BetterCloud

SaaS Data Security Report 2021

Top Risks in File Security

The new importance of SaaS file security

In 2020, remote work became widespread, speeding digital transformation and SaaS adoption. Along with this rapid realignment came new SaaS file security requirements and user collaboration needs, as well as challenges for organizations of all kinds.

Some organizations rose to the challenge, while others are still striving. When it comes to SaaS file security, you can't secure what you can't see. So for organizations looking for the starting point: it's visibility into the entire SaaS environment. This includes all users, all files, and all applications. Organizations with superior visibility are best poised to implement processes, policies, and automation to easily safeguard corporate data assets.

With the rise of SaaS, employees expect to collaborate and share files in order to do their jobs. Add remote work that is accelerating digital transformation—and it all means that file security has never been more important. As IT enables and empowers their organizations through the power of SaaS tools, they must also secure data in a way that maximizes user collaboration and productivity.

To understand SaaS file security today, we surveyed more than 500 IT and security professionals and examined internal BetterCloud data from thousands of organizations and users—all to understand top challenges, priorities, and the magnitude of data loss and sensitive information leakage.

Key takeaways on SaaS file security in 2021

Lack of visibility into SaaS data plagues IT: Nearly half of organizations say their top security concern is not knowing where sensitive data lives.

Well-meaning but negligent users are the biggest data loss risk: More than 70% of organizations say the biggest data loss risk is the well-meaning but negligent employee.

IT doesn't trust users with company data: Only 35% of respondents trust end users to responsibly share and store company data.

Securing user actions within SaaS apps is hard: Nearly half of respondents say they have difficulty securing users' activities within SaaS apps.

SaaS file security violations are out of control: This year, as the world reopened for business, file security violations have spiked 134%, and the types of violations are rampant throughout the organization.

Organizations don't invest enough in SaaS file security: Less than half say they invest enough.

Too few organizations invest in the technology best able to improve SaaS file security: When organizations do invest, about 64% invest in Security Information and Event Management (SIEM) tools, 40% in Cloud Access Security Brokers (CASBs), and 37% in SaaS management platforms (SMPs).

Organizations are rapidly adopting SMPs to solve SaaS file security challenges: 55% of organizations plan to use SMPs within the next 12 months.

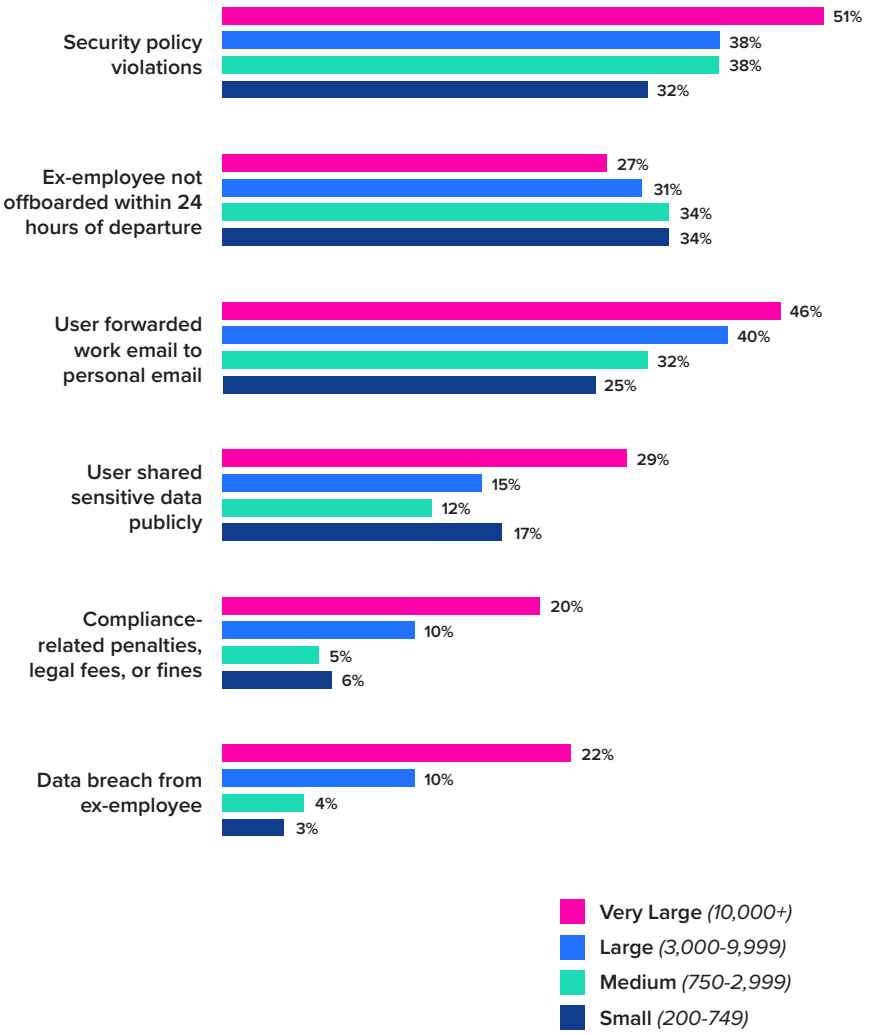
2020 shifted IT priorities more quickly than ever before. As users moved to home offices, security took center stage.

And for good reasons:

More than half of very large organizations reported security policy violations in the past 12 months. Nearly a third reported that users publicly shared sensitive data. Finally, 20% had compliance-related penalties, legal fees, or fines.

It all gives rise to the new importance of file security.

Security-related experiences over last 12 months



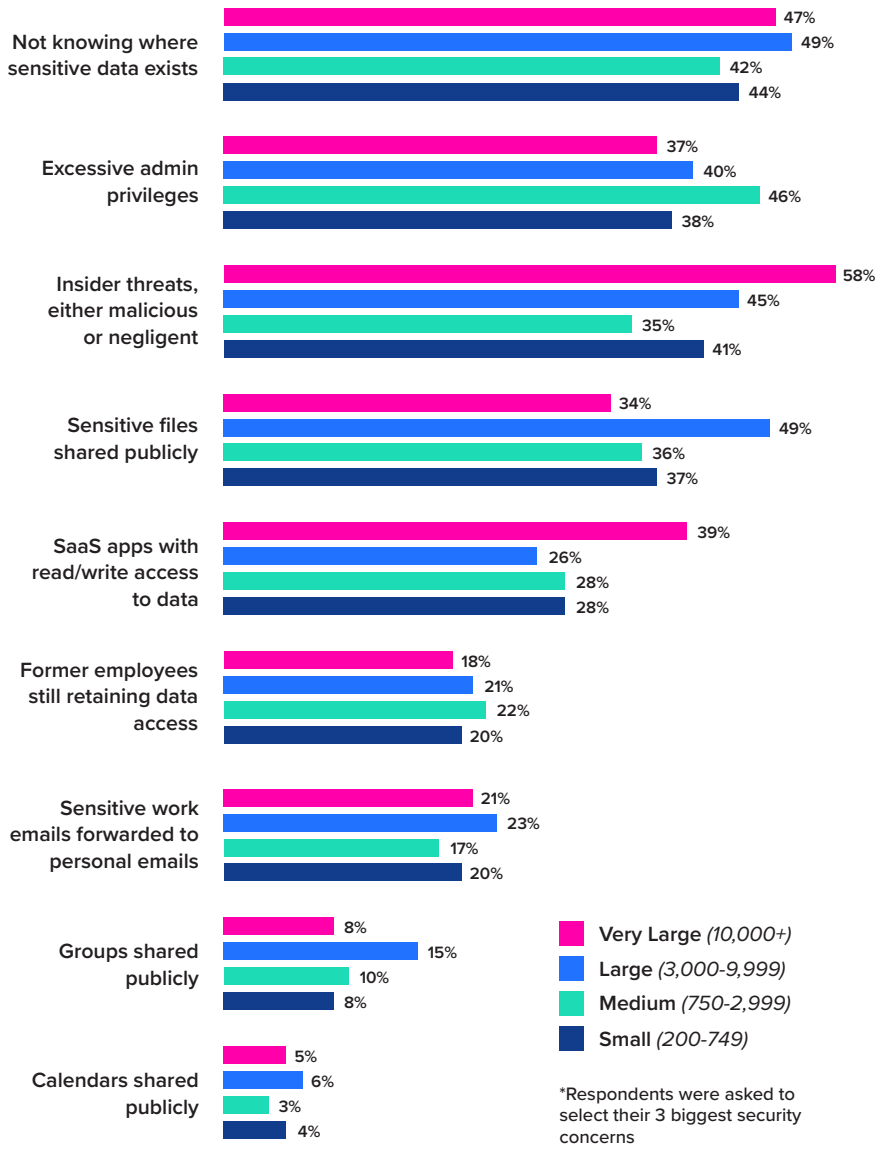
Security concerns mirror this reality.

At the top of the list?

Nearly half of respondents report that they're plagued by *not knowing where sensitive data exists* across their data sprawl.

Very large organizations, in particular, are concerned with insider threats. Meanwhile, large organizations are concerned about sensitive files being shared publicly.

Largest security concerns

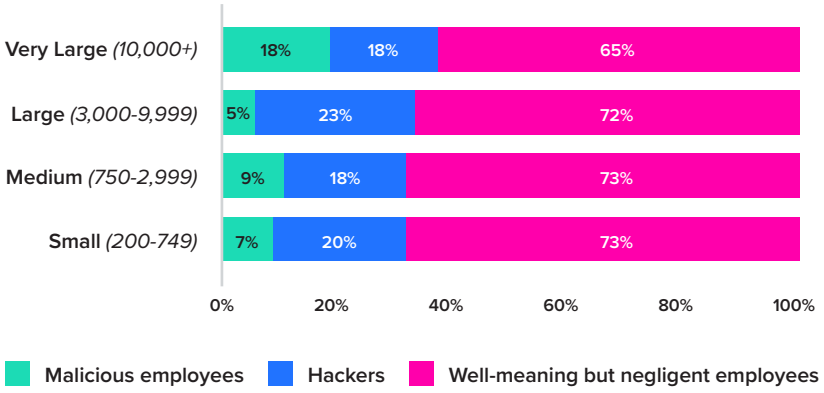


The biggest data loss risk is the well-meaning but negligent employee.

These employees have good intentions and are just trying to do their jobs, but often lack the training or knowledge to keep sensitive information safe.

Negligent employees are by far the biggest threat for organizations of all sizes. However, it's somewhat less of a concern for very large organizations, which likely trade productivity for security with the use of CASBs.

Actor posing greatest threat to data loss



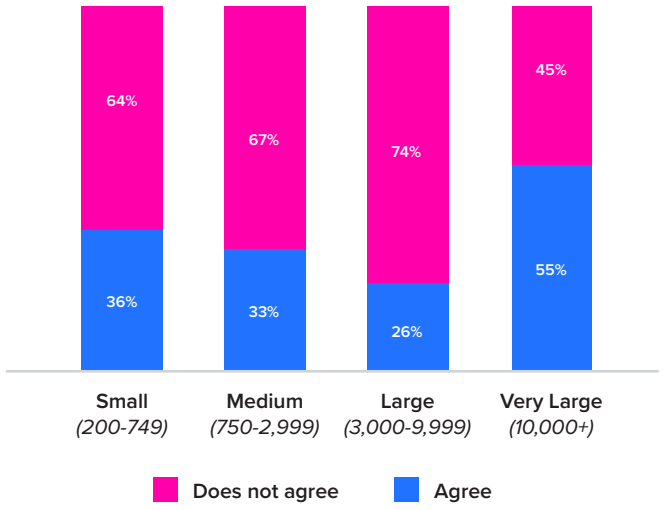
BetterCloud

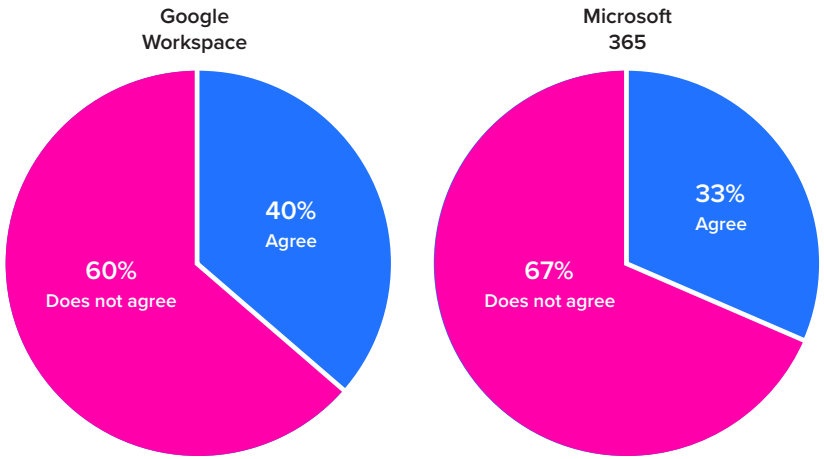
PRO TIP:

To help mitigate data loss from well-meaning but negligent employees, proactively monitor for:

- Sensitive files or folder paths (like accounting or finance) being publicly or externally shared
- Work emails being forwarded to personal email accounts
- 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)
- External domains to which files are shared
- External people with whom files are shared

Trusts end users to responsibly share and store company data





At the same time, IT trust in end users is low.

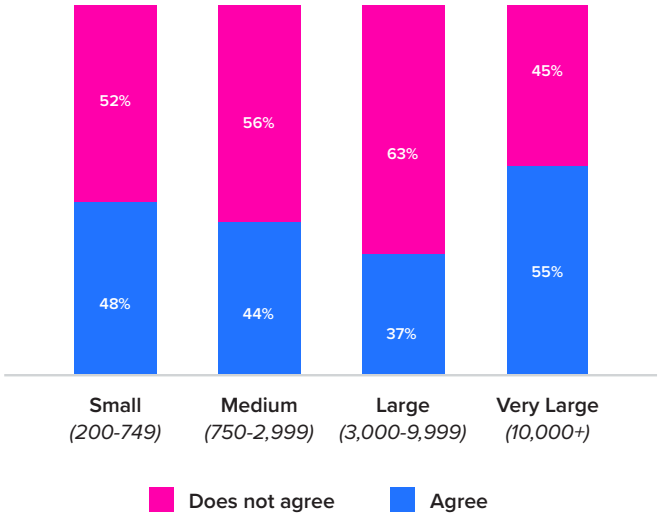
While more than half of very large organizations say they trust end users to responsibly share and store company data, only about a quarter of large organizations express trust in them.

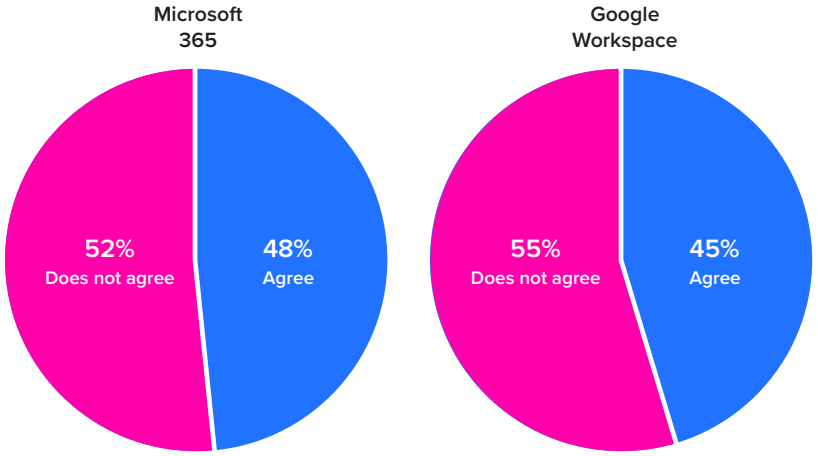
On the end user trust metric, Google Workspace users tend to have a higher level of trust than Microsoft 365-based organizations.

About half of respondents say they have difficulty securing users' activities—and that includes file sharing—*within* SaaS apps.

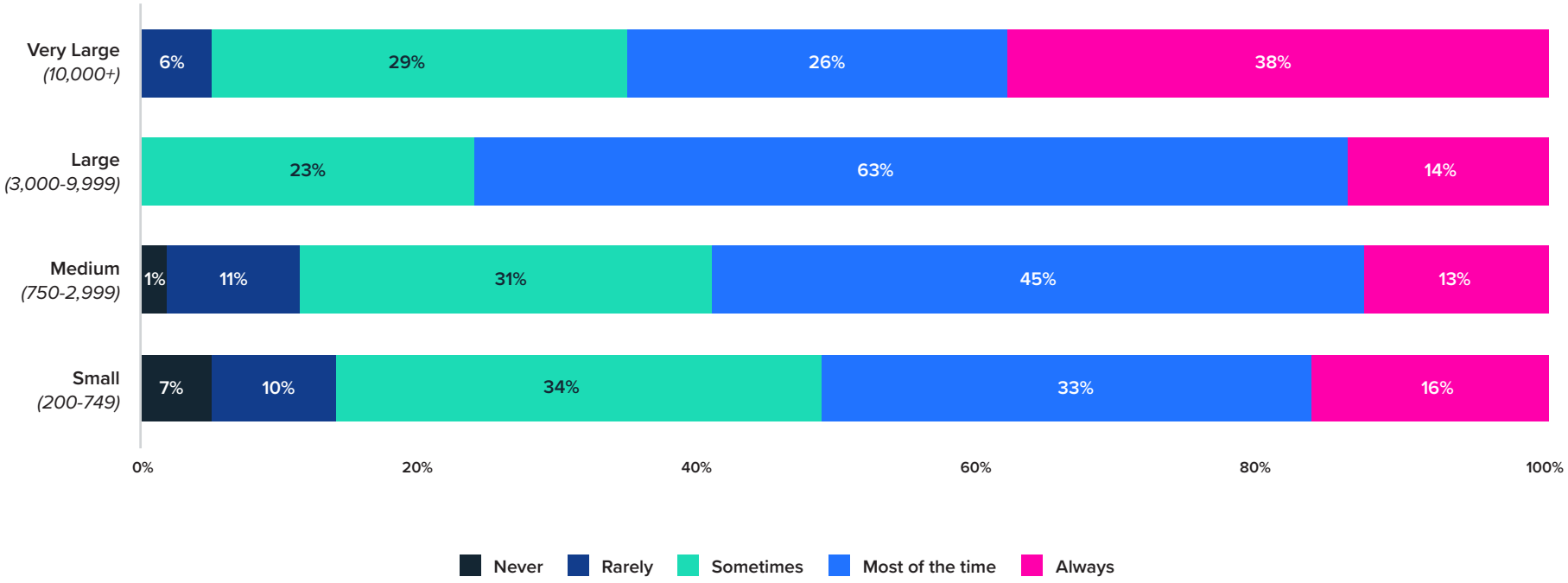
Organizations using Microsoft 365 are more likely to say they have difficulties than those that standardize on Google Workspace.

Has difficulties securing users' activities within SaaS apps





Frequency IT monitors to prevent public sharing of confidential data



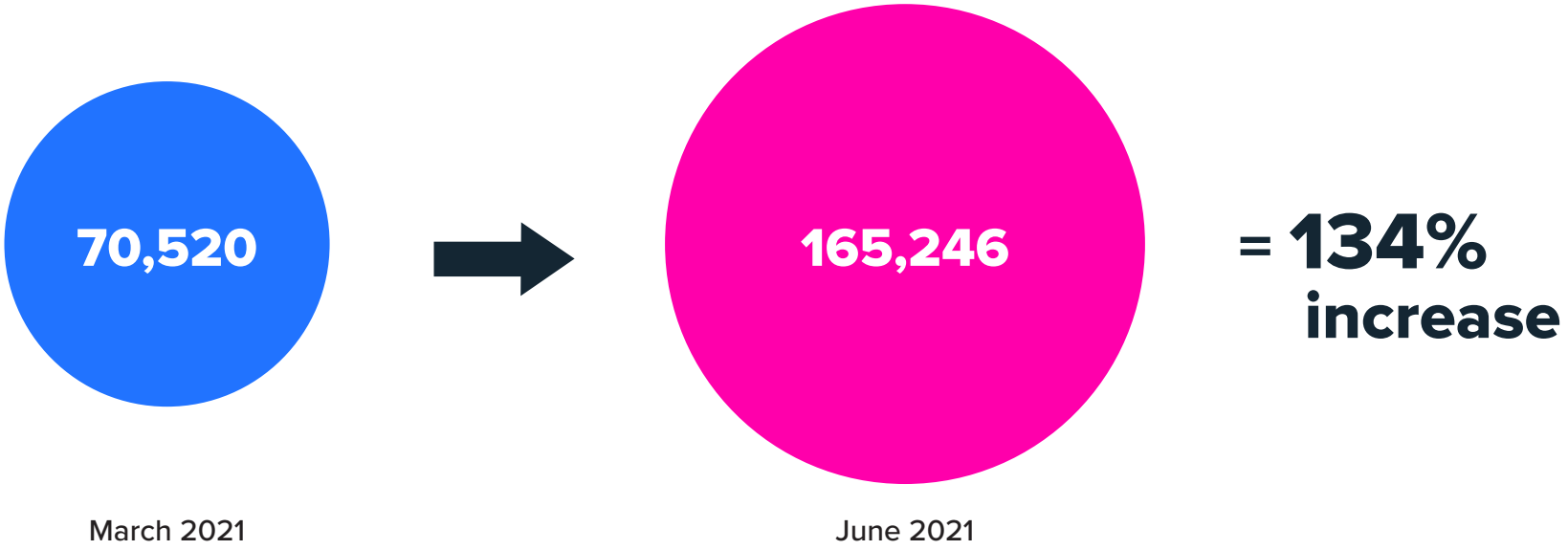
One way to address file security risk is to monitor for any public sharing of confidential data.

However, too many organizations fall into the “rarely” or “sometimes” camps.

Organizations don’t always monitor to prevent leakage of confidential data as much as they should.

FILE SECURITY RISK REALITY CHECK:

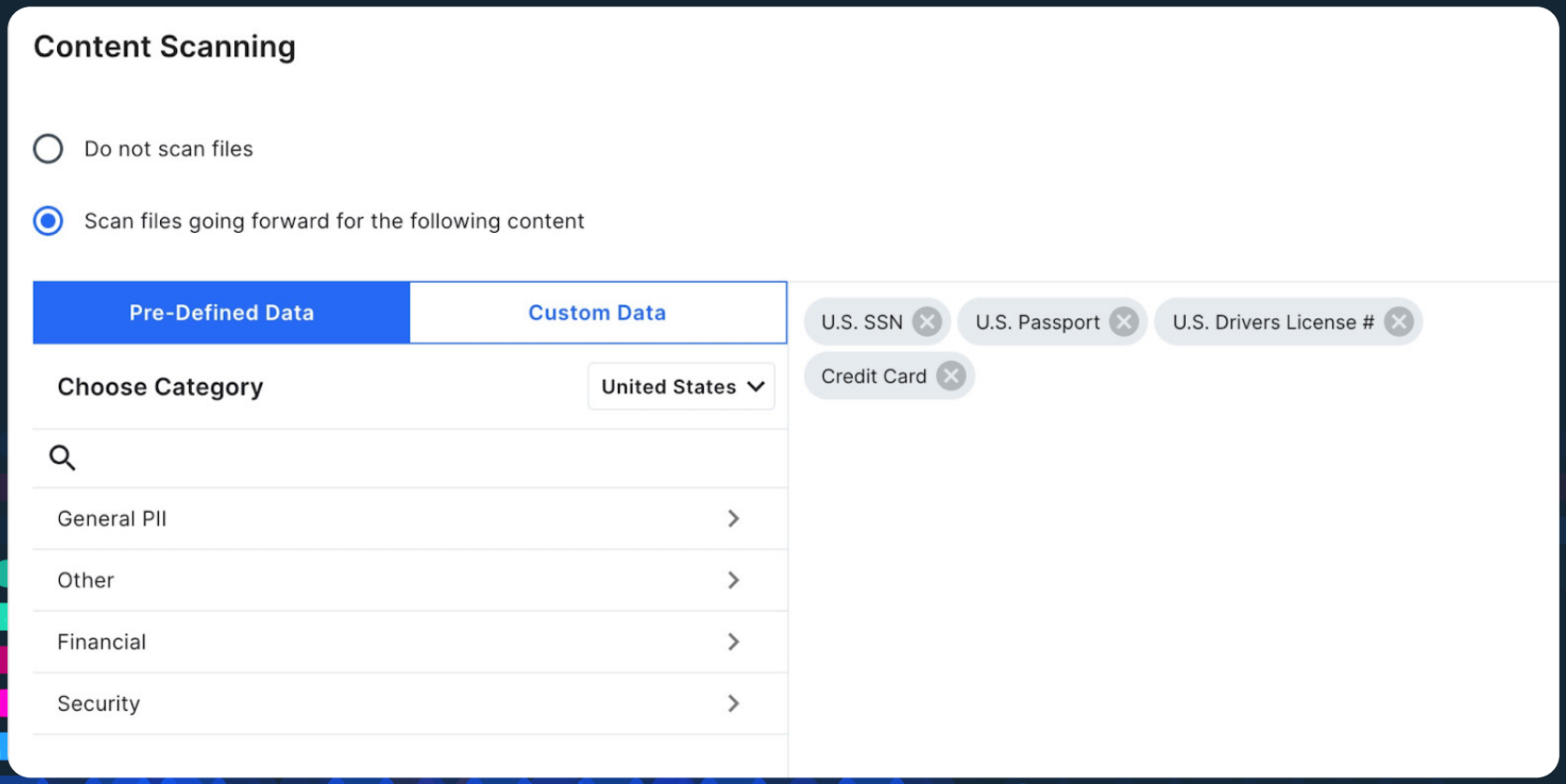
A dramatic rise in file security violations as the world re-opens for business



Source: Internal BetterCloud data, June 2021

PRO TIP:

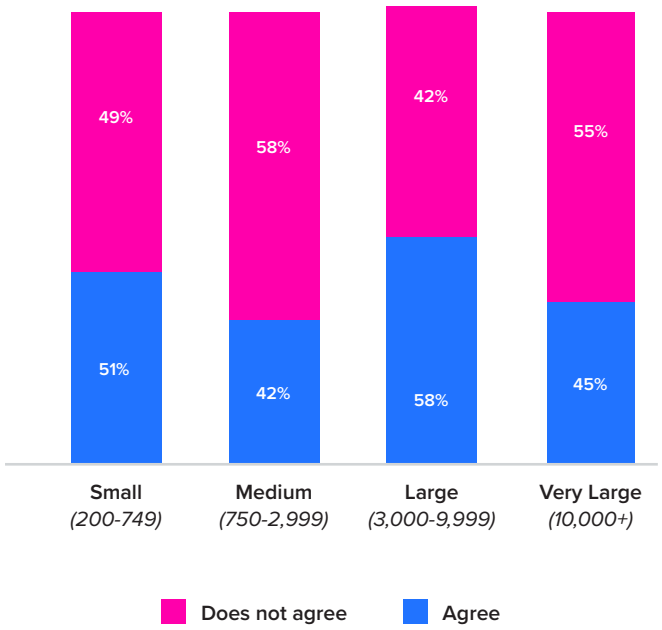
A SaaS management platform (SMP) can alert you if users share sensitive files publicly or externally, or if they create or upload files with sensitive data. IT teams can automatically remediate exposures and take action across applications when sensitive data is discovered.



About half of all organizations don't invest enough to protect data in SaaS apps.

Even though many very large organizations say they always monitor for confidential data leakage, more than half say they don't invest enough to protect data within SaaS applications.

Invests enough to protect data within our SaaS apps



BetterCloud

PRO TIP:

Data protection starts with getting full visibility. You can't protect data unless you know where sensitive information is stored.

There are two key areas to understand: **Which files contain sensitive information, and how are your users sharing them?** Once you have this visibility, the next step is remediation. By automatically remediating any exposures, you can reduce data loss risk and maintain compliance requirements in a scalable way.

FILE SECURITY RISK REALITY CHECK:

File security violations lurk throughout the average organization

Average number of public files	Small (200-749)	Medium (750-2,999)	Large (3,000-9,999)	Very Large (10,000+)
In cloud storage apps	**88,952**	**269,928**	**148,543**	**17,708**
In cloud productivity suites	**71,987**	**51,894**	**122,022**	**2,142,814**

Average number of files with sensitive data	Small (200-749)	Medium (750-2,999)	Large (3,000-9,999)	Very Large (10,000+)
With U.S. Social Security numbers, credit card numbers, or passwords	**102,685**	**52,304**	**191,564**	**464,163**
With general personally identifiable information	**49,978**	**29,659**	**98,388**	**128,368**

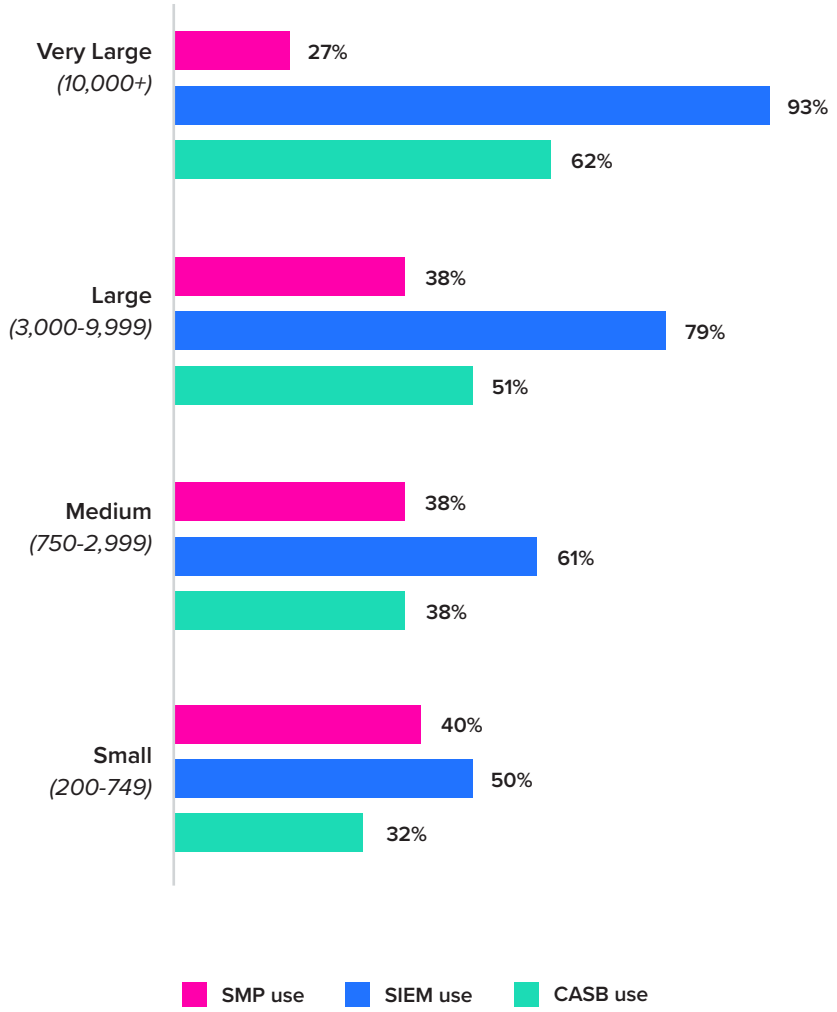
Source: Internal BetterCloud data, June 2021

It's well-known that users don't always pay close attention to sharing setting within your organization's SaaS applications.

If you're wondering just how common file exposures are, this table shows the average number of violations that occur for organizations like yours.

Even larger enterprises using CASBs can't completely control data leakage.

Technologies used to secure files



When organizations do invest to protect confidential information within SaaS apps, the majority tend to invest in the more established technologies.

For organizations of all sizes, the leading technology is Security Information and Event Management (SIEM) software. Next comes a CASB.

SaaS management platforms (SMPs)—which can identify and secure sensitive data across the SaaS stack—are only used by about a third of organizations.

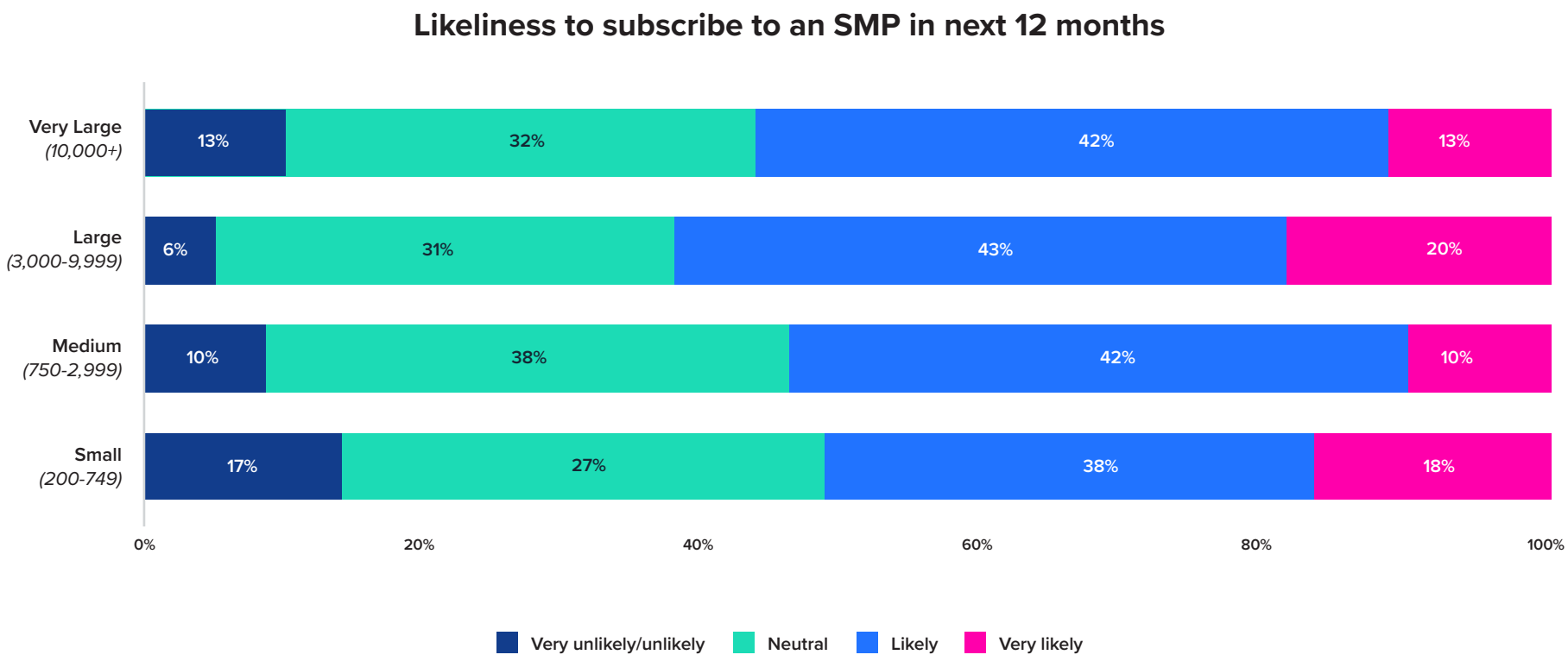
But that looks to change.

More than half **(55%)** of organizations expect to use an SMP in the next year, signaling a growing need to better discover, manage, and secure SaaS apps throughout the organization.

PRO TIP:

When training end users, make sure to include a section on SaaS sharing permissions.

When it comes SaaS apps, comprehensive user training can be an effective mitigation strategy. Training should describe individual sharing permissions in detail (e.g., viewer, editor, commenter) and link sharing options. The curriculum should also include a review of restrictions that can be enabled on the end user side, such as the ability to provide temporary access or prevent people from re-sharing or downloading certain files. This ensures that users know exactly what happens when they choose sharing settings, thereby reducing the risk of accidental data exposure.



It's not just small or medium-sized organizations either.

In fact, organizations of all sizes recognize the need to improve file security and intend to vote with their budgets.

Over the next year, about 63% of very large and large organizations expect to use an SMP.

Industry	% of Internal Files	% of External Files	% of Public Files
Banking, financial services, or insurance	90%	9%	1%
Consumer services	79%	20%	2%
Education - K12/higher ed	78%	15%	6%
Healthcare services	90%	8%	3%
Hotels, restaurants, or leisure	82%	14%	4%
Manufacturing	95%	5%	0.3%
Media	92%	8%	1%
Professional services	89%	9%	2%
Real estate	95%	4%	1%
Retail	91%	7%	2%
Software-as-a-Service (SaaS)	92%	6%	1%
Transportation	88%	7%	5%
Utilities	80%	17%	3%
Overall	**87%**	**11%**	**2%**

FILE SECURITY RISK REALITY CHECK:

File sharing settings vary by industry

Every industry and every company has different competitive imperatives for balancing security with collaboration, user empowerment, and productivity. They also have different security, privacy, and compliance requirements.

Therefore, the degree of public file sharing is driven by this mix.

Education, an industry that serves the public, has the highest percentage of public files. Contrast this with manufacturing, SaaS, and media with their intellectual property protection needs. And then with banking and real estate with their security requirements.

How does your organization compare?

Source: Internal BetterCloud data, June 2021

SaaS file security best practices that you can adopt right now

To achieve greater file security and minimize risk, follow these best practices.

Prevent risky application configurations by reviewing:

- Group privacy settings for exposed groups
- Calendar privacy settings for overexposed calendars
- File privacy settings for overexposed files
- Automatic email forwarding settings

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

Regularly scan 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

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
- Instilling a culture of security
- Investing in end user training

About this report

The SaaS *Data Security Report 2021: Top Risks in File Security* summarizes findings of a SaaS operations survey of 523 organizations with at least 200 users. Our representative sample includes a range of industries and sizes. The sample also includes responses from both IT and security professionals.

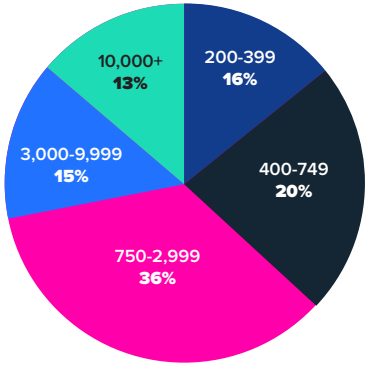
In addition, we analyzed file security violations across BetterCloud users. This analysis includes data from nearly 2,000 organizations with more than 200 users covering millions of users and files across hundreds of SaaS apps. The data comes from BetterCloud's automated scanning with 90+ pre-built data identifiers to find the most common sensitive data types for 25+ different countries. This includes personally identifiable information (PII) like U.S. Social Security numbers, words and phrases that violate HIPAA compliance, profanity, and financial information.

To identify where sensitive data lives across SaaS providers, BetterCloud can perform continual content scans and automate workflows to remediate its oversharing—all to control sensitive data sprawled across the ever-expanding SaaS environment without impairing user collaboration or productivity.

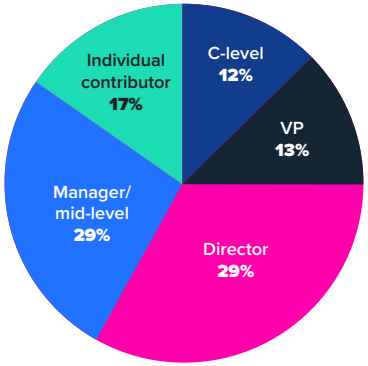
Corporate demographics

N=523, survey data collected from May 3rd to May 28th, 2021

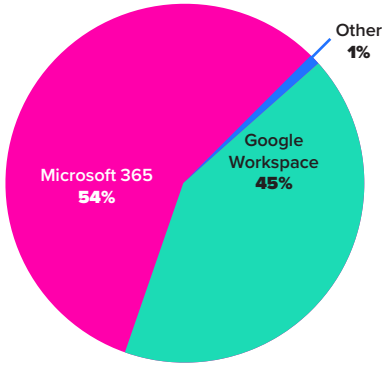
Company size



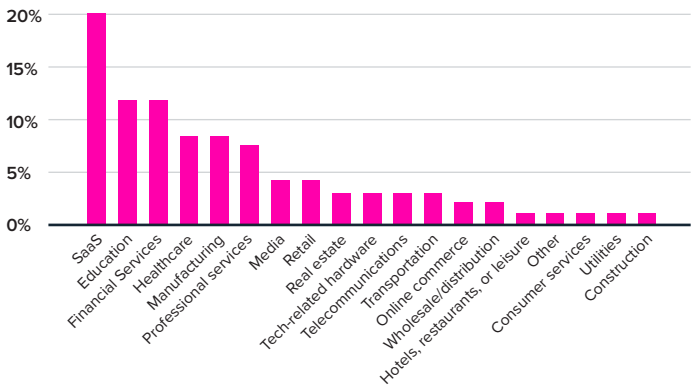
Job level



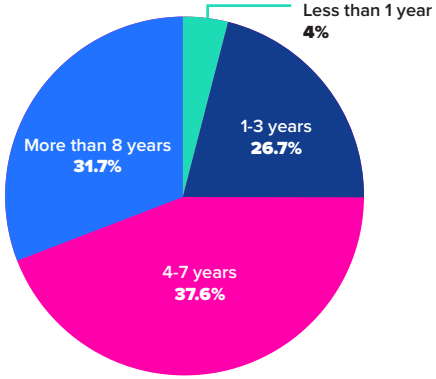
Primary cloud suite



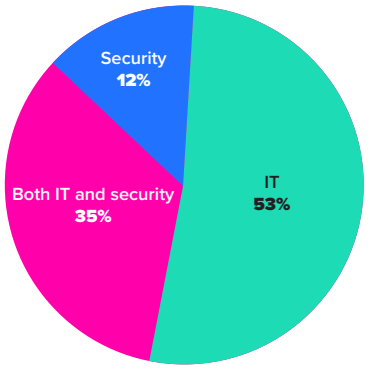
Industry



Length of time using SaaS



Department (IT vs. security)



About BetterCloud

BetterCloud is the leading SaaS management platform (SMP) that enables IT professionals to discover, manage, and secure the growing stack of SaaS applications in the digital workplace. With an expanding ecosystem of SaaS integrations, thousands of forward-thinking organizations like Walmart, Oscar Health, and Square now rely on BetterCloud to automate processes and policies across their cloud application portfolio.

Want to learn more about how BetterCloud can help you discover, manage, and secure your SaaS environment? Schedule a demo.