BetterCloud

The IT Leader's Checklist for SaaS Operations

Every day and at every moment, IT must manage and secure millions of user interactions across SaaS applications in the digital workplace.

Interactions are simply the actions your users take in those SaaS apps; they're the processes users perform, the people they interact with, as well as the data they interact with. User interactions lead to an ever-growing data sprawl, which in turn increases risks of human error and negligence.

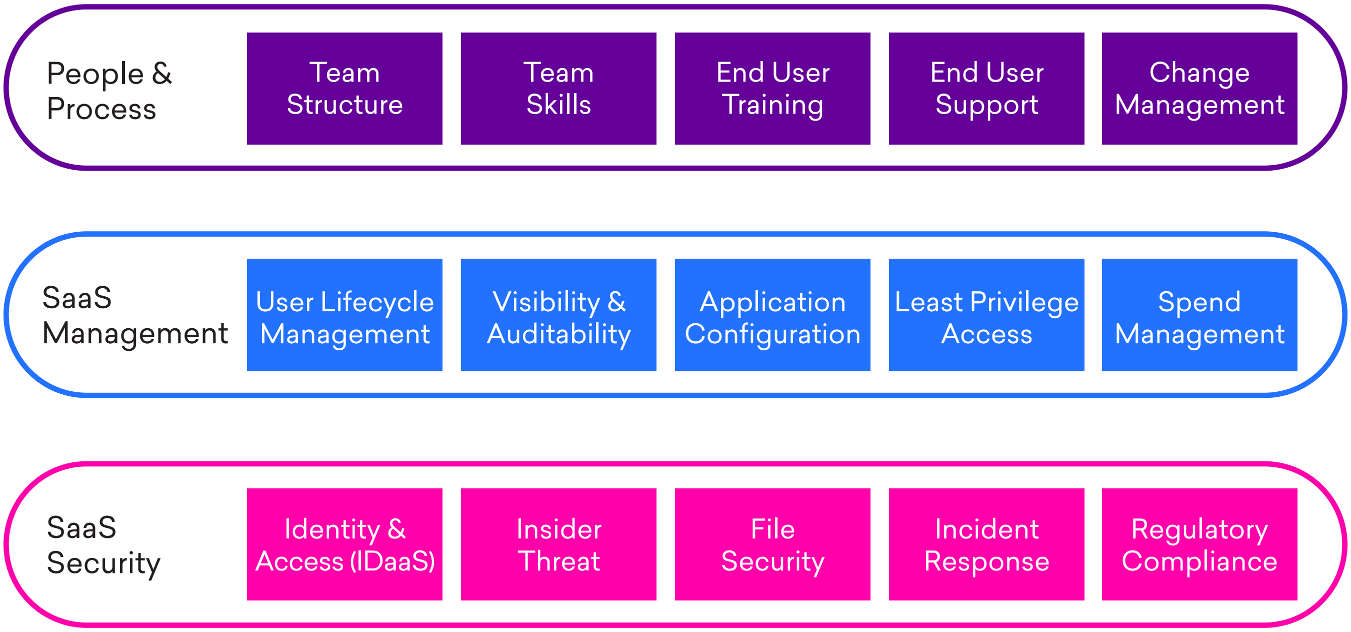
This is why managing and securing the modern enterprise is no easy feat. To get a handle on your SaaS operations, or SaaSOps for short, some key best practices can help.

Use this handy checklist to start tackling the challenge, and steer your SaaS operations to secure and efficiently manage your digital workplace.

What’s SaaS operations (SaaSOps)?

SaaSOps *noun*

: an IT practice referring to how software-as-a-service (SaaS) applications are managed and secured through centralized and automated operations (Ops), resulting in reduced friction, improved collaboration, and better employee experience



People & Process	Team Structure	Team Skills	End User Training	End User Support	Change Management
SaaS Management	User Lifecycle Management	Visibility & Auditability	Application Configuration	Least Privilege Access	Spend Management
SaaS Security	Identity & Access (IDaaS)	Insider Threat	File Security	Incident Response	Regulatory Compliance

SaaSOps has three essential pillars. First, it’s about people and processes. Without the right processes manned by the right team, the remaining pillars are more challenging.

Besides people and processes, SaaSOps is made of two inseparable components: SaaS management and SaaS security. SaaS must be managed with regard to security. And conversely, SaaS must be secured with regard to how it’s managed.

