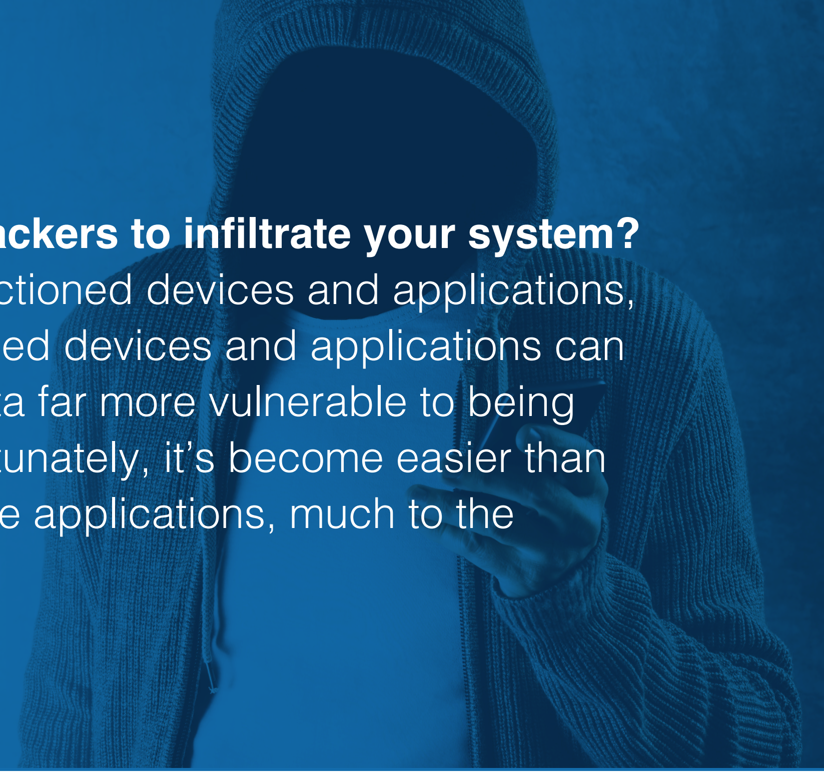
globalscape®
securely connected

BE AFRAID OF YOUR SHADOW: WHAT IS 'SHADOW IT' AND HOW TO REDUCE IT



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

If your employees are using unsanctioned devices and applications, then the answer is yes! Unsanctioned devices and applications can leave your IT infrastructure and data far more vulnerable to being exploited by cybercriminals. Unfortunately, it's become easier than ever for employees to access rogue applications, much to the chagrin of busy IT staff.

80% of IT pros report end users using unsanctioned devices and applications.

– IT Business Edge

Since it's become common for employees to bring their own laptops, tablets, and smartphones, administrators are put in a position to manage applications of unknown origin and inadequate security standards. It often falls to the IT professionals to make sure these shadow IT efforts don't result in a fractured technology ecosystem that leaves networks vulnerable to a devastating attack.

"[…] more than 80 percent of IT pros said their end users have gone behind their back to set up unapproved cloud services, with a whopping 40 percent reporting their users 'going rogue' five or more times." IT Business Edge, Majority of IT Pros Worry about Shadow IT Use

While people generally have good intentions and are just trying to meet business goals, employing shadow IT is indicative of a situation where employees are leaving security standards by the wayside.

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

SECTION 1: WHAT IS SHADOW IT?

Also known as “stealth” IT, shadow IT refers to the employee 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. It’s a “do-it-yourself” practice of IT that is far from secure. While the workaround can offer a short-term fix, it is a security risk that can have a direct effect on your bottom line and reputation. The Ponemon Institute says the average data breach last year cost companies an average of $4 million.

70% of unauthorized access to data is committed by an organization’s own employees. Gigaom Research, Shadow IT: Data Protection and Cloud Security.

Whether it’s financial resources, business plans, personnel records, trade secrets or customer lists and sales projections, your business relies on data. When hackers access your data they can have a direct effect on your bottom line and reputation.

> **70%**
>
> **of unauthorized access to data is committed by an organization’s own employees.**
>
> *– Gigaom*

SECTION 2: THE 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 when it comes to shadow IT, and they are often practicing shadow IT because they don’t know about or have access to user-friendly or secure tools. For that reason, they often seek a workaround to get the job done.

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. Any application or device that is used within your organization must go through a full vetting process to ensure that it doesn’t interfere with your security measures.

According to Ed Tech Magazine, 33% is the estimated percentage of successful attacks on institutions that will occur in shadow IT resources by 2020.

Shadow IT puts the privacy of sensitive consumer and corporate data at risk.

It's a Threat to Data Privacy

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 and therefore it would be impossible for IT to fully protect an organization's data and infrastructure.

Shadow IT puts the privacy of sensitive consumer and corporate data at risk. There are particular types of data that require greater levels of protection due to their high value to cybercriminals. It's 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.

It Disrupts IT Processes and Policies

Operational processes and procedures are a critical component 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.

