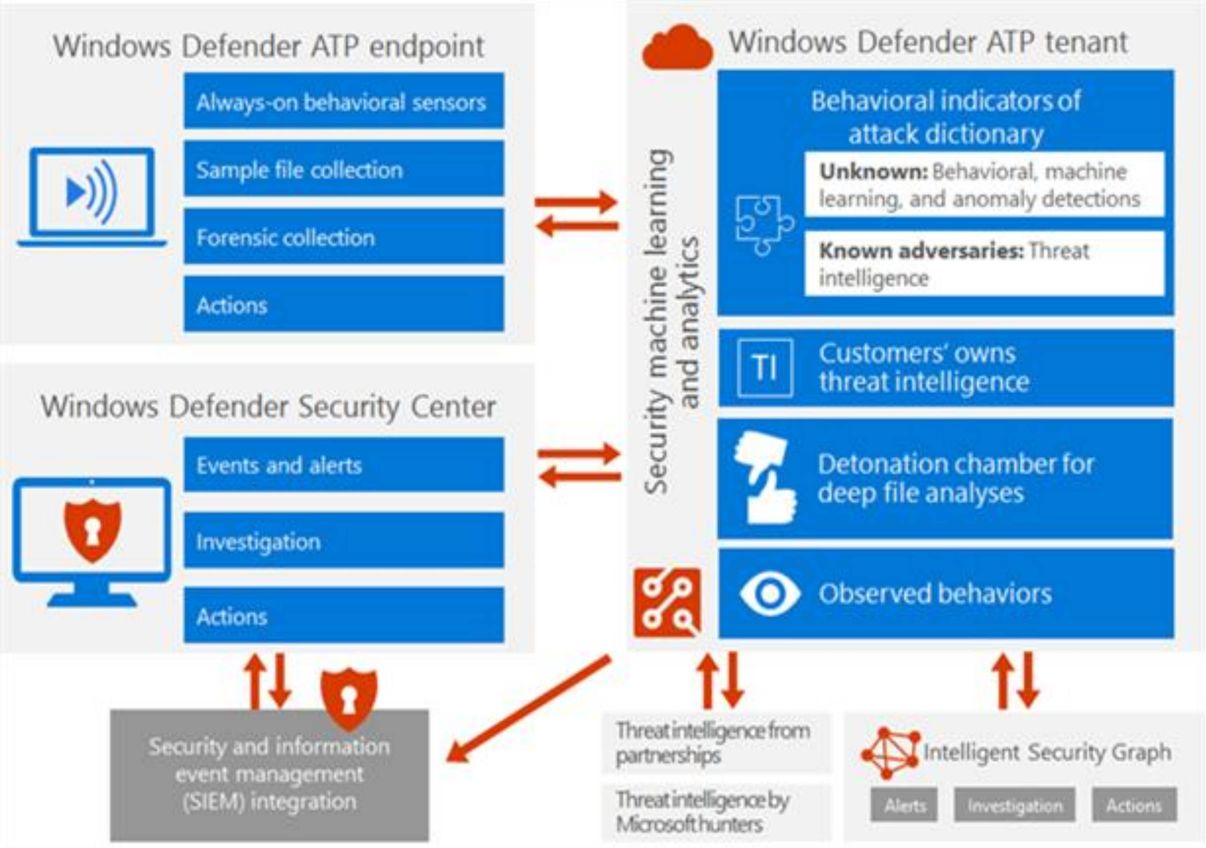
Microsoft Defender ATP Architecture:

Microsoft looked to the capabilities of the cloud to help address the challenges of monitoring and protecting our corporate network from advanced adversaries and threats. Microsoft Defender Advanced Threat Protection (ATP) combines built-in behavioral sensors, machine learning, and security analytics that quickly adapt to changing threats. With this threat intelligence, Microsoft Defender ATP helps us investigate and respond to advanced threats faster and more precisely than ever before.

Architecture:


Windows Defender ATP endpoint
Always-on behavioral sensors
Sample file collection
Forensic collection
Actions
Windows Defender Security Center
Events and alerts
Investigation
Actions
Security machine learning and analytics
Windows Defender ATP tenant
Behavioral indicators of attack dictionary
Unknown: Behavioral, machine learning, and anomaly detections
Known adversaries: Threat intelligence
TI
Customers' owns threat intelligence
Detonation chamber for deep file analyses
Observed behaviors
Security and information event management (SIEM) integration
Threat intelligence from partnerships
Threat intelligence by Microsoft hunters
Intelligent Security Graph
Alerts
Investigation
Actions

Microsoft Defender ATP consists of three main components:

- **Microsoft Defender ATP endpoint behavioral sensors:** These sensors collect and process behavioral signals from the operating system and sends this sensor data to your private, isolated, cloud instance of Microsoft Defender ATP.
- **Microsoft Defender ATP Cloud Security Analytics:** Leveraging big-data, machine-learning, and unique Microsoft optics across the Windows ecosystem, enterprise cloud products (such as Office 365), and online assets, behavioral signals are translated into insights, detections, and recommended responses to advanced threats.
- **Microsoft Defender ATP console in the Defender Security Center**: Security analysts use the web-based Microsoft Defender Security Center to access our Defender ATP data and interact with onboarded endpoints and servers to further research or defend against malicious activity. The Microsoft Defender ATP console is where analysis really happens— it provides a dashboard,

an Alert queue, Machine view, File view, User view, and Search— which can be used to find data about machines, files, users, URLs, and IPs within the enterprise.

Onboarding Methods:

1. Using Local Script
2. Using SCCM
3. Using Group Policy
4. Using Azure Security Center