



2022 ThreatLabz Data Loss Report

Trends and risks of enterprise data
sharing and how to manage them

APP

ThreatLabz Report



Contents

Executive Summary	3
Key Findings	4
The Two Faces of Data Loss	5
Malicious data theft	6
Collaboration data loss	9
Where sensitive data lives	9
Are your files open to the public?	10
Data Policy Violations	12
What sensitive data is leaving the organization	12
How sensitive data is leaving	13
Email Data Sharing Trends	14
Most emailed file types	15
Data Threat Predictions	16
10 Best Practices for Data Protection	17
How the Zscaler Zero Trust Exchange secures sensitive data	20

Executive Summary

Data is the lifeblood of today's digital organizations. One of the biggest challenges organizations face is how to allow users to exchange data freely while keeping it from falling into the wrong hands. Nowhere is the tension between security and productivity more pronounced than when it comes to data sharing.

A recent Zscaler ThreatLabz analysis of the Zscaler security cloud validates how challenging this is:

organizations are experiencing an average of 10,000 data policy violations every single day.

A data loss event may involve an employee emailing a sensitive file, transferring it to a risky cloud location, copying it to an external drive, or making it publicly accessible via a collaboration tool. Data loss can also occur when a threat actor exfiltrates data for malicious purposes, such as in emerging multi-extortion ransomware attacks.

Whatever the nature of the data loss, any of these events can potentially lead to a data breach, where vital corporate data is stolen or accessed without permission. Breaches are occurring more frequently than ever before, incurring more harm and higher associated costs every year. During the past year, thousands of organizations suffered from breaches, including well-known entities like Apple, Uber, TikTok, Robinhood, and the San Francisco 49ers football team.

The IBM 2022 “Cost of a Data Breach Report” found that 83% of organizations suffered from multiple breaches in the past year, with an average cost of \$4.35 million. The Ponemon Institute found that the average cost is \$1 million higher for organizations that do not employ zero trust strategies. The financial impact of a breach comes in a variety of forms, from lost business to regulatory fines, mitigation costs, and more.

Security leaders are aware that they need to implement more effective controls around where data is stored, how it is shared, and who has the right to access it. But this is easier said than done. Too much restrictive control in the name of security can stifle user productivity, collaboration, and, ultimately, creativity and innovation. And when security becomes a barrier to productivity, users tend to find their way around it, often taking even riskier actions. So how can businesses find the right balance?

The basis of this report is the Zscaler ThreatLabz research team's analysis of nearly 6 billion data loss policy violations from November 2021 through July 2022. We'll look at what and how enterprise data is being shared, where it's going, which malicious actors are targeting it, and how you can improve your data-sharing hygiene so as to mitigate risk without stifling productivity.

Key Findings



Organizations experience an average of **10,000 data policy violations every day**.



36% of cloud app data is shared with publicly accessible links. This averages out to over 360 files per organization per day.



More than half of ransomware attacks now include data exfiltration. This is so profitable that some groups now skip the malware component altogether.



Personal identifiable information (PII), such as names and government identifiers, **account for over 84% of data-sharing violations.** Financial and credit card information accounts for another 10%.



Almost 8.4% of sensitive data that is emailed is found in images that can only be restricted using advanced inspection techniques like OCR or AI.

Key Terminology

Cloud access security broker (CASB): A visibility and control point that secures cloud applications to prevent sensitive data leakage and provide threat protection, shadow IT discovery, and regulatory compliance.

Data loss prevention (DLP): A set of defined policies, best practices, and technology solutions designed to detect and protect sensitive data from misuse and exfiltration.

Data leak: Unauthorized exposure or transmission of sensitive data.

Digital attack surface: Publicly exposed pathways with information and interaction points that can be exploited by attackers to gain access to sensitive systems and data in an organization's environment.

Compliance: Regulatory mandates that impose security and data governance policy requirements on organizations within specific industries and regions. Examples: PCI, HIPAA, GDPR, and CCPA.

Data classification: Classification and categorization of data by content type to enforce protection. Examples: public, internal only, confidential, restricted, top secret, and other designations.

Security awareness training: Educating users how to identify and respond to potential threats. Examples: blocking social engineering attempts with verification, reporting possible phishing emails.

Intellectual property: Copyrights, trademarks, patents, source code, and trade secrets. Corporate data: Information necessary to conduct and operate a business.

Identity data: All personal information handled by an organization, including customer, employee, and affiliate records.

Personal identifiable information (PII): Information that can identify individuals, including Social Security Numbers, birthdates, medical history, phone numbers, addresses, credit card numbers, account numbers, and more.

The Two Faces of Data Loss

Data loss occurs both accidentally and maliciously. Accidental data loss accounts for more than half of data breaches: users share data with vendors, partners, colleagues, or customers using poor security hygiene. Focused on doing their jobs, they often don't realize that some information is sensitive or confidential.

Malicious data breaches are typically much more damaging. Insider threats or organized threat actors may exfiltrate large quantities of data and cause substantial damage to the company. This practice has become increasingly common

among ransomware threat families who use it as a secondary extortion tactic. Some malicious actors bypass malware attacks altogether and use data extortion as their primary tactic.

Identifying and preventing oversharing in the course of regular business operations requires a different set of tactics than just preventing sophisticated threat actors who are attempting to cause intentional damage. Protecting against data loss requires strategies that effectively protect against data loss in both scenarios.



Malicious data theft

Data theft is increasingly common and is growing year over year as data becomes more distributed (and therefore vulnerable) and seen as a profitable commodity.

ThreatLabz publishes analyses of malicious threats on an ongoing basis, including research on these common techniques for data exfiltration:

Ransomware attacks. Double-extortion ransomware attacks occur when a threat actor exfiltrates data in addition to using their traditional data encryption tactics. These now account for the majority of ransomware attacks. The “2022 ThreatLabz State of Ransomware Report” points out that [double-extortion attacks have risen 117% year-over-year](#), driven by an increasingly popular Ransomware-as-a-service model that was in use by eight of the top eleven ransomware families in the last

Percent change in double extortion attacks: 2021 vs 2020

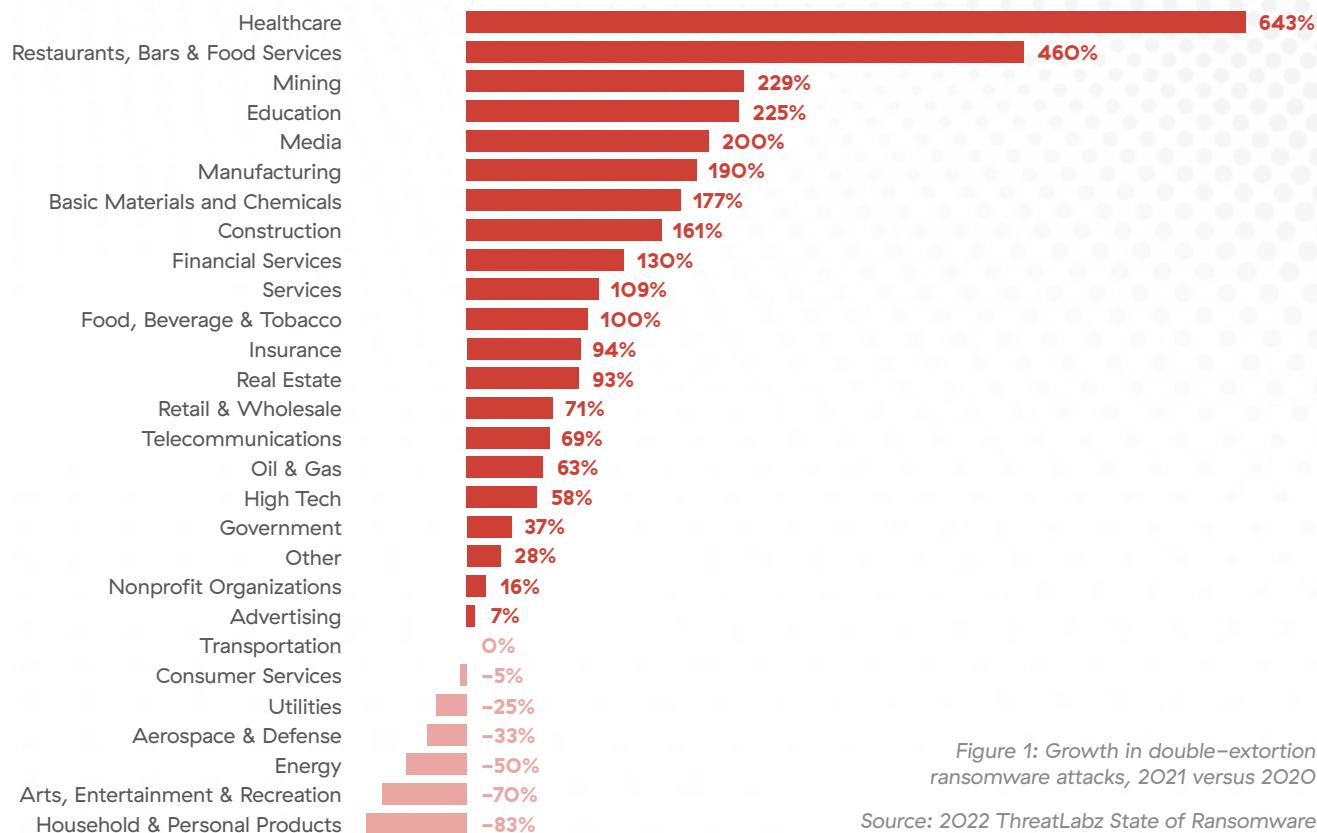


Figure 1: Growth in double-extortion ransomware attacks, 2021 versus 2020

Source: 2022 ThreatLabz State of Ransomware

year. This rate of data extortion has increased even faster in some industries. Healthcare has seen a massive 643% increase in double-extortion attacks, while education has seen a 225% increase.

Some ransomware families are skipping the malware component of their attacks and are focusing solely on data extortion. In 2022, ransomware group Clop [stole and ransomed 5TB of data from a water utility company in the U.K.](#) Stealing

data rather than encrypting it makes the attacks easier to deploy and execute successfully. This method also attracts less attention from law enforcement, as the attacks are not disrupting critical operations.

Phishing attacks. In phishing attacks, threat actors use a range of techniques to trick users into giving them access to sensitive information. For years, phishing has been one of the most common tactics used to compromise organizations. ThreatLabz found the use of phishing [rose another 29% in 2021 compared to 2020](#). The most common objective of a phishing attack is credential theft (which can lead to data exfiltration as a later attack stage), but the next most common target is credit card information. This is particularly true in retail and wholesale organizations, which saw a 436% increase in phishing attacks in the last year as attackers took advantage of increased online shopping as a result of the pandemic.

Supply chain attacks. Threat actors typically target the weakest link, and often that's found in the supply chain. They know that organizations share information with partners and suppliers in the course of their business operations, and that those supply chain organizations are generally easier to compromise than their ultimate target. Supply chains can be exploited in multiple ways. For example, they frequently have

security vulnerabilities that attackers exploit to break into the target organization. This is demonstrated in high-profile attacks like the one perpetrated on [Okta by LAPSUS\\$](#) or the [Kaseya ransomware attack](#). Attackers also steal valuable information from the suppliers directly, as was the case when the ransomware group REvil attacked Quanta (a computer hardware manufacturer) and [stole blueprints for Apple MacBooks](#).

JavaScript-based skimmer attacks. A 2019 report from Symantec found that [over 4,800 websites per month](#) were being hit by formjacking attacks, where attackers insert malicious code into ecommerce payment portals to steal credit card numbers. [Magecart](#) and [FakeClicky](#) are two examples of skimmer groups who have wreaked havoc on ecommerce platforms for years. But this threat is not solely limited to ecommerce sites. Skimmer attacks come in other forms as well, including such as session hijacking. This is an age-old trick where attackers exploit vulnerabilities in network sessions, such as taking advantage of cookies being passed over HTTP to view or steal sensitive data, which can then be sold or ransomed.





Infostealers. Infostealers are a form of malware trojan that connects to a command-and-control server to send information from a compromised system. That information is then sold on the black market or used for extortion purposes. Infostealers continue to grow in popularity as they can be purchased relatively cheaply from thriving malware-as-a-service marketplaces and can be deployed by themselves or as the first stage of a more advanced attack.

Web scraping. Web scraping is typically a bot-aided activity where content is extracted from a website. This could be done for a number of reasons, some legal, some not, such as: making a copy of a website, taking stock or gambling information and converting it into a format that is easier to work with, and others. Attackers use these automated tools to

grab content from publicly available links or exposed applications and help themselves to sensitive data that they can use for malicious purposes.

... And others. Attackers are always coming up with new ways to compromise organizations and profit from their data. What makes it even more complicated is that disgruntled employees and other insiders already have access to data should they choose to do something malicious. Both external and internal attackers use legitimate storage providers as destinations for exfiltrated data. Having visibility and control over where sensitive data is going and how it is being used is a critical component of the defense-in-depth needed to stop malicious attacks, whether they're being waged from inside or outside the organization.

Collaboration data loss

Where sensitive data lives

Today's digital businesses are highly distributed: employees, applications, and data are everywhere. Information is shared across data centers in private and public clouds and with partners and third-party contractors. Access to information is critical for businesses productivity, and there is a wide array of tools that enable it.

But not all data is created equal. Some data must be closely monitored and diligently protected, whether it's critical to the operation of the organization, protected by regulations, or both. We refer to this as "sensitive data," and it includes PII, financial information, and source code.

Our study found that Microsoft OneDrive and Microsoft Exchange are massive repositories of such sensitive data, accounting for over 60% of the total number of sensitive files stored in cloud collaboration apps. IT and security teams must ensure that their organizations are in compliance with local and industry regulations around how that data is being stored and accessed while also maintaining zero trust access control policies, up-to-date patching, and correct configuration.

Along with sensitive data, cloud collaboration apps can also be a hotbed for malware, which can come from multiple sources. Across cloud collaboration apps, we found 1/20th of a percent (.05%) of files contained malware — a small but significant percentage of files with the potential to steal or manipulate the sensitive data housed alongside it.

Percentage of sensitive data in cloud collaboration apps

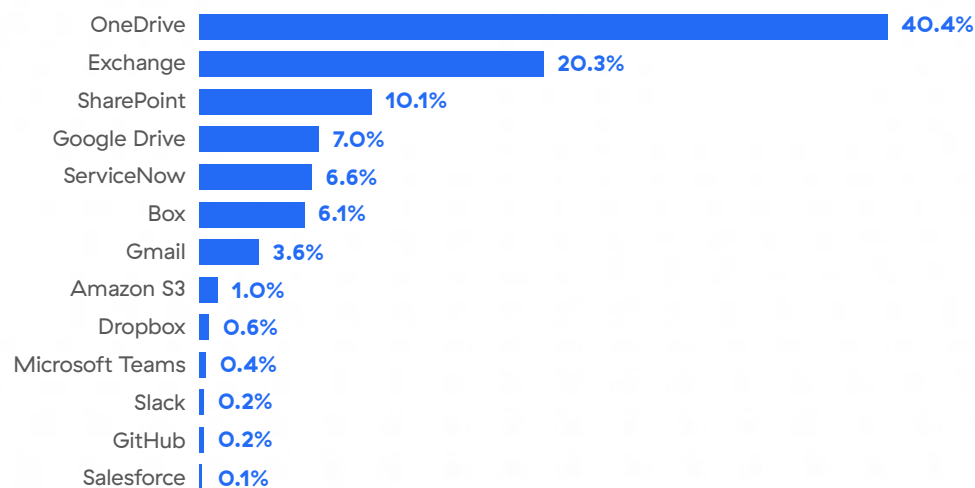



Figure 2: Percentage of sensitive data in cloud collaborations apps



Over half of all files in cloud apps are shared in risky ways, with 36% easily accessible by anyone with the link.

Are your files open to the public?

Employees frequently need to share data both within the company and outside of it with partners, vendors, and clients. Putting guardrails around who can access this data and how it can be handled is the key to mitigating risk. Neither internal nor external stakeholders should have unfettered access to your most sensitive files.

Administrators and employees alike must be particularly aware of their settings on collaboration apps, where the default on new links can be set to “publicly accessible.” These links don’t even require a breach for the data to be exposed. Better awareness about these settings is critical not only from a security standpoint, but also from a compliance standpoint, as some types of data are bound by data sovereignty and handling regulations that are not fulfilled by all cloud apps.

The corporate world has developed some risky collaboration habits, and cloud apps that are built for data sharing make it entirely too easy for employees to overshare. ThreatLabz found that half of all shares from cloud apps are sending data outside the organization, where IT and security administrators have the least amount of control.

More concerning is that 36% of shared files are set with open public links, which translates to an average of over 360 shares per company per day that could be discovered by malicious actors. This massive risk means that anyone who has access to the link can access the data with ease.

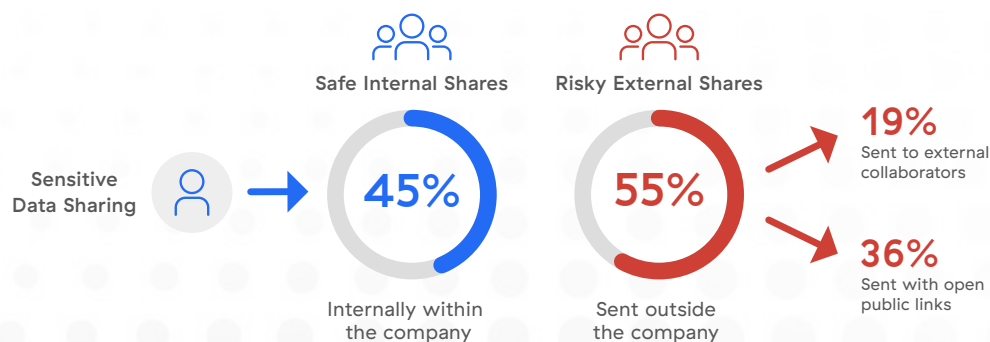


Figure 3: Percentage of files being shared with risky settings

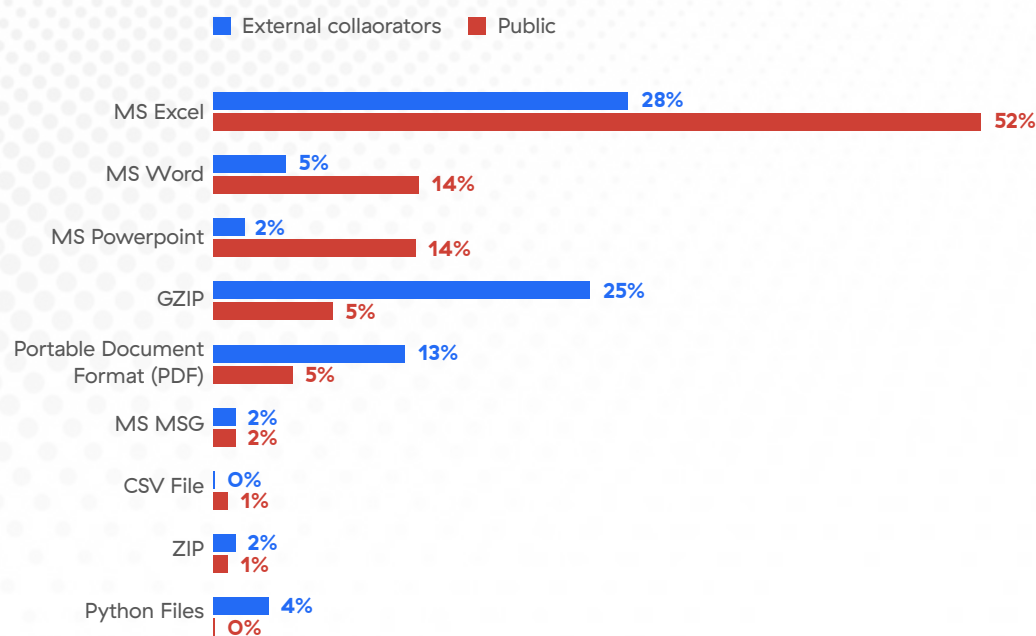


Figure 4: Top file types shared with external collaborators or open public links

One way to help improve your data protection hygiene is to understand what file types tend to contain this sensitive data. Understanding this can help improve data protection hygiene.

- GZIP, Excel, and PDFs are the most-shared file types among external collaborators. Source code files such as Python, C, and JavaScript also make the top 20 list of shared file types.
- Microsoft Office file types, including Excel, Word, and PowerPoint, are the most commonly shared file types to open public links, potentially exposing sensitive data to anyone with access to the URL that may be shared in an email, for example.

Understanding the human element behind data loss

From innocent mistakes by employees to complex attacks staged by malicious insiders and threat actors, data loss begins and ends with people. Here are the six key roles responsible for data loss:

Employees: Human errors and mistakes can lead to the loss of critical information. Examples: oversharing, opensharing, data deletion, and lost or compromised devices.

Administrators: Tasked with configuring system settings, applying patches, enforcing policies, and defining access permissions, administrators can make errors and unknowingly leave an organization exposed to data loss and vulnerable to attacks. Examples: missing fringe systems during patching for a major exploit like Log4j and not immediately applying security controls to new cloud containers and DevOps instances.

Malicious insiders: Employees may intentionally exfiltrate or tamper with important data or give third parties unauthorized access to information. Example: employees destroying and/or stealing data before leaving a role and insiders colluding with attackers or competitors for personal or financial gain.

Leadership: While this may seem like an unlikely source, leaders are tasked with allocating the budget to properly invest in security and critical infrastructure and may overlook important upgrades. Examples: the board denies an IT/security budget request to update vulnerable network architecture.

Affiliates: Supply chain vendors, partners, contractors, and other privileged parties with access to your data and systems can also inadvertently cause data loss. Examples: customer support contractors with access to customer data and systems may be compromised and cloud application vendors may be hit with breaches.

Adversaries: Threat actors target and steal data from organizations for personal gain using techniques and tools like phishing, ransomware, infostealers, scrapers, skimmers, and more. Examples: a ransomware gang that breaches an organization and exfiltrates data before encrypting files to increase the pressure on victims to pay.

Data Policy Violations

What sensitive data is leaving the organization

While the above data looks at oversharing in sanctioned applications, it is also very common for employees to send information out from sanctioned environments. These activities may include emailing a PDF to a partner, uploading a file to a personal Google Drive account, sending sensitive information to a colleague over Slack, or simply copying files to a USB drive. Data loss prevention (DLP) tools can help by scanning content and ensuring that sensitive data is only being shared in ways that adhere to security policies.

Zscaler DLP technology blocks an average of 10,000 DLP violations per day for each of our customers. Roughly half of these (51%) are custom policy violations, and the other half are out-of-the-box policies that we can analyze to better understand what employees are attempting to send.

PII is by far the most common data type being shared, accounting for 84% of out-of-the-box DLP policy violations. Government IDs make up 42%, including identifiers such as Social Security Numbers (U.S.), Aadhar numbers (India), Tax File Numbers (Australia), and Citizen Service Numbers (the Netherlands). Names of customers, employees, or prospects make up another 42% of data that is shared.

Financial information and credit card numbers are the next most popular data type being shared, accounting for over 10% of violations. Medical information accounts for 2.8% of violations across industries.

Source code typically maintains good hygiene, whether due to compliance or to a higher level of data security education and due diligence among developers when compared to other business users. Source code only accounted for 0.2% of all DLP policy violations.



On average, organizations are seeing about 10,000 data loss policy violations every day.

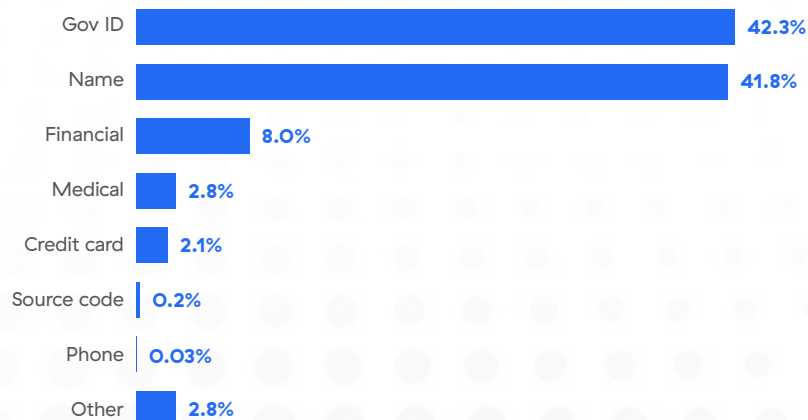


Figure 5: Percentage of DLP policy violations by data type. Excludes custom policies.

How sensitive data is leaving

In their nine-month study, ThreatLabz identified 1,956 different applications that generated DLP policy violations as a result of sharing restricted content. These apps accounted for a wide range of corporate and personal applications: enterprise storage, websites, email, health tracking, marketing automation, finance, insurance, collaboration, document management, entertainment, recruiting, and others.

NetApp, a popular data storage service, accounted for roughly 43% of violations—though the vast majority were violations of custom

policies, so it is unclear what specific data types are triggering the violations.

Amazon Web Services (AWS) accounted for another 10% of violations. Of all the apps in our study, AWS accounted for the highest percentage of credit card, financial, medical, source code, and SSN data policy violations, followed by three Google apps (Google Play, Google Drive, and Google Search) and then Box. As organizations retire on-premises applications for cloud workloads, reliance on AWS and other cloud storage services expands.

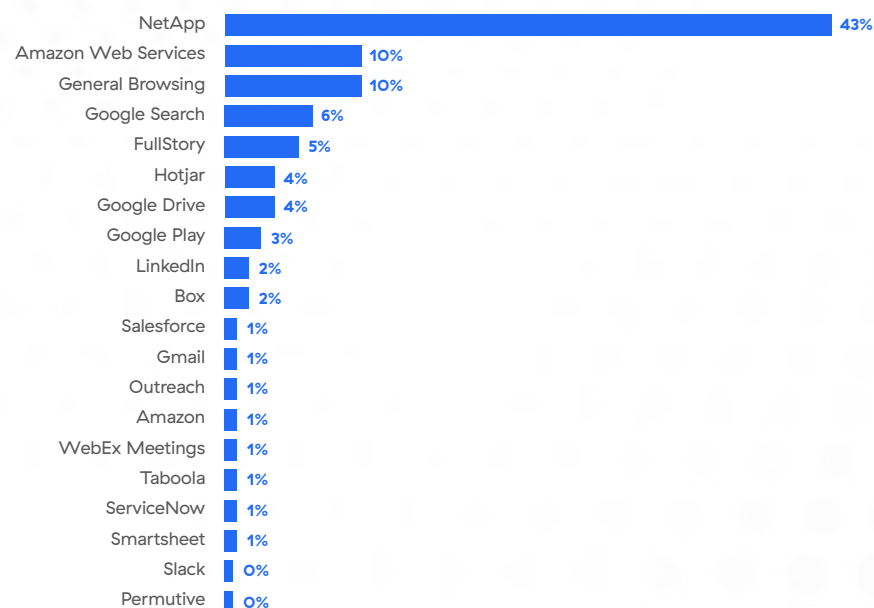


Figure 6: Total DLP violations by app

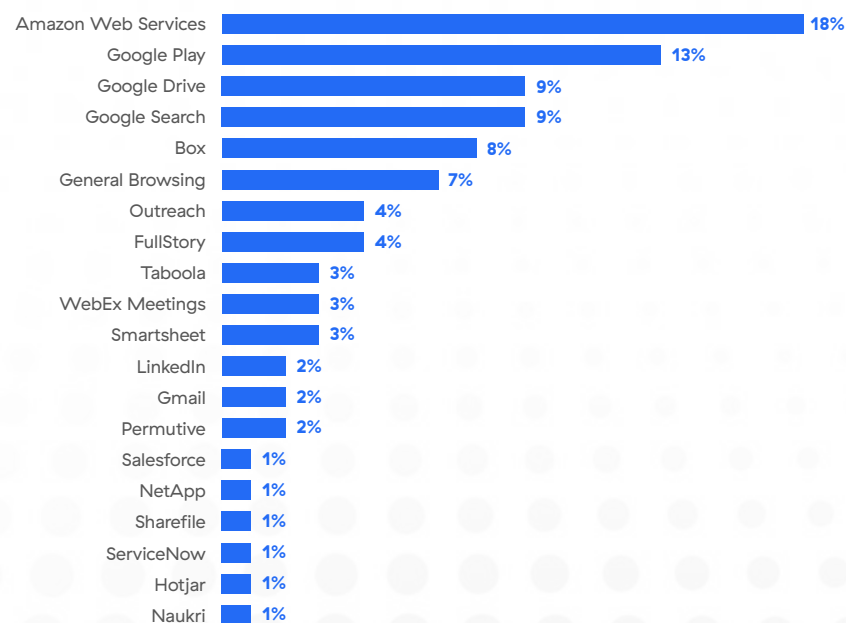


Figure 7: Top apps for credit card, financial, medical, source code, and Social Security Number DLP violations

Email Data-Sharing Trends

Email is one of the easiest and oldest channels for sharing sensitive data, especially for files under 25MB. Users attach and send out files to clients, partners, or even their own personal accounts, either out of convenience or as a way to side-step corporate security. Our study found that email accounts for about 7% of DLP violations.

The rate of data sharing by each email platform is more or less aligned to the market penetration of those email services as a whole. With nearly 2 billion users worldwide, Google Gmail is the most popular email platform for sending sensitive enterprise data, followed by Microsoft Outlook (both corporate and personal) and Yahoo Mail.

Many of the largest files are shared via Microsoft Outlook (part of Microsoft 365), which accounts for over 47% of the total volume of emailed data. Gmail automatically converts files over 25MB to Google Drive links, so the average file size that is emailed is much lower.

Security teams may have additional privacy concerns around email platforms that are hosted in surveillance states such as Russia and China. Mail.ru, Yandex Mail, and RamblerMail (Russia) and QQMail (China) each showed up on our list of webmail clients that are being used to facilitate sharing of data.

Almost 7% of DLP violations occur via email, which is a major risk to today's organizations. Enforcing DLP and tenancy restrictions is the best way to curb this loss.

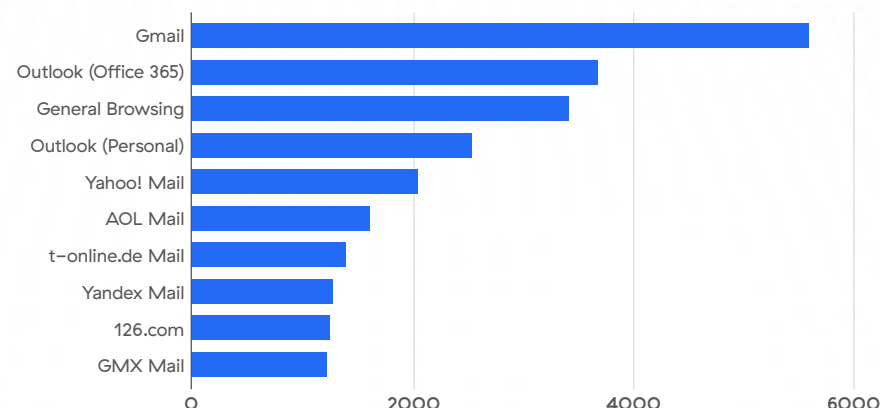


Figure 8: Count of files sent by various email platforms (showing top 10)

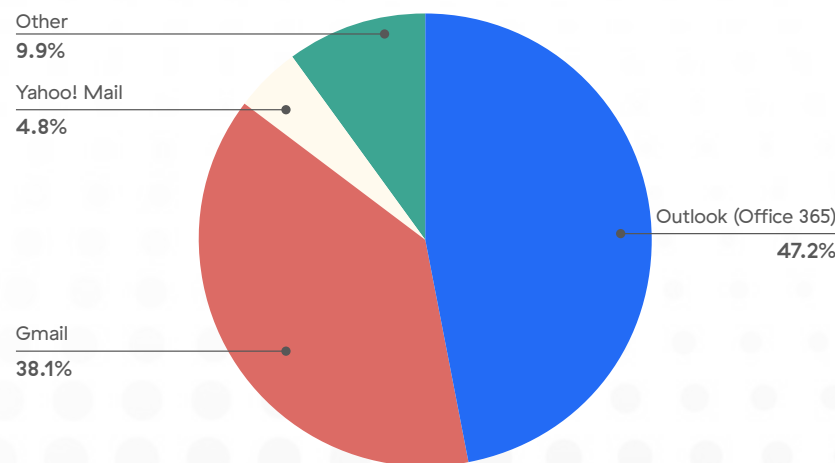


Figure 9: Percentage of data volume sent by various email applications



8.4% of data sent over email are images. Stopping sensitive data in this content requires advanced inspection techniques involving ML or OCR.

Most emailed file types

Our study found 336 different file types being emailed from November 2021 through July 2022. This included a large volume of Microsoft Office documents, image files, web files, and others:

- **12.6%** were Microsoft Office files, including Excel, Word, and PowerPoint.
- **8.4%** were image files (JPEG, GIF, PNG), which underscores the need for OCR DLP protection. Screenshots and other sensitive data can be easily lost by solutions that cannot analyze image content.
- **7.2%** were web files (HTML, CSS, JS).
- GZIP files, while under **4%** of the file count, made up **20.5%** of the volume of data lost, by far the highest single category.
- Text files made up **7.4%** of files lost.

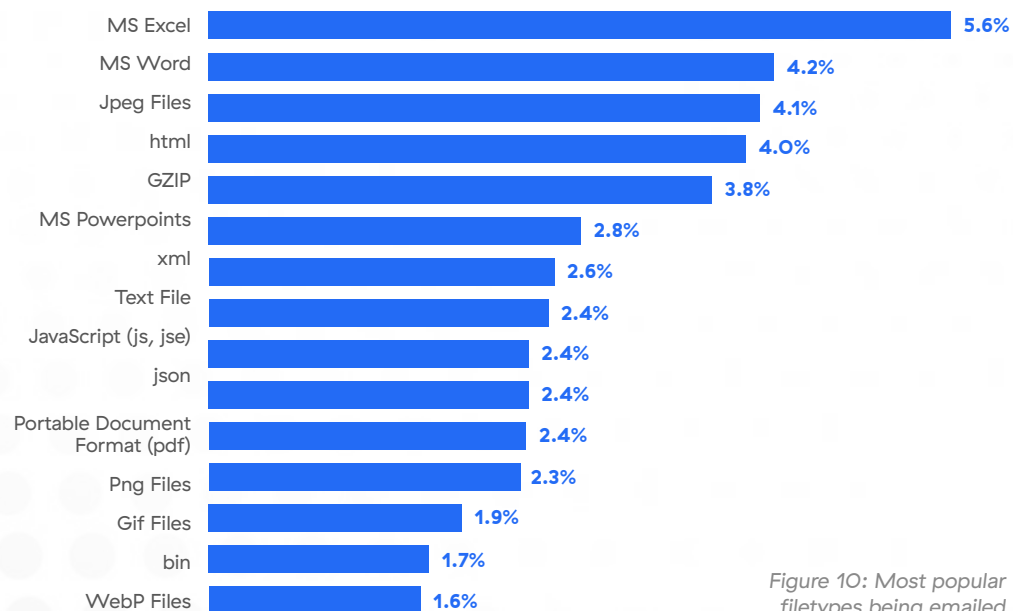


Figure 10: Most popular filetypes being emailed

Data Threat Predictions

Attackers continue to up their game, and the threats you face tomorrow will almost certainly be evolved versions of those you are facing today. In the coming year, we expect to see several threats continue that will impact requirements for data protection against malicious attacks:



New infostealers will look different than those of the past.

Free and premium malware builders have grown in popularity over the past several years and paved the way for novices to join the criminal underworld and ramp up quickly. However, several popular versions of infostealer builders have recently been exposed to contain hidden backdoors, designed by the builder's developers to undercut and profit from the fellow criminals they pretend to serve. We anticipate that sophisticated criminals with skills to do so will move away from purchasing these tainted builders from dark web marketplaces and will build their own never-before-seen infostealers, which will undoubtedly have their own creative twists.



Data extortion will continue to rise.

Some of the most popular ransomware families are moving away from data encryption and leaning toward data extortion. This emerging trend was born out of the success of the multi-extortion tactic that threatens to leak victims' data if they don't pay. Double-extortion ransomware schemes hit the threat scene in 2019 when data backup and recovery solutions became effective enough to thwart encryption-only ransomware attacks. Threat actors have since realized that just the process of encrypting and decrypting introduces more risk into the equation, with the potential for something to go amiss and prevent payout. For example, a large range of security tools can now detect and block ransomware early in the encryption phase of the attack. Adding to this problem, some victims have found the decryption key they paid for doesn't always work, and others have decided it would be faster and safer to recover from backup. We anticipate more ransomware families skipping encryption in favor of data extortion.



Ransomware attacks will continue.

Even with ransomwareless attacks hitting the threat scene in a new way this year, ransomware developers and gangs are not going to disappear any time soon. Expect to see these threat actors continue the trends of qualifying easier targets to reduce sunk costs and stealing sensitive data with multi-extortion techniques to increase the pressure on victims to pay the ransom. Expect dwell times to decrease as advancements in ransomware detection increase the chances that attackers will be caught if they wait too long to strike.



Supply chain attacks will increase.

As target organizations that fit the profile for paying larger ransoms continue to bolster their security measures, compromising a weak link in the supply chain has become the easiest way to gain access to privileged systems and data. Attackers will take advantage of that access to steal data from the supplier as well as from their target organization.

10 Best Practices for Data Protection

In 2022, Gartner established its first ever Magic Quadrant for **Security Service Edge (SSE)**, a new security industry category. SSE acknowledges that protecting a distributed digital business from malicious actors requires three integrated technologies: secure web gateways (SWG) to control internet access, zero trust network access (ZTNA) to control private application access, and cloud access security broker (CASB) to fix misconfigurations and oversharing from cloud apps. The message is clear: data protection is not a stand-alone endeavor, but should be part of a broader security strategy in which organizations should attempt to disrupt attacks at every stage. The ideal outcome is to block malicious actors outright. The next best thing is to mitigate attacks by limiting access and the ability to exfiltrate.

Protecting against accidental and non-malicious data loss requires increased data visibility, DLP policies to control data-in-motion, and a shared commitment among employees and partners to protect the business and treat sensitive data responsibly.

Consider all of these when building and optimizing your data protection program. Here are best practices to help you maximize your data security and hygiene:

1

Know your data

Before you can protect your data, you need visibility and insight into what you're protecting. Scope and understand what sensitive data you need to protect and assign priority to each different type and source based on the business value and potential loss risk. This is also the right time to generate behavior baselines before implementing protection policies. Start building a foundation for your data protection program by first classifying and tagging sensitive data containing:

- Financial statements (accounts payable, stock, liabilities, and others)
- Credit card information
- Intellectual property (source code and more)
- Personal identification numbers (SSN, NIN, tax IDs, and others)
- Health records (medical information, IDs, insurance)
- Contact lists
- Business property (data in Salesforce)
- Other regulated data types for your industry

2 Understand your data loss channels

Establish which channels are important to control, such as email, personal cloud apps, BYOD, web, physical storage devices, and others.

3 Define your risk profile

Develop risk-based policies and rules that strike a balance between control and productivity. You don't want to stifle productivity by locking down data too much. This is why it is important to identify which data, applications, and channels need the most protecting. You can begin by implementing controls that limit the highest-risk activities. This guidance is not limited to DLP policies. You can mitigate data loss by minimizing unnecessary data access using zero trust strategies such as reducing your public-facing attack surface, inspecting internet traffic, implementing granular microsegmentation, and deploying identity-based access control.

4 Invest in integrated DLP technology

Find the right unified platform to enforce your policies and secure all your sources for sensitive data—including identity information, applications, corporate and customer data stores, and intellectual property—with the least amount of complexity and impact to productivity. Look for a platform that protects data in motion across all key channels

with full inline inspection and continuously scans of your environment to uncover and remediate risks, including misconfigurations, compliance violations, permission levels, and entitlements. This functionality should extend to channels like email, applications like Microsoft 365, Salesforce, and Google Workspace, and endpoints themselves.

5 Build your response workflows

Start by defining security groups and team distribution lists. Document your response workflows and develop detailed playbooks that leverage automation using a security orchestration, automation, and response (SOAR) solution, if available.

6 Don't operate in a bubble

Data protection is more than technology, it needs to be part of the company culture. From executives to all employees, contractors, and partners, DLP should be consolidated under a larger data management protection program with continuous C-suite support. Leverage end user notifications and deliver timely security awareness training to educate your employees and the third parties you do business with about data protection. The more they understand goals, expectations, and best practices, the more successful your data protection program will be.

7 Be accountable to metrics and the board

Establish meaningful metrics around your data protection program to track and improve upon. Use these to communicate value and improvement to the C-suite. Many companies track metrics such as IT incidents, data breaches, and hours to investigate. Commit to continuously monitoring and improving your metrics.

