Spotlight on shadow IT

New guidance to help organisations manage rogue devices and services within the enterprise.

Simon B

'Shadow IT' (also known as 'grey IT') is the name given to those unknown IT assets used within an organisation for business purposes.

Whilst often thought of in terms of rogue devices connected to the corporate network, shadow IT can also apply to cloud technologies or services. For example, if users are storing sensitive, enterprise data in their personal cloud accounts (perhaps to access the data from another location or device), then that's also shadow IT. Most organisations will have *some* level of shadow IT, even if they don't realise.

Whatever format it takes, if shadow IT is *prevalent*, then risk management becomes very difficult because your organisation won't have a full understanding of what you want to protect. To help with this, the NCSC has published new guidance that shines a light on shadow IT. The guidance helps system owners and technical staff to better mitigate the presence of unknown (and therefore unmanaged) IT assets within their organisation.

As the guidance explains, it's important to acknowledge that shadow IT is rarely the result of malicious intent. It's normally due to staff struggling to use sanctioned tools or processes to complete a specific task. And if they're resorting to insecure workarounds in order to 'get the job done', then this suggests that existing policies need refining so that staff aren't compelled to make use of shadow IT solutions.

For this reason, the guidance recommends *organisational mitigations* to address shadow IT, as well as a range of technical solutions (including asset management and network access controls). The guidance also points out that the very existence of shadow IT presents you with learning opportunities; your security team should focus on finding where shadow IT exists, and where possible, bring it above-board by addressing the underlying user needs that the adoption of shadow IT is seeking to address.

For example, if staff are using unsanctioned messaging or video conferencing services (with no monitoring in place), then you should provide an approved, supported service that addresses this business need.

Where shadow IT is discovered, it's important you **don't** reprimand staff. If you blame or punish staff, their peers will be reluctant to tell you about their own unsanctioned practices, and you'll have even less visibility of the potential risks. For this reason, the guidance also points out the importance of developing a good cyber security culture, so that staff will be able to communicate openly about issues (including where current policy or processes are preventing them from working effectively).

Organisations tackling shadow IT should understand that technical controls are only part of the solution. By identifying the user needs of your organisation, you can gain insight into why shadow IT happens in the first place, and then respond strategically to help prevent future instances.

Simon B
Security Researcher, NCSC

WRITTEN BY

Simon B
Security Researcher, NCSC

PUBLISHED

27 July 2023

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

PART OF BLOG

NCSC publications