What's Lurking in Your Environment?

How Cyber Leaders Can Address Shadow IT & Hidden Risk

BITSIGHT

Table of Contents

01 Understanding Hidden Risk **3**

What is Shadow IT? 6

Why Does Shadow IT Exist? 8

What are Examples of Hidden Risks? 10

02 Managing Hidden Risk Holistically **12**

How to Discover Shadow IT in Your Network 13

How to Build a Shadow IT Policy 14

Practitioner's Corner: A Real-World Perspective on Risk Governance 16

Practical Steps to Reduce Shadow IT 18

Bitsight Solutions to Address Hidden Risk 22

01
Understanding Hidden Risk

Understanding Hidden Risk

By Tim Grieveson
Senior Vice President - Global Cybersecurity Risk Advisor, Bitsight

Shadow IT continues to be a pressing issue for IT and cybersecurity leaders—but that's the tip of a rather large iceberg concealing a growing number of threats found across today's expanding attack surface.

Missing software patches and security updates, outdated or misconfigured certificates, default or common passwords on hardware, and stealth malware are just a few examples of the risks that these shadow IT solutions can introduce silently and rapidly into the enterprise infrastructure. When high-profile supply chain attacks—like those suffered by Okta or MOVEit—make news headlines, businesses immediately scramble to quickly understand if (and how) they rely on these third parties and how these incidents impact their own data.

As a security leader, you can't protect what you can't see—especially as your organization's tech ecosystem expands at an exponential rate with a mix of hybrid working models and increased reliance on cloud providers encompassing SaaS, Paas, and IaaS. Employees around the world connect to external solutions and services including data, applications, personal and corporate accounts, financial and HR systems, as well as a plethora of collaboration tools (eg. Gmail, Slack, Jira, Zoom, Microsoft Teams, Salesforce, or Workday).

Today many organizations have adopted a hybrid approach to working patterns and no longer is it good enough to put critical services behind a firewall and call them secure.

Tim Grieveson

Beyond an organization's "perimeter" (which in itself has evolved quite a bit these last few years) the average employee's workspace contains multiple devices connected to home or public internet networks. These are often commissioned without the involvement of corporate IT, as they can be purchased on a credit card and available to be used immediately as opposed to waiting for an approved device or application to be provisioned.

Each additional third-party solution or vendor brought into the mix without proper vetting or authorization can introduce new risk. But outright prohibition never leads to good things. The old way of simply blocking access to a whole family of applications or services just drives people further away from corporate visibility and into the shadows.

The inevitable consequence of hybrid working, easy access to services, software or hardware, and cloud-based access is directly driving an increase in shadow IT capabilities being seen across organizations.
So what can cyber leaders do to overcome these challenges, and find the right balance of employee convenience, accessibility, and proper security posture?

This playbook is designed to provide you and your team with a holistic understanding of hidden risks, and arm you with policy and strategy suggestions to protect your expanding digital footprint and infrastructure.

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

Business users demand access from anywhere, at any time and on multiple devices without security controls getting in the way, insisting security teams enable them in a seamless and simple way.

Tim Grieveson

What is Shadow IT?

Shadow IT is the unauthorized use of hardware, software, or cloud applications within the organization. These are typically adopted without explicit approval, oversight, or involvement of the IT security team.

Because shadow IT technologies aren't assessed through the usual procurement, due diligence, and vendor onboarding processes, their security standards might be below your organization's normal risk-thresholds or risk appetite. It is also possible that integrations, configuration, and access requirements may not be fully understood and introduce unknown exposures to existing solutions that have gone through the onboarding process—which can remain undetected for months or years after implementation.

As a consequence, a "shadow supply chain" arises: a complex web of unknown cloud applications, user accounts, data, and access permissions scattered across the infrastructure and the internet—often with limited documentation, absent or inadequate security assessment, support, or disaster recovery arrangements in place.

of IT professionals find SaaS sprawl challenging to manage.

of all SaaS applications in use are unsanctioned. [1]

[1] Source: 2023 State of SaaSOps, BetterCloud

Business owners tend to assume the cloud service provider will take care of security, when in fact it's often a shared effort—if not entirely the organization's responsibility. It is generally much easier to remediate any vulnerabilities in collaboration with the vendor before implementation as opposed to after, and of course, much more sensible than recovery or remediation after a cyber incident or data exposure—which could have wider ramifications to the enterprise in terms of operational disruption, costs, reputation, loss of revenue or regulatory compliance, fines, or sanctions.

Diminishing visibility presents a multifaceted challenge for CISOs and cybersecurity leaders. As employees increasingly turn to readily available and easily deployable but often unauthorized applications and services, an organization's digital landscape becomes fragmented, difficult to govern and oversee comprehensively. This in turn may contribute to business disruption, lost revenue, damage to reputation, or even a security or privacy incident.

> **"Uncovering hidden risks addresses issues of regulatory compliance, integration complexity, strategic management of IT assets, and prioritization of resources—all of which impact budget, profitability, efficiency, and effectiveness.**

Tim Grieveson
Senior Vice President - Global Cybersecurity Risk Advisor, Bitsight

Why Does Shadow IT Exist?

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 security protocols, they're not actively trying to create risk. They want to get their work done faster or test a new tool, which often becomes the ongoing production solution without any security or IT involvement—until something stops working or has a security compromise. And this is often an indicator that there's room for improvement when it comes to workplace management technology.

Security professionals need to work on building relationships with employees, ensuring they understand how seemingly innocuous actions can inadvertently harm the organization or cost more in the long term due to extended incident investigation, remediation, or support.

of surveyed employees aren't completely satisfied with their workplace tools and technologies, and experience challenges with available solutions. [2]

[2] Source: 2023 Workplace trends & insights report, Beezy

Sometimes they don't realize even the seemingly smaller installations need to be run through IT. Other times, they're in a hurry and simply don't want to wait for IT's green light.

Shadow IT, then, arises due to a number of reasons:

- Digital transformation and the need to scale operations fast
- Hybrid workers not realizing that personally managed SaaS tools might introduce risk
- Approved tools or SaaS services not providing the required functionality
- Slow or ineffective processes to request assets or services
- Restrictive IT requirements or distrust of IT's ability to deliver
- Lack of awareness around onboarding process or Acceptable Use Policy
- Budget sits within business budget and not IT

> **"Blocking access can create unnecessary user friction and cause employees to circumvent processes further. We need to empower users to use sanctioned tools and work with them to identify shadow IT to enable the organization safely."**
>
> **Ryan Swimm**
> GRC Program Manager, Bitsight

What are Examples of Hidden Risks?

Shadow IT can encompass enterprise-grade tools or consumer tech—but they're not inherently more of a risk to your company than any other authorized vendor. These applications are not dangerous, per se—but they can be when they're used without IT security involvement or scrutiny.

Imagine a scenario where a file is too big to send via Gmail (the approved email app), so someone decides to use Dropbox instead. That's shadow IT.

Other examples include:

- Task management tools like ClickUp, Trello, or Asana
- Communication tools like Skype, Zoom, or Jitsi
- Messaging tools like WhatsApp, Signal, or Telegram
- Physical devices like flash drives and smartphones
- Cloud storage and file-sharing tools like Google Drive, Dropbox, or OneDrive

of all HTTP/HTTPS malware downloads originate from common SaaS services like OneDrive, Sharepoint, Google Drive, or GitHub. [3]

With today's remote office environment, employees around the world are accessing your organization's network from home or open internet points. Add your third-party vendors (and their employees) into the mix, and cybercriminals have quite a few doors to potentially infiltrate.

> **"Shadow IT is not Bring Your Own Device (BYOD), where the organization has some degree of ownership, control, and accountability. It becomes an unknown risk—unless they find a way of harnessing shadow IT as part of their monitoring and assessment processes.**
>
> **Tim Grieveson**
> Senior Vice President - Global Cybersecurity
> Risk Advisor, Bitsight

[3] Source: Threat Labs Stats for November 2023, Netskope

02

Managing Hidden Risk Holistically

How to Discover Shadow IT in Your Enterprise

The key to addressing shadow IT is enabling visibility, transparency, and collaboration. Detecting hidden assets requires continuous monitoring and scanning of the enterprise—at scale, in a repeatable and manageable way. 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 enterprise.

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

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

As the digital supply chain continues to expand, managing cyber risk across its increasingly complex attack surface can be challenging. Cybersecurity leaders need to get a handle on risks across all digital assets irrespective of location—such as in the cloud, different geographies, subsidiaries, or suppliers, and across remote workforces and regulatory jurisdictions. 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.

> **"SaaS and IaaS services pose challenges. Let's say the Google suite is approved for emails, calendar, and file sharing—organizations still struggle with managing various instances of the same application and controlling what data can go to the corporate instance versus a personal or third-party owned instance required for collaboration."**
>
> **Ryan Swimm**
> GRC Program Manager, Bitsight

How to Build a Shadow IT Policy

The challenge with shadow IT isn't really the need for new tools—it's the fact that people use them without approval. This usually happens because they perceive security policies as restrictive and antagonistic toward their productivity, which makes shadow IT a process issue, rather than a technological issue.

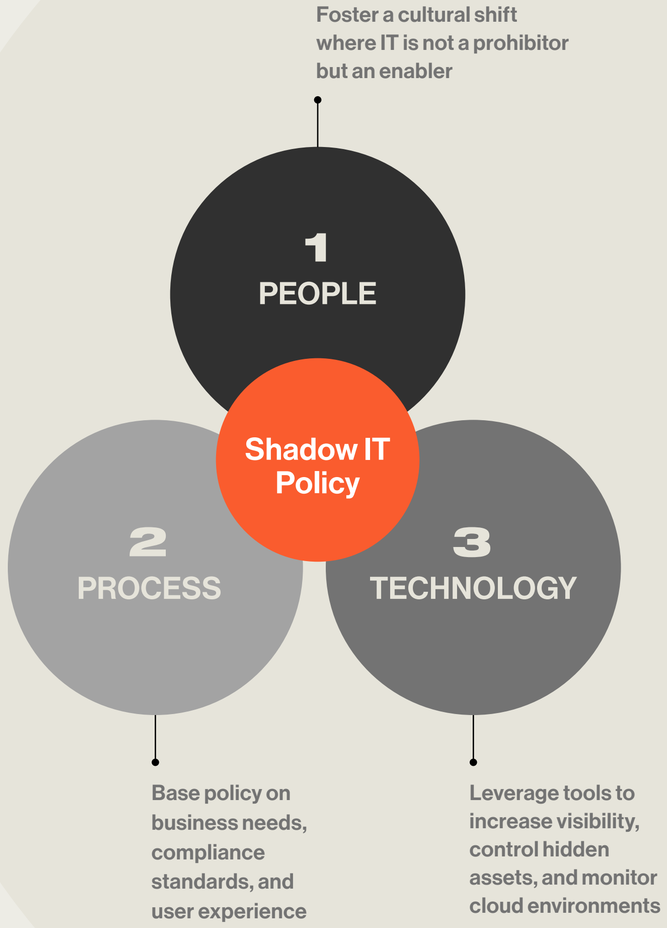
So how can leaders encourage employees to involve IT without reducing their autonomy? Put simply, the solution to Shadow IT relies on people, processes, and technology.

Incorporating new apps isn't necessarily detrimental to the organization, but they must be addressed appropriately. Your company-wide policy should not be perceived as restrictive, but protective of the company's data. New hires should acknowledge the shadow IT policy during onboarding, and all staff should provide an annual acknowledgment to reinforce it.

The policy should include the following sections:

- Statement and Purpose
- 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.



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:

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 needs, 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.

Practitioner's Corner: A Real-World Perspective on Shadow IT and Risk Governance

By Ryan Swimm
GRC Program Manager, Bitsight

The specter of shadow IT looms large, and Bitsight is not immune to this concern. Our primary challenge is securing our data and applications while empowering users to perform their duties efficiently.

Tackling shadow IT begins with formulating an effective policy that is well-known to all users. Bitsight has established internal policies, namely our Code of Conduct, Acceptable Use Policy, and Vendor Review Policy, to address hidden risks. These policies play a crucial role in educating users about the nature of data Bitsight handles and processes, emphasizing the collective responsibility to safeguard it. They also delineate the roles and responsibilities pertaining to data protection and compliance obligations.

> **Beyond Bitsight's SPM and TPRM applications, we deploy tools like Mobile Device Management (MDM) software and a Cloud Access Security Broker (CASB).**
>
> Ryan Swimm

To identify instances of shadow IT, Bitsight leverages its products. Utilizing Security Performance Management (SPM), we can pinpoint potential shadow IT risks through various vectors, such as Desktop Software and Server Software. These risk vectors enable us to detect unsanctioned vendors not included in our internal Vendor Risk Management (VRM) program. The Vendor Discovery tool within Continuous Monitoring (CM) further aids in confirming existing vendors and uncovering potential unsanctioned ones by cross-referencing against our CM and VRM vendor lists.

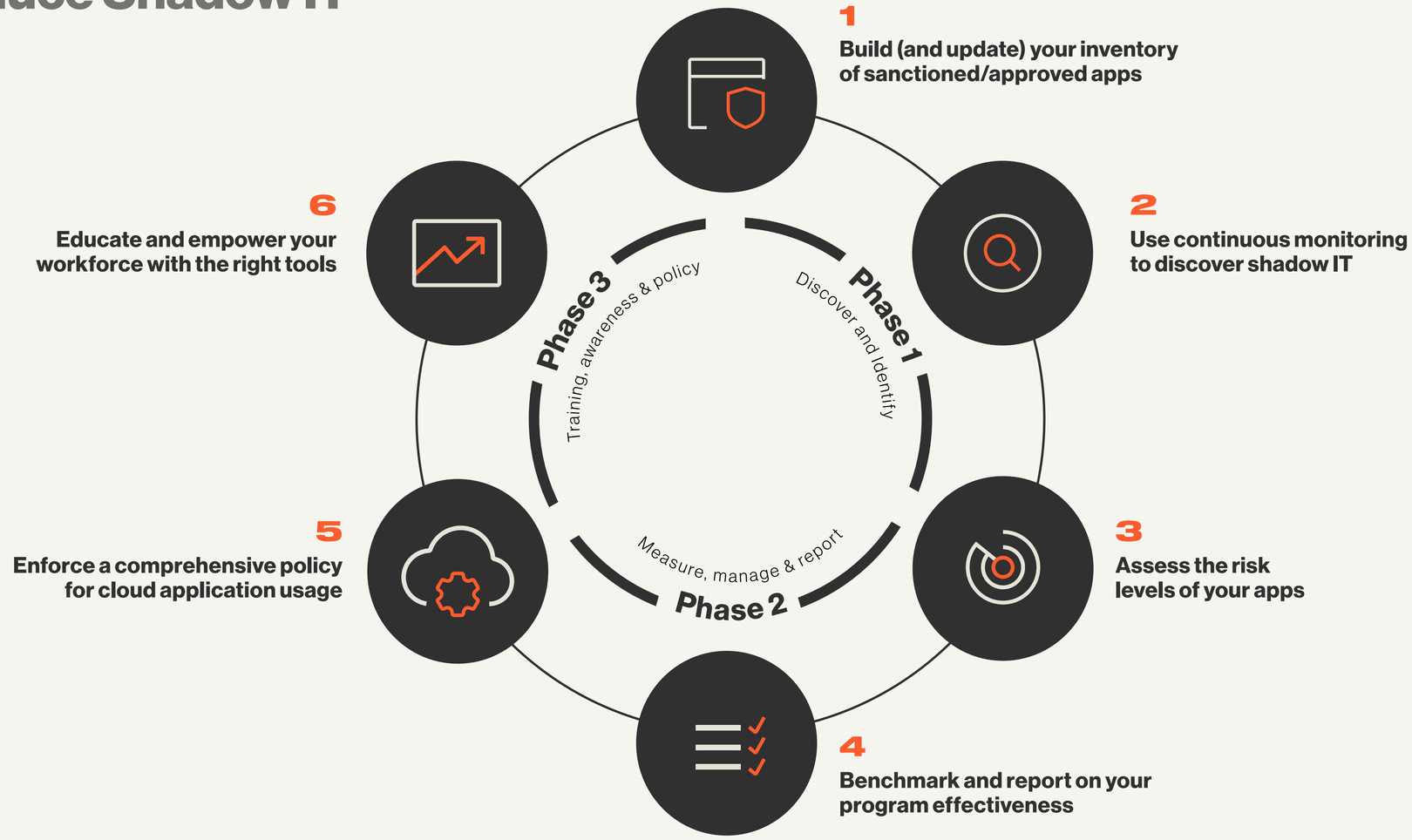
Beyond Bitsight's applications, we deploy tools like Mobile Device Management (MDM) software and a Cloud Access Security Broker (CASB). MDM software is strategically placed on all endpoints to identify locally installed software, with the capability to block any unauthorized installations. Our CASB, integrated into all user endpoints, surveils applications via web traffic, providing usage statistics and reports. This allows us to identify users employing non-sanctioned applications, monitor frequency, and scrutinize processed data. The CASB also empowers us to block traffic to specific categories of web activity (e.g., gambling, crypto-mining) or implement URL block lists.

