

## HOW ADVANCED THREAT PROTECTION WORKS

The primary agenda of Advanced threat Protection are *Early detection* (detecting the threats before they have access to the critical and sensitive data or breach systems), *Adequate protection* (the capability to defend against detected threats swiftly), and *Response* (the capability for mitigation of threats and response to security incidents).

To achieve the goal for advanced threat protection services and solutions must offer several components and functions for comprehensive ATP:

- *Real time visibility*: With continuous monitoring and real time visibility, an early approach to a threat can be taken which can save from tremendously costly resource utilization and data information.
- *Context*: For security effectiveness, threats are prioritize and responses are organised effectively.
- *Data awareness*: There should be proper understanding of the organisational data, its sensitivity and value and also other factors that contribute to the formulation of an appropriate response.

The three key areas where ATP mainly focuses are:

- Halting or mitigating the threat before it breaches the system.
- Counter actions that have already occurred due to an attack.
- Interrupting the progress of threat ensuring it doesn't proceed further.

## BENEFITS OF WINDOWS DEFENDER ATP

Advanced threat protection services gives benefit in providing access to a global community of security professionals and organisations for dedicated monitoring the network, tracking, and sharing information about emerging and identified threats. ATP service providers have access to the global threat information which are sharing over the networks, augmenting their own threat intelligence and analysing the information with third parties. When a new threat is been detected, ATP service providers update their defenses to ensuring protection against the threat. This global community plays an important role in the maintenance of the security of enterprises around the world.

Organisations tend to implement the advanced threat protection for better detection of threats in early stage and which can help quickly to formulate a response to minimize the damage and recover an attack occurred. A good security provider focuses on the lifecycle of an attack and manage threats in real-time. ATP providers immediately notify the enterprise regarding the attacks that have occurred, its severity level and the response which could be initiated to stop the threat in its tracks or minimize the data loss. Advanced threat protection solutions helps in securing critical data and systems either in-house or as a service, no matter where the attack originates or how major the attack or potential attack is perceived.