

Supplementary Budget – Briefing Note

2022 Budget

End User Device Security

Briefing Note required for:

- items +/- \$50,000 or more
- changes in FTE
- Council Priority requests

Dept	Division	Item	Base Supp	Amount	FTE Impact
FBITT	ITT	Defender for Office 365	B	\$40,000	

Background:

The most common method that malicious software is spread to our devices is through links and attachments in e-mails or documents shared to the user by an external party.

Defender for Office 365 is a product which attempts to protect end user devices from viruses, phishing and e-mail compromise by testing links, attachments and shared documents before the end-user has the option to view them. The product runs across the entire Office 365 suite of applications including: Outlook, Teams, OneDrive, SharePoint, etc. Whenever a link, attachment or shared document is presented to a user, Defender will open it in a protected virtual space to look for potentially malicious intent. If the item passes the inspection, the user has the option to proceed. If malicious intent is suspected, the user is prevented from opening it, but an administrator can override this.

This offers better protection than traditional anti-virus for two reasons:

- 1) Links, attachments, and shared documents are tested before they are opened on your computer. Traditional anti-virus scans files after they are on your machine.
- 2) Traditional anti-virus works like a vaccine. It must know about the virus before it can remove it. Defender for Office 365 watches the behaviour of the item it is opening. This allows for a greater possibility of protecting us against something there is no patch for yet.

Comment:

