DATA GETS PERSONAL:

2019 GLOBAL DATA RISK REPORT FROM THE VARONIS DATA LAB

53% of companies found **over 1,000 sensitive files** exposed to all employees

On average, **every employee** had access to **over 17 million files**

CONTENTS

VARONIS

YOUR FILES CALLED.
THEY WANT THEIR PRIVACY BACK.

The future holds more accountability for data protection and privacy for companies, not less. Organizations that are not accountable for their data will need to catch up – and quickly.

Implementing a comprehensive plan to mitigate risk can be an uphill battle if an organization simply does not know where to begin. Organizations that perform risk assessments learn how attackers may exploit their data protection weaknesses *before* a data breach, so they can prioritize remediation tasks and bolster their defenses.

To shed light on data risk, we examined over 785 Data Risk Assessments performed by Varonis engineers to understand the prevalence and severity of exposed sensitive files and evaluate what companies are doing – or failing to do – to secure their most critical data.

DATA AT RISK

On average, every employee had access to **17 million files** and **1.21 million folders**

53% of companies found **over 1,000 sensitive files accessible to every employee**

51% of companies found **over 100,000 folders open every employee**

22% of folders were **open to every employee**

The average company found more than a **half million sensitive files** (534,465)

17% (117,317) of all sensitive files were **accessible to every employee**

58% of companies found **over 1,000 stale user accounts**

53% of data, on average, **was stale**

PER TERABYTE STATS

On average, companies analyzed
70 TB of data

On average, companies found
3,441 exposed, sensitive files per terabyte

On average, companies found
28,645 exposed folders per terabyte

VARONIS

BY THE NUMBERS

Total Data	**54.58 petabytes**
Folders analyzed	**4,332,290,346**
Folders with global access	**953,616,561**
Files analyzed	**53,885,498,652**
Files with global access	**13,445,993,510**
Total number of user accounts	**12,754,608**
Average number of folders per TB	**128,782**
Average number of files per TB	**1.46 million**

ABOUT THE REPORT

The 2019 Global Data Risk Report is a consolidated report that captures findings of Data Risk Assessments performed on 785 organizations – a representative sample from many industry segments and sizes.

In those 785 organizations, we analyzed Active Directory and data permissions structures. 727 organizations also used Varonis automated classification to analyze the sensitivity of their files' contents.

Every year, Varonis performs thousands of Data Risk Assessments for organizations that want to understand where sensitive and classified data reside in their growing hybrid environments, learn how much of it is overexposed and vulnerable, and receive recommendations to reduce their risk profile.

In our 2019 report, Varonis analyzed 53.8 billion files, **a nearly ten-fold increase** over the 6.2 billion files analyzed in our 2018 report.

**For this report, "everyone" indicates every employee within the organization.*

KEY TERMS

Sensitive files contain credit card information, health records, or personal information subject to regulations like GDPR, HIPAA and PCI.

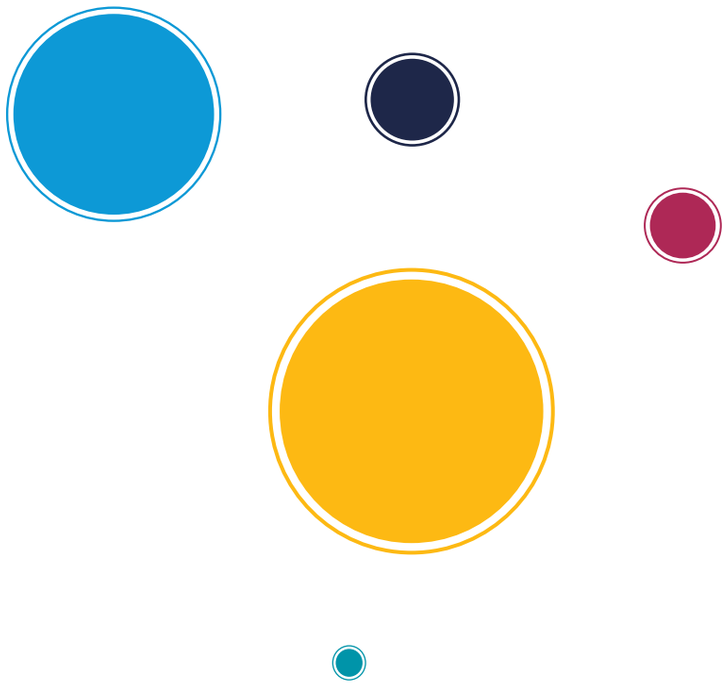
Exposed files and folders are folders that are accessible to every employee.

Global access indicates files and folders open to everyone (all employees). This data represents the biggest risk from attack.

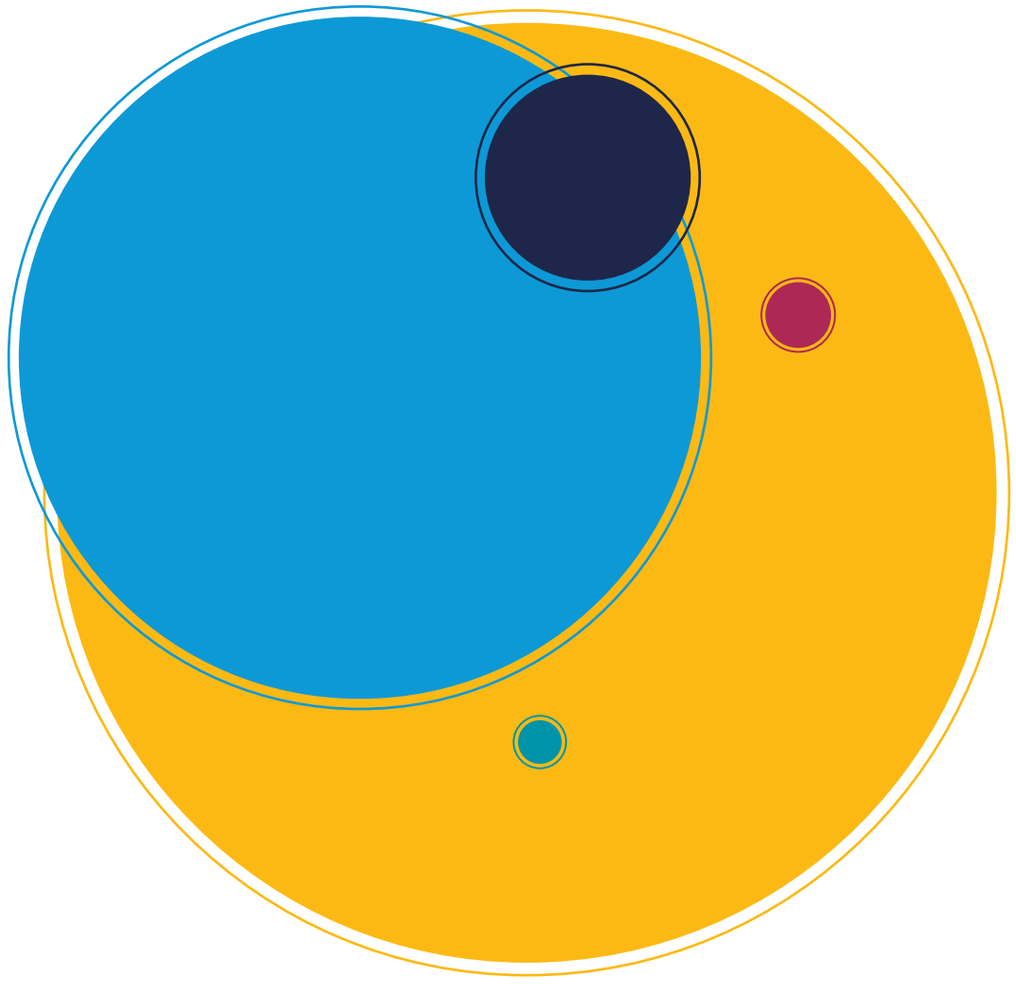
Stale data is information no longer needed for daily operations.

Stale user accounts (aka "ghost users") are enabled accounts that appear inactive, and often belong to users who are no longer with the organization.

2018 REPORT



2019 REPORT



Total Data

Files Analyzed

Folders analyzed

Average number of files per TB

Average number of folders per TB

The 2019 Varonis Global Data Risk Report includes data from a random sampling of 785 companies with all organizational identifiers removed.

VARONIS

FIRMOGRAPHICS

Overexposed data presents a major risk to organizations regardless of size, industry or location.

This report encompasses Data Risk Assessments performed in more than 30 countries and across 30+ industries including financial services; healthcare, pharma and biotech; manufacturing; retail; energy and utilities; technology; government (local, state, and national) and defense; and education.

Most organizations have applied permissions to more folders than they can realistically manage: the average terabyte had almost **17,000 uniquely permissioned folders**. That means someone has granted permissions to that folder for a specific user or group. These folders will need ongoing review to make sure permissions stay current. Permissions may contain both individual users and groups of users.

To make matters more complicated, many of these permissions had "inconsistent" inheritance. This is a technical term for malfunctioning: they're granting or restricting access incorrectly.

On average, over 804 folders in each terabyte had permissions that were "inconsistent." Also, many permissions list users or groups could not be resolved, which most likely means they no longer exist (e.g., they've been deleted from Active Directory). On average, 2,500 access control entries (SIDs) lwere "unresolved."

PRO TIP

In addition to permissions, you can apply additional "preventive controls," like encryption, through digital rights management (DRM). If you've got accurate classification, this is a great extra step to mitigate some of the risk of data loss. These kinds of controls are typically defined broadly. For example: "No file should leave our protected network if it contains personal information." When organizations want to apply more granular access control, they're back to making decisions about sets of data. Tighter DRM policies often end up aligning with folder access controls, so it's important to keep them up to date.

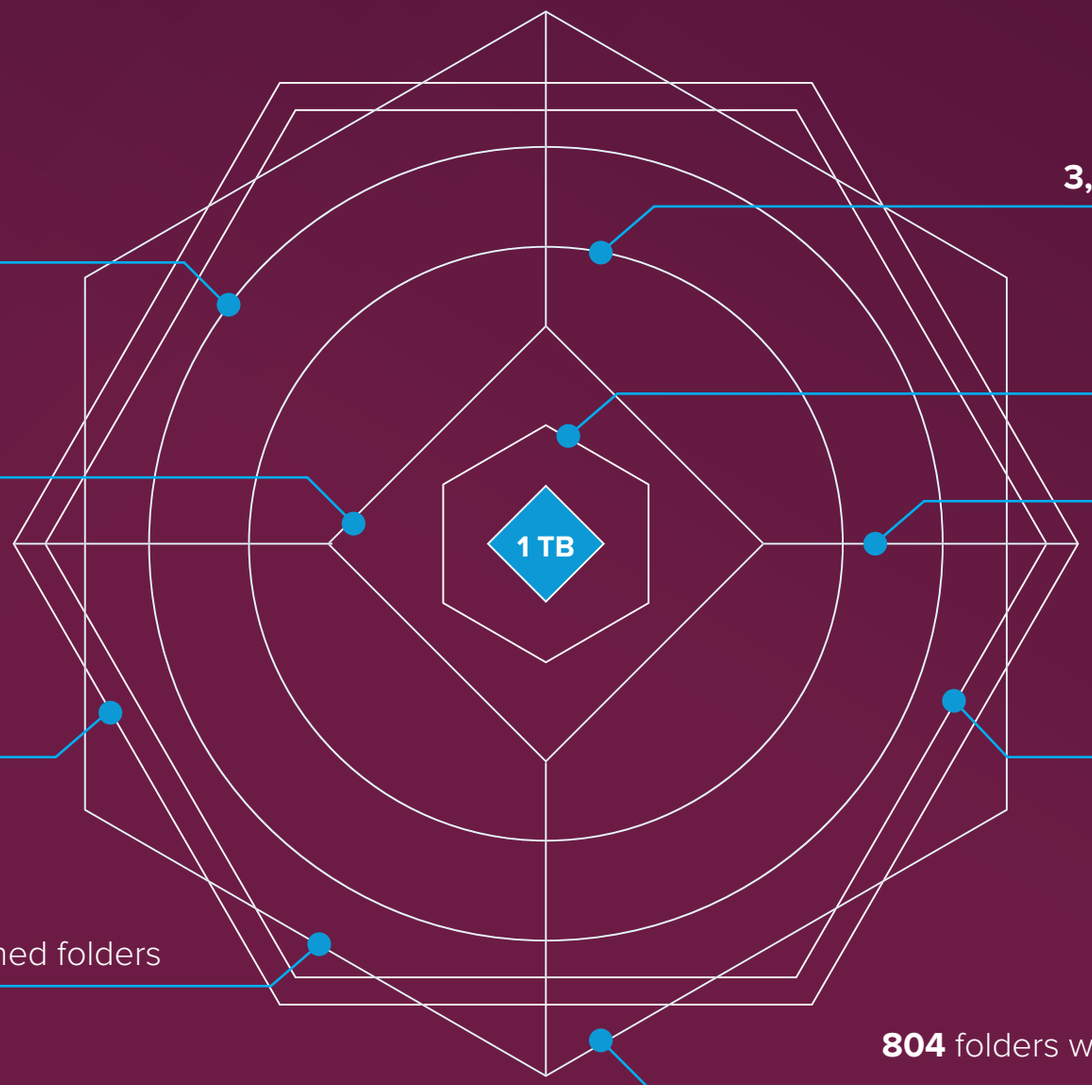
ANATOMY OF A TERABYTE

What's interesting about a terabyte is how much work goes into them – not just to create the files themselves, but to organize and manage the files inside. On average, **each terabyte contained 1.5 million files. About 1%, or 20,000 of those files, contained sensitive information,** like financial, health or other personal information.

Files are organized into containers for management and protection. **On average a terabyte contains 129,000 containers** (i.e. folders, directories, sites, libraries, etc.). Folders reflect decisions and structure – they're used to organize files by project, team, date, and more. If you're reading this, you're probably using a computer, and files and folders are part of your life.

Access controls, or permissions, are the primary mechanism used to protect files and folders. Access controls are usually applied and managed at the folder level – managing means setting the folder up correctly from the beginning, and reviewing permissions regularly. You can manage permissions for some individual files (Office 365 makes this more common), but it's not realistic to manage thousands or millions of them.

AVERAGE STATE OF DATA PER TERABYTE



1.462 million files

3,441 exposed, sensitive files

15,512 stale, sensitive files

28,645 exposed folders

128.782 folders

19,900 sensitive files

2,471 unresolved SIDS

17,041 uniquely permissioned folders

