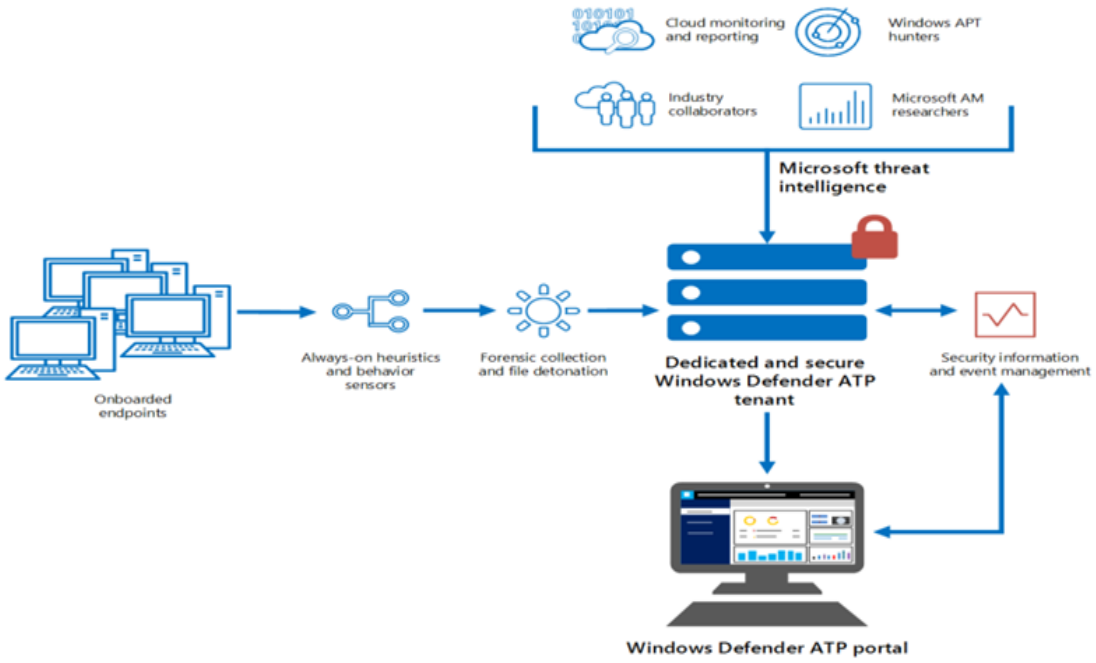
Windows Defender Advanced Threat Protection

WHAT IS ADVANCED THREAT PROTECTION

In todays' world Cyber threats are emerging more frequently and prevalently. It becomes tough job for any organizations to be able to quickly assess their security posture, including impact, and organizational resilience in the context of specific emerging threats. Avoiding malware attacks and hacking of sensitive information and data is the prime concern of an organisation. Windows Defender ATP is one of the most effective solution these attacks and threat analysis.

Windows Defender ATP (Advanced Threat Protection) is a cloud based centralized management console to correlate alerts and manage defences against sophisticated malware, hacking-based attacks targeting sensitive data and threat analysis.

Advanced Threat Protection (ATP) refers to a category of security solutions that defend against sophisticated malware or hacking-based attacks targeting sensitive data. It is ISO 27001 certified security platform for intelligent cyber threat protection, detection, investigation, and response. . It protects endpoints from cyber threats, detects advanced attacks and data breaches, automates security incidents, and improves security posture and data privacy.



The ATP comprises of *Endpoint behavioural sensors*, *Cloud security analytics* and *Threat Intelligence* which makes the platform unique and different from other threat protection softwares and services.

The primary goal of ATP are:

- *Early detection:* Detecting potential threats before they have the opportunity to access critical data or breach systems.
- *Adequate protection:* The ability to defend against detected threats swiftly.
- *Response:* The ability to mitigate threats and respond to security incidents.