BetterCloud

2020 SaaSOps BUYER'S GUIDE

Everything you need to know to buy
a world-class SaaSOps platform

BetterCloud

TABLE OF CONTENTS

How to Use This Guide

The right SaaS Operations (SaaSOps) solution can drive enormous benefits, such as threat reduction, cost savings, and productivity gains. Researching and choosing the best solution requires careful consideration. This buyers' guide is designed to help you critically evaluate and choose the optimal SaaSOps solution for your organization.

It provides a look into the emerging SaaSOps landscape and the challenges that led to its creation. We've also included the key use cases and product capabilities you should consider when evaluating SaaSOps solutions. Finally, this guide provides additional resources to learn more about the SaaSOps market.

What is SaaSOps?

While the rise of SaaS applications has increased productivity and collaboration for employees, it has created a slew of new challenges for IT. SaaS creates a massive, complex, interconnected data sprawl that grows by the day. Think of all the data objects that reference, interact, control, and/or rely on each other, such as: users, groups, mailboxes, files, folders, records, contacts, calendars, third-party apps, logs, metadata, permissions, devices, etc.

SaaS Operations, or SaaSOps, is a new discipline for IT and security teams that has emerged out of the need to manage and secure SaaS applications. 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 is defined as a 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**

SaaSOps requires a new organizational structure, new skills, new end user training and support, as well as new technology products. SaaSOps introduces a new concept for IT in the digital workplace: control and secure the user, not the infrastructure or perimeter.

Historically, IT was concerned with the network perimeter, but SaaS applications have made perimeter-based security obsolete. Devices and data are not hosted on-premises anymore, so the idea of creating a network in a corporate data center and protecting it with a firewall is no longer relevant. The shift to the cloud means the network perimeter has dissolved.

With the advent of SaaS, employees no longer just work 9-5, at the office, on one device. They use a panoply of unmanaged devices—smartphones, mobile devices, tablets, Chromebooks—from multiple locations at any time. This makes the traditional perimeter an abstraction, something that no longer exists in practice.

All of these macro changes mean that IT must shift to a different security model. In SaaSOps, the area of focus is shifting to something new: your user, and how they're using SaaS apps. Why?

- Users are closest to data, which is what IT is ultimately trying to protect. Confidential business data, trade secrets, IP, employee data, and customer data all lives in SaaS applications today. Users are interacting with this data every day to do their jobs—changing, updating, and sharing it continuously. To protect sensitive data, IT has to control and secure who has access to it.

- Users have a lot of freedom and power with SaaS applications (and as a result, IT teams are losing control). They can share data freely with just about anyone inside or outside the org: colleagues, partners, customers, contractors, even competitors. They can adjust permissions and sharing settings on their own, add themselves to distribution lists and groups, and share data publicly on the web. Of course, all of this freedom is by design. It's what makes SaaS such a powerful productivity tool. But the very beauty of SaaS—the openness and ease of sharing data—is also its most dangerous risk.

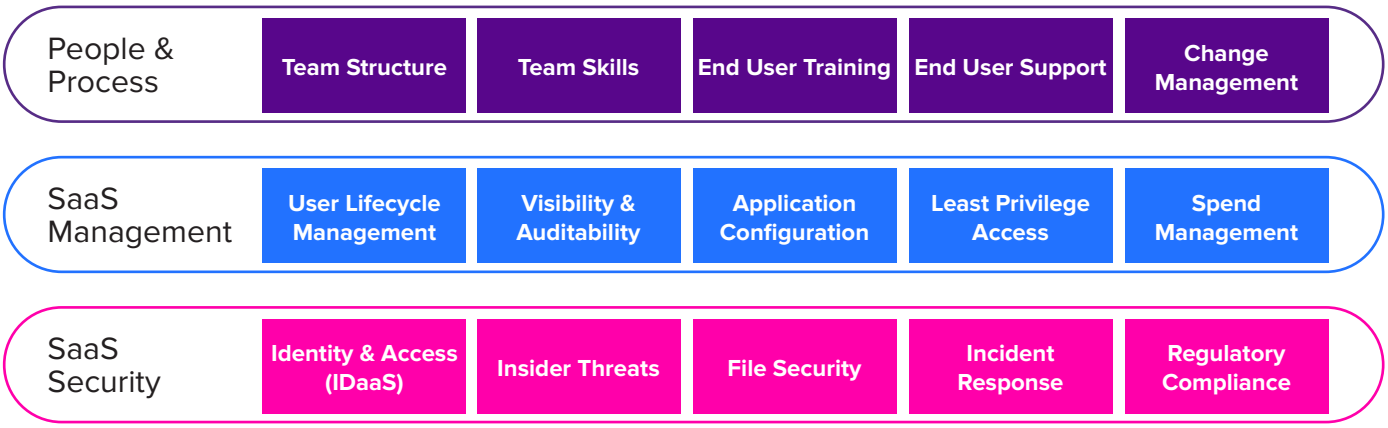
- Users are creating a tremendous SaaS sprawl. They're using multiple apps (e.g., Office 365, G Suite, Slack, Dropbox, third-party apps, custom apps) on multiple devices

(e.g., laptop, Chromebook, tablet, mobile phone). As SaaS adoption grows, so does the amount of data living in those SaaS apps, which in turn creates an enormous information sprawl. The bigger that sprawl is, the harder it is to get visibility and stay in compliance.

The benefits of adopting a SaaSOps philosophy and platforms include time savings, cost savings, reduction in human error, achieving and maintaining compliance, data security, reduction in IT ticket volume, and a more productive, engaged workforce.

SaaSOps Disciplines

SaaSOps has three essential disciplines.



First, is People and Processes. Without the right processes manned by the right team, the remaining disciplines are more challenging.

Beyond people and processes, SaaSOps is made of two inseparable technology components: SaaS Management and SaaS Security.

As the number of SaaS applications grow, it becomes more difficult and time consuming to manage via administrator consoles. Not to mention, each application has varying levels of sophistication and automation, making application management inconsistent. SaaS Management saves time on common tasks by consolidating the administration of data,

users, and controls across SaaS applications into a single, easy-to-use platform.

With each application offering varying levels of sophistication around visibility and control, it's impossible to guarantee the security of sensitive data and remain nimble enough to address any threats that arise, without shutting down access to key collaboration features. SaaS Security keeps employees productive while maintaining the necessary security posture for your business by monitoring potential threats, remediating any issues, and automating security policies.

Why existing tools are not enough

Finding a mechanism to manage SaaS users, find sensitive data, or take action in SaaS applications is relatively simple. There is no shortage of options for "managing" or "securing" SaaS applications. Collecting all of the relevant SaaS data, turning it into operational context, and pairing it with a complex workflow engine, however, is a whole other matter.

Below is a list of the current solutions organizations have tried to use to solve SaaSOps challenges and why they are insufficient:

Application Administrator Consoles: Since SaaS applications are owned and managed by distinct companies, the individual administrator consoles only provide context on and enable IT to take action in a single application. The administer consoles also vary across applications, making it difficult to remember how to do simple tasks across applications. IT needs to understand the whole picture of their digital workplace and it's impossible to do that when users and data are managed in a myriad of silos that offer different levels of control.

Additionally, SaaS companies are focused on building their products functionality, not building complete administrator consoles. Therefore most administrator consoles lack the visibility and automation functionality that administrators need when overseeing a digital workplace.

Identity as a Service (IDaaS): While an IDaaS is an important part of a SaaSOps solution for

controlling users access to applications, it is not a complete SaaSOps solution. An IDaaS is a solid solution for basic provisioning and deprovisioning across SaaS applications, however, they lack the deep user lifecycle management actions required to fully execute a lifecycle event, such as onboarding or offboarding users. IDaaS vendors lack the ability to take critical actions, such as data transfer, email forwarding, group settings management, and calendar sharing as well as the customization options needed for these processes, including suspending a user and then waiting for a set number of days before deleting a user's account. Furthermore, IDaaS vendors do not provide functionality to assist with the security stance of assets, least privilege administrator, or the ability to manage day-to-day SaaS administration.

Cloud Access Security Broker (CASB): CASBs focus primarily on SaaS data security - including encryption of assets, inline blocking of sharing assets, and network security. CASBs overlap with SaaSOps platforms in the areas of Data Loss Prevention (DLP - also referred to in this as "File Security") and sensitive content identification functionality. However, these platforms lack operational context on users and data to properly target specific security events. Without context into users and data, CASBs are unable to differentiate between normal, approved user collaboration versus a true security event. Additionally, CASBs do not offer granular actions for remediation within SaaS applications. This leads to CASBs' data security methods being extremely intrusive and disruptive to employees' productivity. As an example, if a user shares a file with sensitive information externally, a CASB will allow administrators to block the sharing; while a SaaSOps platform will have functionality to unshare the file, notify IT about the sharing of a sensitive file, or even send the file owner an email asking if they intended to share the file and a link to unshare the file. Finally, CASBs do not offer a solution for automating repetitive workflows, such as onboarding/offboarding, or policy violations, such as group or administrator configurations, all of which are key aspects of SaaSOps.

Integration Platform as a Service (IPaaS): IPaaS solutions are great for using simple logic

to take action across multiple applications. However, these solutions were not built for IT and do not ingest information from SaaS applications, leaving users to take action without any insight into the data or settings. Additionally, there's no complex logic (ie. transfer documents to a user's manager) or advanced sequencing of events (ie. customizing onboarding based on department). These platforms simply act on an individual trigger and take user-level - not admin-level - actions.

SaaS Spend Management: SaaS Spend Management tools are point solutions designed to identify shadow IT and unused SaaS licenses. These tools listen to the organization's finance system and alert IT when an employee has purchased a license for a SaaS application on their own. They also listen to individual applications via API to understand login and usage information, and offboard users if a tool is not being used. These tools are valuable for uncovering SaaS licenses, but they do not provide the full functionality needed to manage or secure the applications once identified. Additionally, the offboarding capabilities offered for unused licenses lack the granularity needed to delete a user's account (ie. no ability to transfer files to a user's manager or set up email forwarding).

The alternative: SaaSOps platform

What IT requires today is a simple way to correlate information across all SaaS applications and protect against SaaS threats. A solution that enables IT to see all SaaS data normalized across applications and stay on top of user interactions as they occur. Instead of waiting to hear of a problem in SaaS applications, IT teams should be able to respond to security threats in real-time. These responses should be flexible in how they define and remediate threats and limit the impact on employee's workflows. For that, organizations need a SaaSOps platform.

A SaaSOps platform aims to give IT more visibility into their murky SaaS environment; more actionable insights and less noise; a way to automate routine operational tasks while embedding security best practices. It also offers protection for organizations against

unauthorized data access, data loss, and data theft.

SaaSOps platforms underlay all product functionality with a powerful engine that normalizes data and creates an graph of data objects. This graph is the foundation of the operational context needed to effectively manage and secure applications. If done well, the operational context created by SaaSOps platforms enables IT to automate more of the day-to-day management of users and secure SaaS environments in a way that is not disruptive or prohibitive for users.

Do you really need a SaaSOps platform

Now that you understand what SaaSOps is and how organizations use it, it's time for a broader conversation. Does your organization need a SaaSOps platform?

Your organization may not be ready for complex, cross-application security policies and, instead, simply need a solution to fully automate user onboarding or offboarding across SaaS applications. Adoption of SaaSOps comes in phases, but if your organization has a digital workplace (or is moving towards becoming one), you need SaaSOps to manage and secure all of your applications. Without it, you're flying blind and it's only a matter of time before the promise of SaaS is going to backfire, if it hasn't already.

Automating operational processes through a SaaSOps platform ultimately allows IT to focus on strategic initiatives that drive the business forward. This propels your IT team to become a partner to the business, not a cost center. Not to mention, the benefit of ensuring manual, repetitive processes are completed in-full every time, rather than hoping every IT admin has completed a 78-step cross-application process correctly every time.

The SaaSOps Solution Essentials

Now, we get into the meat of what makes up a SaaSOps solution. There are 10 essential use cases that SaaSOps covers:

User Lifecycle Management	Onboarding, offboarding, and mid-lifecycle user changes are extremely manual and repetitive processes that IT needs to automate in order to reduce the risk associated with human error and free up valuable time.
Visibility & Auditability	Monitoring users, data, and admins across applications is critical to ensuring a secure environment. IT teams need to centralize this information from multiple applications into a single view in order to effectively manage and secure their environment.
Application Configurations	With so many end points for hackers to exfiltrate sensitive information, IT needs to ensure user, group, and file settings are set correctly in the start and remain secure.
Least Privilege Access	Least Privilege Access allows IT to limit administrator access to the settings and controls needed for the individual to do their job.
Spend Management	By pairing product utilization insights with automated policies, IT can recoup money that was previously spent on unused licenses.

Identity & Access Management	Identity and Access Management ensures that only authorized people from authorized locations can access applications. By centrally managing user identities and controlling access to resources, IT can secure sensitive data.
Insider Threat	Employees, contractors, partners, and privileged administrators can pose the greatest security threat to organizations. SaaSOps platforms dynamically identify changes and suspicious behavior to stop data loss or outsider infiltration.
File Security	IT needs a tool to discover sensitive content stored across SaaS applications and automatically remediate the oversharing of sensitive information without manual intervention by IT.
Incident Response	Incident Response gives IT an organized way to address and manage potential breaches before they happen. When a breach does occur, SaaSOps platforms limit the damage, reduce recovery time and cost, and help identify the source of infiltration.
Regulatory Compliance	Understanding and responding to threats in real time is imperative for organizations to maintain compliance with regulatory requirements.

User Lifecycle Management

In an ideal world, a user would never have to worry about having access to the right SaaS applications, correct permissions and settings within those applications, or accurate profile information when lifecycle changes occur. In reality, most IT teams lack the bandwidth to manually make user lifecycle changes quickly and the visibility to ensure SaaS data is up-to-date.

When these challenges extend to user offboarding, it creates a massive security threat. Ex-employees retain access to sensitive data and SaaS applications long past their last day,

leaving organizations continually vulnerable to data leaks and insider threats.

The key to onboarding, offboarding, and everything in between is automating manual actions throughout the process. Using automation, IT teams can:

- Save time
- Reduce human error
- Enhance security

Leveraging a SaaSOps platform, IT can manually control user lifecycle changes and build automated workflows to handle the repetitive steps in onboarding, offboarding, and mid-lifecycle processes. A SaaSOps platform has deep context around users, allowing IT to build customized workflows based on departments, managers, or locations. By partnering with the business, IT can automate all of the routine workflows to ensure users have proper access to applications, groups, and settings from day one all the way through the user's departure from the organization.

Since user lifecycle changes can happen at any time, SaaSOps platforms are able to automate workflows based on changes - such as when a user added to an application or a user's department is modified - or on command. With user lifecycle macros, IT teams can trigger a workflow to take a number of predetermined steps in real-time. This eliminates the reliance on a specific administrator revoking a user's access and the risk previously associated with manual steps.

BounceX builds "magical offboarding experience" with BetterCloud

BounceX, an online platform that allows companies to recognize website visitors, is celebrated for changing how marketers interact with potential customers. Just four years after its launch in 2012, the company won the distinction of being the fastest-growing software company in the United States. Since then, its growth has continued—to the point

where it was becoming a hindrance for IT. Large groups of new hires created exponentially more work for the IT employee charged with onboarding them. Other projects were set aside as IT was forced to stop everything and configure a growing number of SaaS accounts.

WHY BOUNCEX USES BETTERCLOUD

BounceX leverages BetterCloud to reduce the average time to onboard a user across different platforms from about 45 minutes to between 5 to 10 minutes. The IT team leverages automated workflows to replace time-consuming manual processes with automated actions and reduce the risk of human error. They have fully automated offboarding, so the instant an account is disabled in Namely, permissions to other critical systems are automatically withdrawn.

> "With the help of BetterCloud, we built a magical offboarding experience."
>
> **- Chloe Becquet, Director of IT, BounceX**

Visibility and Auditability

The digital workplace consists of dozens, even hundreds of applications. In this world, it is virtually impossible to get full visibility into assets or to understand the interactions taking place between them. Which users belong to which groups? What settings are administrators changing? Who is sharing files with external third parties? This lack of visibility not only blinds IT teams to the risks that exist, it also makes it impossible to mitigate those risks.

For organizations that have merged with or acquired companies, this challenge grows exponentially as every company has their own instances of applications and there's no clear way to manage users or see the data and interactions taking place across instances of the same application.

SaaSOps platforms must centralize the data and administrator controls across SaaS applications into a single platform to make it easier to visualize all the assets and users and audit administrator activity. SaaSOps platforms must also be able to centralize multiple instances of a single application for a complete view across an organization's entire environment.

By giving IT teams visibility into applications, SaaSOps platforms can surface critical insights, like how data is shared with people outside the organization and user settings across different applications and instances of a single application. This information can then be funnelled into an alerting system and/or an automated policy engine for management and security.

essence

Essence achieves broad visibility across SaaS applications with BetterCloud

Essence began life as a small, data-driven digital ad agency with a single IT person and grew into a global powerhouse, majority-owned by WPP, the world's largest advertising company. SaaS applications like G Suite helped the company to scale, but also created risk. While G Suite's accessibility made it easy to get work done anywhere, it also meant G Suite was easier to compromise.

WHY ESSENCE USES BETTERCLOUD

Essence uses BetterCloud to get broad visibility across multiple domains with multi-

instance connectors. SaaSOps flags sharing violations with alerts and ensures proper privileged access management with delegated admin access. Essence has created custom integrations to extend the power and security controls of BetterCloud across their SaaS environment.

Application Configurations

SaaS applications have a myriad of settings and controls for users, groups, and files that enable users to collaborate at a greater speed. Unfortunately, IT is not only responsible for configuring these settings upon initial purchase of an application, but they are also responsible for listening to risky changes in settings as employees add files, change group settings, and collaborate with users outside of your company (such as partners, contractors, or agencies). With thousands of settings available within a single application, it's nearly impossible for IT to monitor these configurations without a system in place.

A SaaSOps platform needs to be able to identify changes in settings, including user, group, file, and folder settings. SaaSOps platforms should be able to use that information in real time to alert IT of suspicious behavior. Once identified, that information needs to be fed into a workflow system that has been set up to assess the potential risk to the business and automate the appropriate remediation path.

Remediation paths must be configured using the administrator actions available in SaaS applications, such as changing the settings, suspending the user, or sending a notification via email or Slack to the appropriate teams.

Instacart delivers user satisfaction with BetterCloud

Instacart, the popular grocery-delivery service, strives to deliver for customers while its IT team aims to please employees. A cohort of 13 engineers and help desk staff serve about 1,200 employees and contractors — including a large contingent working in co-working spaces in Instacart-serving cities. As the company scaled, IT began putting automation in place, including an identity management system that took care of authentication. However, what Instacart was missing was an effective way to authorize (and de-authorize) the use of apps and the ability to audit their usage.

WHY INSTACART USES BETTERCLOUD

SaaSOps gave Instacart new visibility into application settings and user configurations, and data security. Through this visibility, they discovered and remediated improperly shared documents and calendars, minimizing the risk of accidental exposure. The team also set up alerts to remind IT about the age of contractor accounts in Slack to ensure these accounts are handled in a proper amount of time. These actions helped IT receive a very high NPS (Net Promoter Score) from other employees, reflecting an upswing in sentiment.

> "BetterCloud talks to all of the systems that don't necessarily talk to each other."
>
> **- Max Gerhardt, IT Engineer, Instacart**

Least Privilege Access

Each SaaS application has predetermined levels of access for administrators and there's no consistency across applications. IT teams have to retrofit these inflexible roles to administrator's responsibilities and oftentimes that means giving out access to more data and controls than are necessary for the individual to do their job. By giving out too many permissions, organizations are at a greater risk of an accidental or malicious security breach.

Additionally, most organizations have been forced to give out these blanket administrator permissions to so many users that they have no visibility into how many administrators they have and who really needs this level of access.

It is critical to ensure that administrators only have access to what they need, since excessive privileges can increase the risk of a security incident or data breach. SaaSOps platforms need to provide configurable administrator roles and permissions that allow administrators to have access to the controls they need, and nothing else. With custom roles, IT teams can control access to sensitive data and settings, and enhance security across the entire environment.

Administrator roles should be configurable based on application, instance, access to data objects (such as users, groups, or files), type of control (such as the ability to edit document settings versus delete a document), and the ability to trigger an automated workflow. A SaaSOps platform should also allow for an unlimited number of roles and permissions. This level of granularity and flexibility safeguards against administrators gaining access to data objects and controls they do not need.

Finally, a SaaSOps platform should allow IT to audit the number of administrators in an environment and alert IT if the number exceeds a set threshold. This information can then be ported into an automated workflow engine, which can remediate any threats. By limiting the number of administrators, organizations reduce security risks and greatly minimize the damage that hackers can inflict, if an administrator's account were hacked.

Middlesex Health

Middlesex Hospital secures their environment with BetterCloud

Middlesex is much more than just a hospital. Today, they are a fully connected, comprehensive network of expert health care providers. Middlesex Health exists to provide the safest, highest-quality health care, and the best experience possible for their community. Its core values include the pursuit of excellence, upholding honesty, cooperation and collaboration, supporting innovation, and delivering compassionate care. Because patient privacy depends on HIPAA compliance, healthcare organizations are bolstering their data protection strategies to meet regulatory requirements and secure sensitive health information. The IT team is responsible for Middlesex Health, which has one hospital, three external emergency departments, and three urgent care centers.

WHY MIDDLESEX HOSPITAL USES BETTERCLOUD?

SaaSOps created a more secure environment for Middlesex Hospital and empowered them to improve time efficiency, data accuracy, and security. By leveraging BetterCloud's deep insights and analytics, Middlesex was able to track what exactly led to a breach and whittle down the number of super admins on their domain from 12 to 2. Reducing the number of admins is best practice and ensures there are fewer points for errors.

Spend Management

Spend management is understanding your license costs across SaaS applications and saving money by recovering or re-allocating unused licenses without interrupting the business. When organizations purchase SaaS applications, they want to ensure that end

users are actually using the applications to which they have been given access.

SaaS IT administrators must be able to track licensing and usage to ensure the organization is not spending money on unused licenses. SaaS vendors do not have an incentive to help customers spend less money on their software, so IT has to implement their own processes and tools to rightsize software spending.

SaaSOps platforms give IT visibility into who is using their licenses and a way to automate license management to recoup the costs associated with underutilized licenses and offboarded users. SaaSOps offer alerts to notify IT teams when users have not logged into applications and automated remediation paths to offboard users (ie. transfer their data) and delete unused licenses. This process often leads to savings of hundreds of thousands of dollars a year for organizations.

Since SaaSOps focuses on not hindering user productivity, SaaSOps platforms should offer a method of approval by the end user, so IT is not deleting applications that users actually need.

FULLSCREEN

Fullscreen Media reimagines HR + IT with BetterCloud

Fullscreen Media is a social content company that helps brands and stand-alone talent grow, engage, and monetize their social audiences. Founded in January 2011, the company grew to nearly 1,000 employees in less than 10 years but was plagued by miscommunication between HR and IT. New hires would sometimes show up at the door of the IT room with no warning; lengthy onboarding processes reflected badly on the company and left some new employees unprepared. In addition, a lack of visibility into departing employees and offboarding processes was creating waste in the form of money spent on unused licenses.

WHY FULLSCREEN MEDIA USES BETTERCLOUD?

Fullscreen Media has been able to rebuild the relationship between HR and IT using BetterCloud, Namely, and a bit of ingenuity. IT replaced manual offboarding processes with BetterCloud's automated workflows, deprovisioned stale accounts, and reallocated unused licenses. These processes saved Fullscreen Media $100,000 in license costs right out of the gate.

Identity and Access Management

One of the most important benefits of SaaS is that users can access apps from any device, at any time, from anywhere. Before granting access to corporate data, companies have to verify end users are really who they say they are. For this to happen, there has to be a secure authentication between that user and their applications.

The goal of an Identity and Access Service is to ensure users are who they claim to be and to give them the right kinds of access to software applications, files, and other resources at the right times. With tools like multi-factor authentication (MFA), privileged identity management (PIM), single sign-on (SSO), privileged access management (PAM), and directory extensions, identity-based security has tightened the authentication protocols in place.

It ensures that only authorized people from authorized locations can access resources and applications. By centrally managing user identities and controlling their access to resources, Identity and Access Management softwares (such as IDaaS vendors) protect the new perimeter created by SaaS applications and create a strong first layer of security.

Insider Threat

SaaS applications are independently owned and do not share a common language for settings and controls. This creates a lot of confusion for users, as it's easy to believe a setting will further enable collaboration when it's actually opening the door to leak sensitive data. IT has historically tried to combat this with end user education, but given the sprawl of SaaS applications, it's unrealistic to assume users will remember this level of granularity for dozens of applications.

To compound the issue, users have more access to change settings, making it easier than ever for users and administrators to make changes that seem innocuous, but create serious problems for the organization's security posture. SaaS sprawl has made it nearly impossible for IT teams to stay abreast of the changes and potential threats across a digital workplace.

SaaSOps platforms should dynamically identify changes and negligent or nefarious user behavior to stop data loss or outsider infiltration. Suspicious changes and behavior should also be paired with the operational context stored on users, groups, and data. With this level of intelligence, IT has the information needed to assess the risks and impact of an insider's actions - which are critical to prioritizing an appropriate response.

Detected threats should be fed into an automated policy engine to apply the appropriate response. Automated responses must be customizable and have the ability to take action across multiple applications in order to stop the threat from spreading. A common example of this is when a threat is detected in a file sharing application, IT can build a policy to change settings on any sensitive data at risk, end all sessions on the user's devices, suspend the user in an IDaaS platform to shut off all access to additional applications, and notify IT and/or the user's manager via email or Slack.

Rather than applying blanket policies to all users and documents though, SaaSOps platforms leverage the operational context on user and data to run the appropriate policy.

This granularity ensures users are not harming the company's security posture, while retaining access to the tools they need to be productive.

Khoros manages SaaSOps smarter with BetterCloud

Khoros, a leading customer engagement platform, was formed in March 2019 when Lithium Technologies and Spredfast finalized their merger agreement. The combined company offered integrated workflows and actionable insights to optimize engagement over social media, messaging, and other digital channels. To optimize internal processes and help Khoros realize the value of the merger, IT committed itself to automating repetitive and manual tasks that were using up valuable resources.

WHY KHOROS USES BETTERCLOUD?

By centralizing their applications in one place and extending BetterCloud's native integrations with multiple custom-built integrations, Khoros has been able to reduce the number of manual steps in their routine processes and get greater visibility into users, application settings, configurations, and data security. Visibility combined with an automation platform has strengthened the company's security posture and minimized the risk of insider threats, including employees retaining unnecessary access to applications with sensitive data - such as Github.

"Using BetterCloud to help manage licenses helps us get better visibility into how our employees are using our SaaS applications."

- Andy O'Rourke, IT Automation Specialist II, Khoros

File Security

Unstructured data such as documents, presentations, and spreadsheets will represent over 80 percent of all data within an organization by 2025. This data can include confidential information about customers, strategic business plans, corporate intellectual property, and other sensitive or proprietary information. These documents and resources are commonly stored within multiple repositories that span SaaS applications.

SaaS applications give end users the power to share files publicly, with external users, and domain-wide. IT is unable to see all of the data stored across applications, including which files contain sensitive material, how files are shared, or who is sharing them. The lack of visibility creates blind spots that IT teams are not privy to, yet somehow responsible for securing. Privacy laws, potential data breaches, and violations compound the need to solve this complex and seemingly overwhelming business challenge.

A SaaSOps platform must display a list of all files stored across SaaS applications, so IT can filter by common attributes or search for overexposed files. Since file settings are constantly changing and IT cannot realistically maintain a hold on them, real-time information on files should be fed into an alerting system that notifies IT of risky behavior and can trigger an automated policy to remediate the threat.

SaaSOps platforms also need to be able to discover which files contain sensitive content, such as personally Identifiable Information (PII), words or phrases that violate HIPAA compliance, profanity, and financial information. SaaSOps platforms can run audits on existing files as well as share real-time information on sensitive content with the aforementioned alerting and policy engines. This ensures an organization's most sensitive data is protected without manual intervention by IT.

INTERCOM

Intercom achieves a better employee experience with BetterCloud

Intercom is a fast-growing business messaging platform with five offices around the world. The IT team is passionate about giving new hires an extraordinary, five-star experience without sacrificing security and productivity. Their onboarding aims to enable new employees to have access to the applications and tools that they need to get started right away. The IT team does not believe that there is an all-or-nothing approach when it comes to using SaaS apps; they want to give some leeway to employees to choose the SaaS apps that they need while IT secures user interactions across the digital workplace.

WHY INTERCOM USES BETTERCLOUD

BetterCloud helps Intercom strike the balance of security and productivity for their end users. By using BetterCloud, Intercom has been able to set up alerts to scan files for sensitive data and streamline policy enforcement and remediation without hindering employee's workflows. By leveraging BetterCloud's increased operational intelligence, Intercom has reduced friction and enhanced security of their most sensitive data.

"With BetterCloud, I don't have to choose between saying no to our employees and putting the organization at risk. There is a third way that offers both security and freedom of choice."

