Shadow IT

Managing 'unknown assets' that are used within an organisation.

This guidance helps you to better identify and reduce the levels of 'shadow IT' in your organisation. It's been written for system owners and technical staff, so that they can better mitigate the presence of *unknown* (and therefore *unmanaged*) IT assets within their organisation.

What is shadow IT?

The term 'shadow IT' (also known as 'grey IT') refers to the unknown assets that are used within an organisation for business purposes. Since these are not accounted for by asset management, nor aligned with corporate IT processes or policy, they're a risk to your organisation. This could result in the exfiltration of sensitive data, or spread malware throughout the organisation.

Whilst often thought of in terms of devices, shadow IT also applies to cloud technologies. For example, if users are storing sensitive, enterprise data in their personal cloud accounts (in order to access it from another location or device), this is also shadow IT because the personal cloud storage probably isn't covered by your organisation's risk management process. Most organisations will have *some* level of shadow IT, but if shadow IT is *prevalent*, risk management becomes more difficult because you won't have a full understanding of **what** you need to protect, and what you value most.

It's important to acknowledge that shadow IT is rarely the result of malicious intent. It's normally due to employees struggling to use sanctioned tools or processes to complete a specific task, so they'll adopt unofficial measures to help them complete their work.

Some common reasons that lead to shadow IT include:

- not having enough storage space
- not being able to share data with a third party
- not having access to necessary services (for example development tools)
- not having a sanctioned video conferencing (or instant messaging) tool
- not being able to request assets or services through a corporate system (or the process for doing this being ineffective/slow)
- approved tools or SaaS services not providing the required functionality
- not realising that use of devices or personally managed SaaS tools might introduce risk

Shadow IT is not BYOD

With an effective BYOD policy, your organisation has ownership and some level of control of corporate data and the resources permitted on the users device, allowing the risk to be managed. This is **not** the case with shadow IT. There might not be a risk, there might be a critical risk. The organisation simply doesn't know. Shadow IT is therefore an unmanaged risk.

What can you learn from shadow IT?

Though clearly not desirable, the existence of shadow IT presents your organisation with learning opportunities. If employees are having to resort 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 shadow IT solutions. Security people should focus on finding where shadow IT exists, and where possible, bring it above-board by addressing the **underlying user needs** that shadow IT is seeking to address.

Most importantly, you should always take a positive and no-blame approach to people who have been forced into adopting shadow IT. 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.

Types of shadow IT

This section covers the main ways that shadow IT is most likely to manifest in your organisation, and the threats this may introduce.

Unmanaged devices

A widely understood area of shadow IT is unsanctioned devices on a network. This can include:

- personal devices belonging to employees on the core enterprise network
- equipment providing a critical service that is incorrectly configured
- IoT or other smart devices employees have introduced without security approval (smart doorbells, digital assistants, printers, etc.)
- wifi access points to provide coverage or types of access that the organisation has not provided
- servers or VMs brought in by an employee (or contractor) to provide a service without approval

Any device or service that's not been configured by your organisation will probably fall short of the required security standards, and could damage the network and your services (by introducing malware, for example). They could also be added into botnets or become cryptominers, causing additional damage.

Unmanaged services

Less well understood are shadow cloud services. This can include:

- unapproved messaging or video conferencing services with no monitoring in place
- external cloud storage services to share files with third parties (or to allow staff to work from home using an unauthorised device)
- using third-party tools that could be gathering corporate information
- unmanaged cloud tenancies used by developers as testing environments

- project management or planning services used as an alternative to corporate tooling
- code stored in unmanaged repositories

Threats posed by shadow IT

Shadow IT can introduce threats not present on corporate IT. This can include:

1. **Data theft**
   Many of the controls that organisations apply to devices and services (such as encryption and allow/deny listing) are unlikely to be applied effectively on shadow IT. Protecting data is a concern as you can't be certain where your data is, where it is being processed, or where it ends up. If you don't have control of the services processing data (or devices that hold data), you can't be sure appropriate backups are being made. This can expose an organisation to threat of ransomware, legal issues around data handling, reputational damage and recovery costs.
2. **Exploitation of services or devices**
   Controls such as well-configured firewalls, application allow listing, antivirus software and multi-factor authentication (MFA) can help to reduce the risk of compromise. For shadow IT, you can't assume that these controls are in place. This applies not to just traditional work devices (such as phones, laptops and PCs), but also embedded devices that have an internet connection that have been set up (for example) by a building manager. This can expose an organisation to the threats from malware (including ransomware), network monitoring, and lateral movement.

Mitigations for shadow IT

At all times, you should be actively trying to limit the likelihood that shadow IT can or will be created in the future, not just addressing existing instances.

Organisational mitigations

It is important to re-iterate that most shadow IT is typically **not** the result of intentional rule-breaking, rather the result of staff trying to 'get their job done' where corporately-provided equipment and services are not adequate. In many cases, staff may not realise that they are placing the organisation at risk.

More specifically, organisations should:

- Avoid unnecessary lockdowns of enterprise IT, such as preventing external collaboration with cloud storage, or not having an instant messaging platform. If you can anticipate your users' needs, you may be able to prevent shadow IT from starting.
- Implement an effective and simple process for addressing users' requests, which should be put in place as quickly as possible. Again, if users don't feel their needs are being addressed promptly, it encourages them to implement their own solutions.
- Have processes whereby users can quickly get access to services that might be outside what is normally available, in a controlled way, and that can be brought under increasingly tight control as needed.
- Introduce processes that can bring the unsanctioned service under control, such as by migrating data into corporately supported platforms.
- Develop 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. A healthy cyber security culture makes it more likely for people to report instances of shadow IT. They will be reluctant to come forward if they fear they (or other members of staff) will be reprimanded. In other words, a poor security culture means you're much less likely to detect shadow IT.

Help with addressing specific user needs

The NCSC has produced a range of guidance that can help organisations address common technology challenges in a safe and secure manner. By providing these services, you may prevent your staff adopting shadow IT to fulfil their genuine user needs:

- guidance on choosing an enterprise instant messaging solution
- guidance on choosing a video conferencing service that meets your business needs
- guidance on how to deploy and use a cloud service securely

- guidance on how to make sure your organisation is prepared for an increase in homeworking

Technical mitigations

There are a range of technologies and commercial solutions that can help organisations manage the risk of shadow IT on the enterprise network. This includes X.509 certification, network scanners, cloud access security brokers (CASBs), secure access secured edge (SASE), and unified endpoint management (UEM).

+ Show all

Network access controls Show

Asset management Show

Network scanners Show

CASB Show

UEM Hide

Unified Endpoint Management (UEM) tools seek to monitor, manage and secure your organisations end point devices from a single dashboard. If deployed well, then any device connecting to the network that isn't owned by the organisation should be identified as shadow IT, at which point you then either remove it, enroll it, or adopt it. However note that in large organisations, onboarding many different classes of device can be highly resource intensive.

PUBLISHED

27 July 2023

REVIEWED

27 July 2023

VERSION

1.0

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector