Shadow IT and its significance in modern B2B environments

Imagine a castle that is safe from intruders because of the complexity of the design and the presence of guards who don't allow any trespassing. This castle stands firm in its position until some insider sabotages security by inadvertently opening a gateway from inside without the knowledge of the guards.

Shadow IT is similar to the story of Trojan horses and insider threats in a B2B environment. Just like the inadvertent actions of guards expose the castle to intruders, employees may unknowingly open a gateway for cybercriminals by introducing vulnerabilities through unauthorised software or devices.

This part of information technology that employees, for their convenience, bring into use without the knowledge of IT administrators comprises shadow IT. It's the use of unauthorised software or IT resources in an enterprise network that has not been officially approved or assigned by the IT team itself.

Although an old-school problem, shadow IT still breathes life into modern cybersecurity concerns. Research by CISCO revealed only 8% of enterprises know the scope of shadow IT use within their organisation when 80% of end users rely on software without clearance by IT and 83% of IT staff administrators admit to using unsanctioned software or services.

Shadow IT is likely to gain momentum in organisational settings as people become more tech-savvy. According to predictions by Gartner experts, 75% of employees will likely acquire, modify, or create technologies outside of IT's visibility by 2027. With numerous risks lurking within, organisations must implement measures that can put shadow IT at bay. Let's understand how.

Reasons why shadow IT emerges within organisations

The desire for increased productivity often leads employees to use unauthorised tools, which contributes to the formation of shadow IT. The goal

here is the efficiency that comes with downloading unofficial tools. For a while, what appears to be unlocking the key to productivity may soon expose the organisation to security threats.

Shadow IT may not always result from employees alone; sometimes, teams are also responsible for its adoption. According to Gartner, business leaders make 38% of technology purchases instead of IT. When teams want to adopt new cloud services, SaaS applications, or any other technology, they have to undergo the procurement process implemented by IT and the CIO.

They approach the IT teams for approval to comply with the company's policies. Often, approval for new apps in a company's IT infrastructure is a cumbersome and lengthy process. This gap in attending to user requests or complaints causes frustration. It causes employees or teams to take shortcuts and take it upon themselves to do away with administrative processes and get work done their own way. As soon as they bypass the cyber protocols meant to safeguard the system, attackers gain access to an unsupervised and unprotected attack surface.

Ever since the pandemic, with remote work gaining popularity, there has been an uptick in employees' reliance on personal devices. Additionally, Bring Your Own Device (BYOD) policies have led to employees becoming a top target. The presence of widely found unauthorised software on such devices provides attackers with easy access to the more secure network of the company.

What are some shadow IT examples?

Hardware

Personal devices of employees—laptops, tablets, and computers—as part of the BYOD policy may be monitored by IT for security purposes. However, employees also bring a variety of unmonitored devices, including IoT devices, USBs, smartwatches, server devices, and smartphones, to the office spaces. If these devices have been previously connected to the organisation's Wi-Fi network and are in range again, the account settings allow them to automatically reconnect. These devices do not have the company's security software installed, and the IT department does not monitor them. They, therefore, have the potential to expose sensitive official data to unauthorised parties.

Shadow software

The distinction between IT-approved and shadow software lies in approval and management. Shadow software is an umbrella term for software applications brought into use on a quotidian basis by employees without the knowledge of the IT department. Examples include utility apps like password managers, VPN clients, and remote access apps; messaging apps like WhatsApp and Telegram; and collaboration tools like Slack, Trello, and Asana.

These applications become an entry point for attackers if the responsible IT team does not install them and the employees decide to take it upon themselves to install free, personal apps downloaded from the internet. These applications tend to be safe when officially assigned, but take a risky turn when used outside of the approved channels.

OAuth protocol

Authorization frameworks like the OAuth protocol are increasingly gaining ground for their convenience in allowing users to access third-party applications without sharing credentials. Even though these frameworks provide granular access control, repeated pop-ups can cause consent fatigue, leading users to grant extensive permissions—connecting to or authorising access to other apps.

Some third-party apps may thus get to collect and store corporate resources, like cloud storage, without the approval of the IT team. The communication between the third-party application and resource server (e.g., API endpoints), which is encrypted in nature, won't allow traditional DLP systems to detect sensitive data leakage. These behaviours by employees, without being mindful of the implications, can unintentionally expose sensitive data about organisations.

Risks associated with shadow IT

Integration challenges

Shadow IT may not well coordinate with the sanctioned IT infrastructure due to variations in technology stacks, protocols, or standards. Differences in data formats, APIs, or business processes do away with technical compatibility,

obstructing a seamless exchange of data between systems. Workflow that takes into account shared information across IT infrastructure for a comprehensive view of the company's operations thus gets disrupted.

Shadow IT resources are not incorporated as a part of IT provisioning for a given department. If the IT teams happen to introduce any changes to the network or network resources, the lack of alignment with sanctioned IT infrastructure may result in data inconsistencies, duplication of efforts, or even security vulnerabilities.

Compliance issues

Organisations dealing with sensitive data about individuals are subject to stringent compliance regulations. Shadow IT increases the likelihood that products and services, along with their vendors, bypass any due diligence before entering the organisation's IT infrastructure.

If apps used by workers fail to adequately secure and archive data as per the requirements of the data protection laws, they become susceptible to regulatory scrutiny. For example, patient data stored by IT users of a healthcare institution in shadow IT storage solutions creates additional points for audits.

In this case, they may be required to audit, identify, and disclose the scope and impact of each incident. This not only exposes sensitive data to potential breaches but also puts the organisation at risk of non-compliance with data protection laws like HIPAA and GDPR.

Data security breaches

Organisations, unaware of shadow IT usage, may never know if threat actors are targeting any of their assets. Personnel in the Security Operations Centre (SOC) may fail to detect signs of attacks originating from outside the scope of their monitoring control.

Shadow IT falls outside the purview of the teams responsible for updating and patching. This invisibility prevents shadow IT from coming under the radar of the organisation's cybersecurity solutions, such as endpoint detection and response (EDR), next-generation antivirus (NGAV), or threat intelligence services.

A study by Forbes Insights revealed that one in five surveyed organisations suffered a cyber attack due to shadow IT. Organisations are helpless in case

bad actors manage to compromise a shadow IT asset. Compromised applications or accounts are costly to remediate (averaging $4.45 million per data breach, according to IBM).

Strategies and best practices for mitigating the risks of shadow IT

Addressing shadow IT is intimidating. It's hard to zero in on a source when there could be hundreds of applications leaking small amounts of information. Let's dive into a few tested and proven methods for mitigating the risks of shadow IT.

Look for spending that points to unauthorised technology use

CISOs should work with the organisation's procurement team and finance department to detect spending that could point to the use of shadow IT. Reimbursement requests by employees for tech spending out-of-pocket are the ideal sources to look into to uncover where shadow IT is in use.

Since these purchases are generally of low value, organisations can implement automated monitoring tools with predefined filters, like those from specific vendors or technology purchases, to spot the sprawl of shadow IT.

Educate employees about the risks of shadow IT

Organisations should understand that workers' intent to use shadow IT is not malicious but to increase productivity. It is important to build up their security competence in addition to awareness training.

It is an impractical idea to even think about making everyone a security specialist, but the minimum competency with which they can determine what's a threat to the organisation is essential to develop.

According to a finding by Gartner, employees provided with training targeted at their technology-related activities are 2.5 times more likely to avoid introducing cyber risk and twice as productive with sanctioned IT than those without such training.

Establish internal shadow IT policies

Often, employees see corporate IT policies as a roadblock to their job efficiency. Organisations need to understand their frustration and teach them about the reasons for policies. Creating policies around the adoption of new technology and regularly informing other departments about it allows IT to vet new applications or services before they're rolled out. Policies should outline concrete steps for the onboarding and management of new applications and tools, along with a clear definition for unapproved technology solutions and reporting such instances of shadow IT upon encounter.

Shadow IT and ISO 27001—what does it mean for your certification?

While shadow IT is a challenge to an organisation's information security, ISO 27001 outlines best practices to help identify and mitigate such risks. ISO 27001 doesn't mention any specific technology but instead provides a framework for organisations to develop their own information security management system (ISMS).

The benefits of ISMS include:

- By fostering open communication between IT and business units, the communication gap between employees and IT gets shortened. IT can quickly approve requests for new applications if it finds them useful for mass use.
- The ISMS process involves identifying and analysing risks pertinent to information security. It also includes the formulation of IT policies outlining procedures for the approval of new software and the risks associated with shadow IT.
- The ISMS promotes employee training and education about information security, highlighting the implications of using shadow IT for organisations. When users understand the risk, they're less likely to rely on unauthorised IT.

ISO 27001 certification speaks volumes about an organisation's strong information security management culture, which translates into increased customer confidence and competitive advantages. The ISO 27001 certification makes it easy to comply with other regulations, like the GDPR and HIPPA, which have overlapping requirements with ISO 27001.

How does Kertos help you discover risky shadow IT?

The lack of visibility into assets beyond the officially approved ones enables shadow IT to be a growing risk for businesses. In the digital world where data breaches, ransomware, and compliance penalties are making the headlines daily, it's high time for businesses to take a risk-averse approach to shadow IT.

Kertos offers a range of solutions targeted at privacy and security risks to an organisation. It's an all-in-one platform specially engineered to help businesses do away with shadow IT. Its data discovery, vendor management, and policy management solutions work in tandem to eliminate shadow IT to a T.

By conducting thorough data discovery, Kertos provides businesses with real-time insights into data silos, processing activities, and IT infrastructure. It identifies the residence of sensitive data, regardless of whether it's present in approved or unauthorised devices, applications, and services, allowing organisations to assess and mitigate the associated risks.

With effective vendor management practices in place, Kertos helps organisations maintain a comprehensive inventory of authorised vendors and their applications. To cut reliance on shadow IT, Kertos provides employees with approved alternatives meeting the required security, compliance, and performance standards.

With its intelligent, customised documentation, Kertos helps organisations automate ROPAs, DIPAs, and TIAs, streamlining the evaluation processes for new technologies. Kertos defines and enforces IT policies for data security, software usage, and procurement, setting benchmarks for acceptable use of technology within an organisation.

For more information about how Kertos can help reduce the risks of shadow IT in your organisation, schedule a demo today.