



The Modern IT Professional's Guide to

# SHADOW IT



**We all do it: quickly sign up for that cool new software to solve a business problem, access that personal app, or sign onto that productivity tool we used at another organization.**

**Statistics show that 58% of IT managers use unapproved tools**, so how can we expect anything different from non-IT employees?

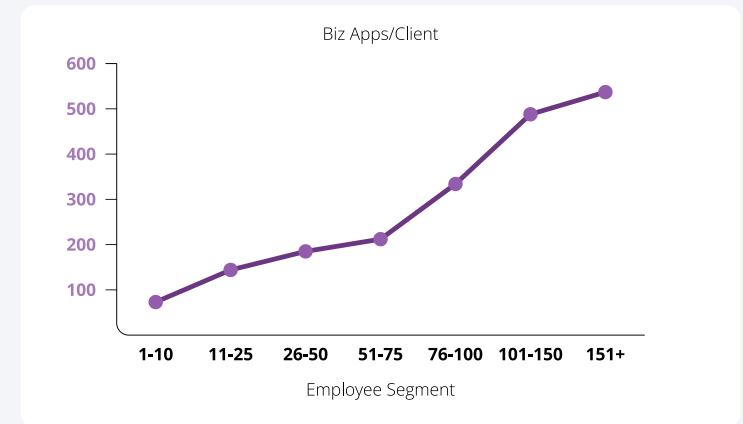
Practice what you preach is the name of the game when it comes to shadow IT. But we know it's tricky to manage alone, so we've built this ebook to help you out.

In this practical guide, we'll show you the impact shadow IT has on an organization, give you the statistics and case studies, share how to evaluate tools, note some security tips, and more. Plus, we've included a quiz to help you determine the severity of shadow IT in your organization.

### **Average number of business applications used\***

\*At a 100-person company. The 2022 Gartner SMP Market Report predicts that 125 of these applications are likely SaaS tools spread across the business.

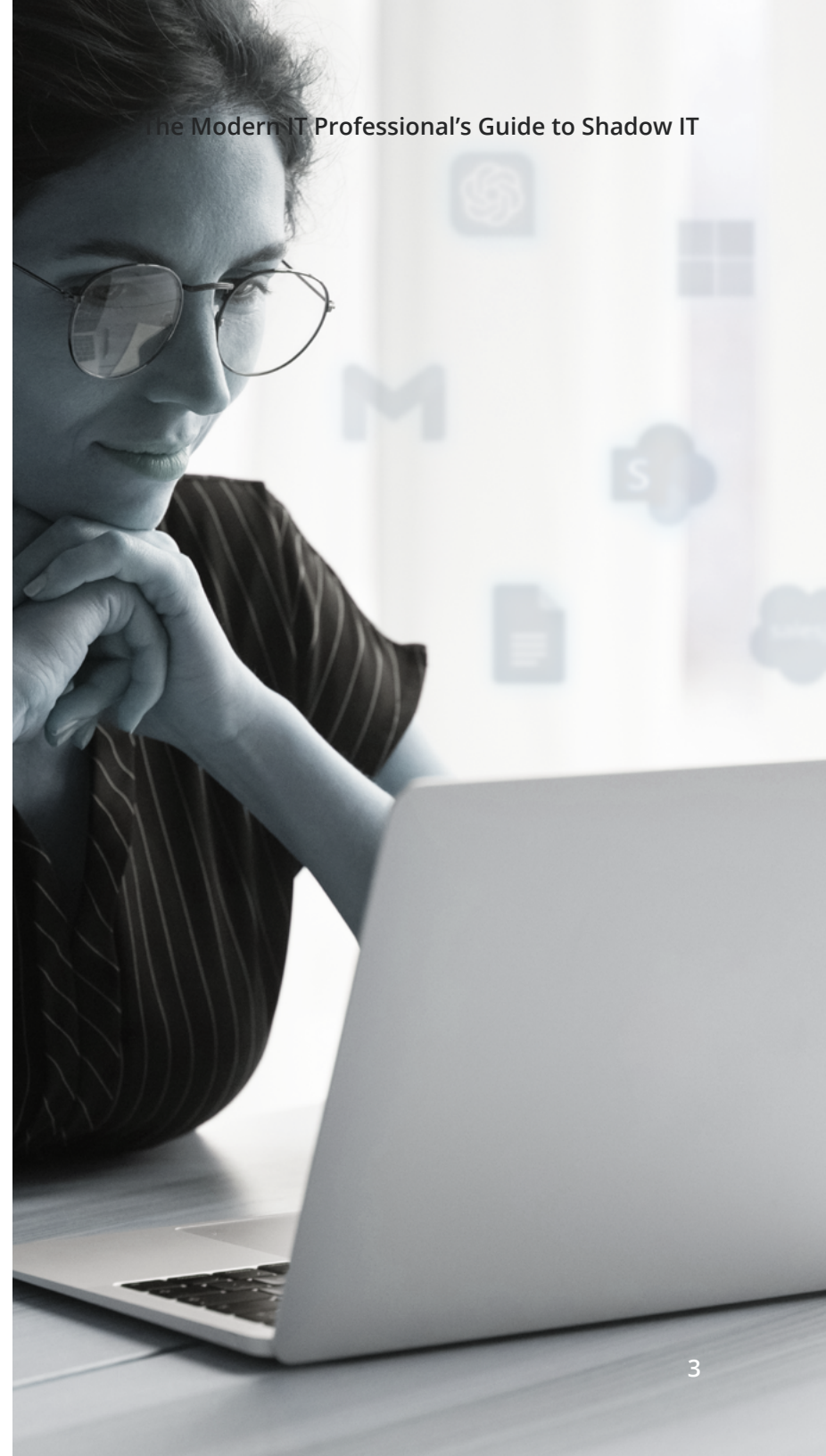
# 334



## What is shadow IT?

“Shadow IT” refers to any IT-related activities happening inside the organization but outside the supervision of the official IT department.

This includes systems, devices, software, applications, and services used without explicit IT approval.



The biggest contributor to shadow IT is the rise of web-based business applications. According to **a study done at Auvik in June of 2023**, nearly 62% of an employee's time is spent working in web applications, versus only 38% in desktop applications. This includes sanctioned SaaS and many tools that are not often not considered, but often house critical business data.

## Some examples of shadow IT are:

### USING UNAPPROVED COMMUNICATION TOOLS

**32% of employees** reportedly fall into this category. If manager Sam doesn't prefer the company's mandated messaging tool, Microsoft Teams, and switches her team to Slack without IT approval, it becomes shadow IT.

### SENDING WORK EMAILS FROM A PERSONAL ADDRESS

In 2020 a whopping 42% of employees reported using personal emails for work purposes. If Vinay has a work policy preventing access to customer contacts outside of the office network, and he works around it to give the best customer service experience after hours, that's a shady problem!

### USING UNAPPROVED DEVICES

Phil from sales loves his iPhone passionately. Instead of using company-approved devices that are subject to mobile app monitoring, he uses his personal phone for work purposes. He connects to the company infrastructure with his unsanctioned device, resulting in one of the riskier examples of shadow IT.

### OPTING FOR A PREFERRED SAAS TOOL

Shania likes to manage her marketing workflow with Asana—she used it at a previous workplace. When she's hired on a team that only has Trello for task management, she avoids the hassle of IT approval and opens a free account for Asana with her new workplace email, bringing the shade of shadow IT to her new job.

Shadow IT comes in many forms, as you can see. There are cloud and SaaS applications to worry about, on-premises network regulations, and bring-your-own-device (BYOD) struggles, among others. But if shadow IT is such a risky issue, why does it continue to occur?

# Why do employees choose shadow IT?

There are several roads that converge on shadow IT, namely innovation, retention, and productivity. Let's take a look at the main reasons employees are turning to shadow IT despite policies that may advise otherwise:



## TO HASTEN INNOVATION

One of the main reasons employees turn to shadow IT is to become more efficient and effective. For example, your development team might opt to use GitHub over your organization's approved coding repository because the GitHub Copilot feature enables them to create code much faster with the help of AI. This not only improves their productivity but also drives innovation in your organization. So, instead of a project taking months, it may take only weeks, allowing for faster iterations and reducing time to market significantly.



## TO BOOST ENGAGEMENT AND RETENTION

Shadow IT can also improve employee satisfaction because they can choose the tools they prefer to use. Plus, since most turn to these tools to improve their effectiveness, engagement levels also increase. According to Gallup, organizations with highly engaged employees are 23% more profitable. Retention also improves. Even within high-turnover organizations, business units with highly-engaged employees see a 18% difference in turnover, while low-turnover organizations see a whopping 43% improvement.



## TO IMPROVE IT EFFICIENCY

IT departments have long been buried under a sea of help desk tickets, but this issue only increased with the rise of remote and hybrid work. In early 2021, 55% of tech workers stated their workload had increased, with **64% in IT operations specifically** claiming the same. Shadow IT helps reduce that workload. As a result, IT teams can focus on more critical tasks that drive the business forward instead of being glorified troubleshooters or gatekeepers. They can strategize, innovate, streamline IT processes, implement more robust infrastructure, and more—all of which will take your company to the next level.

# 6 risks caused by shadow IT

Gartner estimates that **30-40% of IT** is shadow IT. The most significant risks don't necessarily come from the tools or apps themselves, but from the data they can access.

If you have security and/or compliance protocols at work, they could be undermined by shadow IT. But there are also risks outside of data and security. Operations, including onboarding and offboarding processes, and new tool adoption can be impacted. SaaS sprawl and license overage are at risk too.



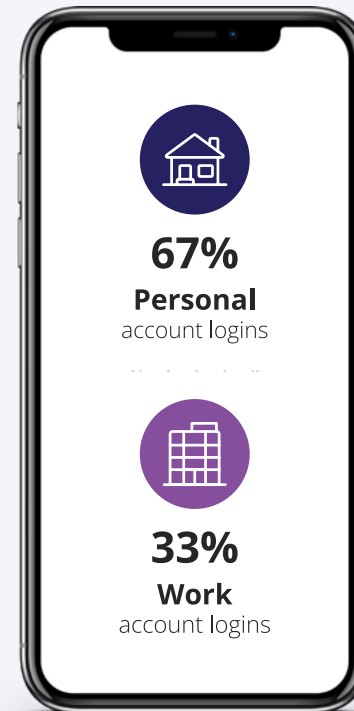
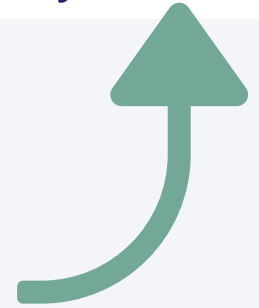
Hey AI, what was the fastest growing shadow IT last year?



ChatGPT

**350%**

Surge in app use, just a month after launch (Nov-Dec 2022)



### For ChatGPT login

- 43%** Google SSO
- 57%** Web Form
- 0%** Microsoft SSO\*

\*ChatGPT started offering Microsoft SSO after we had aggregated our data.

## Let's review some of the different issues caused by shadow IT with real-world examples.



1

### OPERATIONS

Have you ever gone to onboard a new employee only to discover you're out of seats for your organization's primary design tool and you've been paying for an employee who was supposed to be off-boarded among your existing subscriptions?

It's not hard to imagine, especially in a world where most employees login to work applications with username and password credentials rather than single-sign-on (SSO). **Less than 6% of employees are regularly signing in with SSO.** For the other 94% that use usernames and passwords alone, it can be much more difficult to off-board them, making the scenario above more likely than you think!



2

### SECURITY

Shadow IT expands the potential attack surface for cyber threats. Without the stringent controls typically exercised by an IT department, shadow IT tools could expose the organization's critical business data or trade secrets.

A prime example of this type of exposure is an employee who uses work credentials to sign in to a free app not sanctioned by IT. Without monitoring the privacy policy and data regulations, it can be quite difficult for IT to source an attack, were those credentials leaked or stolen through that free app. This could put anything related to that employee's email in jeopardy.



3

### REGULATORY NON-COMPLIANCE

Shadow IT also jeopardizes compliance. With the absence of standard data management, unauthorized tools could mishandle personal data, leading to violations of regulations like GDPR or HIPAA and ultimately costing the company hefty fines.

For example, healthcare organizations deal with a large amount of incredibly sensitive data and are subject to many regulations, including HIPAA. If a team within a healthcare organization chooses to use an unapproved cloud-based file-sharing platform to transfer patient data, it could result in a catastrophe if a breach occurs.

**Remember our example from earlier about unapproved communications applications?** Additional risks come into play in compliant organizations where usage of sanctioned unapproved communication tools could prove to be costly. **In 2022, the SEC** issued a **\$1.1 billion dollar fine** to 16 Wall Street firms for using shadow IT communication tools, such as WhatsApp.



4

### SYSTEM INEFFICIENCIES

Another concern is that shadow IT solutions might not be compatible with the other systems your organization uses. It can lead to data silos, system inefficiencies, and other critical problems.

Adopting a new tool that isn't compatible with IT's sanctioned software is problematic for more reasons than the headache it causes the employees who work around it. Company software is connected to other business processes, such as marketing, customer support, and inventory management.

If an employee fails to follow the mandated process, you'll end up with siloed data that is challenging to integrate with the information in the official CRM (if anyone even attempts it), which can lead to discrepancies and a slew of other issues.





### REDUCED VISIBILITY AND ACCOUNTABILITY

Another critical issue with shadow IT is that it can be challenging to establish clear lines of responsibility for data management. If there's a data breach, it's hard to figure out where the fault lies and what issues to address.

**Remember the employee using a free tool with their workplace email?** Imagine your entire marketing team uses an unauthorized cloud-based design tool to create and store product strategies. This vendor could potentially have a data breach that allows bad actors access to these designs. The IT department has no idea this application is being used and hasn't included it in their software inventory. Therefore, identifying the cause of the breach becomes incredibly complicated. It might even end up unresolved.



### FINANCIAL WASTE

Shadow IT can also lead to financial waste. As more employees transition to a non-approved tool, the official platform can go unused. However, the organization continues to pay for it.

Furthermore, some of these solutions are challenging to integrate with company systems, potentially leading to increased costs to achieve compatibility and increase security.

According to Auvik's [2023 Network IT Management Report](#), 20% of respondents stated that **IT budgets and costs represented a challenge** for them, which is just one more reason shadow IT requires immediate attention.

# What's your shadow IT risk factor?

Now that you've read up on shadow IT, you may be wondering, "How many of these issues are currently affecting my IT team?"


Let's introduce a quick quiz that will give you the bigger picture of the impact of shadow IT on your organization.

## SSO: The illusion of control

Think of all your employees are accessing apps through MFA-enabled SSO? Think again!

 **55%**  
Google SSO

 **45%**  
Microsoft SSO

 **94%**  
of all logins were through username/  
password authentication, creating a  
real hassle for off-boarding.



### **NON-SSO ACTIVITY REPRESENTS A SERIOUS COMPLIANCE RISK.**

Cyber-insurance policies require an affidavit that you are accessing software with SSO and/or MFA. Ever checked that box, assuming employees were following your IT policy? You may be at risk should you need to file a claim. Insurers could deny coverage based on misrepresentation of MFA use.