8 Anticipate supply chain attacks

Mitigate the impacts that a third-party supply chain attack has on your organization by assuming that any vendor in your network of suppliers can be breached and expose your business to downstream risk. Conduct data security evaluations of potential vendors and include requirements in your contracts. Address critical supplier dependencies in your business continuity and incident response plans, and apply strict zero trust access policies and controls to third-party users.

9 Implement zero trust architecture

Transform your hub and spoke network infrastructure by upgrading to a secure access service edge (SASE) platform that helps stop data loss, eliminates the attack surface and prevent lateral movement by enforcing the [zero trust](#) principle of least-privileged access using context-based identity and policy enforcement.

10 Review your DLP strategy regularly

DLP policies should be updated on a continual basis. As a leader, you should conduct an annual review of your DLP program (policies, practices, and products) to identify gaps and roll out any major updates needed to keep up with your changing business needs.

Data protection is more than technology, it needs to be part of the company culture.

How the Zscaler Zero Trust Exchange Secures Sensitive Data

Protecting sensitive data with legacy security solutions is extremely challenging. Almost all sensitive data—and more than 80% of traffic overall—is hiding in encrypted (SSL/TLS) traffic, which is increasingly difficult to inspect with traditional security appliances that lack scalability and can create a poor end user experience. Additionally, users and cloud apps have left the network and data center and are no longer behind legacy perimeter-based security controls. And with the myriad consumer and enterprise applications in use every day, it can be exceptionally difficult to maintain visibility into cloud app sharing activity without the proper tools.

The [Zscaler Zero Trust Exchange](#) is a leader in the [2022 Gartner Magic Quadrant for Security Service Edge \(SSE\)](#), delivering superior data protection as part of a unified

platform that eliminates attack surfaces, prevents compromise, stops lateral movement, and prevents data loss. Zscaler solutions are cloud-native, helping organizations solve a range of data security problems at speed and at scale with:

- **Full visibility of sensitive data:** Unlimited SSL inspection from a scalable cloud platform enables complete visibility of all sensitive data, on and off network.
- **Complete inline data control:** Secure all types of sensitive data across Internet, SaaS, Email, Private Apps and Endpoint with a unified enterprise-grade [DLP](#) and [browser isolation](#).
- **ML-powered data classification:** Discover and classify data and risky policies in a fraction of the time with the power of AI. Quickly find and identify data

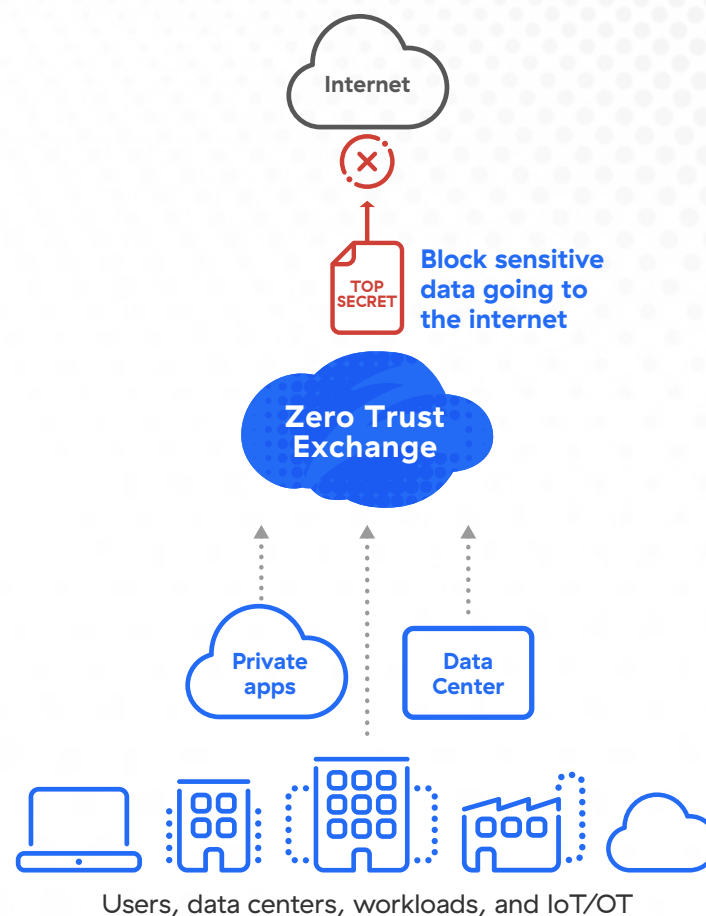


Figure 10: Most popular filetypes being emailed

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

Stay updated on ThreatLabz research by subscribing to our Trust Issues newsletter today.

behaviors and risks with intuitive dashboards that drastically accelerate the deployment of protection policies.

- **Secure cloud app collaboration:** Get complete visibility over data at rest in cloud apps with a multi-mode [cloud access security broker \(CASB\)](#). Prevent dangerous sharing activity and stop malware proliferation with integrated [sandboxing](#).
- **Cloud breach prevention:** Scan cloud apps and platforms for exploitable misconfiguration and quickly remediate with [posture management](#).
- **Advanced data protection techniques:** Leverage UEBA to correlate incidents with user risk along with [advanced techniques](#) like exact data match, indexed document matching, and optical character recognition to secure more data from potential loss.

- **Faster, streamlined workflows:** Reduce incident management with more actionable and reliable insights using advanced UEBA and purpose-built workflow automation.

Because Zscaler Zero Trust Exchange is a fully integrated cloud platform, organizations get a simplified approach to data protection, without the complexity of point products. Zscaler ensures all data in motion and at rest in cloud apps can be protected from loss, while following all users, devices and cloud apps on- and off-network. Delivered from the world's largest security cloud, and built with performance and scalability in mind, Zscaler offers you the proven, unified SASE platform you need to secure data, reduce risk and restore compliance.

To learn more about how Zscaler can help secure you organizations sensitive data and cloud apps, [visit zscaler.com/dp](https://zscaler.com/dp)



| Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.