NHS Digital

Microsoft Windows operating system licences with Advanced Threat Protection

Service overview

Version 3 - December 2018

Information and technology
for better health and care

Contents

Introduction

NHS Digital is now able to offer local organisations Microsoft Windows operating system licences, including Advanced Threat Protection (ATP). This is free of charge to local NHS organisations who agree to implement the ATP facility and fully use the licences.

The ATP facility gives local organisations better cyber security protection in their own right. And, since it is also linked into the NHS Digital Data Security Centre (DSC), it improves cyber security protection for local health and care communities, and the NHS as a whole.
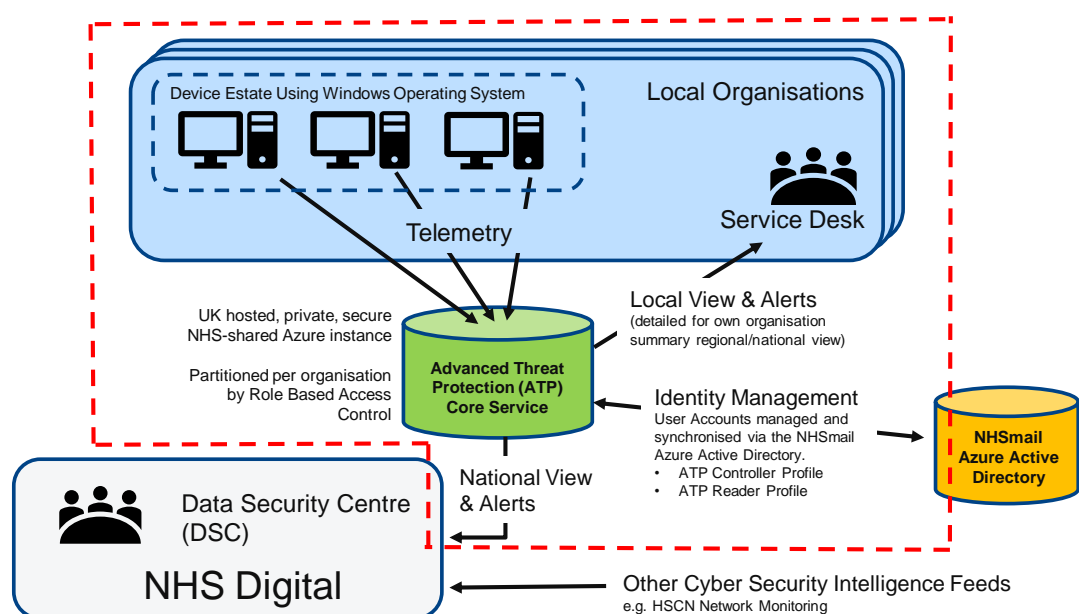
How does it work?

The Microsoft Windows operating system licences are the standard Enterprise E5 version of the licence for client devices.

ATP monitors the Microsoft Windows operating system on a PC or Laptop device for any abnormality in its working. If it sees any abnormality, then it alerts local management and, if configured by the local organisation, it can automatically isolate a machine to stop any malware infection spreading.

ATP also gives advance warning of increased cyber risk by reporting system status against know risk factors via its "secure score" capability. For example where the latest security patches have not been applied or other security features of Windows 10 have not been fully utilised. This allows local organisations to act to minimise vulnerabilities before they can be exploited by an attacker.

Because ATP is provided as part of an NHS national system, the same alerts are used to give an NHS enterprise-wide view of system status, to device level, in real time. This allows the DSC to be able to more quickly and effectively co-ordinate NHS overall response to cyber threats as they evolve. It also allows local organisations to see a developing regional or national threat too.

Windows 10 and ATP Service Overview

The Windows operating system licences provided allow local organisations to use either Windows 7, 8 or 10 version software and deploy ATP to both their existing estate as well as to new devices being deployed.

What are the benefits?

Local Organisations get free Microsoft Windows client software that they would otherwise need to purchase locally from revenue funding. This releases money for direct patient care for five (5) years until April 2023. The software includes ATP functionality that significantly improves local cyber security for an organisation. The software also includes local device encryption (Bitlocker), as well as the Defender Antivirus product and other features. These can replace other locally purchased alternatives and thus save additional local cost

Accountable Care Systems are assured that their constituent organisations are running on secure desktop platforms and can get a clear view of their cyber threat status across their system from their ATP portal.

The NHS collectively has a real time understanding of cyber risks and threats at national level and is better able to respond to cyber threats, in real time as they occur and to ensure that the right interventions are taken to protect the wider system. Through the central purchase of the licensing, the NHS has also obtained a significant cost saving for the licences, releasing NHS money for direct patient care.

What are the costs?

Windows operating system licences including ATP are provided free of charge to local organisations who agree to implement ATP and use the Windows licence fully.

Local organisations will continue to bear the following costs for other elements of their estate, as currently, including:

- Device hardware
- Staff training
- Deployment, operation and maintenance resources

What are the terms?

The terms are included within a Service Agreement between NHS Digital and the local organisation joining the service. The key points are as follows:

- NHS Digital makes the service available until 30th April 2023
- Local organisations provide accurate forecasts for devices installed/licences required, updated at least annually (for Software Asset Management purposes)
- Local organisations must implement ATP within 180 days of licence allocation and maintain ATP throughout the agreement
- Local organisations agree to share their ATP information with NHS Digital Data Security Centre (only)
- Local organisations agree to adhere to the terms of the national agreement with Microsoft that provides the software to them.

How to sign up to ATP and obtain free Windows licences

To sign up, a service agreement with our licensing partner Bytes Software Services needs to be completed and returned. You can contact Bytes via nhsea@bytes.co.uk or by calling 01372 418 763

FAQs

Does my organisation have to join this service?

No. It is optional. However, central funding for Windows operating systems licenses will not be available to organisations who are not part of the service. Also, the enhanced cyber protection that ATP enables at both local and NHS enterprise-wide level will not be available as the local organisation will not be connected.

How do I join the service?

To join, an authorised individual must request a Service Agreement from nhsea@bytes.co.uk.

The sign-up process is electronic. As part of the Sign-Up process you will need to:

- Confirm the details for your primary contact and senior responsible owner (SRO)

- Confirm the numbers of machines of each type (Windows 7,8 and 10) and some other basic details about how you manage your infrastructure.

- Confirm your forecast for the numbers of Windows licences your organisation will need for the next 5 years

- Confirm your plan date for completing your transition to Windows 10

- Confirm the names and the **NHSmail @nhs.net** email addresses for your ATP administrators (note: ATP Administrators must have a valid NHSmail account)

- If you are acting on behalf of a number of other organisations, e.g. a Shared Service or CSU acting on behalf of a number of CCGs, then you will need to confirm the details of which organisations you are including.

Do I have to implement Windows 10 to be part of the service?

Yes. All NHS organisations joining the service must commit to migrating from their current Windows 7/8 estates to Windows 10 by no later than 14th January 2020. The Windows 7 operating system will be unsupported after that date and will thus represent a significant and increasing cyber risk to the whole NHS system. Note that NHS organisations have already successfully migrated more than 160,000 NHS devices to the Windows 10 operating

system[1], and guidance and support to help trusts with their migration is provided as part of the service.

If I do join, can I choose to leave the service at a later date?

Yes, you can choose to leave at any time. On leaving, rights to use the Windows licensing provided will cease and you will need to take out your own new agreement with Microsoft in the usual way, and at your own local cost. Use of ATP will also be discontinued.

Can NHS Digital terminate the service agreement?

Yes, but only in the event of breach by a local organisation. For example, if the local organisation fails to implement or disconnects the ATP feed to the NHS Digital Data Security Centre, or fails to provide required information to allow NHS Digital to manage its Software Asset Management (SAM) obligations to Microsoft. Or if the local organisation breaches any other terms of the national agreement with Microsoft

Can I increase the number of licences at a later date?

Yes. Once your organisation joins the agreement then NHS Digital will provide the number of licences that you need to remain compliant for as long as you remain within the agreement. If the number of licences you need changes then email nhsea@bytes.co.uk to request more.

How has NHS local input been taken into account in developing this service?

We worked with an advisory group of approximately 90 local organisations (trusts, CSUs, CCGs, HIS, CICs etc) to develop the service offering. More than 20 of these organisations acted as early adopters for ATP to prove it prior to full national deployment being authorised.

A user group is being maintained as a focal point for ongoing development of the service during its life. Ongoing NHS feedback is welcomed via atpfeedback@nhs.net

Can I use Long Term Service Branch (LTSB) or do I have to use Current Branch Windows 10

Organisations need to be using current branch windows 10, and must update to latest Windows 10 versions on a minimum annual basis. Note that Advanced Threat Protection (ATP) is a constantly developing service, so new features become available with each release of Windows 10.

The minimum version of Windows 10 that fully supports the NHS way of working in which local organisations have control over their local devices as part of a shared NHS-wide service (using Role Based Access Control) is Version 1703.

---

[1] 160,000 devices as of December 2018

Does ATP just cover Windows 10 or can it also be used with Windows 7 and 8?

ATP can be used on all of Windows 7, 8 and 10 versions and it is a condition of the Service Agreement that ATP is implemented on all devices running these software versions. The functionality for Windows 7 and 8 devices is not as comprehensive as for Windows 10. The ATP service continues to develop with each successive Windows 10 release so new features will become available with successive releases.

Are virtual desktops included?

Yes. Both thick and virtual/thin client deployments can be included.

What does ATP do that my local anti-virus product can't do?

ATP knows how Windows should be working. If anything abnormal happens, it knows that something is wrong, even if it doesn't know exactly what is wrong. Because ATP is an integrated part of the Windows operating system it can then respond immediately to address the issue before it spreads. Since ATP is provided as part of an NHS national system, an alert that there is an abnormality on a device is shared with the NHS Digital Data Security Centre in near real time (minutes). The national picture is also shared with other NHS entities (e.g. other partners within an accountable care system) so all have the visibility of a developing threat that they need to take the appropriate response.

Do I need to keep running a local anti-virus product once ATP is installed?

This is a local choice. The Windows licensing provides both ATP as well as the Windows Defender Anti-Virus product. Local organisations may decide that ATP and Defender Anti-Virus together are a more effective alternative protection to their current arrangements. Or they may wish to continue with their existing anti-virus service. Windows ATP and existing anti-virus solutions can run together and are complimentary.

Does the service monitor servers and mobiles too?

We are piloting this capability. The NHS ATP service is currently licenced only to monitor the desktop/laptop device estate running the Windows desktop/VDI client operating system. The NHS instance of ATP can monitor servers running Windows, or any devices running other operating systems such as IOS, Linux or Android. However, at this point, the various options for such monitor are being considered.

What intervention capability will the NHS Digital Data Security Centre have in my estate?

Local organisations continue to be responsible for managing their estate and will lead on any intervention necessary within their estate. The NHS Digital Data Security Centre team response to any threat identified within a local estate will be managed with the local organisation responsible.

Will other local organisations see detailed information about my estate?

No. Each organisation's information is securely partitioned via Role Based Access Control (RBAC) and the information generated by ATP is available only to the organisation that is responsible for the devices, and the NHS Digital Data Security Centre. All local organisations taking part in the service will however be able to view the national and regional summary information of threat status to better inform their own local threat planning and response.

Where is the information taken by Windows Analytics and ATP held?

For ATP, the data taken from each Windows device is held in a secure private cloud hosted Azure instance for the NHS. Azure is a Microsoft product. ATP data is hosted in the UK, but there are potential occasions where information might be shared outside the UK (e.g. Support Calls) .

Windows Analytics Data (an optional service available under the licence) is not guaranteed to be hosted in the UK.

Note that NHS Digital is responsible for the service as the contracting NHS party. The service meets Crown Commercial Services (CCS) and NHS data security requirements. Please refer to the full Microsoft Service terms for further detail.

A Data Privacy Impact Assessment (DPIA) for ATP from atpfeedback@nhs.net

Do we have to run Windows Analytics?

No. There is no mandatory requirement or central recommendation for local organisations to implement and run Microsoft Windows Analytics. Local organisations may choose to use this Microsoft service or not as they wish.

A Data Privacy Impact advisory notice for Windows Analytics is available from atpfeedback@nhs.net

How does this new service compare to the former NHS Enterprise Threat Detection (ETD) service?

The ETD service ceased in June 2018 and has been superseded by ATP within the NHS.

ETD was an 'after the event' expert analysis provided by Microsoft that is shared back with the NHS. The data used within ETD was sourced from the error reports generated by Windows-based devices across the world. This provided NHS with insight and analysis to help improve our cyber protection and cyber response. ETD was built on the basis of information from a far wider pool of devices than just the NHS. This expertise is essentially replicated by the "Threat Analytics" part of ATP but provided directly to local organisations rather than via the DSC.

ATP is a real time protection service that can spot and respond to issues as they arise even if they have not been seen before ('zero-day attacks'). It generates and makes available a much richer and deeper set of system-level information that can be analysed by local organisations and the NHS Digital Data Security Centre themselves.

Does ATP share personal or patient information with NHS Digital, other NHS organisations or Microsoft?

ATP records machine level information and will flag filenames, but does not access patient records or documents such as word/excel/emails and does not record or share patient information. The only personal information that ATP does record is user ID, in order to identify unusual activity that would indicate a security compromise. For this reason, ATP is accorded a high data security classification and managed accordingly by NHS Digital.

Does this mean I can use any Microsoft products for free?

No. The centrally funded licensing is only available for Windows desktop operating systems, and only for those organisations that agree to implement ATP via the Service Agreement.

The full scope of what is included within the Microsoft Windows E5 licence purchased under this agreement, and the comparison with the Windows Professional or E3 licences that local organisations may currently have is available at https://www.microsoft.com/en-gb/windowsforbusiness/compare

Note that the licences are Upgrade licences. This means that local organisations must have initially purchased their devices with qualifying OEM licences.

How will my current agreements with Microsoft be changed?

Microsoft will novate the relevant Windows licensing from your current agreement to the new NHS Digital national agreement. We recommend that you consider joining the new service prior to your next annual payment date or renewal under your existing agreement so you will not have to make any additional local payments for the Windows software that we can otherwise make available for free.

Do I get a refund for the unused part of my current local agreement for Windows?

No. We therefore strongly recommend that NHS organisations consider joining the new national agreement before their next annual payment or renewal is due.

Do I have to use the Windows operating system for all my devices?

No. ATP provides additional security for devices running the Windows operating system, which represent the vast majority of devices in use in the NHS today. Other devices use other operating systems and local organisations are free to decide which devices they use within their estate. ATP is not currently centrally funded for non-Windows operating system devices.

Which NHS organisations can be part of this agreement?

The principle is that any organisation delivering predominantly NHS funded care can be part of the service. This includes trusts, CCGs, GPs, CSUs and ALBs. It also includes CICs and commercial providers who are providing IT services for NHS organisations.

The service does not currently extend to local authorities, care homes, community pharmacies, dentists and opticians, or independent sector provider non-NHS activities.

When does the agreement end and what happens after?

The service is approved and funded to run for 5 years until 30th April 2023. The decision to cease or continue the service will be taken in sufficient time to allow local organisations to plan to put in place alternative arrangements.

Do I have to manage or report on Windows licensing provided as part of the service?

Yes. NHS Digital is responsible for meeting software asset management requirements for the licensing provided under this agreement and will monitor and report usage and compliance via access to ATP data that local organisations agree to share as part of the service agreement. However, more detailed verification may be required and local organisations must keep their own up to date records of usage of Windows Operating Systems and VDI within their estate.

Is the licensing provided perpetual and can we keep it after the agreement expires?

No. The Windows licensing used within this service is subscription based, so expires on 30th April 2023.

Why do I have to have NHSmail email addresses for my ATP Administrators?

The ATP service needs to validate administrator identity with an Azure Active Directory. Since the vast majority of NHS organisations already have NHSmail accounts (even if it is not their primary/preferred email system) then it was decided to use this existing national resource and its 24 x 7 service support arrangements rather than replicate elements of it solely for ATP.

Note that you cannot use your own local Active Directory to validate identity for ATP administrator accounts, nor can you connect or integrate it with the ATP service.

What are the Service Support Arrangements?

We expect to be able to issue licence keys within 48 hours of acceptance of a correctly completed Service Agreement. This process is managed by our licensing partner Bytes.

The **ATP Implementation Guide** explains how to set up and deploy ATP. This guide is provided to the nominated contacts in the Organisations' Service Agreement.

The **ATP User Guide** explains how to use and manage ATP once live. Again, this is provided to nominated contacts in the Organisation's Service Agreement.

For any implementation and service issues not covered by the above organisations should contact atpfeedback@nhs.net

Do we have to reactivate Windows 10 licence keys?

No. You do not need to reinstall or reactivate existing licence keys for your estate, but please use the new licence keys provided going forwards.

How are major clinical and applications providers being managed to ensure their compliance with Windows 10?

The NHS Digital Windows 10 and ATP programme team and Microsoft will be working closely with the major national applications vendors to ensure that they maintain compliance with Windows 10. This will include applications managed by NHS Digital and other central NHS organisations as well as commercial vendors. Further details will be provided at a later date as part of the wider Service Management regime to support the national roll out.

Where can I get more information about Windows Advanced Threat Protection?

Please contact atpfeedback@nhs.net