It's a Threat to Compliance

What's expensive and a huge hindrance to an organization's ability to operate and grow? Quite simply: compliance violations. Shadow IT can eliminate or greatly reduce the amount of visibility IT has over the IT infrastructure. Without visibility and control over the user activities and data transfers happening with shadow IT, an organization is left vulnerable to data loss. At the same time, the lack of visibility and control in shadow IT-enabled environment can easily lead to compliance violations if your sensitive and regulated data is unnecessarily exposed to security risk.

It’s 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, then they’re not taking into consideration the potential need for IT support if a problem occurs. At the same time, they may not realize that IT already has a similar tool in place or they could’ve worked together to find a tool that supports their business needs while still maintaining a secure, compliant, and productive environment. Taking the extra steps and collaborating with IT in advance will also save a great deal of time and money, as opposed to getting in a position where choosing to use an unauthorized tool may mean that IT can’t support it or it may take more time to resolve technical problems.

Gartner Research reports that shadow IT management will account for 35% of total IT expenditures in 2016.

35%

of total IT expenditures in 2016 are related to shadow IT management.

– Gartner Research

SECTION 3: SIGNS THAT SHADOW IT IS A PROBLEM

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.

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.

If you don't offer tools such as collaboration, reporting, file sharing, file transfers and no one complains about it, then it's very likely that shadow IT is alive and well.

A Drop in Requests or Complaints

Silence is another good indication of shadow IT. If employees were requesting certain solutions and have seemingly fallen silent, it's 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.

SECTION 4: HOW TO GET AHEAD OF SHADOW IT

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.

Take a Look at Existing Processes

By evaluate existing tools and policies, you may find shortcomings where your users are being enabled to create a shadow IT infrastructure. Reviewing these tools and policies is an easy first step in managing unsanctioned tools.

Talk to Your Employees

Survey or audit your employees' data management and transfer processes. We all know that users do what's easiest for them and they will often try harder to find a work-around, rather than to be compliant. Instead of continuously fighting that battle, try to work with your employees to establish common ground. Understanding why they are work-arounds can help you determine a better route, such as more training or new tools to prevent any additional shadow IT problems.

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.

SECTION 5: SHINING THE LIGHT ON SHADOW IT

Reducing the practice of shadow IT can be achieved with the right strategy and tools in place. Among the tools that support a shadow IT-free environment includes the managed file transfer (MFT) platform. MFT can help organizations manage the secure movement of data from one location to another. With the right MFT platform and vendor, IT can centralize the management of data, allowing for greater visibility and control. The visibility function of MFT can position IT to have a more thorough understanding as to how data moves throughout an organization. Visibility also gives IT a strategic advantage, so security or productivity issues can be addressed before they become a major problem, such as a data breach or compliance violation.

Visibility gives IT a strategic advantage, so security or productivity issues can be addressed before they become a major problem, such as a data breach or compliance violation.

Employees practice shadow IT because they want to accomplish their business objectives in the most efficient way possible. To some degree, shadow IT can seem like an efficient way to accomplish an objective. It seems inexpensive and an easy way to get the job done, but it's also a security risk, in part to the way shadow IT limits IT's visibility over the infrastructure. In addition to visibility, the right MFT platform will lend itself to a more efficient infrastructure through automation capabilities. Automating data transfer processes with MFT will not only help meet SLAs, but it will also ensure greater accuracy among your critical business processes, while also saving a great deal of time in comparison to manual processes.

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

Workspaces for EFT is easy for end users to share files–allowing others to access, upload, and download folders and files securely.

SECTION 6: TOOLS THAT REDUCE SHADOW IT

When an employee's action puts information at risk or compromises compliance, more often than not, there is no malicious intent. Rather, it's a case of employees doing everything possible to remain productive, and losing sight of security and compliance in the process.

If organizations want to ensure that employees follow policies and adopt the secure and managed tools that they provide, IT teams need to truly understand the business needs of the employees. The reality is that security inadvertently takes a backseat to productivity and efficiency. If enterprises have any hope of managing and securing their IT infrastructure and data, they need to provide solutions that easily integrate into the daily routines of their employees.

SECTION 7: GLOBALSCAPE CAN HELP

Say goodbye to shadow IT by choosing a managed file transfer solution that will help you empower your users and still keep your network secure. With Workspaces for EFT, end users don't 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.

ABOUT GLOBALSCAPE

Globalscape is an innovative software company that secures mission-critical exchanges of data across multiple platforms – including remote and mobility solutions – for businesses worldwide. Through superior software, standards compliance and experienced, reliable support, Globalscape secures information exchange for individual, global enterprises, governments, and small and medium enterprises across a wide range of industries.

Contact us today to begin your free trial of Workspaces for Globalscape's managed file transfer platform, EFT™.

www.globalscape.com/managed-file-transfer/trial

Work Cited

"Majority of IT Pros Worry About Shadow IT Use." IT Business Edge. October 21, 2016

"Average Cost of Data Breaches Rises Past $4 Million, Ponemon Says." Information Week: Dark Reading. October 21, 2016

"Shadow IT: Data Protection and Cloud Security." Gigaom. October 21, 2016

"Bring Shadow IT Out of the Dark." EdTech. October 21, 2016

"Why Shutting Down IT Stifles Innovation." IT ProPortal. October 21, 2016

globalscape®
securely connected

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Road, 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