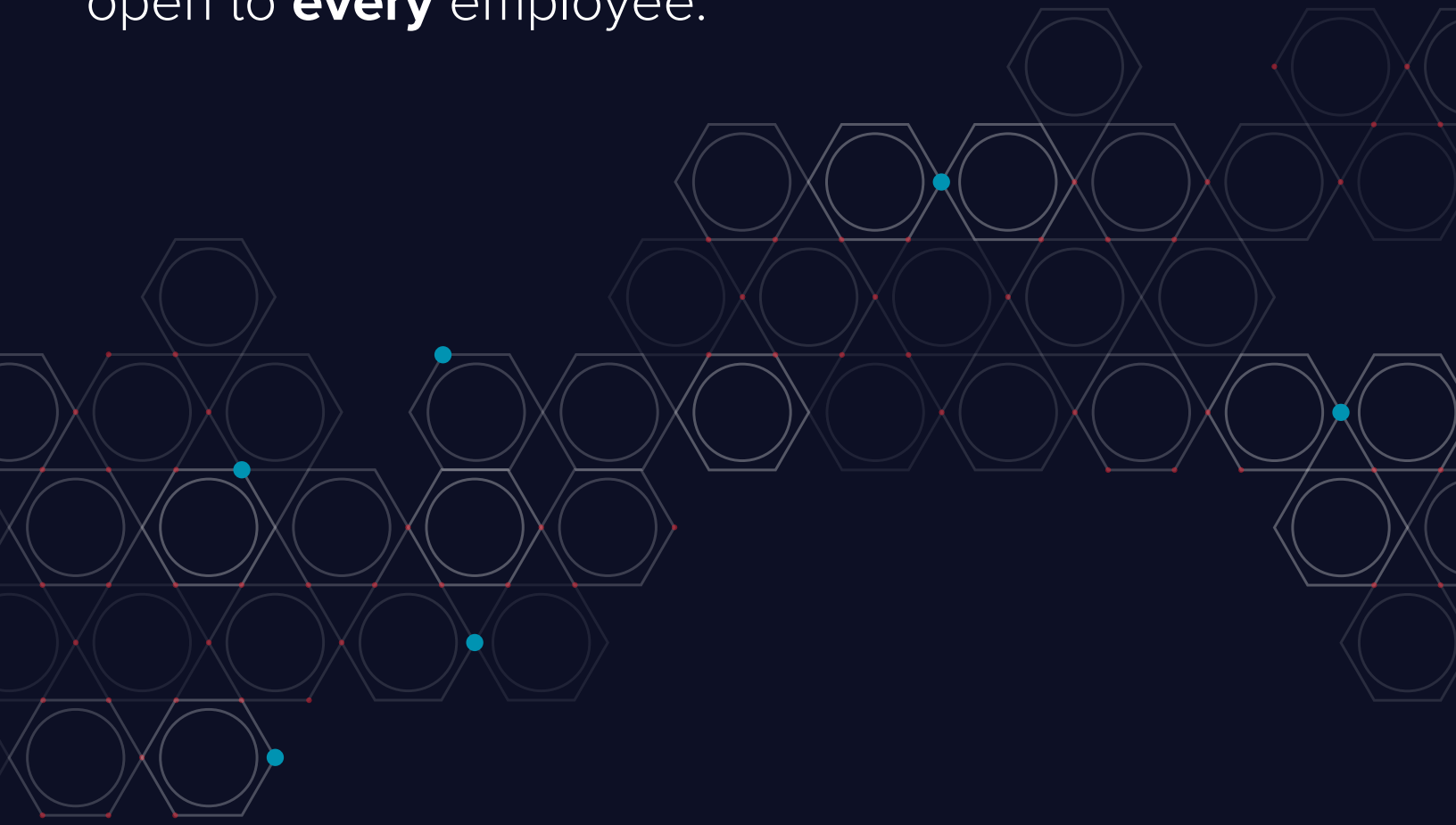
2017 Varonis Data Risk Report

47% of organizations have at least 1,000 sensitive files open to **every** employee.



VARONIS

An Analysis of the 2016 Data Risk Assessments Conducted by Varonis

Assessing the Most Vulnerable Data – Files and Emails

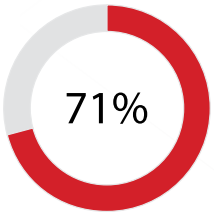
In data breaches, files and emails are often targeted because they are high value assets and usually vulnerable to misuse by insiders and outsiders that transgress the perimeter. While organizations focus on perimeter defenses and chasing threats, the data itself is left broadly accessible and unmonitored.

About the Varonis Data Risk Report

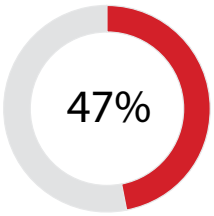
Each year, Varonis conducts over a thousand risk assessments for customers and potential customers. The assessment provides insights into the risks associated with an organization's data, exposing high risk areas and providing recommendations on access remediation to reduce their risk profile. Assessments are typically performed on a subset of the organization's production environment.

The Varonis Data Risk Report provides a glimpse into the vulnerabilities found within a sample of the assessments conducted by Varonis last year.

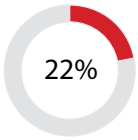
Sample Results:



71% of all folders contained **stale data**, accounting for almost **2 petabytes** of data

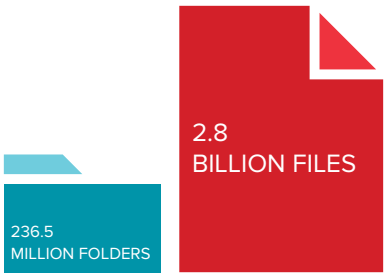


47% had at least **1,000 sensitive files** open to every employee



22% had **12,000** or more sensitive files exposed to **every employee**

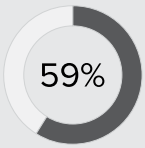
48,054,198 **million** folders were open to **global access groups** (accessible to the **entire organization**)



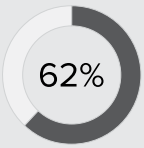
3.79 petabytes of data analyzed

24.4M folders had unique permissions, which increased complexity to enforce a least privilege model for folders containing sensitive data and comply with regulations like GDPR

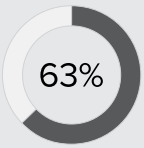
Third Party Research:



don't enforce a least privilege model for access to this data



have access to company data they probably shouldn't see



don't audit use of this data and alert on abuse

source: Ponemon Institute Report, Closing Security Gaps to Protect Corporate Data

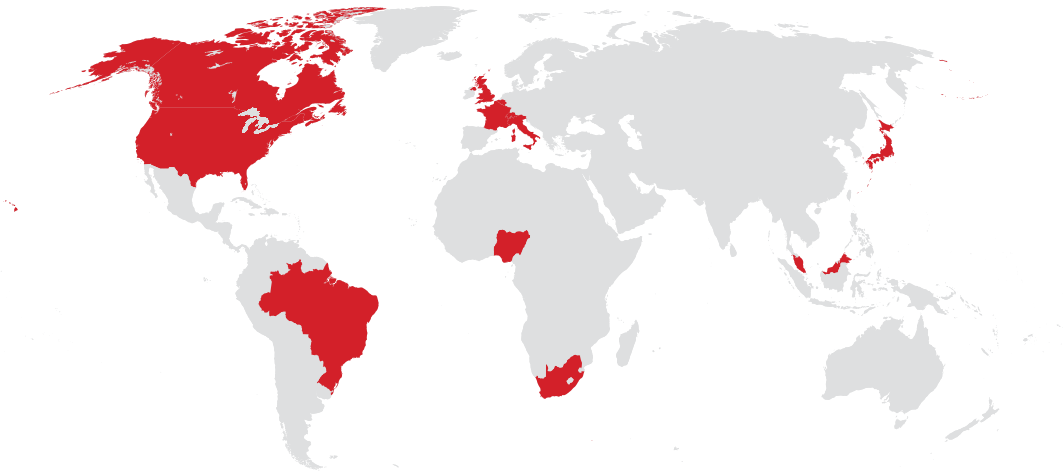
Scope

Data	
Files	**2.8 billion files**
Folders	**236.5 million folders**
Difference	The average folder had **12.2 files**, an increase of **38.6%** compared to 2015's Risk Assessment data
Total Data	**3.79 petabytes** of data
Median	The median amount of data analyzed was **6 terabytes**

The Data Risk Report is a random sampling of 80 reports executed in 2016 with all organizational identifiers removed.

Demographics

No one industry, country or organizational size is immune to the risks of overexposed data.



- 12 countries, including the United States, Canada, United Kingdom, France, Germany and Malaysia.
- 33 industries including Insurance, Financial Services, Healthcare, Retail, Utilities & Energy, Construction, IT and Computer Software, Education and Public Sector.
- 42 organizations with 1,000 or fewer employees; 38 organizations with 1,001 or more employees.

Customer Highlights

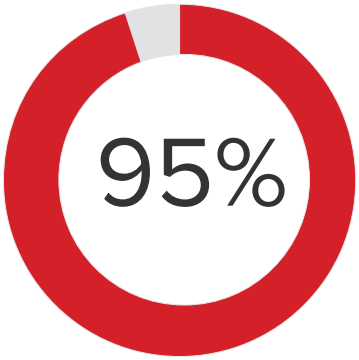
While we can't tell you who they are, we will shed light on specific examples throughout the report.

Most Valuable Players

Let's face it, some organizations are on top of their data security game. They do this by regularly analyzing the type of data they have and the people who can access it through risk assessments like Varonis offers. Look for this symbol to read their stories.

Most Improved Players

Companies are reducing risk faster and more efficiently than before and that starts with identifying vulnerabilities. Look for this symbol to see specific cases where a customer took big steps toward mitigating huge liabilities in their environment



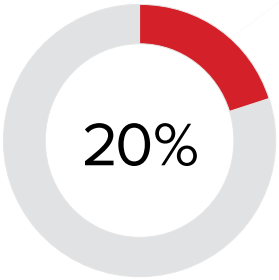
95% of surveyed customers agreed that the Varonis data risk assessment helped identify at-risk, sensitive and classified data.

source: TechValidate Survey | TVID: C41-5EC-01C

Data at Risk

Folders with Global Group Access

Over 48 million folders
with global group access



Average: 20% of all folders
were accessible to global group

Most Valuable Player

- A government entity had only .01%, or 29 folders of 290,000, open to every employee, and they had zero sensitive files open to everyone within the scope of the risk assessment.

Most Improved Players

- A real estate firm identified that **80%** of its 807,663 total folders were **accessible to every employee**; 71% of folders containing sensitive information were also exposed to every employee.
- An insurance firm discovered that **every employee had access to 35%** of their 86.4 million total folders

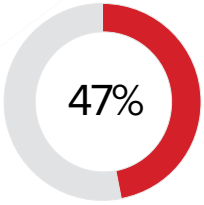
Vulnerability

Description: These include groups such as Everyone, Domain Users and Authenticated Users. Global access groups will allow anyone within an organization to access data with these access controls.

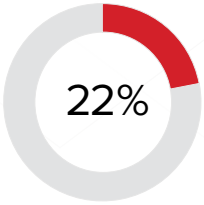
Risk: Failing to reduce or eliminate the use of global access groups will allow anyone within an organization to access data with these access controls. A common misconception is that most data breaches are sophisticated attacks from external sources. In reality, many data breaches are opportunistic or rudimentary in nature, and many originate from an insider, or an insider whose credentials or system has been hijacked. Excessive user access through global groups is a key failure point for many security and compliance audits.

Sensitive Data with Global Group Access

2,665,321 sensitive files were open to global group access



47% had at least 1,000 or more sensitive files exposed to everyone



22% had at 12,000 or more sensitive files exposed to all users

Most Valuable Player

- A company in the construction trade had only .01% of sensitive files (986) open to the everyone group

Most Improved Players

- An insurance company identified **over 1 million sensitive files** open to the **everyone group**.
- A banking institution discovered that **80%** of its 245,575 sensitive files were accessible to **every employee**.

In the News: Pandemonium in Panamanian Law Firm

In April 2016, 11.5 million confidential files and emails, or 2.6 terabytes of data, from the Panama law firm Mossack Fonseca, was leaked to a German newspaper. The Panama Papers, as the breach was dubbed, exposed the quiet law firm's operations and revealed how clients hid billions of dollars in tax havens.

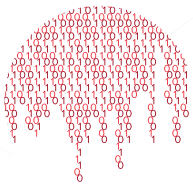
Vulnerability

Description: Many files contain critical information about employees, customers, projects, clients or other business-sensitive content. The data is often subject to industry regulation, such as SOX, HIPAA, PCI, EU GDPR, GLB and more. When global access groups grant access to such data, there is significant risk to the business.

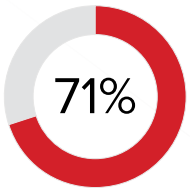
Risk: While any data that is exposed to unneeded user access is problematic, data containing sensitive information requires particularly close attention. These sensitive files include personally identifiable information (PII), credit card numbers, social insurance numbers and personal health information (PHI), as well as business intellectual property, including business plans and product designs. This data must remain tightly controlled, and any breach or leakage of this information may potentially damage the business.

Stale Data

169,060,167 folders contained stale data



1.95 petabytes of stale data found



71% of all folders contained stale data

In 2015, 70% of data analyzed was stale

Most Valuable Player

- An investment management firm had only 21 gigabytes of stale data, representing .03% of its data.

Most Improved Player

- **527 terabytes of stale data** was found in over 35,000 folders at an environmental firm.

Vulnerability:

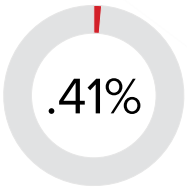
Description: The volume of electronic data that companies manage continues to grow exponentially. Much of this data becomes stale or unused immediately after it is created.

For the purpose of this report, data that hasn't been touched in 6 months or longer is considered stale.

Risk: Stale data represents little value to the business while it's not being used, but still carries with it risk and potential financial liability if used inappropriately.

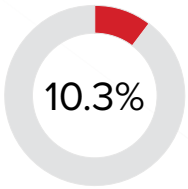
Unused data also adds a management and cost burden to an organization, especially if kept on high-performance storage.

Folders and Permissions

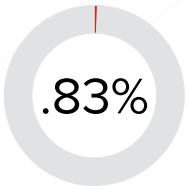


0.41% of folders had inconsistent permissions

1.6% of folders were "protected," or blocking inheritance



24,476,544 million folders (10.3%) contained unique permissions



0.83% of all folders had unresolved SIDs (1,972,360)

Most Valuable Player

- A law firm had only 2 folders with unresolved SIDs amongst the over 463,000 folders analyzed.

Most Improved Player

- A banking institution had **11.6 million folders** with **unique permissions.**

Vulnerability:

Inconsistent Permissions: Folders may be individually protected or may inherit some or all of their permissions from a parent folder. Data is frequently being moved between folders, domains and servers and re-permissioned, causing inconsistencies in the inheritance structure.

Failure to repair inconsistent permissions will lead an organization to believe they have successfully locked-down access to data, while the reality may be quite different.

Protected Folders: Protected folders contain an explicitly defined ACL and will inherit no ACE's from their parent folders. Protected folders found in deeper levels of the file system may contain users and permissions which are not visible at the higher levels, leading an administrator to mistakenly assume that permissions to a folder are configured correctly.

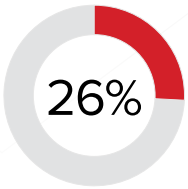
"Unique" Permissions: Unlike folders that inherit all their permissions, or inherit none of their permissions (protected), these folders both inherit ACE's and have ACE's applied to their ACL, making their permissions more complex to analyze.

The more complexity that exists in a file system structure, the more risk there is for users to gain unintended access. Unique permissions increase complexity when attempting to comply with regulations that require sensitive data access be reduced to a need-to-know basis, like the upcoming GDPR.

Unresolved SIDs: Unresolved Security Identifiers occur when a user on an access control list is deleted from AD. They can potentially give unauthorized users (like hackers) access to data.

Accounts and Users

448,224 user accounts were stale but enabled



26% of users had removal recommendations

502,706 user accounts had non-expiring passwords

65,917 security groups had no users

Most Valuable Player

- Only 3% (6,174) of an outsourcing company's 205,800 users were stale but enabled.

Most Improved Players

- An education organization discovered over 231,365 **stale enabled users** (90% of their users) and **100% of their user's passwords did not expire** (257 thousand).
- An insurance firm found that 58% of its 246,865 users had **passwords that did not expire**.
- An outsourcing company spotted **79 looped nested groups** within AD.

Vulnerability:

Users with Non Expiring Passwords: Non expiring passwords allow unlimited time to brute force crack them and indefinite access to data via the account.

Stale Enabled Users: Stale enabled accounts still retain all of the access permissions they were granted while active, and are a target for exploitation and malicious use to access data.

Empty Security Groups: These groups add complexity, and can allow access to more data by becoming a member of the group; a common technique of lateral movement and privilege escalation.

Looped Nested Groups within AD: As many applications and scripts enumerate group membership recursively, looped nested groups can cause application crashes or unexpected behavior.

Varonis is a powerful software suite that protects your file and email servers from cyberattacks and insider threats. We analyze the behavior of the people and machines that access your data, alert on misbehavior, and enforce a least privilege model.

We help thousands of customers prevent data breaches.

NASA
ING
Nasdaq
CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829
EMC²
TOYOTA
LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE
L'ORÉAL

SC MAGAZINE
Deloitte. Technology Fast 500™
Inc. 500
NETWORK computing AWARDS 2015 WINNER
CDM CYBER DEFENSE MAGAZINE THE PREMIER SOURCE FOR IT SECURITY INFORMATION
MOST INNOVATIVE INSIDER THREAT DETECTION SOLUTION
HOT COMPANY USER BEHAVIORAL ANALYTICS SOLUTION
Info Security Products Guide 2016 GLOBAL EXCELLENCE GOLD

VARONIS