

Is Windows Defender Advanced Threat Protection the Best Solution for Digital Health and Care Wales?

ATP - £100,000

- Safe attachments & links – monitors attachments and links to protect against phishing emails.
- Real-time protection – client runs in background of systems to detect threats in real time.
- Attack simulation training – can simulate attacks to test level of protection for systems.
- Advanced hunting – use custom queries to detect known threats, and ensure systems are protected.
- Threat analytics – able to score threats to enable prioritization of mitigations.
- Alerts/ incidents – alerts are not overloaded with information and provide a timeline of changes to the system.
- Reports – multiple reports which can be provided to key decision makers.
- Single console – console has a clean design and is simple to achieve desired actions.
- XDR capabilities – enhanced unified security.
- Machine learning.

	Crowd Strike	ATP	TrendMicro
Payload	Safely detected	Safely detected	Safely detected
WannaCry	Detected and blocked	Detected and blocked	System infected
MS simulation	Detected and blocked	Detected	Detected
TrendMicro Simulation	Detected	Detected	Detected as expected
Ransim	Safely detected – did not even allow installation.	Detected – threats removed.	Detected in console but didn't protect system

TrendMicro - £1,135,030.35 (pa)

- Support for legacy systems.
- 3500 whitecap researchers to detect threats globally.
- Integration with Microsoft API's.
- XDR capabilities – enhanced unified security.
- Third party integration.
- Virtual preemptive patching – patches to vulnerabilities released before vendor,
- Automated sandboxing.
- Day zero threat protection – ability to release patches for vulnerabilities before even the product vendors.

CrowdStrike - £128,000

- Machine learning.
- Custom blocking (whitelisting and blacklisting)
- Exploit blocking.
- IOA (Indicators of Attack) prevention.
- Additional protection specific to ransomware.
- Single console.
- Security Threat Alerts
- API integration.
- Sandbox



May 2017, NHS England “identified 45 NHS organisations including 37 trusts that had been infected by the WannaCry ransomware. In total at least 81 out of 236 trusts across England were affected. A further 603 primary care and other NHS organisations were infected by WannaCry, including 595 GP practices” .

The WannaCry virus was effective due to an exploit known as EternalBlue, and backdoor called DoublePulsar.

EternalBlue is an exploit that takes advantage of a vulnerability in mainly windows operating systems which have desktop operating systems older than and including Windows 7, and Server operating systems before Windows Server 2016; essentially all systems which still make use of the legacy SMBv1 protocol. Older operating systems have this enabled by default, whereas newer operating systems disable this by default (largely in response to the EternalBlue vulnerability).