Running IT the SaaSOps way

Just as SaaS is a fundamental shift in how organizations use technology, SaaSOps is a fundamental shift in how IT manages data, users, and applications. SaaSOps requires a new organizational structure, new skills, new end user training and support, as well as different change management steps.

These checklist items, while by no means exhaustive, will get you started on how you can run IT the SaaSOps way.

Build your SaaSOps team structure with:

- □ One SaaSOps professional for about every 50–150 users. It's a wide range depending on the extent an organization is SaaS-powered. The more an organization uses SaaS and automates processes, the higher the number of users IT can support
- □ SaaSOps roles to configure, troubleshoot, monitor, and administer SaaS applications
- □ SaaSOps team members who can plan and implement IT resources, policies, and procedures that balance employee productivity and security, industry best practices, and regulatory requirements
- □ SaaSOps team members who can collaborate with the security team for high levels of data protection

Find or grow the important SaaSOps skills, such as:

- □ Technical knowledge of best-in-breed SaaS applications
- □ Ability to understand multi-directional user interactions among different SaaS apps
- □ Understanding of end user accounts, permissions, and access rights management

□ Knowledge of API frameworks to create API-based integrations and automations between systems

□ Ability to document SaaS app configurations, processes, and procedures

□ Familiarity with new SaaS app risk assessments and recommendations

□ Experience with SaaS portfolio evaluations

□ Familiarity with new SaaS app implementation

□ Experience scaling SaaS offerings

□ Experience with SaaS app performance monitoring, incident response, and auditing

□ Ability to continuously improve to optimize processes

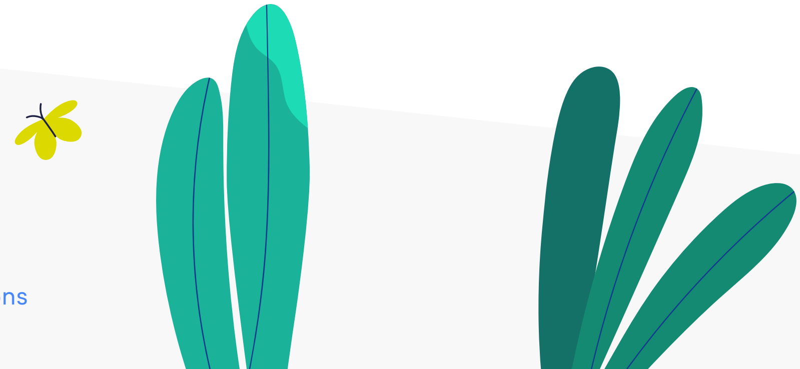
□ Experience with backup and recovery plans

□ Ability to proactively build relationships with other teams and stakeholders across the business

□ Understanding of how to use IT to achieve business goals

□ Ability to think creatively and architect new solutions

□ Passionate about creating an excellent user experience: enabling employees to be more productive, eliminating friction



Provide crucial SaaS end user training and support, including:

- □ SaaS app testing with small groups of employees to identify common trouble spots
- □ Needs assessments to meet audience training requirements
- □ Cross-functional teaming with business functions to maximize user productivity
- □ Ensuring users know how to get the most out of collaboration tools
- □ Ensuring users know meaning of alerts and notifications of potential security violations
- □ Security awareness training for:
    - □ Multi-factor authentication (MFA)
    - □ Data classification and protection at work
    - □ Email best practices, including:
        - □ Anti-phishing for spotting suspicious emails
        - □ Acceptable email attachments
        - □ Sharing information outside the organization
    - □ Strong passwords
    - □ Automatic public WiFi connection dangers
    - □ Web browsing best practices like avoiding suspicious links and downloads
    - □ Personal devices for work—BYOD policies of acceptable device usage and how to harden them

Get started with change management to include:

- □ Change management plans according to the nature of the new SaaS app; if it’s a complete switchover from one tool to a replacement that some may resent, get top management to announce the change
- □ Hands-on training to diminish employee fears of change
- □ Phased roll-outs to give users time to absorb change
- □ Evangelization of preferred SaaS apps
- □ Change, validation, and deployment standardization and automation for fast, efficient handling of all IT infrastructure or SaaS environment changes to minimize impact on service delivery

Managing and securing IT the SaaSOps way

While SaaS management and SaaS security are two parts of the whole SaaSOps pie, it’s important to take a look at each one. In this section, we break each one into its essential best practices. Up first is SaaS management.

Five essential components of SaaS management

The best practices for managing SaaS go into the following broad categories, each with its own checklist:

1. User lifecycle management
2. Visibility and auditability
3. Application configuration
4. Least privilege access
5. Spend management

Maximize productivity and protect data during user lifecycle changes by:

□ Creating standardized and/or automated processes for onboarding. A new employee will need access to apps, files, folders, groups, calendars, sites, etc. that are not only used company wide, but also specific to their role

TIP:

As part of the onboarding process, set up an "IT welcome" meeting with new employees on their first day. This is a good opportunity to explain:

- What policies you have, why you have them, and best practices.
- What technological and IT resources are available to them.
- If there are certain features of SaaS apps that everybody needs to know how to use, walk them through it.

Keep it short—20 mins is great!

For more onboarding tips, check out: Onboarding Isn't Just Provisioning: Are You Leaving Out This Vital Step?

□ Limiting access to data until new employees set up MFA

□ Creating standardized and/or automated processes for mid-lifecycle events. Consider:

- □ When a user changes teams...
- □ When a user gets promoted...
- □ When a user goes on leave/vacation...
- □ When a user joins a project...
- □ When a user needs to reset their password...
- □ When a user's account is compromised...
- □ When a user's device is lost or stolen...

- □ Which new files, folders, calendars, sites, applications, etc. do they need access to?
- □ Which files, folders, calendars, sites, applications, etc. should they no longer have access to?
- □ Which group/OU memberships must be updated?
- □ Do elevated access rights need to be granted?
- □ Do profiles, email signatures, etc. need to be updated? Is an email autoresponder necessary?
- □ Which security steps are needed to prevent unauthorized access?

□ Creating standardized and/or automated processes for offboarding:

- □ Full-time employees
- □ Part-time employees, temporary workers, seasonal workers
- □ Contractors, consultants whose contracts have expired
- □ Vendors, partners, etc.

Including steps like:

- □ Lock the user out of the account (e.g., reset password)
- □ Hide user in the directory
- □ Security cleanup (e.g, delete 2-step backup codes, delete app-specific passwords, disable IMAP/POP)
- □ Device cleanup (e.g., revoke devices from account, wipe device)
- □ Transfer files, folders, groups, calendar events, etc. across apps to manager or service account
- □ Route email, set up auto-reply
- □ Back up data
- □ Enter legal hold (if necessary)
- □ Remove license
- □ Delete account

TIP:

To learn more about the essential steps of a perfect offboarding workflow, check out Offboarding Employees: The Ultimate Checklist for Modern IT Professionals.

Get visibility into your SaaS environment, including:

- □ All SaaS apps used (IT-sanctioned or not)
- □ All users, groups, and files across SaaS apps and instances
- □ Application settings and controls across SaaS apps
- □ Domain access level requests by each SaaS app
- □ Third-party apps installed on your domain
- □ Third-party browser extensions installed by users
- □ Third-party mobile apps installed by users
- □ G Suite add-ons installed by users
- □ Office 365 add-ins installed by users
- □ Spikes in failed user logins
- □ Users who haven't enrolled in (or have disabled) MFA
- □ Users who have not logged into SaaS apps in 30/60/90 days (i.e., inactive licenses)
- □ Total number of super admins across SaaS apps
- □ Empty or unused groups/channels across SaaS apps (consider archiving/deleting to reduce clutter)

TIP:

Review any dependencies tied to specific users and/or accounts. This visibility helps you discover what SaaS systems and processes will break if an account is suspended or the user leaves the organization.

Maintain audit trails that capture:

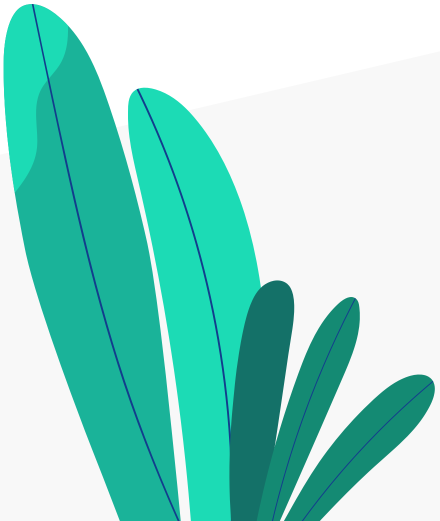
- □ Admin activity across SaaS apps
- □ Audit log file locations
- □ Which users were added and when
- □ Who’s left the company
- □ Which IT admins have access to critical systems across SaaS apps

TIP:

Audit your existing webhooks and scripts. It’s a good idea to know where they live, who’s managing them, and how they’re hosted.

Prevent risky application configurations by reviewing:

- □ Group privacy settings for exposed groups
  - □ Email lists
  - □ Web forums
  - □ Q&A forums
  - □ Collaborative inboxes
- □ Calendar privacy settings for overexposed calendars
- □ File privacy settings for overexposed files
- □ Automatic email forwarding settings



Enforce least privilege access with:

□ Super admin access policies for each SaaS app

□ Granular user access roles for minimum privileges necessary for job

□ Time-limited roles to prevent after-hours or weekend access

Identify unnecessary spending by:

□ Centralizing SaaS usage data

□ Regularly tracking login data to identify unused or underutilized licenses

□ Reassigning/deleting licenses or reallocating less expensive licenses to users to cut costs

Five essential components of SaaS security

Just as there are five key components to managing SaaS, there are five essential components to securing your SaaS environment.

These five components are:

1. Identity and access (IDaaS)
2. Insider threats
3. File security
4. Incident response
5. Regulatory compliance

Once again, each component has its own best practices checklist. While security practices change with evolving threats, a checklist can almost never be exhaustive. However, the checklist in each section provides a good starting point.

Use a good IDaaS solution for:

- □ Users to securely and quickly connect (i.e., authenticate) to SaaS apps
- □ Single sign-on (SSO)
- □ MFA deployment

Continuously guard against insider threats by monitoring for:

- □ Suspicious activity related to data theft, like unusually large file downloads within a short time period
- □ Sharing sensitive files with a competitor
- □ Exposure of confidential or sensitive data (whether intentional or accidental)
- □ Email forwarding from specific users to email addresses outside your domain

Proactively secure data by monitoring for:

- □ Sensitive files being publicly or externally shared
- □ Sensitive folder paths, like accounting or finance, being publicly or externally shared
- □ Sensitive file forwarding to a personal email account (e.g., Gmail, Yahoo)
- □ Sensitive data exposure from executives (e.g., CEO, CFO)
- □ Specific file types being publicly or externally shared (e.g., spreadsheets and PDFs are more likely to contain sensitive information)
- □ Users who should no longer have access to specific files, folders, calendars, etc. (e.g., consultants, interns, employees who've switched teams)
- □ Users who should no longer belong to specific groups/distribution lists (e.g., contractors, employees who've switched teams)
- □ External domains to which files are shared
- □ External people with whom files are shared

And regularly scanning files for:

□ Personal identifiable information (PII)

□ Protected health information (PHI)

□ Payment information

□ Passwords

□ Intellectual property (IP) or trade secrets

□ Executable files (.exe)

□ Encryption keys

□ Keywords that may signal sensitive information, like “Confidential” or “Internal Use Only”

□ Confidential project names

TIP:

Create a dedicated IT email group or Slack channel to centralize relevant, actionable, and important alerts.

Improve SaaS security with an incident response plan, including:

□ Training employees on roles and responsibilities if a security incident occurs

□ Defining the criteria for security incidents and thresholds (e.g., exposure of confidential financial data)

□ Orchestrated and automated remediation across integrated systems (e.g., SIEM, EMM, ITSM)

□ Lessons learned and incident documentation

Comply with regulations by:

□ Having detailed audit logs of user and admin actions for proof of compliance

□ Setting up automated policies for specific regulatory compliance standards (e.g., HIPAA, PCI, and GDPR)

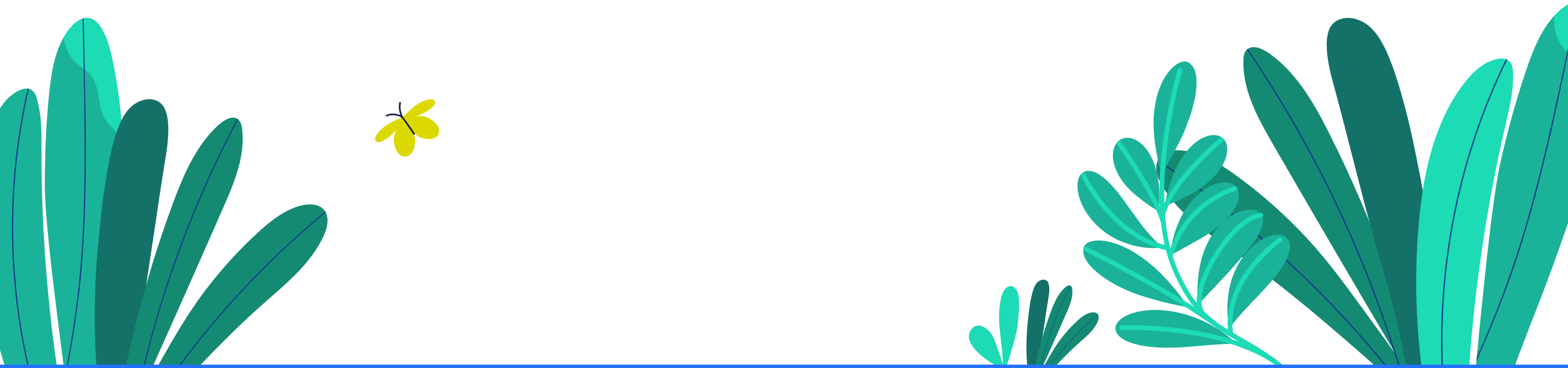
□ Detecting, and remediating, sensitive data exposure and excess admin privileges to ensure compliance

Your next steps in SaaSOps

As you work through this checklist, assess your SaaS environment and identify any gaps. Are there any team members, skills, and/or training you're currently missing but want to have in the future? Is there room to automate and do less manual work? Where are the biggest operational security risks?

Once you've assessed your environment, you can work on a longer-term strategic SaaSOps plan that aligns with business goals and policies. With this, not only can you demonstrate that IT is a value driver and engaged business partner, but you'll also ensure that your organization is set up for success in the digital workplace.

Looking for more SaaSOps info? Check out www.bettercloud.com/saasops/ for in-depth webinars, books, success stories from SaaSOps practitioners, and more.



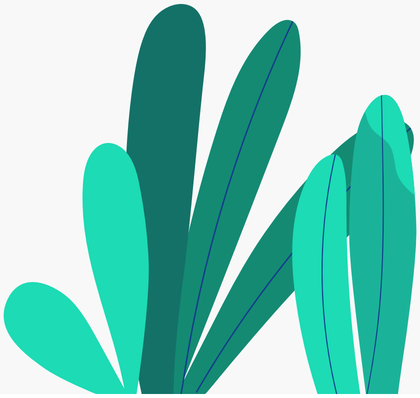
About BetterCloud

BetterCloud is the first provider of SaaSOps solutions to manage and secure the digital workplace. Over 2,500 customers in 60+ countries rely on BetterCloud to automate processes and policies across a company's SaaS application portfolio. BetterCloud is headquartered in New York City with offices in San Francisco, CA and Atlanta, GA.

BetterCloud has offboarded 1 million users and secured 5 billion files to date. To learn more about how BetterCloud can help you manage and secure your SaaS apps, *request a demo*.

BetterCloud

The IT Leader’s Glossary for SaaS Operations



API

Known as Application Programming Interface, it specifies how software components interact, allowing two applications to communicate with each other.

API frameworks

A collection of APIs that make application creation easier and faster by providing reusable components.

Application configuration

Refers to the management of user, group, and file settings/controls. This can apply to the initial configuration of these settings (e.g., when an organization adopts a new SaaS application) or ongoing management, like detecting and remediating when changes and misconfigurations are made to settings in an existing application.

Auditability

Ability to control, track, and view changes made by administrators. It is critical for security coverage and regulatory compliance.

Authentication

Process to grant access to apps by verifying that users are who they claim to be. Authentication solves the first order problem: identity/access.

Authorization

Process to grant access to specific SaaS data, configurations, resources, or functions. Authorization solves the second order problem: user interactions.

Digital workplace

Professional environment where employees are enabled and empowered to use the latest technology to stay engaged and productive.

EMM

Enterprise Mobility Management (EMM) is an enterprise solution to distribute, manage, and secure mobile endpoints, such as phones, tablets, and laptops that are used by employees.

File security

Process to protect the most sensitive data stored in files across your SaaS apps, including customer data, employee data, company IP, etc. It protects files within SaaS applications from being leaked, inappropriately shared, or downloaded to user's computers for unauthorized use.

Heterogeneous environment

A best-of-breed approach that allows organizations to pick and choose cloud applications that best suit their needs, as opposed to keeping with a single vendor.

Homogeneous environment

An approach in IT where organizations standardize on solutions from a single vendor.

IAM

Identity and access management (IAM) refers to policies and technologies that ensure users have appropriate access to apps at the right time.

IDaaS

Identity-as-a-service (IDaaS) refers to cloud-based identity and access management services that are offered on a subscription basis.

Incident response

Umbrella term for activities where an organization recognizes and responds to an event. The purpose is to gather the information required to make educated decisions about how to deal with a specific event and act upon the information gathered.

Insider threat

A current or former employee, contractor, or business partner who has access to an organization's network, systems, or data and is either:

- Compromised (exploited by outsiders through compromised credentials)
- Malicious (intentionally causes harm, either for personal or financial gain)
- Negligent (well-meaning, but accidentally exposes sensitive information)

ITSM

Information Technology Service Management (ITSM) refers to policy-directed activities, processes, and procedures that organizations do to plan, deliver, operate, and control IT services.

Least privilege access

Process of granting a user the minimum permissions required in order to do their job, and nothing more

MFA

Multi-factor authentication (MFA) is the process of granting access to SaaS and IT resources after a user successfully gives two or more pieces of evidence that confirms their identity.

SaaS

Software-as-a-service (SaaS) is a method of software delivery and licensing in which software is accessed online via a subscription.

SIEM

Security Information and Event Management (SIEM) refers to the real-time analysis of security alerts from SaaS applications, IT, and network infrastructure.

SaaS management

Process of managing onboarding, offboarding, and app configurations across SaaS apps. Core tenets of SaaS management include visibility across apps as well as the ability to audit admin activity and enforce a least privilege model. SaaS management ensures that users have the right access to the right data at the right time.

SaaS Operations

An IT practice referring to how software-as-a-service (SaaS) applications are managed and secured through centralized and automated operations (Ops), resulting in reduced friction, improved collaboration, and better employee experience. It does not refer to uptime, performance, or availability of a SaaS app.

SaaSOps

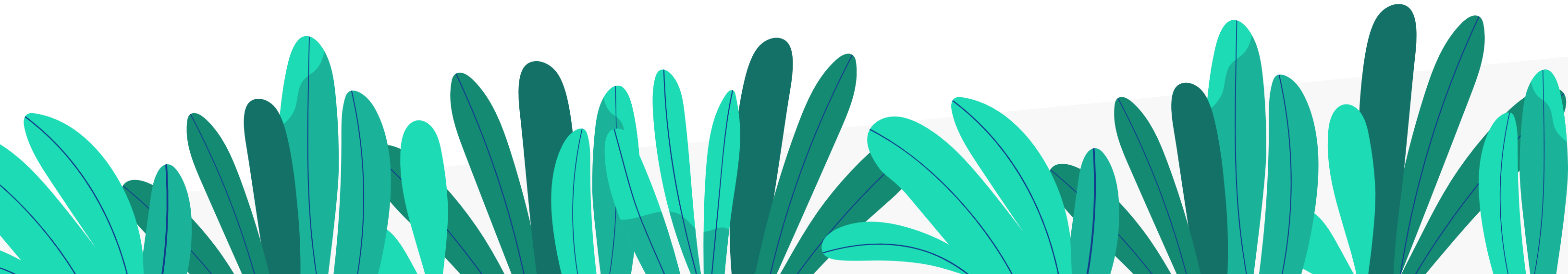
The shortened term that refers to SaaS Operations.

SaaS security

Process to protect mission-critical data in SaaS apps so that companies can avoid data breaches/leakage, compliance fines, loss of IP, loss of competitive advantage, and/or business disruption.

Shadow IT

The use of software, systems, and other IT solutions without IT’s explicit approval or knowledge.



Spend management

Ability to manage and control SaaS costs by centralizing visibility of subscriptions and usage to identify unnecessary spending.

SSO

Single Sign-on (SSO) refers to session and user authentication where a user uses the same login credentials to access multiple apps.

System of record

Information storage that is the authoritative data source. Organizations trust SaaS vendors to house mission-critical, irreplaceable data.

Regulatory compliance

Activities that ensure an organization is compliant with and continues to remain compliant with the rules and bylaws of different regulatory boards (ex. PII, HIPAA, GDPR, etc).

User interaction

The action a user takes to get work done in the digital workplace. It refers to the processes users are performing inside SaaS apps, the people they're interacting with, and the data they're interacting with. (Examples: sharing a Google Drive file with a partner, creating a public Office 365 group, downloading a folder from Dropbox)

User lifecycle management

User lifecycle management (ULM) refers to the processes that occur during lifecycle changes. This includes onboarding and offboarding as well as mid-lifecycle changes. Events like switching teams, promotions, leaves of absence, etc. all require changes in access rights, group memberships, entitlements, etc.

Visibility

Ability to view all of the users, groups, and files in an organization's SaaS applications in a single place. It is key to identify problem areas within an organization's environment.