SHADOW IT

Cheat Sheet

Addressing Hidden Gaps in Network Security

thirdpartytrust

Shadow IT → Unsanctioned hardware, services, and apps that put your business at risk.

Your network contains blind spots of unauthorized access to company data. Cloud computing and remote work are increasing this risk. As the last line of defense in protecting your company's data, here are the steps you should take:

32% of employees use unapproved Cloud-based tools[1].

91% of IT teams compromise security for continuity[2].

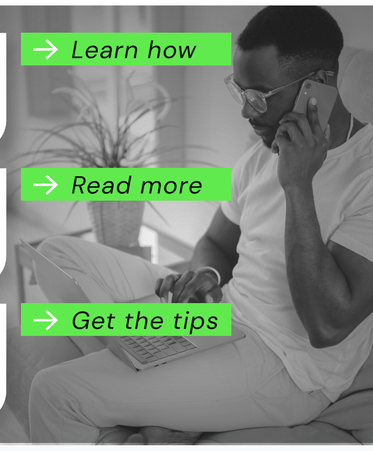
Detecting Shadow IT

1. Establish routine security reviews and education to discover hidden assets in your network. Audit hardware, software, and Cloud services regularly.
2. Classify newly found Shadow IT assets into these categories: Sanctioned, Authorized, or Prohibited. Set deadlines for compliance.
3. Embrace the Shadow IT assets that become authorized, and bring them into line with your security standards.

→ *Learn how*

→ *Read more*

→ *Get the tips*



Addressing Shadow IT

Use these discovery questions:

- ☑ What business need, if any, does this asset satisfy?
- ☑ Do any of our approved tools already cover that need?
- ☑ Is there any other solution that IT could provide?
- ☑ What risks does the Shadow IT asset create?
- ☑ Does the asset benefit many and outweigh the risks?

Make a decision:

- ✓ AUTHORIZE
- ✓ SUBSTITUTE
- ✓ DISCONTINUE

Eliminating Shadow IT

1. Allow for the right tools

Ask employees what tools they need (productivity, collaboration, file-sharing, etc.) and authorize them, so there's no need to turn to personal accounts and Shadow IT.

2. Make binary decisions

Decide if tools are "necessary" or "nice" for your business. Anything deemed "nice" should either be discontinued or put into a vetting process.

3. Offer continuous training

Share policies, recommendations, and best practices to bring everyone up to speed on changing threats and how to protect the organization.

4. Document a policy

Build a non-restrictive company-wide policy covering remote work, and make it easy to involve IT when there's a need for new tools.
Read more >>

5. Enforce strong passwords

Ensure new accounts have unique and strong passwords; make it easier by institutionalizing a password management tool.
Read more >>

6. Use a multi-layered approach

Complement your Shadow IT policy with essential security measures, such as VPNs, MFA, antivirus, encryption, backup, patch management, etc.

7. Leverage dedicated technology

Automated continuous monitoring, network discovery, and risk assessments can be your allies. Read more >>

We can help you find and address Shadow IT in your network.

→ *Get started*

Sources | [1] *2022 Workplace trends & insights report, Beezy* | [2] *HP Wolf Security Report 2021, HP*