Users may resort to alternative tools to achieve their objectives, and as part of our Governance, Risk, and Compliance (GRC) team, we take on the responsibility of devising practical solutions. This involves making users aware of sanctioned tools they might not be familiar with or guiding them to collaborate with their managers to procure a vendor if no viable alternative exists. Our commitment is to provide users with the means to excel in their roles while maintaining the highest cybersecurity standards.

Practical Steps to Reduce Shadow IT

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

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



1
Build (and update) your inventory of sanctioned/approved apps

2
Use continuous monitoring to discover shadow IT

3
Assess the risk levels of your apps

4
Benchmark and report on your program effectiveness

5
Enforce a comprehensive policy for cloud application usage

6
Educate and empower your workforce with the right tools

Practical Steps to Reduce Shadow IT

1. Build (and update) your inventory of sanctioned/approved apps

Maintain an up-to-date inventory of all authorized devices and vendors, and regularly compare this list with the results from network discovery tools to identify any anomalies. As part of your Vendor risk management (VRM) efforts, regularly review and update the list of authorized vendors, and monitor their activities and access levels closely. Use dedicated tools to simplify and automate vendor risk assessments and much as possible, as well as periodic reassessments.

Another factor to consider is vendors' criticality to your supply chain and their potential impact on your business continuity. These factors will help you build a tiering structure, where vendors with access to sensitive information or that are critical to business continuity are subject to more stringent requirements and audits. This ultimately allows your team to prioritize and focus on the highest risks, as opposed to managing all vendors equally.

2. Use continuous monitoring to discover shadow IT

Unusual patterns in network traffic analysis or unexpected connections to unknown SaaS solutions may indicate the presence of unauthorized vendors. If your organization is global or contains subsidiaries, you need 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. With real-time insights into your digital landscape, you can ensure timely detection and response to unauthorized applications and potential vulnerabilities.

See it in action: **Explore Auto Vendor Discovery**

Practical Steps to Reduce Shadow IT

3. Assess the risk levels of your apps

Understand the risks associated with each application in your ecosystem, and more importantly, the data involved within these apps. This will help you prioritize your remediation efforts: a file sharing service might not pose the same risk as a consumer app such as Spotify or Pandora.

In addition, it's important to evaluate whether the discovered services comply with regulatory requirements and relevant standards for your industry, like GDPR, NIS2, HIPAA, or PCI DSS.

4. Enforce a comprehensive policy for cloud application usage

Uncovering cloud services and understanding how they're being used is the first step. Then, you need to implement an ongoing process to sanction, mark for review, block, or offer alternative applications as a solution (Google Drive instead of Dropbox, for example.)

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 to reduce the associated risks.

Periodic policy acknowledgment from employees is a pivotal component in the robust enforcement of a comprehensive shadow IT policy. It serves as a continuous reinforcement mechanism, keeping cybersecurity protocols at the forefront of employees' awareness, and emphasizing the shared responsibility between the workforce and the security infrastructure.

Read the blog: **Keys to Building a Shadow IT Policy**

Practical Steps to Reduce Shadow IT

5. Educate and empower your workforce with the right tools

Make sure you include shadow IT in your cybersecurity training to educate employees about the potential danger of their decisions. Share your policy, provide specific recommendations and best practices, and make them aware that they need to be extended beyond the corporate network and into their homes.

The need to turn to shadow IT will drastically reduce if your employees already have the tools they need to feel productive yet not overly restricted. Ask people what they need regularly—be it communication, productivity, or file-sharing apps, and incorporate them into your stack. Technical teams are now also part of delivering greater employee experiences, by providing better tools, information, support, and unlocking new ways to work. This will make it easier to roadmap your digital workflows, consolidate vendors, and integrate different technologies to deliver maximum productivity, while keeping your 360° visibility.

6. Benchmark and report on your program effectiveness

Establish metrics to measure improvements and define a roadmap (possibly multiyear) aligned to industry recognised standards and regulations such as NIST, ISO27001, NIS2, or DORA—with the aim to continually improve, track progress, and report outcomes to the board and key business stakeholders. It's critical that you have a common set of cybersecurity KPIs or KRIs and a common language to communicate the effectiveness of your security program over time. Include Risk tolerance, Risk appetite and Risk treatment statements aligned to business values, business strategy, and common business outcomes.

Your reports should include context and benchmarks that facilitate conversations with non-technical audiences—especially as cyber regulations like the SEC requirements in the United States strengthen requirements around incident reporting. To communicate and compare your security posture, consider security ratings as part of your disclosure strategy—it's an objective analysis of an organization's cybersecurity performance based on quantitative, continuous data that creates comparable, reliable insights and metrics.

Bitsight Solutions to Address Hidden Risk

In an ideal world, every third-party your organization interacts with would be a vendor that you've assessed, approved, and added to your monitored inventory as part of your third-party risk management (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.

Bitsight Third Party Risk Management streamlines vendor risk assessments and improves visibility over third-party vendors across the extended supply chain. Because TPRM is a holistic function, in addition to vendor risk management and continuous monitoring capabilities, we enable our customers to not only monitor known vendors—but also those that might have gone under the radar.

Bitsight Auto Vendor Discovery instantly surfaces vendor relationships, uncovering hidden risks of previously unknown vendors that you can start monitoring over time. And with Portfolio Analytics, you can contextualize and prioritize risk insights from your third-party ecosystem with extensive data and analytics—proven to correlate to cyber and business risk. With these validated analytics, you can surface portfolio-wide risk insights correlated to cybersecurity incidents, expedite decision making through easy to understand Key Risk Indicators (KRI's), identify, respond to changing third-party risk over time.

