to site if required and subject to staff availability to address any serious problems, chargeable on a time and materials basis if requested by you. We provide a full lifecycle support of equipment as a separate service.

This is a basic backup service provided on a device-by-device basis to enable you to recover a particular device and to restore data to the last known copy prior to an attack, for example a ransomware attack. It is not a full business continuity / disaster recovery service for the organization.

## 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 the service then the only action related to your equipment required is for us to remove the agent from each device on which it is deployed.

We will also remove details of the devices from our management platform and then remove all details of your organization from the platform and delete all historic backups held for each of your devices.

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.

This paid assistance could also include recovering data from backups. However, the basic backup service is intended as a machine recovery service rather than a file-by-file recovery service and we would normally expect that your standard protection would be to take a new backup with a replacement capability and continue from that point forward, discarding any historic backups.