thirdpartytrust | BITSIGHT

Shadow IT

A playbook on policy & strategy for security leaders

thirdpartytrust | BITSIGHT

→ Contents

1 About Shadow IT

thirdpartytrust | BITSIGHT

→ Understanding the Shadow IT Issue

When high-profile supply chain attacks such as SolarWinds or Kaseya hit the news, many businesses were shocked first, and terrified second. Why? Because IT and security teams had to quickly scramble to understand if—and how—their networks were connected to these major companies.

Data breaches don't only happen to business-related networks. In 2021, a US contact-tracing company **exposed** the details of 70,000 individuals after employees used Google accounts for sharing data, as part of an "unauthorized collaboration channel." As employees use Google login credentials at home and at work, private networks are increasingly at risk.

As a security leader, you can't protect what you can't see, especially as your organization's network expands with remote work and Cloud computing:

The average employees' home office contains 9 out of 10 devices connected to the Internet.

Each device can contain personal and business credentials, putting your network at risk with each third party vendor (secretly) becoming a part of your network.

This inevitable consequence of WFH policies and Cloud-based services is directly related to Shadow IT.

This playbook is designed to provide you and your team with the history and gravity related to Shadow IT, while empowering you with policy and strategy suggestions that will help you to protect your network by managing your third party risk.

Whether you're looking for recommendations to make to your board or policies to discuss with your manager, this playbook aims to shed light on the Shadow IT problem most companies face whether they know it or not.

What is Shadow IT?

Shadow IT is the use of hardware, software, or Cloud applications without the knowledge or approval from the IT security team.

These non-approved technologies aren't vetted through the usual IT vendor onboarding process, which means they might have security standards that are below your organization's normal risk-thresholds.

It can be hard to believe that your IT department would miss critical third party vendors being given access to your network, but studies by **Beezy** and **HP** show that:

32%

of workers surveyed admit to using SaaS applications at work without getting approval from IT.

91%

of IT teams felt pressure to compromise security for continuity after the 2020 pandemic.

With the shift to remote work and the rapid adoption of Cloud-based services, the growth of Shadow IT has accelerated, often introducing security and compliance concerns. As a consequence, a shadow supply chain arises – a complex web of unknown Cloud applications, user accounts, data, and permissions scattered across the Internet.

With so many tools available online that are easy to sign up for and install, users have developed a habit of adopting Cloud apps and services to assist them in their work.

When employees bypass IT protocols, they're not actively trying to create risk; they just want to get their work done or test a new tool.

Sometimes they don't realize that even seemingly small installations need to be run through IT.

→ Why does Shadow IT exist?

Shadow IT arises due to several reasons:

- → **Accelerated digital transformation**
- → **The move to remote work and WFH**
- → **The need to scale operations fast**
- → **Restrictive IT requirements**

When the 2020 pandemic **accelerated digital transformation** and remote work, organizations focused on business continuity, often at the expense of cybersecurity. Certain policies were suspended to support the rapid shift to the Cloud as staff tried to get things done.

A **study by HP** found that, after the 2020 pandemic:

91%

of IT teams felt pressure to compromise security for continuity.

83%

of IT teams believed remote work was a “ticking time bomb” for a data breach.

As more people started using their personal devices to work from home, downloads of unsanctioned apps increased.

But Shadow IT existed way before the 2020 pandemic. Corporate users have long ago developed a habit of adopting Cloud apps and services to assist them in their work, sometimes bypassing IT security policies if they found them to be too restrictive or attempting against productivity.

While not a new phenomenon, Shadow IT is increasingly challenging IT security leaders as businesses shift to the Cloud and more apps are added to the network. Teams regularly rely on file storage apps, task management tools, messaging and email platforms, or even Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) systems everyday. One company with dozens of teams and hundreds of employees across unlimited channels Clouds any leader’s chance of clarity in a hurry in this reality.

What are examples of Shadow IT?

Shadow IT can encompass enterprise-grade tools or consumer tech. It's important to note that commercial third parties like the ones below are not necessarily more of a risk to your company than any other authorized vendor. The important distinction is that the following apps and services are both popular for employee personal use and often engaged without IT involvement, marking them as worthy of scrutiny:

Productivity
tools like:

slack ClickUp Trello

VOIP
tools like:

jitsi

Google Suite
tools like:

File-sharing
tools like:

Dropbox

Messaging
tools like:

WhatsApp

Physical devices not monitored by IT but connected to your network are also included, such as personal smartphones, laptops, or flash drives.

It's important to note that these applications are not dangerous per se, but only when they're used as a workaround that's different from the solutions proposed by IT. Imagine a scenario where a file is too big to send via Gmail (the official email app), so someone decides to use Dropbox instead. That's Shadow IT.

The problem is there, and it's worth addressing. With today's remote office environment, employees around the world are accessing your organization's network from home internet points.

This means that anyone else using that same Internet is also connected to the company's network, as well as your third party vendors and their employees, which dramatically expands the attack surface for cybercriminals to infiltrate.

→ Shadow IT By the Numbers

As more unsanctioned apps continue to enter the network, the attack surface expands.

To thrive in this environment, you need to be aware of these key Shadow IT stats:

32%

of employees are using collaboration tools that aren't explicitly approved.

21%

of employees say that solving IT issues has been extremely challenging for them.

58%

of employees aren’t completely satisfied with their company’s technologies.

53%

of employees know their activity on company-owned devices is monitored.

23% of baby boomers, **40%** of millennials, and **63%** of Gen Z think their workplace tools are unreliable, difficult to navigate, or don’t integrate well with others.

SOURCE:

15 Eye-Opening Shadow IT Stats You Need To Be Aware Of

→ *Read more*

2 Shadow IT in the Cloud

thirdpartytrust | BITSIGHT

→ Shadow IT and Remote Work

Employees around the world can today work from nearly anywhere. **Research found that:**

73%

of employees work in hybrid or fully remote settings.

43%

of employees work remotely full-time.

As they travel, so does their work, with their own personal laptops, mobile phones, WiFi connections, and personal accounts (e.g. Google, Zoom, etc.) allowing them to take their virtual offices nearly anywhere they are.

With each of these variables comes loss of control and visibility, two essential components at the core of any secure company's IT strategy and best practices.

BitSight began tracking potential troubles with WFH and security at the height of COVID-19. **Their findings include** the fact that home networks are 3.5x more likely than corporate networks to have at least one family of malware. Likewise, in people's connected homes, more than 25% of all devices have one or more services connected to the Internet.

In follow-up research, BitSight reports that even company-issued devices aren't necessarily secure depending on use. In this case, **BitSight found that:**

52% of company-issued devices were used by family members of employees.

As these devices interact with other systems in the house–everything from TVs to dishwashers–the exposure to five distinct families of malware jumped up to 7.5x more than could be exposed on a corporate network.

What many managers see as a remote work, WFH, or Cloud computing issue is really a Shadow IT issue. As employees use devices on external networks and–perhaps more importantly–mix work and personal computing habits (and accounts), the risk to organizations and their networks grows exponentially.

In order to thrive in this environment, managers need to weigh the pros and cons of risk, educate their employees, and take proactive steps to secure their data and networks even as devices and access are spread globally.

Here are some key areas to consider when planning your Shadow IT protections in light of remote work and WFH demands:

→ Physical devices

All Internet-accessible devices including computers, phones, and USB and Bluetooth devices should be secure upon leaving the office. Employees should have regular check-ins with managers and IT team members to ensure their devices are up to date and/or enabled with security software or user tracking.

→ Employee education

Employee education – Employees at all levels should be enrolled in continuing education modules and discussions around cybersecurity. Specific threats, policies, and best practices should be discussed before, during, and throughout the amount of time a given employee is working remotely.

→ Cloud services

Communication and collaboration services like WhatsApp, Gmail, or Google Docs should be regulated. Many such services utilize SSO across multiple sites, and even services that offer everyday encryption could be compromised.

→ Video services

Similar to the Cloud services mentioned above, video conference platforms like Zoom or Gong, and related VOIP services, should be regulated. Employees should be given access to and held to only using company (as opposed to personal) accounts on these platforms.

→ Apps

Apps, especially on mobile devices, often request access to users' contact information (and in some cases, files, location, etc.) As a result, apps on company devices should be treated as part of the enterprise stack, and should only be allowed once vetted and approved through formal IT processes.

→ Shadow IT and Cloud Computing

Cloud computing, the use of non-centralized hardware and services, has rapidly expanded to include a wide range of functions and business applications. While the expansion of blockchain and Web3 self-profess to give individual users more security, the net effect on organizations could be less insight and control in their networks.

For now, everything from automatic backup and recovery solutions to communications applications, productivity suites, data, analytics and CRM technology, Cloud services likely provide some of your organization's most valued solutions.

They also involve some of your most sensitive information.

There is nothing significantly nor inherently riskier about using Cloud services than other traditional on-site services. However, Cloud services–especially popular tools like the Google Suite, Slack, or Zoom–are increasingly commercial, meaning that employees may have both business and personal accounts attached to them.

Employees may increasingly see no difference between logging in to Zoom, for example, from their personal account than from their work account. It seems like a small detail to some. However, left unchecked, such small actions can become large headaches for risk concerns.

These concerns go beyond employees sharing company data. Using third party apps with varying credentials also opens up vendors and linked companies to data breaches. When they succumb to a breach, it can be disastrous for your digital assets residing in the Cloud.

Cloud security risk arises when organizations store sensitive data in the Cloud or rely on Cloud service providers for high-stakes business operations.

This can include data breaches, potential theft of data, compliance violations, malware attacks, and many other cyber security threats and vulnerabilities.

Managing Cloud security risk requires efficient strategies and powerful technologies that can deliver greater visibility into the risk profile of assets stored in Cloud environments. Consider the following best practices for managing Cloud security risk:

→ Get a holistic view of your network.

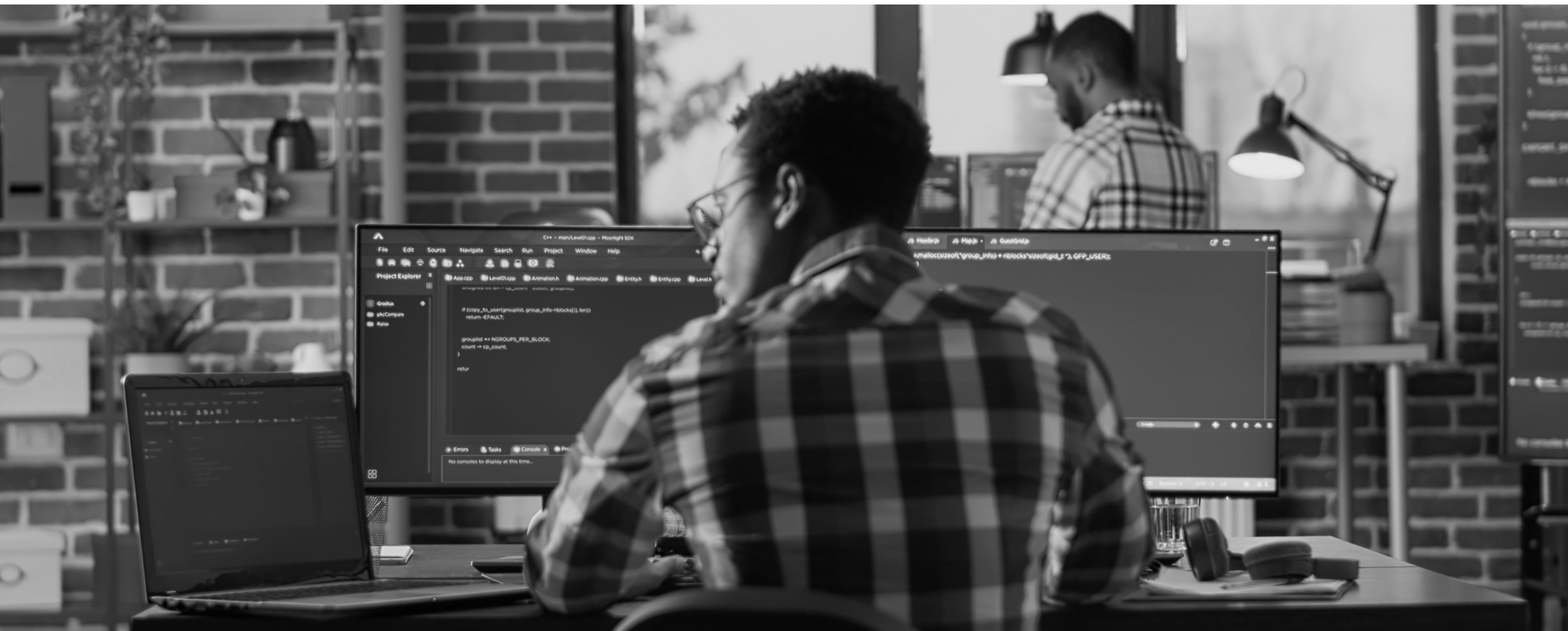
The best way to manage Cloud security risk is to get a clear picture of where the risk lies within your Cloud footprint. The challenge is finding the right technology. Many risk management technologies and manual scanning techniques don't deliver visibility into Cloud services, making it hard to get a complete picture of your digital ecosystem.

→ Rely on external, objective verification of your analysis.

Many cybersecurity solutions deliver only an internal view of your security posture. **Cloud security monitoring** solutions that provide an external view of your attack surface can validate the information you already have, without any internal bias.

→ Upgrade your reporting capabilities.

Superior reporting technology should allow you to summarize program changes, improvements, and **cybersecurity data** quickly and easily. Your reports should also provide a customized and easily understood security framework with context and benchmarks that facilitate conversations with company decision-makers.



3 Addressing Shadow IT

thirdpartytrust | BITSIGHT

How to Discover Shadow IT in Your Network

The key to combating Shadow IT is visibility. The problem with these assets is that they're unmanaged, especially in Cloud instances, where the attack surface can expand significantly without the organization being aware of the risk.

Detecting hidden assets requires continuous monitoring and scanning of the network, and, as it so often happens, technology can help. Manual processes or tools requiring oversight from a member of the IT department can be time consuming, and can fail to monitor every corner of your network.

IT security leaders need a way to proactively discover Shadow IT across their digital ecosystem, without relying on manual reports or asset tracking, as well as the ability to quantify the risk posed by those assets.

Several solutions available on the market were designed for this purpose. The capabilities you should look for include:

- Extended network monitoring, to discover hidden assets and Cloud instances
- Centralized data, to visualize the location of your organization's digital assets, ideally broken down by Cloud provider, geography, and business unit
- Data analytics, to identify areas of critical or excessive risk, determine areas of highest exposure, and prioritize remediation

As your digital supply chain continues to expand, managing cyber risk across its increasingly complex attack surface is challenging. You need to get a handle on the risk hidden across digital assets in the Cloud, geographies, subsidiaries, and a remote workforce. After all, you cannot secure what you cannot see.

Once you achieve full visibility over your shadow supply chain, the next step is to build a Shadow IT policy that covers how to proceed upon finding hidden assets.

How to build a Shadow IT policy

The main problem with Shadow IT isn't really the need for new tools, it's the fact that people use them without IT knowing. This usually happens because they perceive IT policies as restrictive and antagonistic toward their productivity. In this way, Shadow IT is a policy, not a software, issue.

So how can leaders encourage employees to involve IT without reducing their autonomy? Put simply, the solution to Shadow IT relies on people, processes, and technology.

Your company-wide policy should not be perceived as restrictive, but protective of the network. Incorporating new apps isn't necessarily detrimental to the organization, but they must be addressed appropriately. It's important that everyone knows this.

Your policy should include the following sections:

- ☑ Objective
- ☑ Intended audience
- ☑ Ownership
- ☑ Monitoring and enforcement methodology
- ☑ Accountability and employee responsibility
- ☑ Allowable scenarios or exceptions

The goal of this policy is twofold: To educate users so they don't need to turn to Shadow IT; and to be prepared to act if they do.

Addressing Shadow IT

The truth is Shadow IT will exist, so you need to be able to discover, list, and classify Shadow IT assets.

To that end, consider the following categories:

1 ✓ SANCTIONED
(audited and approved)

2 ✓ AUTHORIZED
(not sanctioned yet irrelevant)

3 ✓ PROHIBITED
(not sanctioned and dangerous)

This list should be continuously updated as part of routine security reviews. The next step is to decide what to do with each piece of unsanctioned and prohibited Shadow IT. Before making any decisions, try to understand the use case and the reasons why an employee decided to incorporate that technology.

Some useful questions for this discovery process include:

- ☑ What business need, if any, does this asset satisfy?
- ☑ Do any of our approved tools already cover that need?
- ☑ Is there any other solution that IT could provide?
- ☑ What risks does the Shadow IT asset create?
- ☑ Does the asset benefit many and outweigh the risks?

Depending on how necessary the asset turns out to be, the IT team will move it to the Authorized list, replace it with an existing function, or discontinue its use.

4 Reducing Shadow IT

thirdpartytrust | BITSIGHT

→ Practical tips to reduce Shadow IT

As employees work remotely, company and personal technology converge, making it important for organizations to get a handle on their Shadow IT issues.

Here are the steps you should take to minimize and eliminate your organization's blindspots.

1. Build a comprehensive policy

When employees incorporate new technologies bypassing IT protocols, they're not actively trying to create risk; they just want to get their work done or test a new tool. Sometimes they don't realize even the seemingly smaller installations need to be run through IT, and other times they're in a hurry.

Using the guidelines in the section above, document a company-wide policy that's not perceived as restrictive but protective of the network, and make sure everyone understands that incorporating new apps isn't necessarily detrimental to the organization, but that they must be addressed appropriately.

→ *Learn more*

2. Monitor your Cloud to discover Shadow IT assets

As your digital ecosystem expands, it's critical that you understand which assets are in the Cloud, and whether or not those Cloud instances are configured correctly. If your organization is global or contains subsidiaries, this includes insight and context into where risk may be present in various geographies and business units.

Leveraging purpose-fit solutions and capabilities will help you discover hidden assets in your network as part of routine security reviews, and bring them into line with your security policies. This can include automated

continuous monitoring, network discovery, and risk assessments to identify areas of concentrated risk, as well as identify gaps in Cloud security controls, such as misconfigurations, vulnerabilities, and unpatched systems.

→ *Learn more*

3. Empower employees with the right tools

The need to turn to Shadow IT will drastically reduce if your employees already have the tools they need. Ask people what they need regularly -be it communication, productivity, file-sharing, or help desk apps, and incorporate them into your stack.

This will make it easier to roadmap your digital workflows and integrate different technologies to deliver maximum productivity, while keeping your 360° visibility.

→ *Learn more*

4. Leverage security basics

Complement your Shadow IT policy with essential security measures, such as VPNs, MFA, antivirus, encryption, backup, patch management, **user management** with the least-privilege principle, etc.

In particular, adopting a **zero trust** security model, where each user is verified before they connect to the network, ensures they can only access data, networks, and applications for which they have a business need.

5. Educate your workforce

As remote work expands the attack surface, make sure you include Shadow IT in your cybersecurity training to educate employees about the potential danger of their decisions. Share specific recommendations and best practices, and make them aware that they need to be extended beyond the corporate network and into their homes.

Some of your users may not be aware of the potential security risks that come with downloading an app. Your ultimate goal is to bring everyone up to speed on changing threats and how to protect the organization.

6. Prioritize your remediation efforts

In order to get the greatest ROI for your cybersecurity initiatives, you must allocate your limited resources based on the criticality and level of risk associated with each asset. For instance, you should prioritize remediating any incidents that involve a critical asset with a high risk of breach.

Once again, visibility is the key to give context to your current cybersecurity outlook, as opposed to filtering through massive amounts of data in order to identify the most severe or potentially severe security events. This will help you prioritize decisions and hold appropriate teams accountable for their progress over time.

7. Continuously monitor your program effectiveness

Set up goals to continually improve, track progress, and report outcomes to key business stakeholders. It's critical that you have a common set of **cyber security KPIs** to measure and communicate the effectiveness of your security program over time.

According to **Forrester**, "companies that have implemented formal security performance metrics are more likely to have seen a 10% or greater increase in security budget year over year."

Security ratings are a data-driven, objective, and dynamic measure of security performance, which is why thousands of organizations around the world use this KPI to manage cyber risk where transparency may have historically been lacking.

→ ThirdPartyTrust and BitSight Solutions

All the Shadow IT assets your network may be connected to are, whether approved or not, your third parties. This ultimately makes Shadow IT a third party risk management (TPRM) issue.

ThirdPartyTrust is a third party risk management automation tool that streamlines vendor risk assessments and improves visibility over third party vendors across the extended supply chain. In an ideal world, every Cloud vendor your organization interacts with would be a vendor that you've assessed, approved, and added to your monitored inventory as part of your TPRM program.

In reality, employees often bypass IT security teams and engage with third party Cloud vendors without their approval, and these vendors might go undetected for a while. Which brings us back to Shadow IT.

We at ThirdPartyTrust understand vendor risk management as a holistic capability, which is why, in addition to our vendor risk assessment and continuous monitoring capabilities, we have integrated Netskope capabilities that allow our customers to not only monitor known vendors, but also those that might have gone under the radar.

The ThirdPartyTurst and Netskope integration allows security and risk management leaders to supercharge risk monitoring into the far reaches of their networks, monitoring individual usage activities in the Cloud and across every interaction. This functionality serves multiple use cases:

- ☑ Capturing Shadow IT records, that is, usage of Cloud applications or vendors that IT security is unaware of.
- ☑ Mapping network discovery data into standard third party risk assessment questionnaires.
- ☑ Automating impact score and policy action with custom rules, i.e. if a vendor is used by many users and has access to a high amount of data, increase their potential impact on the business.

Similarly, **BitSight offers Attack Surface Analytics**, a solution that specifically helps program managers discover hidden assets and Cloud instances on their network. BitSight will assess the discovered areas of Shadow IT for their inherent risk to your business, and then help bring them into line with your corporate security policies.

These capabilities will help you achieve 360°, continuous visibility into your digital ecosystem as part of an effective security performance management program. The findings can be used to enhance your controls and configuration, but continuously learning from internal and external data processing (impact, user behavior, service interactions, transactions, etc.).

In a Shadow IT use case, you'll be able to discover unknown vendors with access to your network and:

→ **Gain visibility into digital assets to identify areas of disproportionate risk**

→ **See how many users in your network are engaging with the vendor**

→ **See how much time your users have engaged with the vendor**

→ **See how much data the vendor has accessed, measured in MBs**

→ **Add the vendor to your actively monitored vendor inventory and subsequent TPRM process (risk assessment, scoring, questionnaires, reassessments, etc.)**

→ **Create a rich data bridge between DevOps, GRC, and IT security, where findings are no longer siloed, but shared to increase collaboration**

thirdpartytrust | BITSIGHT

Featured Resources

CHEAT SHEET

Practical Tips for Managing Shadow IT

→ *Learn more*

WEBINAR ON DEMAND

How to Make Risk Management a Priority for Your Organization

→ *Learn more*

STRATEGY GUIDE

The Problem with Passwords: Protect credentials in your supply chain

→ *Learn more*