



CISO's Guide to Reducing the SaaS Attack Surface

Your toolkit for reining in SaaS sprawl to reduce risk and optimize technology investments.

Table of Contents

Chapter 1: What is SaaS rationalization?	3
Chapter 2: Assess your SaaS landscape	4
Chapter 3: Establish SaaS standards	6
Chapter 4: Align SaaS stakeholders	13
Chapter 5: Prioritize quick wins	16
Chapter 6: Measure the impact of your efforts	21
Chapter 7: Contain SaaS sprawl continuously with Nudge Security —	23
Chapter 8: Final thoughts	29

Introduction

Fueling efficient growth in today's distributed workplace calls for modern SaaS governance.

Under current macroeconomic conditions, organizations are transitioning from a pandemic-era strategy of "growth at all costs" to a more balanced approach focused on "efficient growth." In line with this shift, many organizations are looking for opportunities to streamline and consolidate their sprawling cloud and SaaS technology stacks in the effort to reduce spend, minimize risk, and drive greater operational efficiency. This is SaaS rationalization, and it is a cornerstone of modern IT governance.

As evidenced by product data from Nudge Security, the average employee creates 18 different SaaS accounts during their tenure at an organization. From a risk standpoint, that's potentially 18 user identities, 18 places where corporate data may reside, and 18 points of integration with other sensitive or business-critical applications.

The implications of SaaS sprawl extend beyond increased risk. SaaS costs are also on the rise. [Data from Gartner](#) reveals that organizations spend an average of \$1,169 per employee annually on SaaS subscriptions. It's no wonder, given that SaaS subscription models are designed for fast and frictionless end user adoption, making it easy for individual users and teams to readily charge SaaS expenses to corporate credit cards.

Yet, despite the apparent ease of SaaS adoption, value is not always realized. Gartner estimates that a quarter of all SaaS subscriptions are either underutilized or unnecessarily deployed, resulting in squandered SaaS spending and administrative overhead that could be better invested in strategic technology initiatives for top-line revenue growth.

SaaS rationalization attempts to contain the rising costs and security risks associated with SaaS sprawl so that organizations can grow efficiently and safely.

This SaaS rationalization toolkit provides a step-by-step guide for achieving cost optimization and risk management. We provide multiple frameworks, tools, and templates to help you manage your SaaS rationalization efforts. We also provide a roadmap for transforming ad hoc SaaS rationalization efforts into continuous and programmatic successes.

SaaS rationalization is truly a team sport. We wrote this guide with IT leaders in mind, however, we hope that readers in security, compliance, operations, finance, and procurement find the information valuable as well. Let us know your thoughts and feedback by emailing us at hello@nudgesecurity.com.

Chapter 1

What is SaaS rationalization?

SaaS rationalization is the process of identifying and eliminating unnecessary, redundant, and potentially risky SaaS assets within an organization. It involves discovering, evaluating, and removing underutilized SaaS tools and, wherever possible, consolidating overlapping services to maximize financial and operational efficiencies. It also surfaces security risks tied to shadow IT and excessive SaaS access.

A mature SaaS rationalization process allows modern organizations to grow efficiently and safely while also empowering employees to take advantage of new cloud-delivered technologies that accelerate innovation, productivity, and collaboration.

In the chapters that follow, we delve deeper into the steps involved in SaaS rationalization, providing you with the ultimate guide to optimizing your SaaS portfolio.

SaaS Rationalization Outcomes

Uncover and eliminate wasted spending on underutilized or overdeployed SaaS accounts, leading to greater financial efficiency.

 **Reduce Costs**

Minimize Risk 

Shrink your SaaS attack surface, including risky app-to-app integration, to protect your data and minimize exposure to threats.

Meet compliance requirements related to inactive and abandoned user accounts, enhancing organizational security.

 **Accelerate Compliance**

Enhance Operations 

Break down data silos, promoting collaboration across teams and contributing to smoother, more efficient IT operations.

Chapter 2

Assess your SaaS landscape.

A problem well-defined is a problem half-solved—an adage that rings particularly true in the context of SaaS sprawl. Before you can rationalize your SaaS estate, you have to understand what's in it. Thus, the first step of SaaS rationalization is creating a complete SaaS asset inventory.

Easier said than done, right? The decentralized, sprawling nature of SaaS adoption makes SaaS governance a particularly thorny endeavor. Individual teams and departments often adopt and administer their own SaaS tools without input or oversight from IT, finance, or procurement, making it difficult to keep track of all active subscriptions, usage levels, and associated costs at an organization-wide level. This challenge is exacerbated by the dynamic nature of SaaS: new subscriptions are constantly being added, while old ones may fall into disuse or expire, creating a continuously changing SaaS landscape. Furthermore, SaaS applications are built to integrate with each other easily through OAuth, creating a complex web of interconnected services that can be hard to untangle.

Given these challenges, you might be tempted to skip this step or take shortcuts. Resist the urge! If you limit your visibility to only the carefully procured SaaS applications on your “approved” list, or only those that surface in expense reports, or only those managed within an SSO or IdP, this will invariably lead to suboptimal results. In contrast, if you invest time and effort upfront in establishing a repeatable process for creating and updating a SaaS asset inventory, you'll pave the way for an effective and successful SaaS rationalization process and ongoing program.

What to include in your SaaS asset inventory:

Item	Description	Owner / Source of information
SaaS applications	Start with a list of all SaaS apps used across the organization. Include apps managed by IT, as well as those outside of IT governance. For each app, include a description, category and link to the app's login page or vendor's website.	Multiple sources offer partial visibility: finance, security, IT, procurement, business managers, and employees. Compile all into a single source of truth.
SaaS identity and access management	Know who has access to SaaS data and how. Identify all user accounts for each SaaS app. Include authentication method (e.g., SSO, username / password), SSO provider (if any), and MFA status for each account.	IAM team. Can export SSO data for managed SaaS. For unmanaged apps, get data manually from each app owner.
SaaS approval status(es)	Know which governance teams have rubber-stamped SaaS apps by including various approval statuses for finance, GRC, legal, security, vendor management, business line managers, and other required approvers.	Each governance team likely maintains its own approval process and system of record. Compile these sources for your inventory.
SaaS administration and ownership	Central IT no longer "owns" all SaaS. For each app, identify the app business owner, the day-to-day admin, the billing contact, and the technical contact or business technologist. For single-user apps, these roles may all be ascribed to one person.	For paid apps, ask business line managers. For free apps, start with the first user, who often acts as an administrator.
SaaS compliance management	Identify which apps are considered in scope of various compliance regimes and regulations. Note which apps require regular user access reviews to meet compliance requirements.	GRC or legal may have purpose-built compliance tools or maintain info in spreadsheets
SaaS vendor risk management	Create a vendor security and risk profile for each SaaS provider, including infrastructure and cloud hosting info, security program details, compliance attestations and SBOM / SaaS BOM.	Security or the team that handles third-party risk management
SaaS-to-SaaS integrations	OAuth grants are commonly used to connect and share data across SaaS apps. Map your SaaS mesh by listing OAuth grants, scopes, and grantors for each application.	IT / security. Lists of third-party apps connected by OAuth are usually available to each application's admin. For example, admins can access an OAuth grant activity report in Google Workspace.
SaaS data classification	SaaS governance is data governance. Include data classification information to understand which SaaS apps handle sensitive data like source code, PII, or financial data.	While you may be able to infer data classification based on SaaS app category (e.g., a SaaS CRM handles customer data), it's a good practice to also ask end users directly.
SaaS user context and usage	Understanding how, why, and to what extent SaaS apps are used can help you determine the value it delivers to your workforce. Capture user sentiments, NPS, or justification of need. This is also a great way to surface abandoned, forgotten and nice-to-have accounts.	For this information, it's best to go straight to SaaS account holders. Consider launching an internal survey or conducting focus group-like sessions for each app.
SaaS financial & licensing data	Include your overall application spend as well as per user costs. If possible, discover SaaS used for work purpose but purchased with non-corporate expense cards (employees' personal credit cards - it happens.) Capture contract terms and renewal dates. It can also be useful to break down SaaS spend by cost center or dept.	Finance or procurement likely maintain this data or can look through POs and expense reports. Otherwise, you may need to ask business line managers or app owners for contract and subscription renewal data.

Yes, this a lot of data to capture and organize. Feel free to use our [free SaaS asset inventory template](#) to get started. Or, skip the spreadsheet altogether and build your SaaS asset inventory in minutes using Nudge Security.

It's free to get started. →

Chapter 3

Establish SaaS standards.

Once you have a SaaS asset inventory in place, you'll likely start to see obvious areas for pruning. But, put the hedge trimmers down for a minute. Before you start making any cuts, it's important to take a step back and establish a set of SaaS standards to rationalize your portfolio against. Such standards can help to ensure long-term programmatic success and prevent SaaS sprawl from quickly creeping back in after rationalization.

The goal is to establish a standard rubric or scorecard for evaluating which applications should be removed, replaced, tolerated, or expanded. Criteria should reflect the needs and priorities of various stakeholders across the organization, including whether the SaaS application meets security and compliance requirements, supports user productivity, or provides value for money. (You'll find more information on aligning stakeholders below.)

Creating standards helps ensure that SaaS rationalization is not simply a one-time process of cutting costs but rather is an efficient way to maximize the benefits you get from your investments in cloud-delivered technologies. It also enables end users to identify which applications are best suited for their needs and which ones provide less value.

Furthermore, having standards in place ensures that the SaaS rationalization process is fair and consistent across teams and departments—everyone will have to abide by the same criteria when it comes to selecting which applications to keep or discard. That way, no single department or person will have to face the brunt of unhappy employees whose favorite applications have been rationalized out of the portfolio. (We're guessing CFOs can relate to this unhappy fate.)

Sample SaaS rationalization scorecard

This scorecard is an example and should be tailored according to the specific needs and priorities of your organization. To use this scorecard, first establish a normalized scoring criteria across all functional areas, for example, a 10-point scale. Then, designate an owner or team to score applications in your SaaS estate within each area.

Additionally, if your rationalization efforts are highly influenced by a need or mandate to increase IT efficiency or reduce overall technology spend, then consider applying additional multiplier to weight your scores accordingly.

SaaS application	Security & compliance	Business value & fit	User sentiment	Total cost of ownership	Weighted score	Decision
Priority multiplier	1	1.2	0.8	1.6	-	-
Application 1						Remove
Application 2						Replace with
Application 3						Expand
Application N						Right size

Security & compliance

This column assesses if the SaaS application meets the organization's security and compliance requirements. Align this score to your vendor security assessment and / or consider the following criteria.

- Does the SaaS provider comply with the industry-specific regulations and standards relevant to our organization (e.g., GDPR, HIPAA, ISO 27001)?
- Does the SaaS provider have and publish its security policy, privacy policy, terms of use, responsible disclosure / bug bounty program, and security contact information?
- Where is the SaaS provider incorporated and / or headquartered? Where is its infrastructure hosted? Where is our data located?
- How does the SaaS provider handle data security, and what measures do they take to protect our data from breaches and attacks?
- Does the SaaS application offer suitable access control mechanisms to ensure secure user authentication and authorization? Does it support 2FA? SSO? (Note any SSO taxes that apply.)
- What is the provider's policy regarding data ownership, third-party sharing, and retrieval in case of contract termination or service discontinuation?
- How frequently does the provider conduct security audits and vulnerability assessments, and are the results of these assessments made available to us as a customer?
- Has the SaaS provider been involved in any data breaches in the past 2 years? If so, what was the nature, cause, and extent of the incidents? How did the provider respond? How and how quickly did they alert authorities, customers, and other stakeholders?
- Does the SaaS provider publish a software bill of materials, including its data processors which may be other SaaS providers? How often does the SaaS provider update this information?

Business value & fit

This column assesses the degree to which the SaaS application aligns with the company's objectives and enables crucial operations. It evaluates the technical fit, operational efficiency, the application's role in achieving the company's digital transformation goals, and its importance and utility in driving the company's primary business objectives.

- Does the application support or enhance our organization's operational efficiencies? How?
- What role does this SaaS application play in our digital transformation efforts? Does it replace legacy processes or infrastructure?
- Is the application critical to our organization's top-line business objectives?
- Does the SaaS application afford us a competitive advantage in our industry or sector?
- Does the SaaS application offer highly differentiated capabilities? Or, are there other similar applications in our portfolio with overlapping capabilities?
- How well does the application integrate with our existing systems and software?
- What kind of support and service level agreements (SLAs) does the SaaS provider offer?
- Does the SaaS provider have a good track record of uptime and reliability? Is the status page available and regularly updated with accurate, relevant information?
- What kind of customization and scalability options does the application offer to accommodate our future growth and evolving business needs?

User sentiment

This column considers user sentiment towards the application. This area is highly subjective, but that does not diminish its value in the rationalization process. Survey application users with a standard set of questions. This could be as simple as asking a single CSAT or net promoter score (NPS) question, such as, "on a scale of 1 to 10, how likely are you to recommend this app to a colleague or another team in this organization?"

- How likely would you be to recommend this app to a colleague or another team?
- How frequently do you use this SaaS application in your daily work?
- How would you rate your experience with the application?
- How intuitive or user-friendly is the app?
- How long did it take you to learn how to use the app proficiently for your work?
- How well does the application meet your work needs?
- What app features do you consider to be critical? Unique?
- How well does the application integrate with other tools and systems you use?
- To what extent does the application improve your productivity or simplify your tasks?
- Have you encountered any major issues or challenges with the application?
- How responsive and effective is the vendor's support when issues arise?
- If the application were removed or replaced, how would that impact your work?
- Given a choice, would you opt to keep this application, replace it, or do you have no preference?
 - If you answered, "replace it," what application would you prefer, if any?

Total cost of ownership

This column evaluates the return on investment of a SaaS application, accounting for all of the costs to own and operate it versus the benefits it offers. Benefits may include enabling or accelerating topline revenue growth as well as cost reduction or cost avoidance.

- What is the initial cost of implementing the SaaS application, including any setup, configuration, and training fees?
- What are the ongoing operational costs, such as monthly or annual subscriptions, licensing fees, and costs related to updates and maintenance?
- What does the current license and contracting structure look like? When does the contract renew?
- If we choose to not renew under the current contract, would we incur higher costs later to re-subscribe under a new contract?
- Are there any hidden costs, like charges for additional features, storage, or users that might increase the total cost of ownership?
- How much time and resources are required to manage the SaaS application? This could include time spent on updates, troubleshooting, and user support.
- Does the SaaS application integrate with existing systems and software, or do we need additional software or services for it to function optimally?
- How much time and resources are spent on training employees to use the SaaS application effectively?
- What is the potential cost of downtime or disruption to our business operations if the SaaS application fails or becomes unavailable?
- Will the SaaS application provide a return on investment through increased efficiency, productivity, or other measurable benefits?
- What costs does the SaaS application displace or avoid?
- What is the potential cost of switching to a different SaaS application in the future, such as data migration, employee retraining, and potential business disruption?

Final score

This is the sum of all four categories and will help you decide which applications should be permitted and maintained, standardized and expanded, or perhaps even right-sized to only allow for certain use cases, needs justification, and users. It will also help you to identify which applications should be disallowed and removed due to low business value, undue risk, or exorbitant costs, and also which apps could be tolerated but eventually replaced or migrated to a preferred alternative.

Chapter 4

Align SaaS stakeholders.

In modern, distributed organizations, technology decisions are rarely owned by any single department or function. Thus, as you embark on the SaaS rationalization process, it's crucial to identify and engage the wide array of stakeholders involved. Each has different priorities, responsibilities, and concerns that you must address to ensure a successful and inclusive initiative. SaaS rationalization efforts conducted in siloes with a limited set of stakeholders are often met with poor reception and even poorer compliance. Avoid making such mistakes by considering each of the following stakeholders and their roles in the rationalization process.

IT

IT plays a leading role in SaaS rationalization. Whereas IT has traditionally been responsible for the implementation, ongoing administration, and maintenance of business technology, these activities are now commonly performed by SaaS administrators and business technologists outside of IT. This elevates the role of IT from management to governance.

Security

Security plays a crucial role in SaaS rationalization, ensuring that each tool meets your organization's risk and security standards. Their focus is on mitigating risk and maintaining a healthy SaaS security posture. This often spans data protection, access controls, third-party risk management (vendor security), and security operations, including the detection of and response to SaaS threats, such as account takeover attacks, supply chain breaches, and others.

GRC

Governance, Risk, and Compliance (GRC) is responsible for ensuring that all SaaS applications comply with relevant laws, regulations, and corporate policies. They would typically be involved in contract review, data privacy considerations, and risk management relating to the use of SaaS tools.

Finance

The finance department is primarily concerned with the financial implications of SaaS tools, including cost, value for money, and return on investment. Their input would be vital in evaluating the economic efficiency of maintaining, replacing, or discarding specific applications.

Procurement

The procurement team is responsible for negotiating and managing contracts with SaaS providers at the time of purchase and renewal. They often work closely with both finance and legal teams to ensure contracts align with budgetary constraints and comply with legal requirements. Like IT, the role of procurement has shifted in the move to business-led SaaS adoption and may now resemble a governance body or center of excellence.

Operations

The operations team ensures that the chosen SaaS applications align with the organization's operational strategy and goals. They are often concerned with how these tools can enhance workflow efficiency, improve service delivery, and reduce manual tasks. Their perspective is critical in assessing the real-world usability of the applications and how well they integrate with existing operational processes. This team also provides valuable insight into user sentiment, as they are often the ones most closely involved with the day-to-day use of these applications and may be aligned to departments, for example DevOps, ItOps, or SalesOps.

Business Line Managers

Business line managers are vested in selecting SaaS tools that enhance their teams' productivity, collaboration, overall performance, and job satisfaction. They also face budgetary pressure and aim to keep technology spending in line with the business overall. Their deep understanding of their department's unique needs, desires, finances, and operations make them crucial stakeholders in the rationalization process.

Individual Teams & Employees

Never underestimate the importance of the end users—the individual teams and employees who use SaaS tools daily. Their feedback regarding the value, usability, and efficiency of these tools is invaluable. Remember, a tool that is not well liked or used is a poor investment, no matter how feature-rich it may be.

Each of these stakeholders brings a unique perspective to the SaaS rationalization process. Understanding and addressing their various needs and concerns can help foster buy-in and ensure a smoother, more effective rationalization initiative.

Once your standards are established and stakeholders aligned, you are on your way to optimizing your SaaS landscape.

Chapter 5

Prioritize quick wins.

So, you've built your SaaS inventory, you've rallied your stakeholders, and you've created a rigorous evaluation framework. You're ready to start rationalizing your SaaS!

But, where (and how) to get started? By now, you may have discovered hundreds of SaaS applications and thousands of user accounts floating around your organization. To avoid getting bogged down, you need to be strategic in your approach. Here's how to prioritize your SaaS rationalization efforts to maximize impact and earn quick wins.

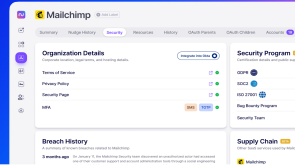
Focus on your biggest SaaS risk centers first.

While it may seem logical to initially focus on the largest SaaS cost centers, there are compelling reasons to prioritize efforts based on the areas of greatest risk. SaaS applications that handle sensitive or restricted data, or present significant risks to the organization, often impose additional governance burdens on IT, security, and compliance teams, even if they are low-cost or free tools.

It is also important to consider that these teams may have stringent policies for third-party risk and acceptable usage that can provide a well-defined threshold for SaaS rationalization. For instance, your organization might have a policy that forbids the use of cloud services hosted in specific geopolitical regions, or requires SaaS providers to demonstrate compliance with SOC 2 Type 2. Any SaaS use that does not meet these criteria can be swiftly rationalized out of the portfolio.

This approach not only showcases the value of the SaaS rationalization process to stakeholders, but also generates momentum for ongoing rationalization efforts.

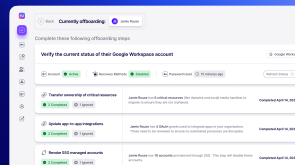
Learn how Nudge Security accelerates vendor security assessments with risk and compliance insights →



Audit former employees for lingering SaaS access.

Are there ghosts lurking in your SaaS portfolio? Before you tackle revoking SaaS accounts of active employees, your first step should be to audit the SaaS accounts of former employees who may have retained access to SaaS apps after leaving the organization. Their accounts may still have active licenses that are not actively being used (hopefully). Review your list of suspended users in your identity provider (and cross-reference it with your HR records if you are uncertain) and then work to identify accounts to remove or licenses to revoke.

Learn how Nudge Security helps to ensure complete employee offboarding and SaaS license revocation. →



Remove abandoned and forgotten SaaS accounts.

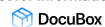
Can you recall every online service you've ever registered for? (Editor's note: Just keeping track of my active streaming subscriptions is a struggle.)

According to Gartner, a staggering 25% of all SaaS subscriptions are either underutilized or excessively deployed, resulting in significant opportunities for cost optimization through SaaS rationalization. Moreover, most regulatory compliance frameworks mandate the removal of inactive accounts within stipulated time frames.

To assess the utilization rates of SaaS accounts, you can use SaaS login or user activity data. However, the most reliable source of information is direct communication with the account holders. A straightforward inquiry, such as "Are you still using that application?" can quickly help identify abandoned SaaS accounts that should be removed from your portfolio.

Learn how Nudge Security automates access reviews to surface inactive and abandoned SaaS accounts. →

Request for information about



Hi there! It looks like you are using DocuBox, an app that is not commonly used by employees in our company.

Can you help us understand why you chose to create an account for DocuBox?

I am starting a new project

I am experimenting

Eliminate redundant SaaS applications.

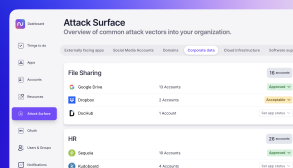
A major contributor to SaaS sprawl is the presence of multiple SaaS tools that serve the same or similar purposes within an organization. Such redundancy is not only inefficient but can also be costly.

Often, different teams or departments within an organization may be using different tools for the same purpose, such as project management or file sharing. Sometimes this is justified due to specialized or highly differentiated needs and features. Yet, in some cases, it's due to a lack of visibility of the SaaS tools already in use elsewhere in the organization. This can lead to operational inefficiencies, data silos, and productivity silos that limit your organization.

To identify these redundancies, start by categorizing your SaaS applications based on their primary functions. Once you have a clearer picture of where redundancies exist, you can evaluate which tools are most effective and universally preferred. Engage all relevant stakeholders in this decision-making process. This includes not just the IT operations team or the business unit leaders but also the end users of these tools. Remember, the aim of SaaS rationalization is not just cost reduction but also improving productivity and user satisfaction.

Once you've decided on the preferred tool(s), create a transition plan to migrate users from the redundant applications to the chosen one(s).

Learn how Nudge Security auto-categorizes and groups similar SaaS applications for comparison. →



Consolidate isolated SaaS tenants.

It's not uncommon to find isolated instances or “tenants” of the same SaaS application or cloud infrastructure being used by different departments or teams. This segregation also often leads to higher costs due to the inability to leverage volume-based pricing.

The first step in addressing this issue is to identify all instances where multiple tenants of the same SaaS application exist. Unfortunately, many SaaS providers won't give you this information directly—instead, their enterprise sales team will tell you how many licenses you should buy for your organization.

Engage with the various teams or departments to understand where segregation exists and why. It could be due to specific requirements, historical decisions, or simply a lack of awareness of the existing instances. Next, evaluate the feasibility of consolidating these tenants into a single, organization-wide instance. This process will likely involve discussions with the SaaS provider, as well as detailed planning to ensure a smooth transition with minimal disruption to users.

Remember to consider the potential impact on data privacy and security when consolidating SaaS tenants. Always ensure that appropriate permissions and access controls are in place to protect sensitive information.

Learn how Nudge Security helps you bring rogue AWS accounts into centralized governance. →



Chapter 6

Measure the impact of your efforts.

Measuring the effectiveness of your SaaS rationalization efforts is paramount to the success of the program. You may have specific business objectives tied to reducing SaaS spend or compliance directives to remove inactive accounts. Yet, beyond your primary objective or KPI, SaaS rationalization can have far-reaching benefits across cost management, compliance, risk, productivity, and employee satisfaction. By measuring and reporting on a comprehensive set of results, you'll stand to gain more support and momentum for continued SaaS rationalization efforts.

Measuring the impact of SaaS rationalization involves both quantitative and qualitative metrics. On the quantitative side, track overall SaaS spend before and after your rationalization efforts to assess the cost savings. Additional quantitative metrics include:

- Reduction in average SaaS spend per employee
- Improved SaaS license utilization
- Decrease in the number of redundant applications
- Increase in user adoption rates of standardized SaaS
- Reduction in new unsanctioned SaaS spend
- Increase in consolidation of isolated tenants and data
- Number of unnecessary SaaS accounts removed
- Number of unnecessary OAuth grants removed

Qualitative metrics are also important when measuring the impact of your SaaS rationalization journey. Consider conducting surveys or interviews with stakeholders—both IT operations as well as end users—to gain insights into their experience with the rationalization process and any improvements in efficiency and user satisfaction.

Qualitative metrics to consider while measuring the impact of your SaaS rationalization include:

- Employee satisfaction
- Impact on productivity and collaboration
- Ease of finding and onboarding standardized SaaS
- Security and compliance improvements
- Overall impact on business processes

Chapter 7

Contain SaaS sprawl continuously with Nudge Security.

According to Nudge Security product data, at a midsize organization of 1,000 employees, a new SaaS asset is created roughly every 20 minutes. And, as long as new B2B SaaS companies continue to emerge to solve a myriad of work challenges, your enterprising workforce will experiment with them. This dynamic can make a well-intentioned SaaS rationalization effort feel like battling hydra: remove one SaaS application and two more are adopted in its place.

Now, that's not to say that SaaS rationalization is a futile endeavor. Rather, your approach to SaaS rationalization should focus on how to operationalize your efforts for immediate impact while also building a foundation for a continuous and automatic SaaS rationalization program.

Enter Nudge Security. From SaaS discovery to SaaS offboarding, Nudge Security helps organizations to manage every step of the SaaS rationalization effort with a focus on collaborative engagement and efficient automation. Here's how Nudge Security can help you take SaaS rationalization from a one-time effort to a continuous part of your overall SaaS governance and security program.

Discover all SaaS assets—in minutes.

Remember that super-detailed SaaS asset inventory template back in Chapter 2?




Well, Nudge Security gives you the ultimate shortcut to building a durable SaaS asset inventory: no spreadsheets, no chasing down colleagues, no sifting through DNS records or expense reports. Instead, simply connect Nudge Security to your Google Workspace or Microsoft 365 environment(s), and it will automatically discover and inventory your cloud and SaaS assets in minutes, including off-network, personal device, and historical SaaS use. And, you'll be alerted as new SaaS assets are created, so you can stay ahead of SaaS sprawl from the outset.

Nudge Security automatically describes and categorizes each SaaS application in your estate, making it simple to search and filter for redundant apps and isolated SaaS tenants to be consolidated, as well as rogue cloud accounts to be brought into centralized governance.

Learn more about our unrivaled, patented approach to SaaS asset discovery. →

Latest Accounts Created

The most recent accounts created by your employees.

7 mins ago	NEW	 Nudge Security	Mike Torello
59 mins ago	NEW	 Atlassian	Willie Tanner
3 wks ago		 Google Worksp...	Thomas Magnus

Surface SaaS risks and security issues.

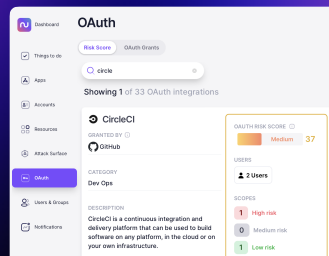
Nudge Security helps you to manage your SaaS security posture. As SaaS assets are discovered, Nudge Security provides detailed SaaS vendor risk and compliance profiles, SaaS supply chain data and breach alerts you won't find anywhere else, and visibility into compromised SaaS accounts and credentials.

To help ensure secure SaaS access, Nudge Security shows you what authentication methods are used for each SaaS account and whether or not accounts have MFA enabled. Nudges and automation workflows help you to work toward complete SSO governance and SaaS security best practices by enforcing MFA.

Nudge Security also maps your SaaS-to-SaaS mesh of OAuth integrations and provides detailed risk scoring based on the permissiveness of each OAuth grant and individual scope. With a nudge, you can easily audit and remove risky and unnecessary OAuth grants to contain SaaS access sprawl to your sensitive data.

The average organization has 10 SaaS apps connected by OAuth to Github.

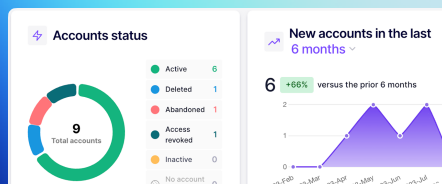
Learn how Nudge Security helps you manage SaaS-to-SaaS risk. →



Track SaaS adoption and usage trends.

Who's most likely to experiment with new SaaS tools in your organization? Which SaaS applications are the most popular? Which ones are growing the fastest? Nudge Security has the answers. It tracks SaaS adoption rates so you can stay ahead of SaaS sprawl. It also helps you identify unused accounts using SSO login data, and user responses to nudges asking "Are you still using this account?"

Learn how identify inactive and abandoned SaaS accounts with Nudge Security. →



Automate SaaS access reviews and remove unnecessary accounts.

Conducting regular SaaS access reviews is a simple, effective way to find and eliminate wasted SaaS spend. What's more, this is a requirement for many many regulatory compliance frameworks, including SOC 2, HIPAA, and others. Nudge Security offers purpose-built playbooks designed to orchestrate SaaS access reviews and the removal of inactive accounts, complete with audit-ready reports.

Discover our playbook for removing abandoned SaaS accounts. →

The dashboard displays a table of SaaS accounts and their removal status:

APP	ACCOUNTS	REMOVED ACCOUNTS	REMOVAL REQUEST STATUS	
Salesforce	38	18	Confirmed	Details
Zendesk	18	0	No response	Details
Bitbucket	45	21	Confirmed	Details

Rein in rogue cloud accounts.

No one wants to get a surprise bill for a long-forgotten AWS developer account that's been compromised and used for crypto mining. Nudge Security not only discovers AWS, Azure, and GCP accounts, but also shows you which accounts are rogue and not centrally managed within your AWS Organizations environment. Our playbook makes it simple to find rogue cloud accounts and bring them under centralized governance.

Read more about discovering rogue cloud accounts with Nudge Security. →

Manage your AWS footprint



Rogue Accounts

2

Managed Accounts

3

Offboard SaaS access fully and quickly.

With Nudge Security, you can feel confident in your ability to fully and efficiently offboard cloud and SaaS access when employees exit or change roles. It allows you to orchestrate account removals to avoid orphaned accounts, reclaim SaaS licenses and costs, and even automate password resets for unmanaged SaaS accounts. All in all, it helps eliminate 90% of the manual IT effort required to complete SaaS offboarding for former employees.

Take an interactive tour of our employee offboarding automation playbook. →

nudge Employee Offboarding Report

OFFBOARDING USER: Departing Martinez | Access removed for 19 accounts

1 Migrated Resources

RESOURCE TYPE	RESOURCE
Projects	SECRETWORKSPACE-1234

8 OAuth Integrations Updated

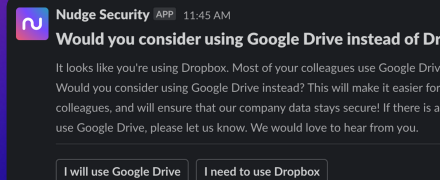
INTEGRATION: Calendly.com → Google Workspace

Nudge employees toward better SaaS behaviors.

Don't let your SaaS rationalization efforts go to waste. You can't stop employees from experimenting with new SaaS tools, but you can guide them to adopt them safely, or better yet, opt to use SaaS applications you've already vetted. Nudge Security makes this automatic and friendly.

As new SaaS applications are introduced, send "nudges" to employees to gain context about why and how the app will be used and to instruct them on enrolling the application in SSO or enabling MFA. Alternatively, create a nudge that asks them to use a preferred alternative application instead. Nudge responses are stored, providing a rich justification of need record.

Read our research to learn how security nudges lead to greater compliance than blocking SaaS access. →



Chapter 8

Final thoughts

SaaS rationalization is an ongoing effort that requires continuous SaaS discovery, collaborative analysis, and automated de-provisioning processes. With Nudge Security, you can build a foundation for a highly efficient SaaS rationalization program that helps you contain SaaS sprawl on an ongoing basis.

But that's just the beginning. In addition to helping you contain SaaS sprawl, Nudge Security also allows you to measure and monitor user adoption of sanctioned and unsanctioned SaaS applications, audit your SaaS security posture in real time, and offboard employees quickly and completely when they leave.

With collaboration and the right tools like Nudge Security, SaaS rationalization can be a powerful way to optimize costs and reduce risks while improving employee satisfaction and productivity. There's never been a better time than now to get started with your own SaaS rationalization program—with Nudge Security at your side.

Ready to take the first step in your SaaS rationalization journey?

Get started with Nudge Security today →

About Nudge Security

Nudge Security helps modern organizations manage SaaS security and governance at scale by working with employees, not against them. With an innovative, patented approach to SaaS discovery, Nudge Security gives IT and security teams complete visibility of every SaaS and cloud asset ever created in their organization, and automated workflows to nudge employees toward more secure practices. Nudge Security was founded in 2021 by Russell Spitler and Jaime Blasco with backing from Ballistic Ventures and was named a “Cybersecurity startup to watch in 2023” by CSO Magazine and a “Most promising early-stage startup” SC Awards finalist.

Learn more at www.nudgesecurity.com and follow [the Nudge Security Twitter account](#) and [the Nudge Security LinkedIn page](#).

nudge