- Incidents
- Integration with Microsoft Cloud App Security
- Onboard Windows Server 2019
- Onborad previous versions of Windows
- Create and build Power BI reports

Conclusion

For a better security platform for intelligent protection, detection, investigation and response, Windows Defender ATP comes into picture. It protects endpoints from cyber threats, detects advanced attacks and data breaches, automatically generate security incidents and improves security posture of the organisation.

The dashboard of Windows Defender ATP which is centralized and customized by the organisation according to their data information and security levels comprising of the security operations, security score, threat analysis, active alerts, machine information which are at risk, alert queue, automated investigation and many more. Windows Defender ATP providers notify the enterprise of attacks that have occurred, the severity of the attack, and the response that was initiated to stop the threat in its tracks or minimize data loss.

For better security awareness and alerts regarding the threat detection, data information security, early response to detected malware and vulnerability, protection for network devices, email gateways and many more in a centralized console for an organisation, Advanced Threat Protection (ATP) plays a major role.

To minimize the damage and data loss and recover an attack, Windows Defender ATP is the most appropriate and recommended advanced threat protection solution. Through the power of the cloud, machine learning and behavior analytics, Windows Defender ATP provides connected pre-breach protection.

References:

- https://github.com/MicrosoftDocs/windows-itpro-docs/blob/master/windows/security/threat-protection/windows-defender-atp/preview-windows-defender-advanced-threat-protection.md
- https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection