THE SHADOW IT EFFECT

HOW TO SECURE YOUR BUSINESS DATA

GLOBALSCAPE

Large enterprises on average use over 1,200 cloud services—over 98% of them are Shadow IT.

- *Cisco, "Gartner Report Says Shadow IT Will Result in 1/3 of Security Breaches"*

Are employees making it too easy for hackers to infiltrate your system?

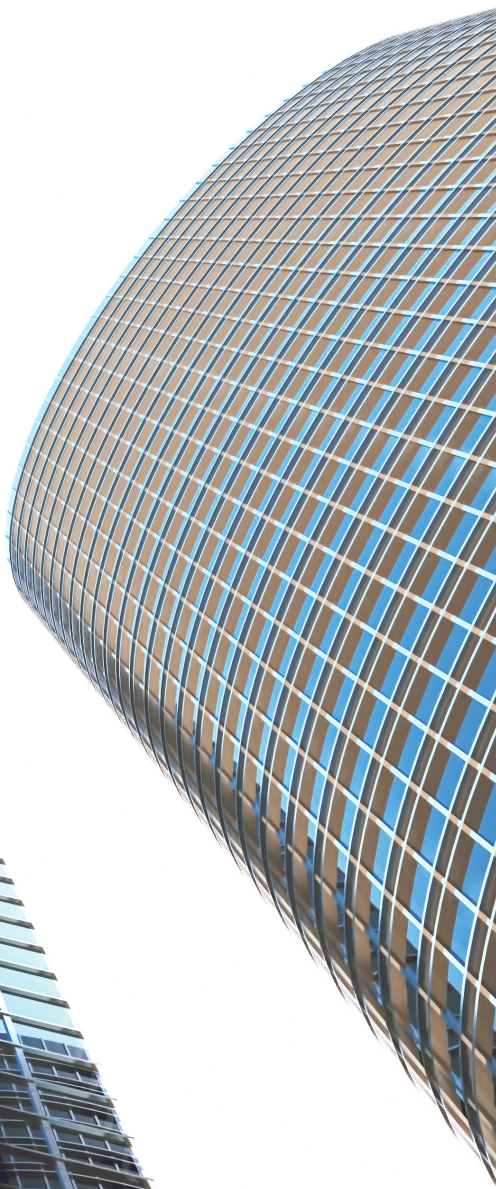
Shadow IT practices can expose your IT infrastructure and sensitive data to a wide array of security vulnerabilities. If your employees are using devices and/or applications that were not IT vetted and sanctioned for your network—also known as shadow IT—then the answer is yes!

In this guide, we not only talk about the growing problem of shadow IT in the workplace, but how you can overcome shadow IT with the right strategy and tools in place.

WHAT IS SHADOW IT?

Also known as "stealth IT," shadow IT refers to the employee "do-it-yourself" practice of using a device or application to accomplish business objectives or resolve IT-related issues outside the scope of IT and their security policies. The practice is a short-term productivity fix, but it is far from secure and can have a direct effect on your bottom line and reputation.

Whether it is financial resources, business plans, personnel records, trade secrets or customer lists and sales projections, your business relies on data. When hackers are able to access your data through shadow IT insecurities, they can have a direct effect on your bottom line and reputation.



...shadow IT may be continuing to causes challenges. Over half of Australian (61%), Brazilian (59%) and British (56%) organizations are not confident they know all of the cloud computing apps, platforms or infrastructure services their organization is using.

- *Gemalto, "Gemalto and Ponemon Institute Study: Big Gaps Emerge Between Countries in Attitudes Towards Data Protection in the Cloud"*

FIVE DRAWBACKS OF SHADOW IT

From some perspectives, shadow IT fuels innovation. It shows how resourceful employees can be when they are trying to accomplish their business objectives. Unfortunately, there are far more drawbacks to shadow IT, than there are benefits. The occurrence of shadow IT does often come from a good place, with employees seeking workarounds in order to "get the job" done in the face of many different variables.

In some cases, there is a lack of awareness within the organization about existing tools and resources. In other cases, they know about the tools. But the tools are limited and do not provide all the features they need to accomplish their goals, which can range from technical functionality to usability.

Of course, good intentions will not reduce business risks. There are major drawbacks that come with shadow IT practices, and these drawbacks can be extremely damaging to an organization's security posture and bottom line.

DRAWBACK #1: SHADOW IT CAN COMPROMISE SECURITY

Hackers are always on the lookout for a backdoor. Unfortunately, that is what an unsanctioned device or application can become a backdoor into your system, compromising your data and IT infrastructure. To ensure that an application or device does not interfere with your security measures, it must go through a full vetting process. Skipping that process creates system vulnerabilities that put your data at risk.

> According to Gartner, 33% of successful attacks experienced by enterprises will be on their shadow IT resources by 2020.
>
> - *QuickBase, "5 Shadow IT Statistics to Make You Reconsider Your Life"*

DRAWBACK #2: SHADOW IT IS A THREAT TO DATA PRIVACY

> 90% of CIOs worldwide are bypassed by line-of-business in IT purchasing decisions sometimes and 31% are bypassed routinely.
>
> - *Logicalis, "Report: The Shadow IT Phenomenon"*

CIOs are increasingly aware of the business risks that follow shadow IT practices, from data security, compliance, and productivity. IT understands how to vet new technology and ensure how it can fit within the IT infrastructure, from security and beyond. Your IT department needs visibility over your organization's IT infrastructure and data to ensure a more secure and productive environment.

Visibility allows IT to get ahead of problems, like catching security vulnerabilities or compliance violation risks. When it comes to shadow IT, there is little to no visibility; therefore, it becomes impossible for IT to protect an organization's data and infrastructure effectively.

Shadow IT puts the privacy of sensitive consumer and corporate data at risk. There are particular types of data—like patient or credit card data—that require greater levels of protection due to their high value for cybercriminals. It is also impossible to protect and monitor the infrastructure or data when shadow IT practices are at play.

An example of this scenario is when an employee uses a consumer file sharing application like Dropbox or Google Drive to share or store sensitive customer data. Sharing data in this manner can easily expose protected information and trigger breach notification laws.

DRAWBACK #3: SHADOW IT DISRUPTS IT PROCESSES AND POLICIES

Operational processes and procedures are critical components of the IT infrastructure. Shadow IT can be very intrusive on the consistency and reliability of these same processes and procedures. Consider how quickly processes can fall apart when the IT staff is dealing with requests to fix problems resulting from shadow IT. For example, this happens when an employee needs to give IT personnel admin access to an unauthorized application or the additional step of adding the application to an IdP or identity service provider.

DRAWBACK #4: SHADOW IT IS A THREAT TO COMPLIANCE

What is expensive and a huge hindrance to an organization's ability to operate and grow? In one word: noncompliance. Data protection regulations standardize security practices to ensure that organizations act appropriately when it comes to managing sensitive and regulated data.

When an organization fails to comply with data protection regulations, the perception is that the organization does not follow best practices for the secure handling of sensitive and protected data. In addition to the risk of expensive fees and penalties, noncompliance can damage public trust.

According to a recent report from the Ponemon Institute, "The Trust Cost of Compliance with Data Protection Regulations," the average cost of non-compliance is $14.82 million. That is nearly 3 times the cost of compliance and increase of 45 percent since 2011.

DRAWBACK #5: SHADOW IT IS EXPENSIVE

There can easily be some degree of duplication when employees are provisioning their own IT resources. If an employee or a department purchases a tool without going through IT, they may not realize that IT has a similar tool available, that supports both their business needs along with IT's.

Additionally, they are not likely taking into consideration the potential need for IT support if a problem occurs. Taking the extra steps and collaborating with IT in advance will save a great deal of time and money.

> Gartner Research reports that shadow IT management will account for 30 to 40 percent of IT spending in large enterprises."
>
> - *QuickBase, "5 Shadow IT Statistics to Make You Reconsider Your Life"*

THREE SIGNS THAT SHADOW IT IS A PROBLEM

SIGN #1: A CLEAR SHADOW IT POLICY DOESN'T EXIST

The reality is that there are many employees that practice shadow IT and they are completely unaware that it's wrong. In some cases they either are not aware or they don't understand your organization's security policies on the use of unauthorized devices or applications in the workplace. If your employees are not clear about your shadow IT policy, then it may be a fair assumption that it's happening within your organization.

SIGN #3: A DROP IN REQUESTS OR COMPLAINTS

Silence is another good indication of shadow IT. If employees requested certain solutions in the recent past and have seemingly fallen silent, it is possible that they most likely found another option.

Alternatively, if you notice that you have low email attachment size limits, or just don't offer tools for common needs (such as collaboration, reporting, file sharing, file transfers, and others), and no one complains about it, then it's very likely that shadow IT is alive and well. If needs go unmet for a moderate amount of time, employees will likely seek out other solutions.

SIGN #2: HELP DESK RECEIVES REQUESTS FOR UNAPPROVED SOFTWARE

As mentioned earlier, there are some employees who may not realize that they are practicing shadow IT. They may be using software that another employee recommended, or it's possible that their department manager licensed a SaaS solution for their team without mentioning that it wasn't an approved solution. In these scenarios, employees sometimes still contact the company help desk for application issues.

GETTING AHEAD OF SHADOW IT IN THREE STEPS

If you find yourself dealing with shadow IT and need help with data management, you're not alone. Here are a few suggestions to help reduce the burden of shadow IT.

STEP 1: EVALUATE EXISTING PROCESSES

By evaluate existing tools and policies, you may find shortcomings within your organization and IT infrastructure. You may discover that your current system enables users to practice shadow IT. Reviewing these tools and policies is an easy first step in managing unsanctioned tools and discovering internal flaws and weaknesses.

