Cledara

The State of Shadow IT

A comprehensive report to understand the usage of unauthorized software in modern businesses.

Introduction

Shadow IT—software employees use without the approval or knowledge of their organization's IT team —is a very common phenomenon. However, it's urgently necessary for companies to bring their full tech stacks into the light.

IT teams can't secure what they don't know about, and by Gartner's estimations, one-third of successful attacks on enterprises are on data located in shadow IT resources.

Cledara has surveyed over 200 businesses to understand the scale and scope of shadow IT in 2023.

This original and exclusive report can help you understand how this phenomenon is likely to impact your business—and where to start looking if you want to reign your team's software usage in from the shadows.

You will learn:

- Which teams are most likely to bypass central software-buying systems
- The applications employees are most likely to use 'in the shadows'
- The prevalence of shadow IT in businesses like yours

Index

About the study

Here's an overview of the companies this data represents, and how Cledara captured it.

Who were the study participants?

This research examined the use of shadow IT in the form of SaaS (software as a service) across 200 companies. The sample included companies from industries with specific data security obligations, including the following sectors:

Financial

17.5%

These companies often hold customers' money and are lucrative targets for hackers.
They have regulatory obligations connected to third-party vendors.

Healthcare

7%

These companies store medical data relating to their direct customers or their customers' end users.
As such, they must comply with HIPAA regulations.

Cybersecurity or Identity

4%

For these companies, shortcomings in their own IT security could lead to their customers experiencing a breach.

Additionally, 27% of the sample companies currently hold SOC 2 or ISO 27001 certificates, recognized industry standards for information security and data protection.

About the study

How did we measure shadow IT usage?

To measure the amount of unauthorized SaaS usage at the companies in the study, all employees at these companies deployed Cledara Engage on their computers. This tool can:

- Spot shadow IT by collecting data on the software employees are using, authorized or unauthorized.
- Survey software usage to understand how often and how long tools are being used.

Each time an employee within the same group loaded the page of an unauthorized Saas product, we counted a single instance of shadow IT usage.

The research covered a period of 30 days during September and October 2023.

Why assess the state of shadow IT?

By the very definition of shadow IT, technology professionals never know exactly how widespread this phenomenon is in their companies.

However, it's essential to estimate the scale of the problem and start tackling it, since shadow IT poses a number of serious risks, some of them business-critical. Namely:

- Security risks. Unsanctioned tools may lack robust security features, and be more vulnerable to attacks and data breaches.
- Data integrity can be compromised. If shadow IT tools use nonstandard backups, there's danger of irreversible data loss.
- Compliance issues. Using unauthorized tools can lead to contract violations and breaches of industry-specific regulations and certificates —and, therefore, hefty fines.
- Unnecessary spend. As departments purchase overlapping tools and services without centralized oversight, unnecessary costs add up.
- Integration problems. When teams use incompatible tools, integration problems can lead to information silos and collaboration issues.

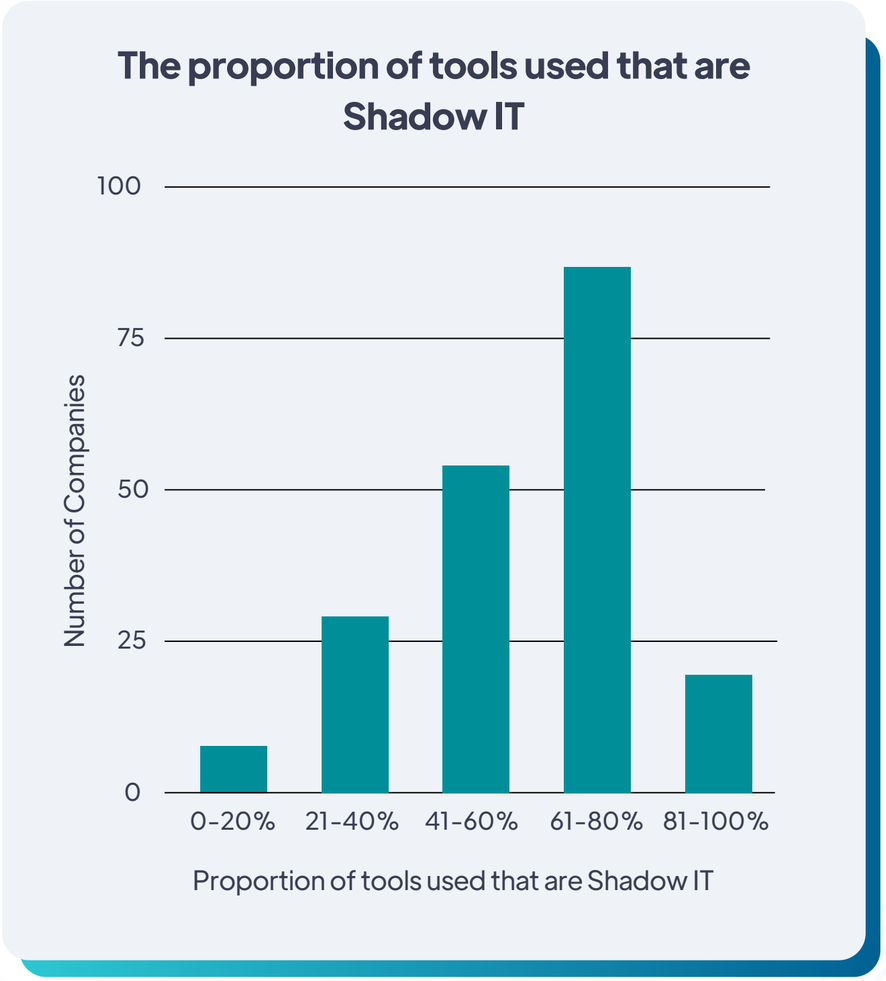
High-level results

Over the 200 surveyed businesses, there were a staggering 23.6 million instances of Shadow IT usage, across 2,259 unauthorized software platforms. This means that, over the course of an eight-hour workday, an employee accessed an unauthorized software platform every 4.9 seconds.

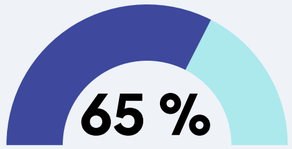
Companies experience Shadow IT usage on average every 4.9 seconds

In fact, shadow IT accounts for more than half of daily software usage for over half the companies surveyed. Whilst this might sound shocking, it corroborates previous survey-based research by the International Data Corporation (IDC). According to this research, Chief Information Officers (CIOs) believe more than 50% of IT spend happens outside of businesses' official IT budgets.

Surprisingly, just 3.5% of companies had Shadow IT usage of less than 20%.



High-level Insights



Of all SaaS applications accessed are Shadow IT

Page 12

On average companies use **75** tools that aren't approved

Page 13

4.9 Companies experience shadow IT usage every 4.9 seconds

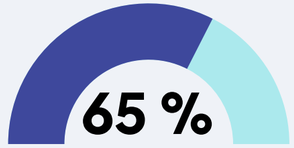
Page 10

ChatGPT is the most used Shadow IT tool. Usage grew 54% in Q4

Page 8

Of unapproved tools related to data operations

Page 8



Of Shadow IT usage is from Sales and Marketing teams

Page 7

Cledara

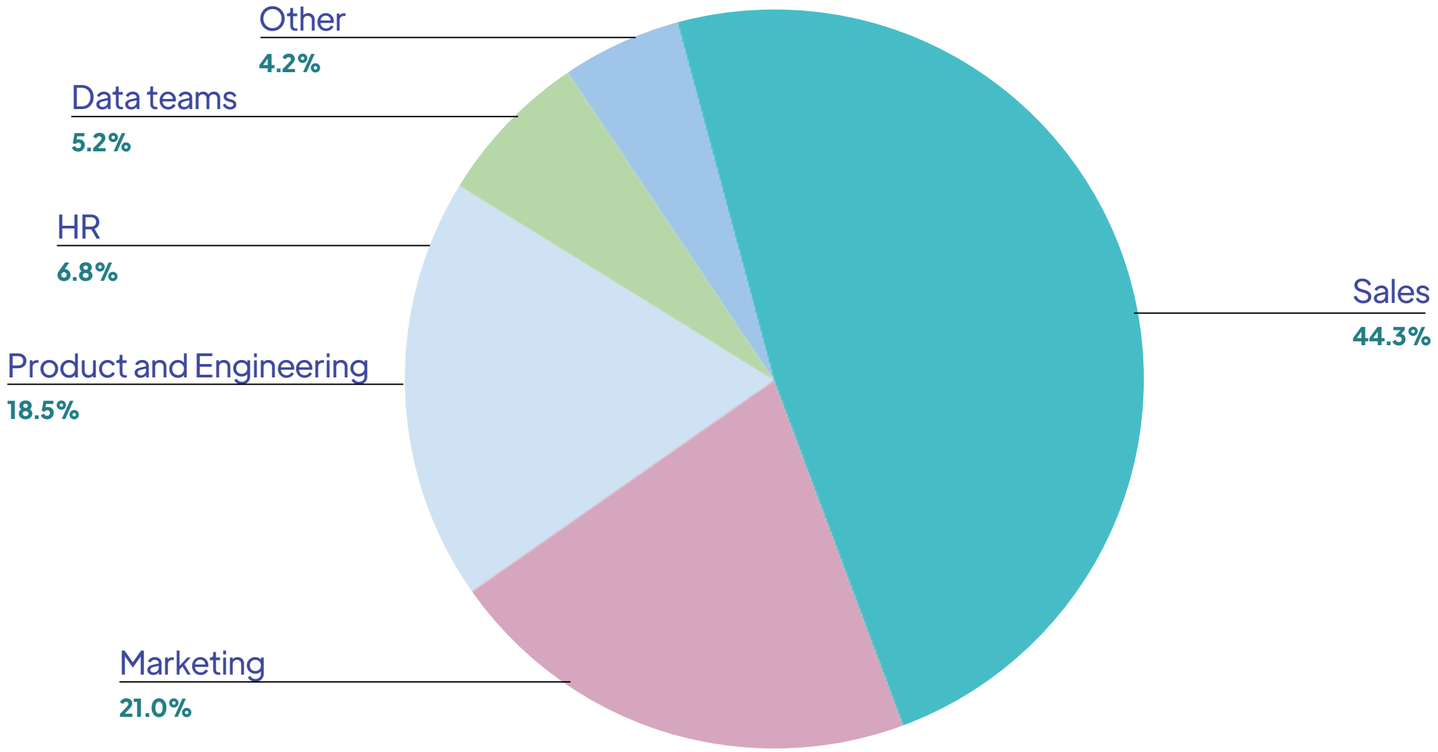
Which teams use the most shadow IT?

Sales and Marketing teams were the biggest shadow IT offenders, and were responsible for 65% of total unauthorized SaaS usage.

Yet, this phenomenon was far from isolated to one department. Shadow IT usage was pervasive across the board, from Finance to HR to Engineering.

Most surprisingly, even the IT departments—those entrusted with managing and mitigating shadow IT risks—recorded usage of unapproved software.

Proportion of Shadow IT usage by team



Cledara

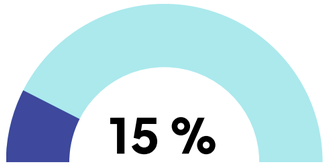
Which applications are most likely to be used as Shadow IT?

ChatGPT was the most popular item of shadow IT, measured by number of users. OpenAI's breakout tool accounted for 0.17% of all SaaS usage in Q3 2023 and has increased to 0.26% so far in Q4 2023.

As AI-powered solutions emerge for ever more workplace tasks, this likely speaks to a wider trend. According to a previous study by Cledara, nearly one-third of businesses have already adopted AI-powered SaaS tools, often without proper IT approval or governance. Other popular AI-powered shadow IT tools include Jasper, Claude, Synthesia, Copysmith, Writesonic, and Copy.ai.

15% of Shadow IT used by companies related to data operations

Analysis shows that :



Of all the unapproved SaaS used are related to the supply, collection, manipulation, transfer, analysis, or display of data.

In some cases, the nature of these tools may be relatively low risk—for example, when Sales teams use Lusha to secure contact information for potential customers.

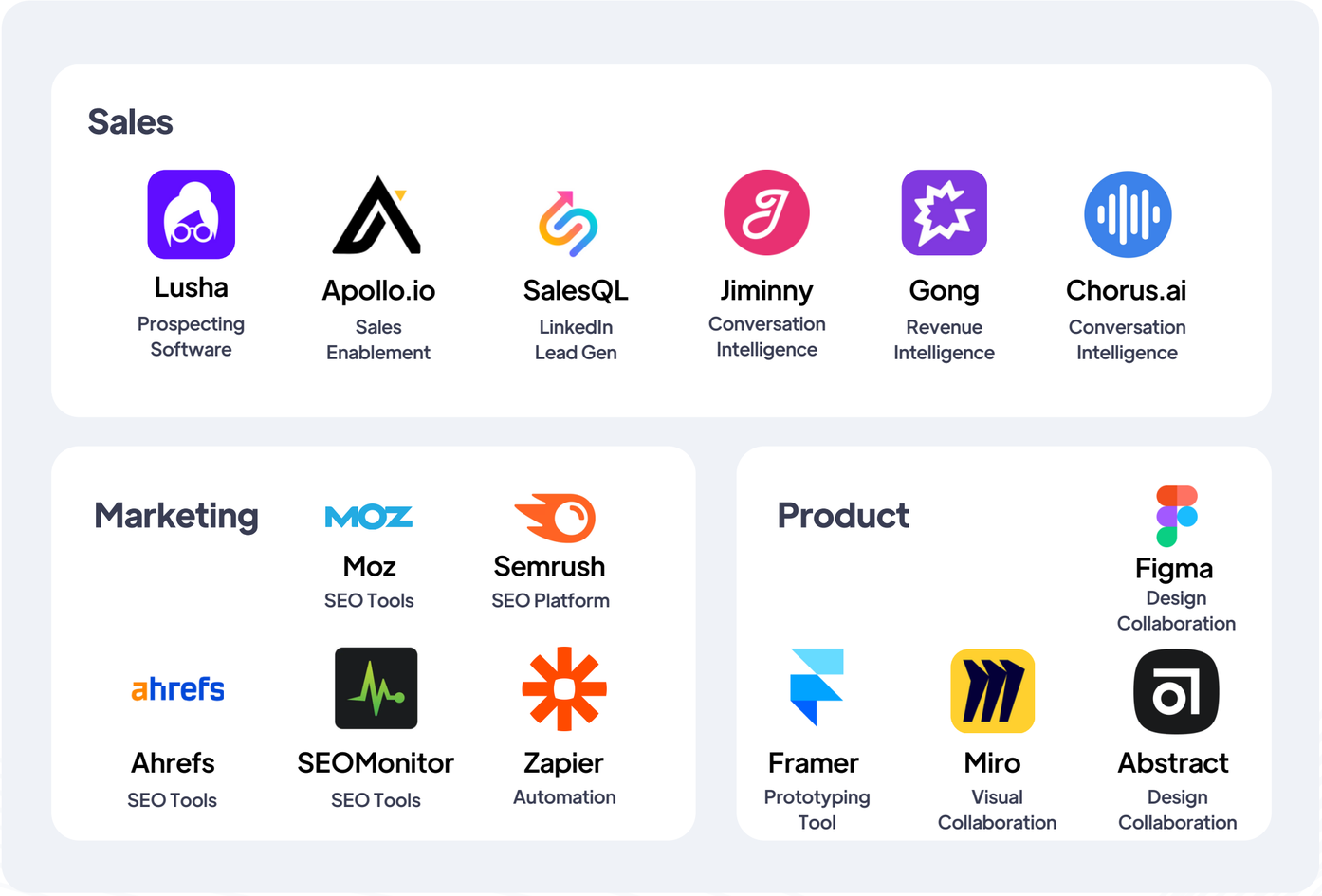
However, in many cases, using shadow IT for data management is a risky game that can result in leaks or loss of crucial information.

Most popular choices for shadow IT by team

- Sales teams frequently purchased prospecting data tools like Lusha, Apollo.io, and SalesQL. They also commonly adopted conversational Intelligence platforms like Jiminny, Gong, and Chorus.ai without central approval, despite their relatively higher price points. This suggests that sales teams are given a lot of freedom to adopt significant tools as they see fit.

- Marketing teams also adopted a lot of data-centric tools without approval, including Moz, SEMrush, Ahrefs, and SEOMonitor. Interestingly, there were also many unapproved users of Zapier, presumably to move data between tools in the marketing stack.

- Product teams organically adopted design tools like Figma, Framer, Miro, and Abstract. They were also significant users of unapproved Notion and Asana accounts.



Trends to watch

Here are three trends from Cledara's data to look out for in your business.

1

Shadow AI: A growing trend

According to Brian Pearson of Robinhood, "Shadow AI could lead to a wave of insider threats" that could be even more damaging to businesses than Shadow IT.

ChatGPT was the most popular item of shadow IT identified in the study—and, according to our earlier report, it's probably the tip of the iceberg. The risks from shadow AI are escalating exponentially, from both data leakage—where sensitive company data is used to train public AI models—to compliance violations—where unmonitored AI activities are breaking security regulations and certificates. That's not to mention the reputational damage that inaccurate, AI-generated content can bring.

In the words of cybersecurity company Imperva's Terry Ray, "If companies are blind to LLMs accessing their back-end code or sensitive data stores, it's just a matter of time before it blows up in their faces."

Conclusion

Security teams must educate employees about the dangers of shadow AI, and promote centrally-approved, compliant AI tools instead.

Trends to watch

Here are three trends from Cledara's data to look out for in your business.

2

Security certificates: no guarantee of robust IT governance

From Cledara's research, companies who claimed compliance with SOC 2 and ISO 27001 actually use 35% more shadow IT than the sample average.

The process of SOC 2 certification has become drastically more complex with the rapid adoption of cloud services and SaaS applications. Securing assets and data now requires persistent vigilance, which can be difficult to enforce given the distributed nature of modern technology ecosystems.

This data point is sobering evidence that many companies overestimate their security posture. It also highlights cultural factors that enable the rise of shadow IT despite compliance goals.

Conclusion

Certificates do not guarantee authentic IT governance. This requires translating policy into practice through stewardship at all levels.

Trends to watch

Here are three trends from Cledara's data to look out for in your business.

3

The word on the street: employees prefer shadow IT

- Employees are 3.5x more likely to use shadow IT than approved SaaS in their day-to-day work.

One of the standout findings of the research was cultural. There's strong evidence that employees strongly prefer to use shadow IT over sanctioned tools. While shadow IT accounted for 65% of all SaaS applications accessed during the study, they account for 78% of all time spent on SaaS products.

This may suggest that employees prefer to use software they select themselves over centrally procured SaaS—or that they're simply not seeking approval for the SaaS they use.

Conclusion

The culture around software procurement channels needs to change, so employees feel empowered to choose their own tools, but seek approval for them.

Spotlight on: Finance

Fintech companies used a considerably above-average number of shadow IT products compared to the study average. This is surprising since recent research by the UK's central bank found that 74% of finance executives named cybersecurity their #1 concern.

According to recent data from Flashpoint, financial services reported the second highest number of data breaches of any industry. As of December 2022, finance and insurance organizations globally experienced 566 breaches, leading to over 254 million leaked records.

These breaches are as eye-watering in cost as they are in frequency.

"The financial services industry paid the second-highest price [behind healthcare] for data breaches last year, averaging $5.97 million," says Prakash Pattni of IBM Cloud. "In today's fast-moving digital economy, it's one of, if not the, biggest threat for the industry."

These alarming numbers underscore the urgent need for the finance industry to address the risks associated with uncontrolled shadow IT usage.

89

Average no of shadow IT products used

↑19%

more than study average

Risks of shadow IT for finance companies

- Fraud - Exposed customer data fuels identity theft and money laundering.
- Fines - Financial regulators impose hefty fines for compliance violations and data leaks. These can amount to 4% or more of a fintech company's global revenue.
- Reputation damage - Data breaches erode consumer trust in new fintech brands, which can severely impact growth.
- Service disruption - Cyber attacks using shadow IT vectors can shut down fintech services and transactions.

Spotlight on: Healthcare

The COVID-19 pandemic forced the healthcare industry to pivot to telemedicine virtually overnight, and this urgent pressure led to a shadow IT sprawl we still see today.

The healthcare sector faces an immense shadow IT problem, with employees at healthcare companies typically using over a hundred unauthorized tools.

The dangers of uncontrolled shadow IT are especially high in healthcare given strict HIPAA regulations around data privacy. In 2022 alone, the Department of Health and Human Services (HHS) imposed penalties of $72.6 million for HIPAA violations.

According to IBM data, healthcare data breach costs reached an average of around $10.93 million per incident in 2023.

Healthcare data breach costs surged to $10.93 million per incident in 2023 per IBM.

105

Average no of shadow IT products used

↑ **40%**

more than study average

Risks of shadow IT for healthcare companies

- HIPAA violations - Unauthorized apps may expose protected health information (PHI), violating privacy rules and incurring major fines. In 2014, two NYC hospitals were fined $4.8 million for a breach caused by shadow IT.
- Data leaks - Breaches of patient PHI, treatment records, or medical research can erode public trust.
- Ransomware - Shadow IT and remote work expand vulnerabilities. Attacks have crippled hospital systems, risking patient lives.
- Fraud - Exposed PHI enables tax fraud, fraudulent insurance claims, and identity theft targeting patients. Losses can reach millions.

Conclusion

The prevalence of shadow IT speaks to a widespread culture problem, connected to the rapid evolution of business technology. It's hard to get a handle on shadow IT adoption since employees often believe they're acting in their company's best interests by using new tools as soon as possible.

According to Terry Ray, of security company, Imperva,

> **"People don't need to have malicious intent to cause a data breach. Most of the time, they are just trying to be more efficient in doing their jobs."**

As the Saas market is flooded with ever more AI tools with dubious or unknown security credentials, IT professionals will need to act fast to change this culture and bring employees onside. Visibility over your team's software products is essential to understand the risks your company is exposed to and keep essential data under control.

How Cledara can help

With a tool like Cledara, you'll gain visibility over the tools your employees use and how much time they spend on them, leaving no space for shadow IT to hide (whilst, of course, respecting your team's privacy by not capturing screen recordings).

You'll also be able to centralize your subscriptions, and upgrade, monitor or cancel software accounts from one simple interface. In a world where over 30% of software spend is wasted, businesses find the solution pays for itself.

Learn More

Cledara

cledara.com