How to score your responses: **Yes = 0** | **Somewhat = 1** | **No = 2**

| QUESTION   | SCORE | QUESTION   | SCORE |
|--|-------|--|-------|
| <b>Applications</b>  |       | <b>Devices</b>   |       |
| Do you have a comprehensive list of all applications in use in your organization, including: desktop, web, SaaS, and cloud applications?   |       | Is your workplace using a BYOD policy and does it clearly define what is and isn't allowed for personal device use?                      |       |
| Is this comprehensive list reviewed on a bi-annual (or more frequency) to ensure that shelfware is removed and new applications are added? |       | Does your workplace have a policy for logging into corporate applications on personal equipment (mobile phones, laptops, tablets, etc.)? |       |
| Do you have a process to map which applications are secured behind SSO/MFA and which ones are not?   |       | <b>Operations</b>  |       |
| Do you enforce patching updates for your organization's installed software?  |       | Is your method for onboarding new software tools easy to understand and use?   |       |
| <b>Users</b>   |       | Do you have an established process for onboarding new employees/contractors to your IT tools?  |       |
| Are your users aware of what shadow IT is and how it can impact the businesses critical data?  |       | Do you also have a process for off-boarding?   |       |
| Do you have established best practices for your IT team to minimize the use of shadow IT to speed up work?                                 |       | <b>Compliance &amp; Policy</b>   |       |
| Do you have monitoring enabled to track which users have access to generic accounts, such as administrator@, hr@, etc.?                    |       | Is your security documentation up to date and re-visited annually at minimum?  |       |
| Do you have monitoring enabled to track users who are using shared accounts amongst employees for a single application?                    |       | Is information about how to use and request new IT tools available and accessible to everyone at your organization?                      |       |
|  |       | Do you have policies in place for how users can request licenses for an existing tool?   |       |
|  |       | Do you have policies in place for how to request a new tool and what info to provide?  |       |

**SCORE TOTAL:**

SCORE

RESULT

0–8

**Shadow IT is a minimal risk at your organization.** Regular training and review of policies is essential to keeping IT secure, so please keep up the good work.

8–17

**Shadow IT is creeping up on you.** It looks like there is some room for improvement in your security policies, but introducing an application monitoring tool and making some quick policy revisions might be enough to help keep you ahead of the risk.

19–26

**Don't look behind you... Shadow IT is a threat to your organization.** There's a good chance it is impacting you already—time to invest in training and tools to help your IT team take back control.

26–34

**Living in the shadows!** Oops—it looks like you've let the shadows creep in a little too close. This ebook is here to help. We'll walk you through concepts that can help you scale back on tool sprawl and reduce operating costs to maximize your IT team's reach.

**If you scored 6 points or higher on the quiz, you'll want to take a hard look at your IT practices, especially around SaaS.**

Consider how you onboard employees and contractors, offboarding for all software users, and the kinds of training you have in place for topics like password hygiene, account sharing, and license management.

In the next section of this ebook, we'll discuss how to make a policy in response to the growing threat around shadow IT, and shed light on the best practices for choosing tools to help.

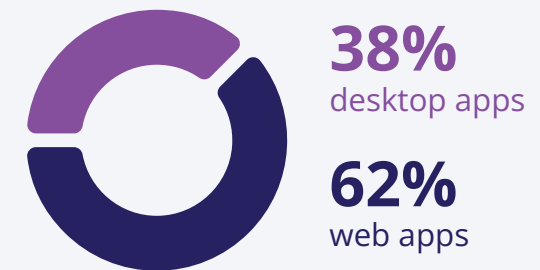
# How to create a shadow IT policy

The National Institute of Standards and Technology (NIST) has created a cybersecurity framework that works well for managing shadow IT.

Let's take a quick look at the concepts involved and how to apply them to your own organization.

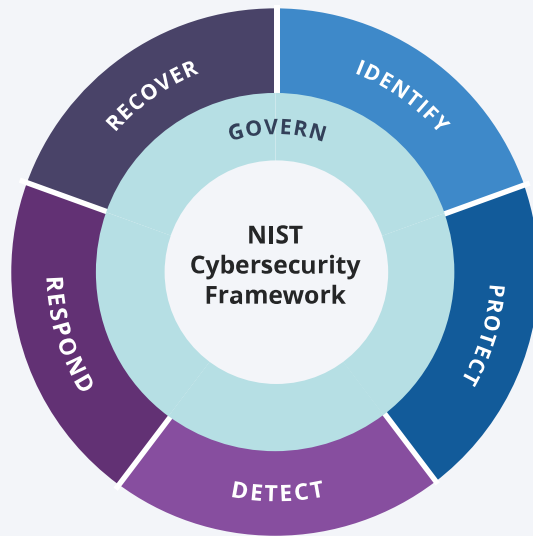
## Where employees spend the most time

Employees are spending less time on desktop applications and more time on the web to get their work done.



### TOP 5 WEB APPS USED:





## Using the NIST framework

Organizations can use the six functions outlined by NIST to set up an action plan for tackling shadow IT. Your plan should cover all six, because the functions are related to one another—missing or skipping a step could leave a gap for bad actors to take advantage of.



### GOVERN

Establish and monitor cybersecurity risk management strategy, expectations, and policy. Inform how an organization will achieve and prioritize the outcomes of the other five functions in the context of its mission and stakeholder expectations.



### IDENTIFY

Help determine the current cybersecurity risk to the organization. Understanding assets (e.g., data, hardware, software, systems, facilities, services, people) and the related cybersecurity risks.



### PROTECT

Support the ability to secure assets through awareness and training; data security; identity management, hardware, software, and services of physical and virtual platforms); and the resilience of technology infrastructure.



### DETECT

Enable timely discovery and analysis of anomalies, indicators of compromise, and other potentially adverse cybersecurity events that may indicate that cybersecurity attacks and incidents are occurring.



### RESPOND

Take action regarding a detected cybersecurity incident. This function covers incident management, analysis, mitigation, reporting, and communication.



### RECOVER

Restore normal operations in a timely manner to reduce the impact of cybersecurity incidents and enable appropriate communication during recovery efforts.

## What does a completed plan look like using this framework?

Take a look at the worksheet below, which includes some possible plans in gray. Download the fillable pdf to be able to replace these examples with your own plans on the following pages.

| NIST FUNCTION  | SHADOW IT SECURITY PLAN   |   |
|--|---|---|
|  <p><b>GOVERN</b></p>   | <p><b>Ensure steps in place to regularly manage sites of shadow IT risk:</b></p> <ul style="list-style-type: none"> <li>• Write a BYOD policy.</li> <li>• Ensure a compliance policy is written and shared by IT personnel.</li> <li>• Establish an employee/IT policy around the usage of shadow IT.</li> <li>• Establish an employee/IT policy around the usage of personal applications on corporate assets.</li> <li>• Establish an employee/IT policy around the usage of shared accounts across corporate assets.</li> <li>• Establish an employee/IT policy around how employees should request new applications be added in the organization.</li> <li>• Establish an employee/IT policy on how applications should be decommissioned.</li> </ul> |   |
|  <p><b>IDENTIFY</b></p> | <p><b>Create an inventory that has the following information outlined, per application:</b></p> <ul style="list-style-type: none"> <li>• Application Name</li> <li>• Application Publisher</li> <li>• Application Internal Point of Contact</li> <li>• Application External Point of Contact</li> <li>• Application Initial Use / Adoption Date</li> <li>• Application Approval State</li> <li>• Application Purpose Internally</li> <li>• Application URL(s) where necessary</li> <li>• Application Version(s) where necessary</li> <li>• Application Deployment Mechanism</li> <li>• Application Security Measures (SSO/MFA)</li> </ul>   | <p><b>Create an inventory that has the following information outlined, per user:</b></p> <ul style="list-style-type: none"> <li>• User information (name, email, contact)</li> <li>• Main user account in use</li> <li>• Additional user accounts that user has access to</li> <li>• Applications the user has access to</li> <li>• Primary account is SSO/MFA enabled</li> <li>• Additional accounts are SSO/MFA enabled</li> </ul> <p><b>Answer additional questions:</b></p> <ul style="list-style-type: none"> <li>• What type of data is in cloud applications and do these applications adhere to my compliance standards?</li> <li>• Which tools in my arsenal can identify and track shadow IT?*</li> <li>• Which user accounts are being used to access software?</li> </ul> |

\*If you don't have one in place, we'll discuss what to look for in tools that can help in the next section!

**NIST FUNCTION**

**SHADOW IT SECURITY PLAN**



**GOVERN**

Ensure steps in place to regularly manage sites of shadow IT risk:







**IDENTIFY**

Create an inventory per application:

Create an inventory per user:

Answer additional questions:



| NIST FUNCTION  | SHADOW IT SECURITY PLAN  |   |
|--|--|---|
|  <b>PROTECT</b>   | Keep attendance at security training sessions or implement a virtual learning method that is trackable for compliance purposes.                |   |
|  <b>DETECT</b>    | <p><b>Answer these questions:</b></p> <p>Where do I go to find information about who is using a tool, what they are using it for, and why?</p> | <p>Do I have a policy in place to implement when shadow IT is detected (whether it is disabling access to or enabling training on the threat)</p> |
|  <b>RESPOND</b>   | <p><b>Answer these questions:</b></p> <p>When shadow IT is discovered, who is responsible to remediate?</p>                                    | <p>Who is responsible for updating documentation?</p>   |
|  <b>RECOVER</b> | <p><b>Answer this question:</b></p> <p>What steps can I take to restore sanctioned processes and minimize future shadow IT appearances?</p>    |   |

# Evaluating tools for your business

Evaluating new tools can be a tedious process, which is why it can help to have a checklist of what to look for.

As you take demos for software or try different manual processes, keep the following in mind:

- What does the tool track** (SaaS, network traffic, BYOD, compliance, etc.)?
- Where does the tool pull data from** (applications, browsers, devices, connections)?
- Who is responsible** for using the tool or reporting on it (me, my manager, others)?
- When or how often does the tool pull data** (daily, weekly, monthly, annually)?
- Why will this tool help** prevent shadow IT (visibility, security, alerting, etc)?
- Does this tool align** with my security and compliance requirements (if you don't have any in place, check out the previous section)?
- Any other industry or business **specific concerns**?

*Chances are good that if a product or process has satisfactory answers to the above questions, it will do a good job mitigating shadow IT risk.*

Here's another example that's been filled out for

**Auvik SaaS Management (ASM):**

| QUESTION                               | AUVIK SAAS MANAGEMENT ANSWER   |
|--|--|
| What does the tool track?              | SaaS applications, including desktop and browser apps and workspaces   |
| Where does it pull data from?          | Application history, login information   |
| Who can use the tool?                  | Easy to use and automated for many actions   |
| How often can it pull data?            | Automatic and manual options   |
| Why does it help with shadow IT?       | <ul style="list-style-type: none"> <li>• Reducing SaaS redundancy</li> <li>• Reporting on what applications are in use</li> <li>• Reinforcing on/off boarding standards</li> </ul> |
| Does it align with the NIST framework? | ASM is excellent at the Govern, Identify, Detect, and Respond functions.   |
| Other notable concerns?                | <ul style="list-style-type: none"> <li>• Improves visibility</li> <li>• Alerts to vendor breaches</li> <li>• Keeps an inventory for compliance</li> </ul>                          |

## From evaluation to implementation: How Brightworks MSP found success with Auvik SaaS Management



Managed service providers (MSPs) face growing challenges caused by their customers' increased usage of shadow IT, specifically SaaS applications. And customers themselves are recognizing the need for SaaS management to address these challenges. According to the [2022 CompTIA State of the Channel Survey](#), 47% of MSPs said customers specifically asked them for a SaaS management solution.

**That's where Auvik SaaS management (ASM) comes in.** One MSP, Brightworks, implemented ASM and saw immediate benefits.

The Brightworks Group is a digital transformation and cloud transition IT service company offering cloud-based managed services to companies in a range of industries such as Healthcare, Financial Services, Engineering, Dental, Distribution, Manufacturing, Dermatology, Multi-Location Businesses, and more.

With a focus on delivering high-quality service, Brightworks has a reputation for providing innovative solutions to meet the needs of its customers. However, with the increasing adoption of SaaS applications, the company faced new challenges in managing the cost and usage of these applications. Brightworks needed a solution to give them visibility into their clients' SaaS ecosystem and help them manage their customer's licenses efficiently. They also required a tool to identify and address compliance issues and reduce customer risk.

By using ASM to run an automated assessment and having a stack-ranked list of shadow IT, Brightworks detected areas to improve in customer environments quickly.

**"Sometimes [employees] don't understand that they're not supposed to use unauthorized solutions for work. It's just a human error kind of problem," said Doug Miller, Brightworks' CEO.**

Thanks to Auvik SaaS management, brightworks was able to detect several unauthorized solutions and stop their continued use. This additional benefit to their standard service has saved their clients money on unnecessary expenses by identifying and removing these rogue applications.

"The license monitoring and management capabilities—probably top the list of most valuable features in terms of everyday utility. You can go to customers and say, 'You have 100 licenses of Office 365 E3, but you only use 95, so we can adjust your licensing and save some money.'"

ASM also works to cut time from MSP client onboarding, as SaaS documentation done manually can take days, which ASM reduced to a couple of hours.

**Want to see how Auvik SaaS Management helps curb shadow IT? [Check out the 14-day free trial.](#)**

# Shadow IT: A quick summary

So you're coming to the end of this ebook—what have you learned about shadow IT?

If you take nothing else from what we've covered, consider the following:

1. **The key definition:** "Shadow IT" refers to any IT-related activities happening inside the organization but outside the supervision of the official IT department. This includes systems, devices, software, applications, and services used without explicit IT approval. The largest shadow IT threat currently is web-based applications.
2. **The key culprits:** Everyone is at risk of using shadow IT because it can improve efficiency, speed up innovation, and create comfort and employee engagement.
3. **The key risks:** Business operations, security, compliance, visibility, and finances are at risk due to shadow IT. And it's still a manageable issue to tackle—if you get ahead of it as soon as possible.
4. **The key framework:** Any standardized security framework can be built to include shadow IT prevention. We recommend following NIST functions and mapping them to tasks that are actionable for you.
5. **The key questions:** The checklist supplied for evaluating business tools to help manage shadow IT risk can be revisited whenever you are ready to get some assistance with mitigating this risk.

It may seem like a lot to ask initially, but the payoff for your IT team will be huge if you take time to educate other employees and put policies in place to prevent shadow IT. Your organization can be more efficient, cost-saving, and compliant about shadow IT thanks to your growing light of expertise.

# Discover, Monitor, Manage and Secure SaaS Apps

## Eliminate shadow IT with Auvik SaaS Management

### Powerful and automated discovery

Discover and automate the documentation of your entire desktop, business, and SaaS applications inventory. Our powerful solution works in the background, requiring no additional effort to document.

### Access and account inventory management

Understand where risks come into play across the entire app stack. Be alerted and stay up-to-date on compliance risks in your business, such as employees sharing accounts or using service accounts.

### Understand risky shadow IT

Quickly spot what applications employees are adopting in the shadows that are putting your critical business data at risk.

### SaaS health scorecard

Understand where to begin with your SaaS health score.

### Visually compelling and powerful reports

Reports across the entire SaaS stack, such as: compliance & discovery report, employee off-board checklists, license review, and quarterly business review on Shadow IT adoption.

### Streamlined employee offboarding

Prepare a checklist of all the applications the employee used in their role. Share reports internally & externally to empower HR, IT, and business leaders with the information they need to properly offboard an employee.



## Your full inventory in 30-minutes

Out-of-the-box installers for the most common RMM and endpoints tools allow for rapid deployment of our technology for an instant inventory.

## Free support

**Need help?** We're always here. Submit your question or email us at [support@auvik.com](mailto:support@auvik.com) as often as you need to.



## Get a Free Shadow IT Scan

[START MY SAAS SCAN](#)

Uncover and address hidden IT dangers before they become full-blown security breaches. Access the results for 14-days and export them from the system with our powerful reporting.

## How SaaS monitoring and management can help



### Discover and manage

Understand all SaaS apps in use and take control of your SaaS environments.



### Maximize savings

Identify Shadow IT and SaaS app redundancy to cut unnecessary spending.



### Reduce risks

Identify vendor security incidents, prevent login sharing, and stop personal accounts for corporate apps.



### Save yourself time

Automatically build employee on-and-off-board checklists and stop tracking SaaS apps manually.