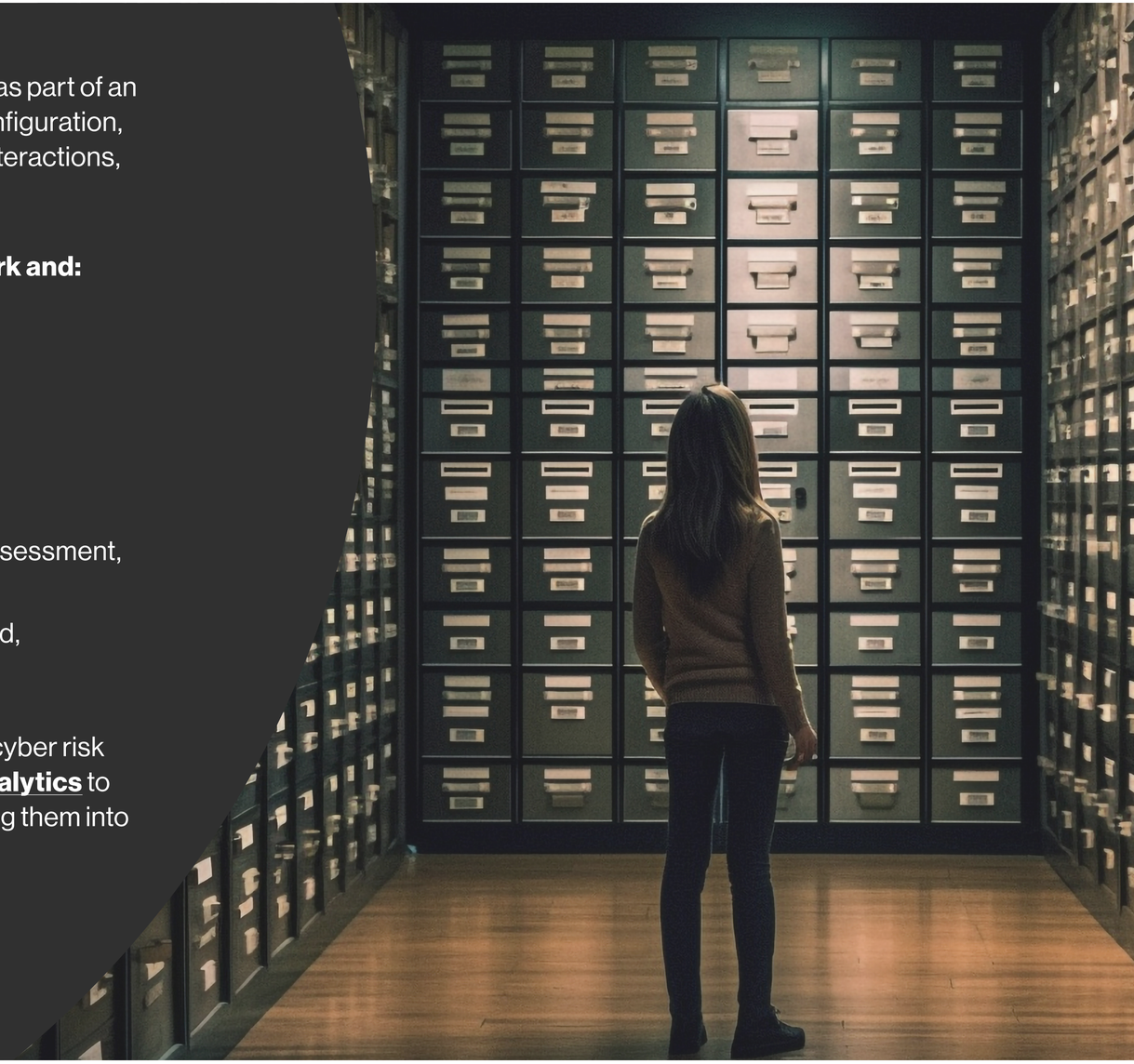
These capabilities will help you achieve complete and continuous visibility into your digital ecosystem as part of an effective cyber risk management program. The findings can be used to enhance your controls and configuration, but continuously learning from internal and external data processing (impact, 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:

- Contextualize cyber risk in a scalable way
- Translate cyber risk into business risk and effectively communicate to stakeholders
- Address hidden risks through immediate visibility into third-party connections
- See how many users in your network are engaging with a vendor, and for how long
- 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

While uncovering shadow IT in your supply chain is crucial, the real game-changer lies in truly holistic cyber risk management—addressing what's within your own network as well. Bitsight offers **Attack Surface Analytics** to discover hidden assets across your infrastructure, assess their inherent risk to your business, and bring them into line with your security policies.

Explore Bitsight Solutions



Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT