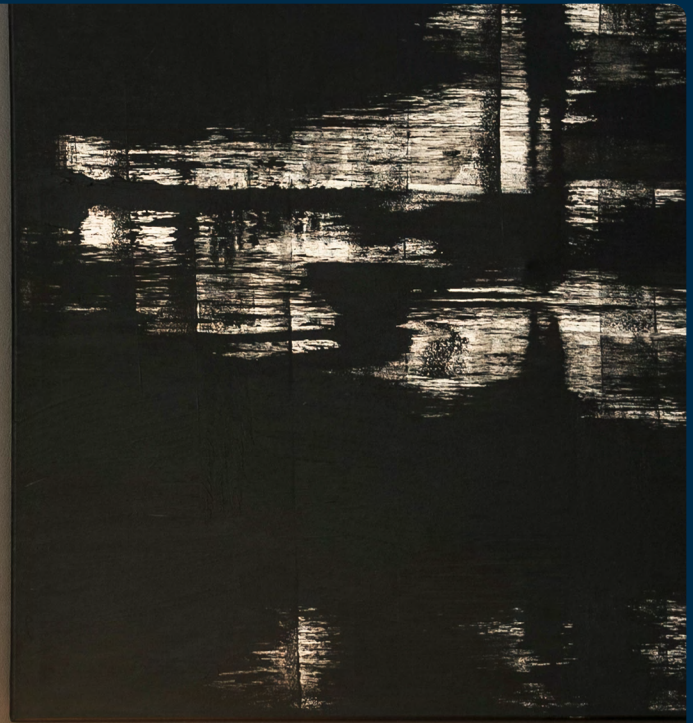


eBook




Casting IT into the Shadows



Introduction

In any fast-paced work environment, employees are eager to streamline their work and solve urgent problems. They want to get their work done quickly, efficiently, and effectively. Why is this a problem? Because too often they accomplish this with the use of unauthorized applications that sidestep official processes perceived as slow or cumbersome.

This creates blindspots for IT organizations that we call **shadow IT**. And those blindspots can lead to catastrophic failures.



Shadow IT refers to the use of information technology systems, devices, software, applications, and services without explicit organizational approval.

This happens when employees or departments deploy technology independent of the organization's IT infrastructure (typically) to address immediate needs or improve productivity. While shadow IT has the potential to drive innovation and efficiency, it introduces significant risks and challenges in areas of security, compliance, and governance.

This problem is not a new one, but it seems to compound exponentially every year. The workforce is increasingly tech savvy. They may be asked to do more with less resources, or they may be motivated to overperform and exceed their targets and goals. They may work from home, with better (and unsupervised) access to their personal devices, which they may prefer to the ones given to them. And they certainly have an endless list of easily available, high-powered, and purpose-built cloud-based services ready to be used.

Whatever drives shadow IT, it's here to stay. And while the bottom line may appreciate the increased productivity shadow IT delivers, the risks of catastrophic failure are too real to ignore.

This ebook dives into:

The various forms of shadow IT

What motivates Shadow IT

What you stand to lose without a program in place to mitigate Shadow IT

Examples of Shadow IT

84%

of SMEs are concerned about Shadow IT.¹

37%

of the breaches SMEs have experienced so far this year stem from shadow IT.²

^{1,2} IT Trends Report: Detours Ahead: How IT Navigates an Evolving World

Storing work files on personal cloud storage accounts.

Using unapproved video conferencing tools for meetings such as video transcript generators.

Using personal software on a personal device to complete projects or work.

Signing up for SaaS applications directly without informing IT.

Downloading free software to use in place of officially sanctioned programs (email clients, calendars, note taking apps, etc).



Different Aspects of Shadow IT

Shadow IT is generally classified by the type of technology it fosters. You can look at shadow IT in three distinct ways:

1

Hardware and Devices:

Employees using personal laptops, smartphones, tablets, and other devices for work-related activities. This includes Bring Your Own Device (BYOD) practices, where personal devices are used across company networks and data.



2

Software Applications:

Unapproved packaged (off-the-shelf) software, ranging from simple desktop applications to complex enterprise solutions, can be installed by employees.



3

SaaS / Cloud Services:

Employees signing up for and using cloud services without IT's knowledge. This includes an endless list of products often aimed at personal and professional efficiency.



Among the various forms of shadow IT, SaaS is the most common.

Why is that?

These applications are attractive to employees because they are easy to access, require no installation, and often come with low or no upfront costs. Plus, it's almost impossible for you to completely stop someone from using cloud-based apps (compared to how hardened device policies can automatically prevent unwanted software installations). Common examples of SaaS shadow IT include services like Dropbox, Trello, Google Docs, Google Drive, WhatsApp, and Zoom.

SaaS shadow IT tends to fall within two buckets:

Network-accessed shadow apps are those that employees access directly over the internet without IT department approval. These apps often bypass corporate firewalls and security protocols, introducing new attack surfaces that can access sensitive data (by way of the third party app).

OAuth-enabled shadow apps pose an even greater threat due to their deep integration capabilities. OAuth allows 3rd-party apps to access user accounts on other services, potentially leading to extensive data breaches and loss of control over critical systems. The lack of oversight on permissions granted to these apps can create security gaps.

Understanding Shadow IT From The Employee Perspective

It's important to remember that despite the scary name, shadow IT is almost never motivated by malicious intent. In fact it's quite the opposite!

Employees tend to seek out new solutions to help them get their work done, and they will do this on their own if they believe their organization doesn't provide the necessary IT support or tools to make their jobs easier. While this "lack of support" may be real or simply perceived, understanding why employees resort to shadow IT is crucial for organizations aiming to address and mitigate its risks.

Common motivations:

Efficiency and productivity

There could be hundreds of scenarios where employees can find an unsanctioned SaaS tool better than the sanctioned alternative. For example, there could be a tool that they used in their previous job or one that offers more capabilities that they specifically need. In such cases, they tend to believe that the "unapproved" tools are more efficient.

Collaboration and communication

Tools that facilitate better communication and collaboration, especially in team-oriented environments, are particularly attractive. Employees may adopt apps that enhance their ability to work with colleagues, partners, and clients.

Remote and decentralized work

The rise of remote and hybrid work environments has made it easier for employees to adopt shadow IT. Without direct oversight from a central IT department, or centralized management and control over the network they use, employees in different locations or working from home may use a variety of unapproved tools.

Storage and file-sharing needs

IT-sanctioned storage and file-sharing solutions may lack the flexibility, capacity, or ease of access required for certain tasks. Employees, especially those working with large files or collaborating across locations, often seek out alternative options that offer more convenience and scalability. With these tools, employees can share files with colleagues, clients, agencies, and partners without the need for complex VPNs or slow email attachments.

Cost considerations

In some cases, departments may have limited budgets for new technology. Shadow IT allows them to bypass formal budgetary constraints and access low-cost or free tools to achieve their goals.

Exploring new tools

Another allure of shadow IT is the opportunity it provides to experiment with new tools (such as AI applications) that are not yet available through official channels. These tools may not have undergone the rigorous security and compliance checks necessary to ensure they are safe for use within the organization, risking sensitive data exposure. Employees may also want to use popular tools (like ChatGPT) to make their jobs easier even though they are strictly against company security policies.

Low-Cost Signup, High-Cost Risks

The allure of free trials, low costs, and ease of sign-ups entices more employees to adopt shadow IT, bypassing official channels to quickly access tools that meet their immediate needs. SaaS trials may offer extensive (sometimes complete) access to features, and they embed methods of authentication that integrate with accounts users already have set up. For example, it takes only a simple click to login with Google or GitHub to try a new tool.



This introduces a multitude of risks that can jeopardize the security, compliance, and efficiency of an organization.

Security Vulnerabilities

Data Breaches:

Unapproved apps may not meet the organization's security standards, leaving sensitive data exposed to unauthorized access or cyberattacks.

Malware and Ransomware:

Unapproved apps serve as vectors for introducing malware or ransomware into the organization's network. These malicious codes can disrupt operations, encrypt data, and demand ransoms, causing significant financial and reputational damage.

Insufficient Incident Response:

When shadow IT is detected too late, the organization's ability to respond to security incidents is hindered. Unapproved apps might not be integrated into the company's incident response plan, delaying containment and remediation efforts.





Compliance Issues

Regulatory Non-Compliance:

Many industries are governed by strict regulations concerning data protection and privacy, such as SOC2, GDPR, and HIPAA. Shadow IT can lead to the storage and processing of data in ways that violate these regulations, resulting in legal penalties and reputational damage.

Data Residency:

Unapproved cloud services may store data in locations that do not comply with the organization's data residency policies. This can lead to breaches of data sovereignty laws, where data is transferred and stored across international borders without proper authorization.

Audit Failures:

Shadow apps complicate the auditing process by creating blindspots in the IT infrastructure. Auditors may find it challenging to verify compliance and data handling practices when apps and services are used outside official channels. Without a SaaS management system that centralizes access reviews for SaaS apps, IT teams face severe security and compliance risks.

Unauthorized Access and Changes to Data

Data Exposure:

Shadow IT may lead to unauthorized access to sensitive data. Without proper access controls and authentication mechanisms, data stored in unapproved apps can be easily accessed by malicious actors.

Insider Threats:

Employees using shadow IT might inadvertently or intentionally share access to sensitive data with unauthorized parties. This lack of oversight increases the risk of insider threats, where individuals with legitimate access misuse their privileges.

Data Integrity Issues:

Unapproved apps may not have adequate mechanisms to ensure data integrity. Unauthorized changes to data can occur, either through malicious intent or unintentional errors, leading to corrupted or inaccurate information that affects business operations and decision-making.



Financial Implications

SaaS Sprawl:

The unchecked proliferation of SaaS applications: without centralized management, organizations might end up paying for multiple tools that serve a similar function, leading to wasted resources. Employees may also fail to fully utilize all the features of these tools, resulting in poor ROI for the business.

Untracked Expenses:

Unauthorized subscriptions, recurring fees, and unmonitored renewals can significantly inflate IT budgets. Without clear visibility into where funds are being spent, finance departments face budget overruns and difficulties in financial planning.

Operational Challenges

Lack of Integration:

Unauthorized applications often do not integrate with existing systems, creating data silos and hindering cross-team collaboration. This fragmentation slows down processes as employees need to manually transfer data between systems or duplicate their work across multiple platforms, drastically reducing overall productivity.

Support Limitations:

Troubleshooting becomes a major issue with tools that the IT department is unfamiliar with. IT teams are often unable to provide adequate support or manage unauthorized applications, leading to longer downtimes and unresolved technical issues.

Reputational Damage

Loss of Credibility and Customer Trust:

Compliance violations can lead to public scrutiny and regulatory penalties, but the bigger issue is the hit to credibility. Clients, investors, and the market as a whole consider non-compliance as a failure in governance and risk management, which can lead to a damage to company reputation and its ability to attract new businesses/customers.

Disruptions:

Service disruptions stemming from shadow IT can negatively impact the customer experience, leading to poor reviews and increasing dissatisfaction.

Conclusion

As businesses continue to embrace SaaS, shadow IT will continue to lurk in the darkness. But unlike other behaviors deemed “bad” or “dangerous,” shadow IT should not be a reason to abandon policies that empower employees to use SaaS applications. Even though it presents risks, shadow IT highlights the innovation, agility, and productivity SaaS can bring to your business. The way IT can bring shadow IT out into the light is through an effective SaaS management solution, where IT teams regain and maintain control over organizational security and compliance while empowering employees to leverage new technologies.

By embracing the shift from reactive to proactive, IT teams can anticipate potential issues, optimize SaaS spending, and prevent security risks before they occur. If you are unsure about your next step toward a proactive approach, [download our eBook on SaaS management](#) to learn how to start building a program to manage SaaS from the beginning, eliminate shadow IT and SaaS sprawl, optimize your software investments, and secure your SaaS landscape – all while simplifying IT.

Don't let Shadow IT jump out and scare you.



Learn more about why SaaS management is the next pillar of IT.

[Download the eBook](#)