STEP 2: TALK TO YOUR EMPLOYEES

Survey or audit your employees' data management and transfer processes. It is human nature for most users to choose the path of least resistance, sometimes trying harder to find a work around as opposed to complying with internal security policies or best practices.

Instead of continuously fighting that battle, work with your employees and establish a common ground. Understanding why they use a work-around can help you determine a better route, such as more training or new tools to prevent any additional shadow IT problems.

STEP 3: KEEP IT SIMPLE

Make it easy for employees to follow a secure data management or file transfer policy. Keep communications simple, clear, and direct. Provide end-user training on the policy annually, and to all new employees.

Be sure to update the entire company on system security risks, communicating their role in preventing those risks.

80% of workers admit to using SaaS applications at work, in many cases without IT approval

- *Skyhigh Networks, "What is Shadow IT?"*

TOOLS THAT EMPOWER IT AND END USERS

Shadow IT practices reduce operational visibility and system controls. When an employee's action puts information at risk or compromises compliance, more often than not, there is no malicious intent. Rather, it is a case of employees doing everything possible to remain productive. If organizations want to ensure that employees follow security policies and best practices, then they must take steps to understand the business needs of their end users. They also need to have the right strategy and tools in place.

Among the tools that support a shadow IT-free environment, you will find a managed file transfer (MFT) platform and an integration platform as a service (iPaaS). Both platforms provide the visibility and control needed to empower your IT department and keep shadow IT at bay.

MANAGED FILE TRANSFER (MFT) PLATFORM

A managed file transfer platform is a mechanism of file transfer to manage the secure, visible, and efficient exchange of data. An organization can better meet their growing and evolving business needs when they have a MFT platform streamlining their complex processes and workflows.

With the right MFT platform and vendor, IT can centralize the management of data, allowing for greater visibility and control over their IT environment. In a disparate IT environment, shadow IT is difficult to identify and manage. An MFT platform keeps IT in the driver's seat, giving IT the control needed to mitigate shadow IT risk.

Here are a few key things to look for in an MFT solution:

- Military-grade security and compliance, built for the enterprise
- Comprehensive auditing and reporting
- Maximizing uptime through high availability and active-active clustering
- Maximum automation and system visibility
- Easy integration with other vendor products
- Secure mobile management

INTEGRATION PLATFORM AS A SERVICE (IPAAS)

With an iPaaS platform, end users can connect to systems and data, while IT maintains the level of security and control needed. An iPaaS platform also helps IT democratize integration work, which reduces IT integration project delays and helps make shadow IT unnecessary. End users can create the connections they need with drag-and-drop ease; however, IT maintains control and has the final say.

The things that matter for security compliance, like permissions, access, and data paths are rightfully put under IT's control, making it a win-win for all parties involved.

Here are the key things to consider when evaluating a platform:

- Range of usability
- Level of IT visibility
- Creating at scale and repeatability
- Flexibility to integrate SaaS, APIs, and homegrown microservices
- Security features and permissions
- Ability to integrate with on-premises systems

The right iPaaS solution provides a low-code, user-intuitive platform that can be used to create data and application integrations quickly and securely in both the cloud or on-premises environments.

An iPaaS platform handles the configuration, deployment, and optimization of an integration for the user. Using pre-built, reusable connectors and process rules, iPaaS enables users to make faster, less error-prone integrations among multiple applications and services, without waiting for their projects to make it through IT's queue.

GLOBALSCAPE CAN HELP

By choosing an MFT platform for your file transfer processes or an iPaaS platform for your data and application integrations, you can keep your network secure and empower your end users—reducing your shadow IT risks.

WORKSPACES FOR EFT

With Workspaces for EFT, end users do not have to ask for help or worry about violating internal policies. Workspaces is easy for end users to share files of virtually any kind via any web browser, allowing others to access, upload, and download folders and files.

Employees are empowered to share files in a way that they have become use to, but now they can do it in a secure way, all while providing you with the enhanced governance and visibility of your data.

With Workspaces for EFT you can:

- Empower your end users with secure file sharing between employees and external partners
- Retain full control and visibility of your data
- Integrate with Outlook for person-to-person file transfers
- Securely send files from your browser
- Generate reports on file transfer activity

TRY EFT NOW >

EFT

KENETIX

Kenetix is a secure, reliable, and innovative integration platform as a service (iPaaS) focused on quickly getting the right data in the right places in the right format. Kenetix easily connects data across all of your cloud applications like Salesforce and SAP.

With Kenetix you can:

- Centralize your data
- Empower business units outside of IT to create their own integrations and workflows
- Rapidly create complex integrations and connect microservices and APIs
- Save time and effort by automating as many routine integration tasks

TRY KENETIX NOW >

KENETIX

MAKE BUSINESS FLOW BRILLIANTLY

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit **www.globalscape.com** or follow the blog and Twitter updates.

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249, USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support

GLOBALSCAPE