**DATA UNDER ATTACK:**

# 2018 GLOBAL DATA RISK REPORT FROM THE VARONIS DATA LAB

*58% of companies have over 100,000 folders open to everyone*

# CONTENTS



VARONIS

# SENDING OUT A DATA SECURITY SOS

Organizations often fail to pay close attention to what goes on before a data breach: the early warning signs that point to failures in data protection that allow attackers unfettered access to important information once they've breached a corporate network.

Mapping the millions of unprotected files and folders within an organization serves as a data SOS that inspires action before the next major breach occurs – it's a signal that cannot be ignored.

To build this map, we examined Data Risk Assessments performed by Varonis engineers throughout 2017 to gauge the prevalence and severity of exposed critical information and sensitive files, and evaluate what companies are doing (or not doing) to secure their most critical data.

## DATA AT RISK

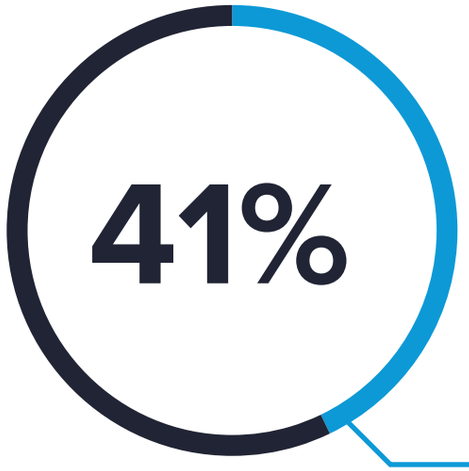
**21%** of **all folders** are open to **everyone**

**58%** have over **100,000 folders** open to **everyone**

**54%** of **data is stale**

**34%** of **users are enabled**, but **stale**

## EXPOSED SENSITIVE FILES




of companies have over **1,000 sensitive files** open to **everyone**

# ABOUT THE REPORT

The 2018 Global Data Risk Report captures findings of Data Risk Assessments performed on 130 organizations – a representative sample from many industry segments and sizes.

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

For this year's report, Varonis analyzed over 6 billion files, more than double the number in our 2017 report.

VARONIS

## KEY TERMS

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

**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.

**Inconsistent permissions** occur when folders or files inherit extra access control entries from their parents, or fail to inherit access control entries from their parents. Users may be unintentionally granted or deprived of access.

| | |
|---|---|
| **Files** | **6.2 billion** files analyzed |
| **Average number of files per TB** | **1.1 million** files |
| **Average number of folders per TB** | **84,081** folders |
| **Folders** | **459.2 million** folders analyzed |
| **Average Folder** | The average folder has **13.6 files** |
| **Total Data** | **5.5 petabytes** of data analyzed |
| **Median** | The median amount of data analyzed is **11.1 terabytes** |

The 2018 Varonis Global Data Risk Report includes data from a random sampling of 130 companies with all organizational identifiers removed.

For this report, “everyone” includes every employee within the organization. All calculations are based on averages unless otherwise indicated.

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 50 countries and across 30+ industries including insurance, financial services, healthcare, pharma and biotech, manufacturing, retail, utilities and energy, construction, IT and computer software, education, local, state and regional governments.

VARONIS

**RISK SPOTLIGHT**

# ACCESS OVERLOAD

Attackers look for unsecured folders as soon as they land on a network, and folders open to global access groups – Everyone, Domain Users, or Authenticated Users – give them easy access to business plans, intellectual property, customer and employee data, credit card information, and more. Files open to anyone via an anonymous link represent additional risk.

Globally accessible data puts organizations at risk from 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.

Regulations like the EU General Data Protection Regulation (GDPR) set the stage to penalize companies that fail to protect personal information that often resides in unsecured files and folders.


of companies with over **1 million** folders have over **100,000** folders open to **everyone.**

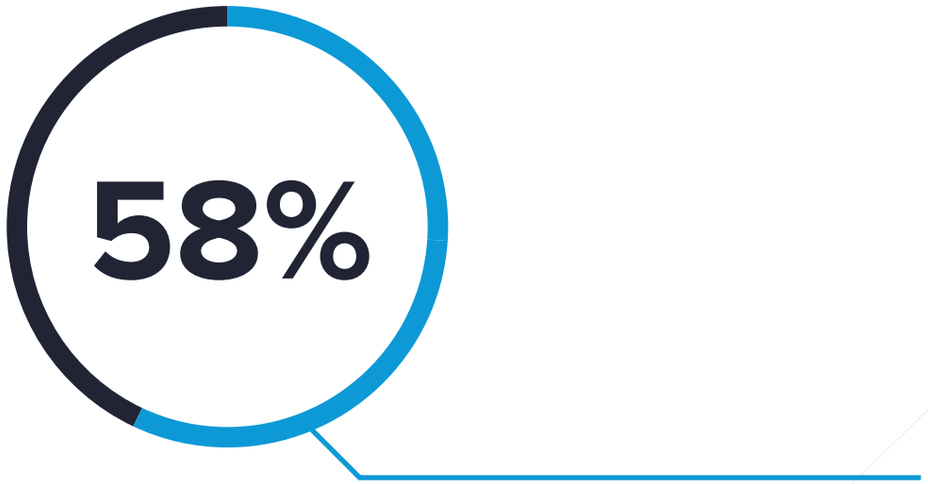
## OPEN ACCESS

**30%** of companies have over **1,000 sensitive folders** open to **everyone**

**41%** of companies have over **1,000 sensitive files** open to **everyone**

**88%** of companies with over **1 million** folders have over **100,000 folders** open to **everyone**

**21%** of all folders in a company are open to **everyone**




of companies have over **100,000 folders** open to **everyone**

## BEST PRACTICE CHECKLIST

# ACCESS OVERLOAD

Global groups - including Everyone, Domain Users, and Authenticated Users - allow everyone in an organization to access these folders.

IT professionals estimate it takes about 8-6 hours per folder to locate and manually remove global access groups: they must identify users that need access, create and apply new groups, and populate them with the right users.

To achieve least privilege, it's critical to restrict access to only those who need it: manage users, eliminate broken inheritance and permissions inconsistencies, and lock down sensitive data.

VARONIS

## BEST PRACTICE CHECKLIST

- ☐ Identify and remediate global access groups that grant access to sensitive and critical data
- ☐ Ensure that 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

RISK SPOTLIGHT

# TICKING TIME BOMB

Sensitive stale data includes critical information about employees, customers, projects, clients, or other business-sensitive content.

This data is often subject to regulation including SOX, HIPAA, PCI, and GDPR – and 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.


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


of companies have **over 1,000 stale sensitive files**

## STALE DATA

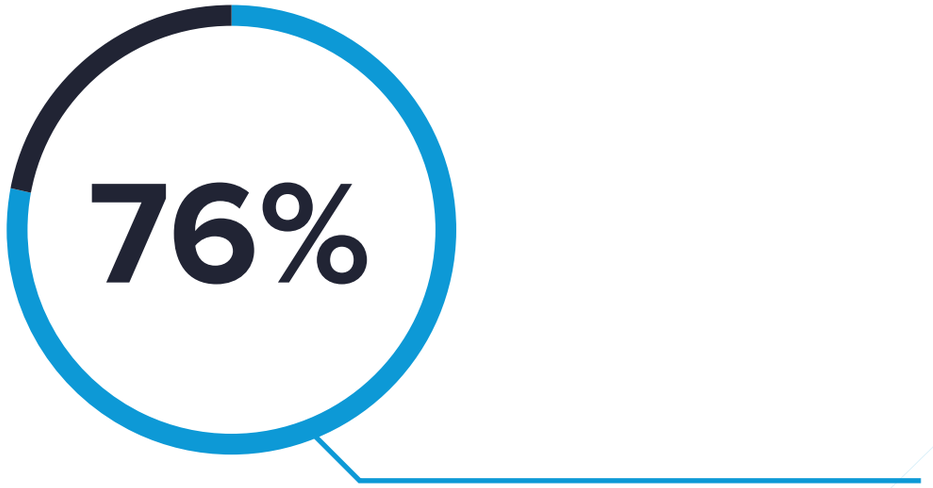
**54%** of a company's data **is stale**

**76%** of folders in a company contain **stale data**

**74%** of companies have **over 1,000 stale sensitive files**

**61%** of companies have **over 5,000 stale sensitive files**

**85%** of companies have **over 100,000** folders that contain **stale data**




In companies that have over **1 million folders**, approximately **76%** contain **stale data**

## BEST PRACTICE CHECKLIST

# TICKING TIME BOMB

While organizations focus on keeping attackers out, all too often the data itself remains widely accessible and unmonitored. That's like putting all your defenses and resources into building the strongest, highest castle walls, but leaving your crown jewels draped on the coat rack beside the front door.

Stale data quickly becomes a security liability and unnecessary storage expense. In order to reduce risk, it's important to identify stale data and determine what data can be moved, archived, or deleted - and to establish consistent policy to manage stale data moving forward.

VARONIS

## BEST PRACTICE CHECKLIST

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

## RISK SPOTLIGHT

# GHOST IN THE MACHINE

Hackers, like burglars, often look for the easiest and quietest ways to get in and move around. User and service accounts that are inactive and enabled (aka “ghost users”) are targets for penetration and lateral movement.

Ghost 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 ghost users is a security step organizations often overlook. If these accounts are left unmonitored, attackers can steal data or cause disruption without being detected - placing your organization at risk.


of companies have **over 1,000 stale user accounts**

## STALE USER ACCOUNTS

**34%** of users **are enabled** but **stale**

**64%** of user accounts **are stale**

**65%** of companies have **over 1,000 stale user accounts**


of companies have **over 1,000** enabled but **stale users**

## BEST PRACTICE CHECKLIST

# GHOST IN THE MACHINE

Outdated user permissions and stale accounts are a target for exploitation and malicious use. Most attackers target data, but they reach their target by hijacking accounts.

Users with unnecessary access to sensitive data represent high risk to the company – and stale but enabled accounts are an unnecessary security risk.

Review stale enabled accounts to determine if they are necessary, and delete or disable accounts as needed.

VARONIS

## BEST PRACTICE CHECKLIST

- ☐ 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

## RISK SPOTLIGHT

# TOXIC PERMISSIONS

Access requirements change over time as projects and teams come and go, and users join, change roles, or leave the organization.

It is important to know exactly who uses – and no longer uses – data to be surgical about reducing access without causing any headaches.

VARONIS


of companies have over **10,000 folders** with **unresolved SIDS**


of companies have over **1,000 folders** with **inconsistent permissions**

## DATA AT RISK

**1 TB** contains **84,081 folders**

**1 TB** contains **1.1 million files**

**12%** of a company's folders are **uniquely permissioned**

**10%** of users have removal recommendations, and are likely to have **more access** to data than they require


of a company's folders **are protected** (not inheriting permissions)

## BEST PRACTICE CHECKLIST

# TOXIC PERMISSIONS

The more complex a file system structure, the greater risk for overexposure and security vulnerabilities.

Update data and access in order to maintain a secure environment, ensure resources are used efficiently, and close security loopholes that might otherwise be exploited or become vulnerable to brute-force attacks.

VARONIS

## BEST PRACTICE CHECKLIST

- ☐ Simplify access management procedures and standards help lock down potential exposure of sensitive data from insider threats
- ☐ Decrease the amount of data any compromised account can access, making an attackers' 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 recertify 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

## RISK SPOTLIGHT

# PWNED PASSWORDS

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 rotated also have a higher likelihood of showing up in breached password dumps. Administrative accounts with non-expiring passwords are an attacker's best friend.

The most common reason users change their passwords is because they've forgotten them. Half of people surveyed cited this as the most common reason to change a password. In contrast, despite the increasing amount of hacks in the news cycle, only 1 in 5 Americans said they change their password as a result of a hack in the news.


of companies have over **500** users with passwords that **never expire**

## EXPIRED PASSWORDS

**14%** of enabled users have **expired passwords**

**46%** of companies have over 1,000 users with **passwords** that **never expire**

**65%** of companies have over **500 users** with **passwords** that **never expire**


of users have a password that **never expires**

## BEST PRACTICE CHECKLIST

# PWNED PASSWORDS

IT must disable non-expiring passwords 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.

VARONIS

## BEST PRACTICE CHECKLIST

- ☐ Set expiration dates for user account passwords
- ☐ Enforce password length and complexity requirements
- ☐ Use multi-factor authentication wherever possible
- ☐ Monitor login activity and account lockouts to spot potential attacks
- ☐ Enforce Password History to discourage users from alternating between several common passwords

# 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 DELL EMC TOYOTA LUXEMBOURG INSTITUTE OF HEALTH L'ORÉAL