- Emanuele Sparvoli, Head of IT, Intercom

Incident Response

The longer it takes to discover a threat, the more damage it can potentially inflict. With users interacting with thousands of settings and files across hundreds of SaaS applications at any given moment, it's impossible for IT to keep track of security threats. Additionally, the remediation steps necessary after an incident are manual and span across multiple applications. Responding to a threat can take IT hours, days, or even weeks due to the dispersed nature of the digital workplace.

IT needs a SaaSOps platform that includes monitoring capabilities across SaaS applications to notify IT when there's a potential incident. Rather than inundating IT with alerts, SaaSOps platforms retrieve stored operational context on the user or file in order to only notify IT when an incident is a concern, rather than normal user behavior. Of course, not every incident has the same level of urgency attached to it. A SaaSOps platform provides IT with the means to categorize the severity of events.

A SaaSOps platform should also be able to resolve any issues with a workflow engine that can take action across multiple SaaS applications. In effect, the SaaSOps platform needs to be the hub around which a customizable workflow for managing incidents can be crafted. IT can configure workflows to start a particular remediation process based on the severity of the event.

An important part of incident response is maintaining a log of all actions taken to close the threat or breach. Since operations are centralized in a SaaSOps platform, it is able to build a record of the incident as well as the entire process surrounding that incident for investigation and regulatory compliance.

Finally, SaaSOps platforms must also integrate with existing Information Technology Service

Management (ITSM) solutions in order to plug into larger incidence response workflows. This integration allows IT to resolve issues that are not just on SaaS applications - such as collecting a user's device, wiping the user's cell phone, or revoking access to any on-premise systems - and maintain a central log of all issues that have been resolved.

Betterment

Betterment keeps tabs on external file sharing with BetterCloud

Since 2010, Betterment has had one mission: to help people make the most of their money so they can live better lives. Using cutting-edge technology, they empower their hundreds of thousands of customers to manage their money – for today, tomorrow, and someday – through personalized, expert advice; automated money management tools; and Tax Smart strategies that help keep taxes low across accounts. Betterment does all of this while complying with the high security the industry requires.

WHY BETTERMENT USES BETTERCLOUD?

Betterment leverages BetterCloud to gain insight into sensitive data sharing and has created policies to automatically remove access to files that are shared externally after a specific number of days. Their file security policies have reduced the back and forth required to communicate about these sensitive files, which can number in the hundreds or thousands, and increased ITs effectiveness and ability to focus on more strategic tasks. BetterCloud has strengthened Betterment's security posture by picking up where other security tools leave off.

> "BetterCloud strengthened our security posture and made our team more effective."
>
> **- Kevin Torres, Corporate IT Manager, Betterment**

Regulatory Compliance

Regulatory compliance applies to the 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). IT has to maintain different regulatory protocols for who can have access to what, where information can be stored, how it can be shared - the list is endless and it's difficult to remember all of the requirements. It's impossible to enforce these regulatory standards across the data sprawl created by the digital workplace.

By normalizing the data across applications, SaaSOps platforms enable IT to visualize all of the users, data, and settings across applications. This foundation is critical to creating policies across applications to enforce the same types of behavior around settings and file sharing. SaaSOps platforms help manage company risk by creating guardrails to protect users from violating regulatory compliance standards.

SaaSOps also offers configurable workflows to correct regulatory violations in real-time to ensure your company is always compliant. Create policies to take care of the manual tasks needed to maintain compliance, such as automatically unsharing files containing HIPAA or PII information.

Excella

Excella, Inc. excels in IT automation with BetterCloud

Efficiency and security are both high priorities at Excella, an Agile Technology Firm that helps federal agencies and commercial and nonprofit clients adopt agile technologies and modernize their infrastructure. As use of SaaS increased, IT Director Colleen Alaimo sought a better way to quickly onboard new consultants to Office 365 and gain visibility into user actions to ensure they were complying with security and data protection policies.

WHY EXCELLA USES BETTERCLOUD?

Excella has connected over 20 applications to BetterCloud, creating a single source of truth for all SaaSOps. Leveraging BetterCloud's API, Excella has automated over 90 manual steps and achieved newfound visibility into how information was being shared. These workflows have reduced friction, enhanced security and reduced the burden to remain compliant with different regulatory standards.

> "BetterCloud makes it faster and easier for us to achieve compliance. It is an IT admin's dream."
>
> **- Colleen Alaimo, IT Director, Excella**

The Technical Capabilities of a SaaSOps Solution

Now that you understand the eight essential capabilities of a SaaSOps platform, we'll dive deeper into the technology that makes up a SaaSOps solution. This will help you differentiate a complete SaaSOps platform from new entrants in the SaaSOps market and point solutions.

	BetterCloud	Native Admin Consoles	CASB	IDaaS	Workflow Automation	SaaS Spend Management
Cross-application user, group, setting and file ingestion through APIs	Yes	No	Only files	Only users & groups	No	Only users
Normalization of application data	Yes	No	No	No	No	No
Real-time intelligence for alert detection and policy violations	Yes	Limited/ No - Depending on Provider	Yes	Limited - only users & groups	No	Limited - only users
Single or bulk orchestration	Yes	Limited	Yes	Limited - only users & groups	No	Limited - only users
Automated and on-demand workflows	Yes	Limited	Limited - only files	Limited - only users & groups	Yes	Limited - only users
Custom role-based privileges	Yes	No	No	No	No	No
Custom integration connections	Yes	No	No	Yes	Yes	No

Cross-application user, group, setting and file ingestion through APIs

In order to get complete visibility into your SaaS applications, SaaSOps platforms should connect to best of breed SaaS applications via APIs - not agents, or proxies/reverse proxies. APIs give a real-time view into activity in the SaaS application and do not slow down access to applications. Additionally, APIs allow IT to take actions directly in the applications, while a proxy and other forms of connection only allow IT to block access to sites or files

Normalization of application data

SaaSOps platforms ingest the data across SaaS applications in real time, capturing metadata on billions of events from users, files, settings, and groups. Normalization is the only way to make sense of a large number of data objects. IT can then drill down to focus on specific objects, such as a particular user or an attribute like a public file.

Real-time intelligence for alert detection and policy violations

Visibility is important but, with the amount of data created by the digital workplace, it's critical for SaaSOps platforms to make sense of data objects and changes as they are made. There must be an engine powering the SaaSOps platform that listens for suspicious events and policy violations, and notifies IT of critical threats. There should be templated alerts for common threats as well as custom alerts for specific use cases. This benefits IT to detect incidents and prevent attacks well before there's a breach.

Single and bulk orchestration

To help IT remediate any issues identified, SaaSOps platforms should ingest the actions available in the native administrator consoles - such as changing files, groups, or user

settings. Actions ideally are categorized by whatever the administrator is viewing - for example, if IT is viewing files, the actions available should be related to files. SaaSOps platforms also offer the option to take an action on a single data object or multiple objects at once.

Automated and on-demand workflows

SaaSOps platforms save valuable time and reduce the risk associated with manual tasks with an automated workflow engine. Workflows can be customized for repeatable processes, such as onboarding or offboarding, as well as security policies, such as file sharing or groups settings policies. The key difference between a SaaSOps platform and other existing solutions is the ability to automate a set sequence of actions across applications.

Custom role-based privileges

To ensure administrators only have access to the controls needed, the whole SaaSOps platform should be controlled by custom roles and privileges. These roles can be configured by integrations, data objects, controls, and access to configurations. These permissions are then enabled and enforced through the UI, which means IT never has to give out excessive permissions to administrators in the native applications.

Custom integration connections

The number of SaaS applications are growing at an exponential rate in terms of both the number of applications and the number of users interacting with those applications. In order to create a central SaaSOps platform, IT needs to be able to extend the platform by connecting it to any SaaS application that exposes its own API. This should be flexible in a way where teams can build the actions and alert types that match their needs within these applications.

People & Processes

SaaSOps is not just technology, but a new practice within IT. SaaSOps professionals are in charge of training end users to get the most out of SaaS applications and optimize their productivity. In instances where their organization is not already on SaaS, they are the leaders in preparing and supporting their orgs for a successful transition to SaaS.

As part of purchasing a technical product for SaaSOps, you need to ensure your team and processes are aligned with this new way of operating. The People and Processes discipline of SaaSOps contains 5 key elements to help with organizing your team to create a full SaaSOps practice:

- **Team Structure** - How is your team structured? What is the right way to structure your team around a SaaS environment? SaaS is too interconnected to separate your team by application or function. You have to rethink how your team is structured to support your environment and employees.

- **Team Skills** - IT is no longer maintaining servers, troubleshooting data centers, and adding storage. Now you have to think about integrating applications and training users. These are new skills and teams need to have the skills to support a SaaS environment.

- **End User Training** - IT is responsible for supporting users in this new world. Do you create a help desk for self-service or only offer support through Slack or a ticketing

system? SaaSOps professionals have to understand their users enough to know the best way to communicate with employees and provide service where they need it.

- **Change Management** - This is a huge problem when it comes to SaaS applications because users and administrators have access to potentially dangerous collaboration features. SaaS applications are pushing out thousands of releases a year, how do you make sure users and administrators know how to use and secure SaaS applications as they are constantly changing?

Enter BetterCloud

SaaS adoption is one of the fastest growing and complex challenges IT has had to manage. SaaS applications also contain all of an organization's most valuable and sensitive information, making it even more critical for IT to properly manage and secure them.

Bettercloud is the leading SaaSOps platform that enables IT professionals to efficiently identify, manage, and secure all of their SaaS applications so they can effectively support a "best-in-breed" strategy inside their organization. BetterCloud makes the best better.

With a library of APIs to ingest data, a suite of SaaS actions and alerts, and a robust workflow engine to apply management and security policies, BetterCloud is a flexible platform that scales as your digital workplace grows and evolves. BetterCloud improves IT's:

- Visibility through a central dashboard to view users, groups, files, and setting across SaaS applications
- Efficiency by saving time on common tasks with centralized administration so you can focus on what's most important
- Control to keep employees productive while still maintaining the necessary security posture for your business
- Extensibility to leverage these platform capabilities to your current and future digital workplace

BetterCloud as your SaaSOps Solution

BetterCloud is the only provider to meet the new criteria for today's SaaSOps platform, managing and securing the many SaaS applications employees use to perform their daily jobs.

BetterCloud ingests and normalizes users, groups, and data across SaaS applications to consolidate the administration of applications into a single, easy-to-use platform. These dashboards shed light on all of the digital assets and users across applications and help IT understand the interactions taking place between them.

BetterCloud is the first SaaSOps platform to be granted a patent for our unique approach to creating rich relationships between the data across all of an organization's SaaS applications. This technology allows the combination of activity feeds from SaaS applications to provide a new level of operational intelligence. BetterCloud leverages this technology to give IT meaningful insights and dynamically enforce real-time policies on their users

What makes BetterCloud work as a SaaSOps solution:

- BetterCloud can adapt to any size best-in-breed environment, whether an organization is just starting out with GSuite or has hundreds of applications used by employees every day
- Get visibility and deep insights into SaaS users, groups, and files in order to manage and secure applications without disrupting employees
- Support the full range of SaaSOps use cases - including day-to-day management, identifying suspicious behavior, remediating threats, automating routine processes, and assisting with regulatory compliance
- Hundreds of out-of-the-box templates for alerts and automated workflows to make adoption quick and easy
- Detect known areas of concerns and eliminate insider threat blind spots

and data across all of their SaaS applications.

The platform makes it possible for organizations to discover, monitor, and report on threats, attacks, and other abnormal activity from across SaaS applications with business context. With this level of granular alerting, customers realize accelerated threat detection and rapid incident response across the entire security ecosystem.

All of this information is layered into a robust workflow engine that actively identifies configuration changes and suspicious user behavior, and automates the necessary actions to continue a routine process (such as onboarding/offboarding) or resolve the security threat. With a central repository of over 300 administrator actions designed for day-to-day SaaS management, IT has access to the tools they need to manage and secure applications on a one-off and automated basis.

The BetterCloud ROI story

SaaSOps Platforms have a very strong and compelling efficiency, cost savings and risk reduction ROI. Let's first consider efficiency and cost savings ROI. Start by looking at the number of employees joining your company annually, leaving your company annually and changing roles during the year.

Then consider your costs for IT to administer this. Every task or workflow (series of steps) has an associated cost. This cost is often averaged across any given business, but IT leaders know, not all tasks are created equally. Some are very complex and take hours, whereas some are as simple as clicking a few buttons. In fact, in many cases one task executed manually can be repeated time and time again due to mistakes or incomplete steps while executing the original request. When implementing a SaaSOps platform, most companies strengthen and improve their processes.

ROI Calculations:

1. Automating Manual Processes (IT labor hours)

Each time a user is onboarded, offboarded, changes roles or a group is created or membership changed there is a cost associated with that activity. With BetterCloud those tasks can be automated.

To translate this automation into cost (or value delivered) we use a fixed plus variable costing model. We do this for every series of actions or tasks that we are now automating with BetterCloud's workflows. Every workflow (or series of steps) has a fixed cost (think about it like a ticket price) and then a variable cost for each action taken (cost per action)

> ***Example #1:*** Onboarding - In a perfect world, every person who joins the organization has access to all applications necessary to be productive day one. The reality is that usually there is a slow and steady stream of access granted over time, with ticket after ticket after ticket submitted. With a SaaSOps platform, not only account provisioning, but the granular administration of onboarding (like putting people into groups, channels and setting permissions) can be automated and immediate. In fact with the "wait for approval" steps, access can be branched, controlled and granted based on various permission gates all while being editable and capable of iternation when any part of the tech stack changes.

> ***Example #2:*** Automating Groups privacy settings and membership - Many companies will say that groups are owned by the owners and not by IT. However, many companies still have IT manage key groups like company wide ones, office or location groups and some of the additional larger, non-team type of groups. In addition, most IT departments create a group and then turn it over to a group owner, so that they can manage the initial settings. With BetterCloud we can automate both the default settings when a group is initially created and memberships.

2. License Reclamation and Management

Assigning licenses in a timely and efficient manner is a continuous struggle in today's world of using best in breed applications. As the sprawl of SaaS applications grows more and more, ownership of license management comes into the IT departments' responsibility. With a SaaSOps platform, license management can become automated and consistent with that ability to manage the true lifecycle of an account after a user has left an organization.

Usage monitoring and inactivity reporting is another key part of managing SaaS spend. Having the ability to audit who is using which applications allows for a verification step to run independently from offboarding to ensure all licenses are allocated correctly and additional resources are not being spent purchasing additional, unneeded licenses.

3. Risk Reduction

Now let's consider risk reduction around data protection, governance, and compliance ROI. Practically each and every user within your organization's SaaS applications has access to various types of data. Whether that data lives within the files they own, groups they belong to, emails they can access, calendars they are a part of, or elsewhere, it is paramount to have the ability to identify information, audit the information, and then take action upon your findings in both a one-off and automated fashion.

With a SaaSOps platform, companies have the ability to maintain a full grasp over their SaaS data and see value by reducing the time spent identifying risks, reducing time spent containing risks, and ultimately decreasing the likelihood of future risks to your data occurring.

Here are a number of threat areas for consideration:

- Sarbanes-Oxley compliance
- Super admin sprawl
- Privacy policy violations

- Users without multi-factor authentication enabled
- Email being automatically forwarded to personal email addresses
- No visibility to documents shared publicly containing PII
- No visibility to leavers that still have access to sensitive data
- No visibility to misconfigured group settings
- No visibility to calendars exposed publicly
- No visibility to files titled “Password”
- No visibility to files shared with personal email addresses or competitor email addresses

Example #1: File Security - Many native admin consoles do not provide the ability for an administrator to see all of their files in a single place. This issue compounds when a company is using several SaaS applications that store files. A SaaSOps platform is needed to understand who has access to which files, which files contain sensitive information, which files are over-exposed, and much more.

Without a SaaSOps platform in place, there is an abundance of ambiguity around your file exposure, which in turn leads to large scale risks if an issue occurs. What’s the value of finding a configuration that makes data public on the internet? DivvyCloud estimates that cloud misconfigurations cost companies nearly $5 trillion over the last two years.

Example #2: Offboarding - For offboarding, we recommend 24 steps for G Suite alone. When companies have even more SaaS applications, that number grows exponentially. Most companies without BetterCloud might think they do not need that many, or that simply suspending or deleting a user may be enough, but there

are some critical questions that highlight some very real security concerns with offboarding users in a timely, efficient fashion, including:

- How are files accessed after the employee leaves the company?
- Did the employee have email forwarding setup to their personal email account?
- Who gains access to the employees inbox or files for the purposes of business continuity?
- How is the license managed if the account goes into a legal hold, or needs approval before unassigning a license?

There are often steps happening outside of what teams currently consider to be their “offboarding” process. There is the immediate return on investment (ROI) of not being breached and proactively protecting your organization from both malicious and innocent actors.

In summary, from automating manual processes to free up IT teams’ time to focus on more strategic projects, to providing a one stop shop for license allocation and management to providing a more secure, collaborative data and file exposure posture, there is a very strong and compelling ROI for a SaaSOps Platform. Work with a BetterCloud SaaSOps expert to develop the ROI specific to your company.

Don’t take our word for it though - the best way to understand the real ROI of a SaaSOps solution is to hear from those who already have one. To learn more from adopters of SaaSOps, check out BetterCloud’s SaaSOps Stars Volume 1.

The Future of SaaSOps

Not all SaaSOps platforms are created equal as this buyers guide highlights. And this is best shown by understanding the differences between adjacent products and SaaSOps products.

It is these SaaSOps platforms that present the brightest light for the future of the market. These modern solutions are great for providing visibility into SaaS applications, automating manual tasks, detecting threats detection, and remediating threats, all while delivering a demonstrable ROI.

As the modern SaaS landscape continues to evolve, SaaSOps solutions have proven they are able to adapt and stay ahead of the market to deliver a tool that will provide value today and in the future.