Azure Advanced Threat Protection (Azure ATP) Overview

What is Azure ATP?
Azure ATP, is a new cloud service which helps security team to detect and investigate advanced attacks and insider threats across the entire scope of users and entities in the network – On premises, cloud and hybrid environments.

Azure ATP fuses together unique machine learning algorithms, world-class security research, and the breadth and depth of the Microsoft security graph. It will help protect from both known and unknown attack vectors, aiming to detect threats early in the kill chain before they mature into actual damage.

Azure ATP brings the capabilities of our current on-premises behavioral analytics solution, Microsoft Advanced Threat Analytics (ATA), to the cloud. Building on the in-depth threat detection capabilities of ATA, Azure ATP will help our customers protect their identities.

When will Azure ATP be released in GA (General Availability)?
Azure ATP GA is planned for Q1CY2018.

How will Azure ATP be licensed?
We have not yet announced the pricing or licensing model for Azure ATP. This will be announced closer to the GA release date.

How does Azure ATP differ from what Windows Defender ATP and Office 365 ATP do?
Windows Defender ATP protects and detect malicious activity on end points. Office 365 ATP protects against malicious E-mails (attachments and links). Azure ATP detects and helps investigate compromised accounts and Active Directory specific attacks, based on behavioral analytics and detection of known advanced persistent threats.

What data does Azure ATP collect?
Microsoft will collect and store information from your configured servers (e.g. domain controllers, member servers) in a database specific to the service for administration, tracking, and reporting purposes.

Information collected includes network traffic to and from domain controllers (such as Kerberos authentication, NTLM authentication, DNS queries), security logs (such as Windows security events), Active Directory information (structure, subnets, sites) and entity information (such as names, email addresses and phone numbers).

Microsoft uses this data to:
• Proactively identify indicators of attack (IOAs) in your organization
• Generate alerts if a possible attack was detected
• Provide your security operations with a view into entities related to threat signals from your network, enabling you to investigate and explore the presence of security threats on the network.

Microsoft does not mine your data for advertising or for any other purpose other than providing you the service.

Do I have the flexibility to select where to store my data?
When onboarding the service for the first time, you can choose to store your data in Microsoft Azure datacenters in either the United States or Europe. Once configured, you cannot change the location where your data is stored. Microsoft will not transfer the data from the specified geolocation.

Is my data isolated from other customer data?
Yes, your data is isolated through access authentication and logical segregation based on customer identifier. Each customer can only access data collected from its own organization and generic data that Microsoft provides.

How does Microsoft prevent malicious insider activities and abuse of high privilege roles?
Microsoft developers and administrators have, by design, been given sufficient privileges to carry out their assigned duties to operate and evolve the service. Microsoft deploys combinations of preventive, detective, and reactive controls including the following mechanisms to help protect against unauthorized developer and/or administrative activity:

• Tight access control to sensitive data
• Combinations of controls that greatly enhance independent detection of malicious activity
• Multiple levels of monitoring, logging, and reporting

Additionally, Microsoft conducts background verification checks of certain operations personnel, and limits access to applications, systems, and network infrastructure in proportion to the level of background verification. Operations personnel follow a formal process when they are required to access a customer’s account or related information in the performance of their duties.

Azure ATP Vs. Advanced Threat Analytics

What is the difference between Azure ATP and ATA?
Azure ATP uses on-premises Active Directory data as one of its data sources, but beyond detecting just on-premises Active Directory specific attacks and threats, it is focused on hybrid environments and integration with other cloud services.

ATA is an on-premises product that helps to protect enterprises from multiple types of advanced targeted cyber-attacks and insider threats.
We have ATA Lightweight Gateways running on our domain controllers. What is the best practice to deploy Azure ATP?

Azure ATP uses a different “Sensor” than the ATA Lightweight Gateways. If you’d like to enjoy the functionality of Azure ATP, then you should gradually remove ATA Lightweight Gateways from DCs and install Azure ATP Sensors on those DCs.

It is not supported to deploy both Azure ATP Sensor and ATA Gateway on the same server.

Technical FAQ

What is the tech community website for Azure ATP?
http://aka.ms/azureatpcommunity

What are the prerequisites for Azure ATP?
Connectivity from the domain controller or from the Standalone Sensor to Azure ATP cloud service, *.atp.azure.com on port 443. Both firewall and proxy connections are supported.

What is the update process for Azure ATP sensors?
There are 2 types of updates for Azure ATP Sensors:

As cloud service, we expect the service to update very frequently (several times a month) so we introduced a new update concept in the sensor side called “Evergreen” – this means that as long as there are very minor changes to the Sensor, the Sensor is able to upgrade itself while running (with almost zero downtime). Those upgrade is transparent and is not involving any risk to the operating system (think about AntiVirus upgrades).

Azure ATP has “major” upgrades that will require full MSI install on the Sensor, for that there's a part of the configurable toggle button that allows you to control whether major updates are being done automatically. This scenario should be very rare as most of updates will be minor using the Evergreen method mentioned above.

We follow a standard change control and testing process where we first update non-production environments. Only when this is completed and validated do we move to production. How can this be achieved with the Azure ATP Sensor?
We recommend excluding the Sensor minor updates from this policy, as this is not a full product upgrade, but rather an ‘agent refresh’. If you do not apply this policy on Antivirus signature/upgrades, then you shouldn’t apply it on the Azure ATP Sensors.
I have noticed that all Sensors updated from version X to version Y - What is the expected update frequency of Sensors?
Several times a month. During the preview phase of Azure ATP, it might be even more frequent.

**Sensor Performance** - I see high CPU usage on my domain controllers, and it looks like the Sensor agent is causing it. Should I be concerned?
The sensor will use CPU if it is available, and this should not be a problem. If other processes need the CPU resources and the sensor service prevents that from occurring, then the problem should be reported to Microsoft.

After successful installing the sensor, the service won't start. The service is stuck at “Starting”. What might be wrong?
Check the sensor log directory under c:\program files\azure advanced threat protection sensor. If you see this error - "System.DirectoryServices.Protocols.LdapException: The supplied credential is invalid." - then you will need to review the user defined on the Configuration page Under Directory Services. This should be a valid username/password combination for your on-premises AD environment.

We already have Azure Security Center/Log Analytics. Does Azure ATP need its own separate workspace? Can we link them?
Right now, Azure ATP is not connected to Azure Security Center. Azure ATP has its own management portal within your organization's Azure Active Directory tenant so it is managed separately.