804 folders with inconsistent permissions

PRIVACY BY DESIGN: NOT SO MUCH

Global access groups, such as Everyone, Domain Users, or Authenticated Users, give insiders and outside attackers that get in easy access to files inside. Globally accessible data puts organizations at risk from insiders, malware and ransomware attacks: it takes just one click on a phishing email to set off a chain reaction that encrypts or destroys all accessible files.

The files we analyzed included data subject to regulations like GDPR, PCI, HIPAA and the upcoming California Consumer Privacy Act (CCPA). Exposed data can cost companies: regulations like the EU General Data Protection Regulation (GDPR) penalize companies that fail to protect personal information that often resides in unsecured files and folders.

KEY FINDINGS

53% of companies have **over 1,000 sensitive files open to every employee,** up from 41% last year

15% of companies found **more than 1 million folders open to every employee**

Across the entire dataset, **22%** of **all folders were exposed to every employee,** up from 21% last year

80% of companies with over 1 million folders found **over 50,000 folders open to every employee**

WHY ARE GLOBAL GROUPS SO HARD TO FIX?

On average, companies found **14,643 folders containing sensitive data** open to every employee.

Overexposed data is a common security vulnerability. **IT professionals estimate it takes about 6-8 hours** *per folder* to locate and manually remove global access groups to identify users that need access, create and apply new groups, and subsequently populate them with the right users.

VARONIS

BEST PRACTICE CHECKLIST

- ☐ Identify and remediate global access groups that grant access to sensitive and critical data
- ☐ Ensure only appropriate users retain access to sensitive, regulated data
- ☐ Routinely run a full audit of your servers, looking for any data containers (folders, mailboxes, SharePoint sites, etc.) with global access groups applied to their ACLs
- ☐ Replace global access groups with tightly managed security groups
- ☐ Start with the most sensitive data and test changes to ensure issues do not arise

RIGHT TO BE FORGOTTEN: WHAT WAS THAT AGAIN?

Sensitive stale data includes critical information about employees, customers, projects, clients, or other business-sensitive content. This data is often subject to regulations, including SOX, HIPAA, PCI, and GDPR.

Data kept beyond a pre-determined retention period can expose an organization to additional liability. Stale data can be expensive to store and manage, and poses an increased (and unnecessary) security risk.

Despite the May 2018 EU General Data Protection Regulation (GDPR) and upcoming California Consumer Privacy Act (CCPA), companies continue to amass sensitive data that's no longer needed for business.

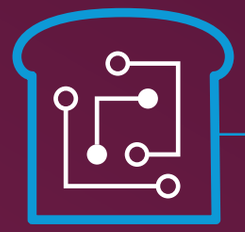
The vast majority of companies have stale sensitive files, and the problem is only getting worse.

VARONIS

KEY FINDINGS

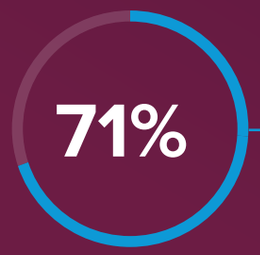
of companies found over

1,000 stale, sensitive files



15,511 sensitive files

per TB are **stale**



of companies found over

5,000 stale, sensitive files

SWIMMING IN A SEA OF STALE DATA

Overall, **72%** of folders in a company contain **stale data.**

On average, we found more than half of a company's data is stale. This data is scattered throughout a company's systems.

While organizations focus on keeping attackers out, all too often the data itself remains widely accessible and unmonitored.

Determined attackers will keep trying to find a way in. Once they get inside, you'll want to ensure your most valuable information is hard to get.

VARONIS

BEST PRACTICE CHECKLIST

- ☐ Follow the principles of Privacy by Design: minimize the sensitive data you collect, minimize who gets to see it, and minimize how long you keep it
- ☐ Identify stale data – especially sensitive information
- ☐ Archive or delete stale data if no longer needed

53% of a company's data is **stale**

95% of companies found over 100,000 folders that contained **stale** data

(IN)ACTIVE DIRECTORY

58% of companies **found over 1,000** stale user accounts

To access data on network file stores, a user or service needs an account. These accounts are usually stored in Active Directory. User and service accounts that are inactive and enabled (aka “ghost users”) are targets for penetration and lateral movement.

Inactive user accounts can lie dormant, going unnoticed day to day, yet still provide access to systems and data. Stale, but still enabled, user accounts are a great way for hackers to “test the waters.” Stale user accounts that are no longer active create noise that can make security more difficult for organizations.

Hunting and eliminating stale accounts and non-expiring passwords are security steps organizations often overlook. If these accounts are unmonitored, attackers can steal data or cause disruption without detection.

Companies, overall, are doing a better job at reducing stale user accounts, but they’re far from perfect: half of all user accounts are stale, and over a third of all companies we examined found more than 1,000 enabled but stale users.

VARONIS

BEST PRACTICE CHECKLIST

- ☐ Know that most attackers target data, but they reach their target by hijacking accounts
- ☐ Make sure stale accounts are disabled and monitored for re-enablement and activity, or deleted
- ☐ Implement procedures to ensure that all user accounts are active, governed and monitored
- ☐ Understand what constitutes normal behavior on both user and service accounts so you can better spot inactive users and behavioral anomalies
- ☐ Boost your organization’s anomaly detection capabilities and response processes

40% of companies found **over 1,000 stale, but enabled,** user accounts

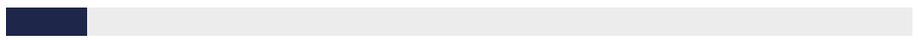
On average, **50%** of user accounts were **stale**

TOXIC PERMISSIONS:

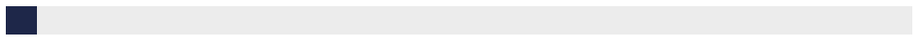
76% of companies found **over 1,000 folders** with **unresolved SIDs**

58% of companies found **over 1,000 folders** that had **inconsistent permissions**

27% of a company's users had **removal recommendations**, and were likely to have more access to data than they require



15% of folders were **uniquely permissioned**



Only **5%** of folders were **protected**

VARONIS

BEST PRACTICE CHECKLIST

It's important to know exactly who uses – and no longer uses – data, so that you can be surgical about reducing access without causing any headaches.

- ☐ The more complex a file system structure, the greater risk for overexposure and security vulnerabilities
- ☐ Simplify access management procedures and standards to help lock down potential exposure of sensitive data from insider threats
- ☐ Decrease the amount of data any compromised account can access, making an attacker's target that much harder to reach
- ☐ Work to attain and sustain a "least-privilege model" where users have access to only the data they need. To do so:
  - ☐ Eliminate global access
  - ☐ Simplify permissions structures
  - ☐ Ensure that all data has an owner or steward
  - ☐ Periodically re-certify access to data to spot those that have changed jobs or left the organization
  - ☐ Use automation to discover accounts that look like they may have access to data they don't require

PASSWORDS: CHECK EXPIRATION DATE BEFORE CONSUMING DATA

38% of all users sampled have **a password that never expires**

Very few (if any) accounts should have passwords that never expire. Users with non-expiring passwords give attackers a large window to crack them using brute force. Once breached, they provide indefinite access to data. Passwords that aren't periodically changed are more likely to appear in breached password dumps. When attackers find administrative accounts with non-expiring passwords, it's their lucky day.

VARONIS

BEST PRACTICE CHECKLIST

- ☐ IT must disable non-expiring passwords wherever possible and set passwords for all users to expire at set intervals
- ☐ If an account requires a static password, make sure it is extremely long, complex and random to help protect from brute-force attacks
- ☐ The use of enterprise-wide password managers, two-factor authentication, and monitoring and alerting on suspicious failed login attempts are also great ways to mitigate attacks that stem from poor password practices

76% of companies found **over 1,000 folders** with unresolved SIDS

11% of enabled users have **expired passwords**

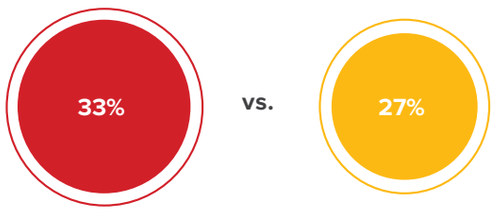
61% of companies found over 500 users with **passwords that never expire**

EXPOSURE BY FILE SIZE

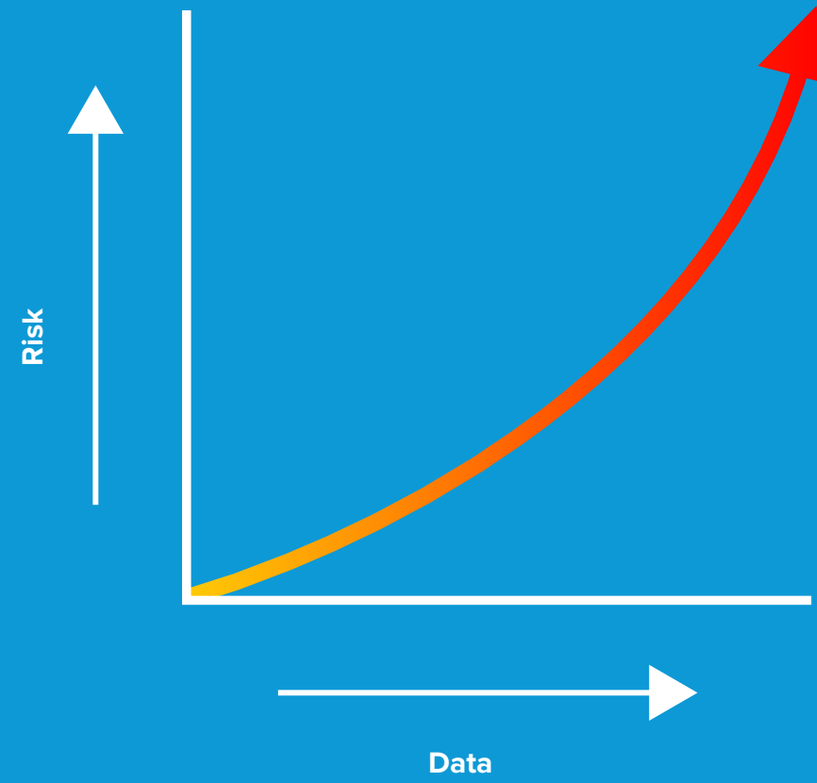
Organizations that store more data have a harder time protecting it.

Organizations with over 100 terabytes of data had a higher percentage of folders open to everyone (27% vs. 19%).

Companies with more data also had more users who belonged to more groups than they needed: 33% had removal recommendations compared to 27% in organizations with less data.



On the bright side, organizations with more data seemed to have better controls around user accounts, as they had a lower percentage of stale but enabled users (21% vs. 27%).



DATA RISK ACROSS INDUSTRIES

Energy & Utilities

2% of files analyzed were sensitive
14% of sensitive files were exposed
25% of folders were exposed
Averaged 35,298 exposed, sensitive files
Averaged 3,230 exposed, sensitive files per TB
Averaged 20,396 exposed folders per TB

Healthcare, Pharma & Biotech

2% of files analyzed were sensitive
15% of sensitive files were exposed
18% of folders were exposed
Averaged 113,491 exposed, sensitive files
Averaged 4,691 exposed, sensitive files per TB
Averaged 27,191 exposed folders per TB

Financial Services

2% of files analyzed were sensitive
21% of sensitive files were exposed
21% of folders were exposed
Averaged 352,771 exposed, sensitive files
Averaged 3,791 exposed, sensitive files per TB
Averaged 42,787 exposed folders per TB

Retail

1% of files analyzed were sensitive
14% of sensitive files were exposed
17% of folders were exposed
Averaged of 12,444 exposed, sensitive files
Averaged 858 exposed, sensitive files per TB
Averaged 17,324 exposed folders per TB

Government / Military

2% of files analyzed were sensitive
12% of sensitive files were exposed
15% of folders were exposed
Averaged 75,204 exposed, sensitive files
Averaged 3,068 exposed, sensitive files per TB
Averaged 22,248 exposed folders per TB

Manufacturing

1% of files analyzed were sensitive
21% of sensitive files were exposed
23% of folders were exposed
Averaged 20,315 exposed, sensitive files
Averaged 2,264 exposed, sensitive files per TB
Averaged 32,146 exposed folders per TB

DATA RISK BY REGION

EMEA

- **3%** of files analyzed were sensitive
- **15%** of sensitive files were exposed
- **15%** of folders were exposed
- **Averaged 88,790 exposed, sensitive files**
- **Organizations averaged 4,724 exposed, sensitive files per TB**
- **Averaged 24,385 exposed folders per TB**

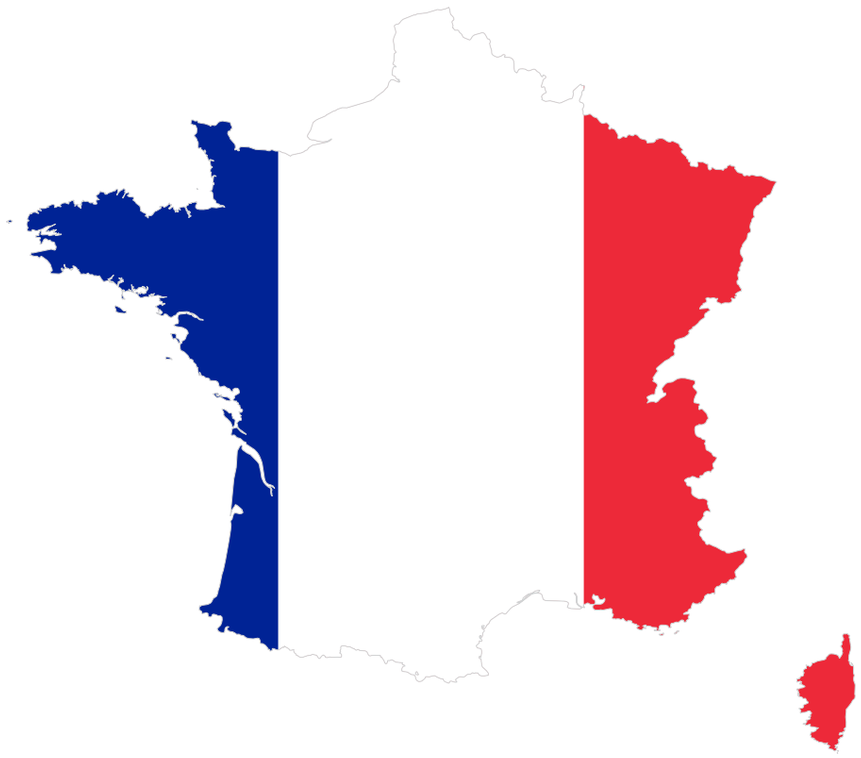
North America

- **1%** of files analyzed were sensitive
- **17%** of sensitive files were exposed
- **22%** of folders were exposed
- **Averaged 143,308 exposed, sensitive files**
- **Organizations averaged 2,958 exposed, sensitive files per TB**
- **Averaged 31,221 exposed folders per TB**

APAC

- **0.4%** of files analyzed were sensitive
- **26%** of sensitive files were exposed
- **23%** of folders were exposed
- **Organizations averaged 4,309 exposed, sensitive files**
- **Averaged 897 exposed, sensitive files per TB**
- **Averaged 25,391 exposed folders per TB**

DATA RISK BY COUNTRY
FRANCE



4.22% of files analyzed were sensitive

—

12% of sensitive files were exposed

48% of data on average, was stale

—

12% of users were uniquely permissioned

39% of users had passwords that never expire

—

28% of users had removal recommendations

12% of folders were exposed

—

Organizations averaged 150,878 exposed, sensitive files

28%, of users, on average were stale but still enabled

—

68% of folders contained stale data

Averaged 5,395 exposed, sensitive files per TB

—

Averaged 19,771 exposed folders per TB

DATA RISK BY COUNTRY
GERMANY

0.63% of files analyzed were sensitive

—

19% of sensitive files were exposed

58% of data on average, was stale

—

15% of users were uniquely permissioned

40% of users had passwords that never expire

—

33% of users had removal recommendations

17% of folders were exposed

—

Organizations averaged 57,993 exposed, sensitive files

23%, of users, on average were stale but still enabled

—

79% of folders contained stale data

Averaged 2,816 exposed, sensitive files per TB

—

Averaged 31,691 exposed folders per TB

DATA RISK BY COUNTRY
UNITED STATES

1.15% of files analyzed were sensitive

—

18% of sensitive files were exposed

54% of data on average, was stale

—

15% of users were uniquely permissioned

28% of users had passwords that never expire

—

26% of users had removal recommendations

22% of folders were exposed

—

Organizations averaged 156,023 exposed, sensitive files

27%, of users, on average were stale but still enabled

—

72% of folders contained stale data

Averaged 3,125 exposed, sensitive files per TB

—

Averaged 32,633 exposed folders per TB

DATA RISK BY COUNTRY
CANADA

1.7% of files analyzed were sensitive

—

10% of sensitive files were exposed

57% of data on average, was stale

—

12% of users were uniquely permissioned

29% of users had passwords that never expire

—

25% of users had removal recommendations

18% of folders were exposed

—

Organizations averaged 28,291 exposed, sensitive files

32%, of users, on average were stale but still enabled

—

74% of folders contained stale data

Averaged 1,453 exposed, sensitive files per TB

—

Averaged 18,421 exposed folders per TB

DATA RISK BY COUNTRY
AUSTRALIA

0.31% of files analyzed were sensitive

—

29% of sensitive files were exposed

59% of data on average, was stale

—

15% of users were uniquely permissioned

33% of users had passwords that never expire

—

29% of users had removal recommendations

27% of folders were exposed

—

Organizations averaged 4,413 exposed, sensitive files

21%, of users, on average were stale but still enabled

—

80% of folders contained stale data

Averaged 936 exposed, sensitive files per TB

—

Averaged 28,711 exposed folders per TB

DEFINITIONS:

Permissions are access control lists (ACLs). An ACL is comprised of access control entries (ACEs). In Windows-based environments, these entries are called “Security Identifiers,” or SIDs – a number that refers to a user or group stored in Active Directory or on a local system.

Unresolved Security Identifiers (Unresolved SIDs) occur when the reference is unfound, as when a user on an access control entry is deleted from Active Directory but remains on the access control list. Unresolved SIDS increase complexity and may be exploited to gain unauthorized access to data.

Uniquely permissioned folders ensure need-to-know access, but must be maintained or soon become outdated. An unnecessarily high number of unique folders increases management burden and complexity. A uniquely permissioned folder may have both directly applied permissions and “inherited permissions,” (permissions that flow down from its parent folders), or may be “protected,” so that only directly applied permissions take effect.

Inconsistent inheritance occurs when folders do not inherit their permissions correctly from parent folders. They may have missing or extra entries, may expose important data to users who should not have access, or may be inaccessible to users that require access.

Removal recommendations: Removal recommendations are provided by Varonis based on patented algorithms that detect when a user no longer needs access to data they presently have access to.

[1]Accounts may also be stored in other directory services like LDAP, NIS, or locally on the servers themselves

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, specializing in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyberattacks by analyzing file activity and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

Live Demo

Set up Varonis in your own environment. Fast and hassle free.

info.varonis.com/demo

Data Risk Assessment

Get a snapshot of your data security, reduce your risk profile, and fix real security issues.

info.varonis.com/start

VARONIS

WHAT VARONIS CUSTOMERS ARE SAYING

"Varonis has been a huge help for my company with various projects, and crucial for GDPR. Also has enable(d) us to automate some of our manual processes.

- UK-based financial company

"Varonis has given us much needed insight into our network and environment we never had before.

- IT administrator, healthcare organization

NASA ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL