



5 STEPS TO OFFICE 365 SECURITY WITH VARONIS

Silver
**Microsoft
Partner**

CONTENTS

INTRODUCTION	3
OUTCOME 1: PRIORITIZE RISK AT SCALE	4
OUTCOME 2: REDUCE RISK	7
OUTCOME 3: KEEP THINGS LOCKED DOWN	9
OUTCOME 4: DETECT THREATS	10

OUTCOME 5: INVESTIGATE	13
CONCLUSION	15
START A FREE RISK ASSESSMENT	16
ABOUT VARONIS	17

INTRODUCTION

In today's data-dependent, cloud-enabled world, it's more important than ever to know that critical data is secure, but many organizations struggle to answer important questions about their data, like:

- **Where is sensitive data stored?**
- **Where is it at risk, stale or overexposed?**
- **Who accessed my sensitive data, and who is accessing it now?**
- **How do I reduce risk without breaking anything?**
- **Can I detect threats to my sensitive data, like sophisticated insiders or APT's, and investigate quickly?**

Organizations that can answer these questions are better able to visualize, prioritize and remediate risk, as well as detect and respond to threats quickly and conclusively.

This white paper describes how Varonis and Microsoft help organizations answer these questions and achieve meaningful data protection outcomes.

OUTCOME 1

PRIORITIZE RISK AT SCALE

To quickly quantify and prioritize risk across data stores, most organizations use automated classification. Classification needs to be accurate and quantify the amount of sensitive data in each file – a file with 1,000 personal identifiers inside should not be scored the same as a file with 1.

False positives inflate risk, as they incorrectly indicate the presence of sensitive data; false negatives deflate risk, as they miss instances of valid sensitive data. Varonis' pre-built policies and algorithms find regulated information with very high accuracy. Results show how many matches found in each file and of which types.

Analyze results quickly through the Varonis UI. Rule creation and tuning are easy, and Varonis updates rules regularly to find data subject to new regulations. With accurate classification, organizations can feel confident applying labels and DRM policies through integration with Microsoft Azure Information Protection (AIP).

To prioritize risk, it's also important to quantify risk at the container level (folders, libraries, etc.). Automated classification usually uncovers thousands of sensitive files; many inherit permissions from containers that are accessible to too many people. A poorly restricted folder or library may represent a thousand times more risk than any given file inside it – files may contain hundreds or thousands of sensitive records, but folders, sites and libraries can contain thousands of files.

Varonis combines its accurate classification with permissions and usage analysis to rank folders in terms of risk – where sensitive data is concentrated and exposed at both file and container levels. Varonis identifies and reports on exposure through global groups, external links, and excessive group memberships. Results are available through the UI and out-of-the-box reports.

Once exposures are identified, it's easy to visualize how permissions are applied and inherited up and down the hierarchy. It's also easy to understand usage at the file and container level, which is critical to determine whether data is active and who should take responsibility. Varonis also identifies stale, sensitive data, so organizations can quickly archive, quarantine or delete at-risk files that are no longer needed.

Only Varonis provides both accurate classification and the context required to prioritize risk – Varonis provides this visibility for large, complex hybrid environments. Organizations without Varonis must frequently review thousands of files, one by one, with no prioritization or context about the hierarchy, how permissions are structured, or usage patterns. This makes it impossible to determine the right course of action (e.g. delete, quarantine, restrict) or whom to consult.

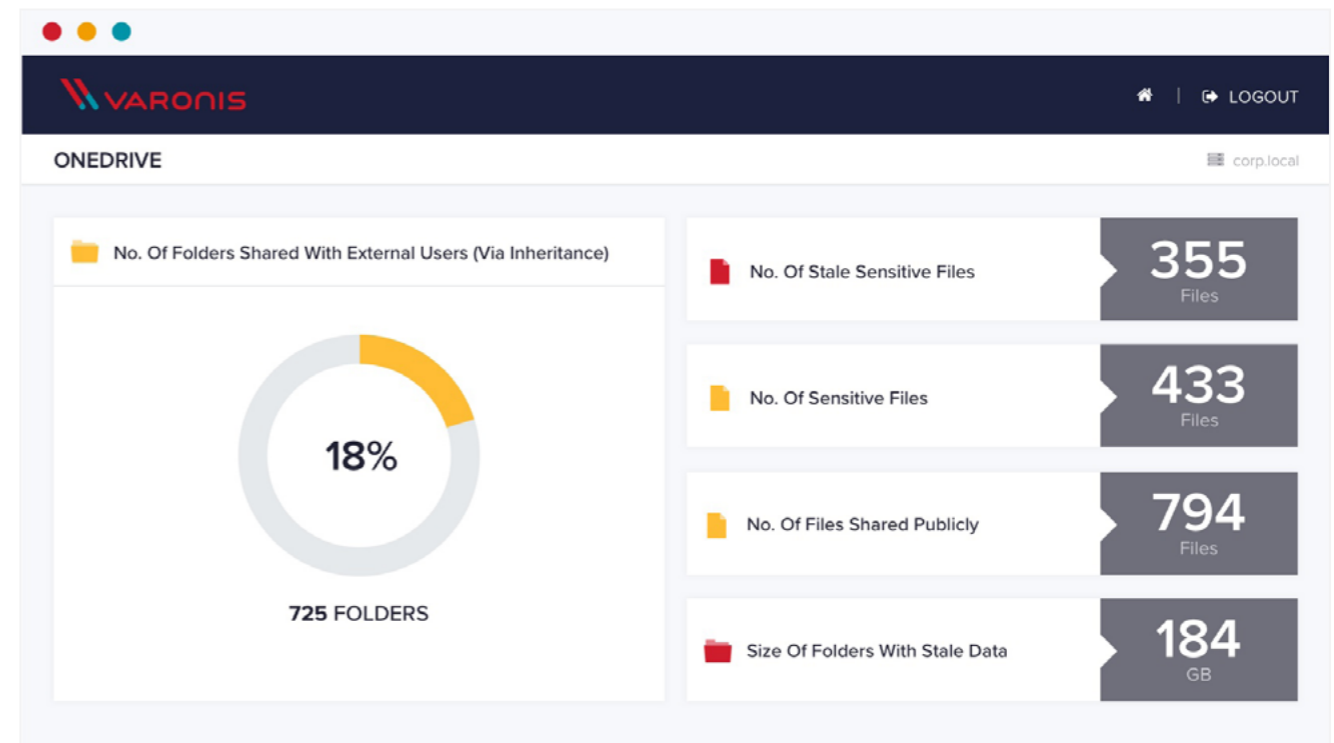
THOSE WONDERFULLY USEFUL AND RISKY LINKS

Sharing files through links has become very popular, but links should be pruned or eliminated regularly when they're no longer needed.

Varonis automatically reports on:

- Externally shared files
- Externally shared files that are stale
- External users with links
- Active external users using links
- Inactive external users that have links

Once risk is visualized and prioritized, remediation can begin. Automation makes remediation realistic.



OUTCOME 2

REDUCE RISK

In order to protect data stored in Office 365, it's important to optimize permissions. Sites and libraries exposed to too many people increase the risks from insider threats and compromised accounts. Permissions should be restricted to those that need access and regularly reviewed by owners or custodians.

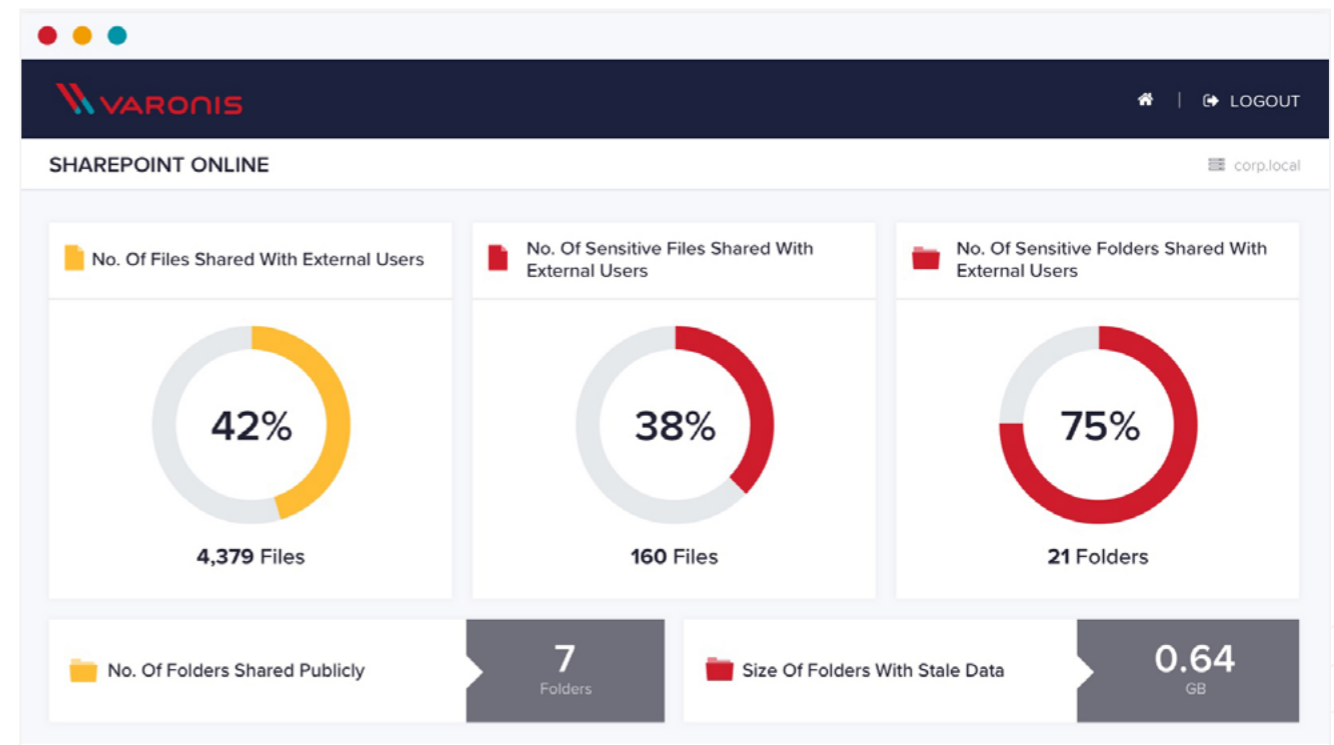
To optimize permissions, it's critical to understand exactly how access controls are applied and effective permissions at all levels of the hierarchy – sites, site collections, lists, folders, libraries, and documents. It's also critical to analyze actual usage – no one wants to risk disrupting workflow.

If you hear a colleague say, **“why don't we just encrypt anything sensitive and restrict it to internal users,”** first, take a deep breath, then remind them:

- The principle of least privilege is still pretty important
- Relying on one kind of control is typically a bad idea
- Oh yeah, insider threats
- Lots of data that doesn't necessarily match a classification rule still deserves protection. (See OPM as a case study in how to underestimate the importance of non-classified data).

The most efficient way to right size permissions is to simulate changes prior to making them, to ensure no users or processes will be disrupted. Test a change in Varonis' sandbox to see users that have been using data with the permissions you're hoping to remove. Once you know who needs access, make sure they keep it -- create a new group or add them to an existing one, and then make your changes. Varonis calculates dependencies to prevent issues, logs and reports on changes and errors, and provides unlimited rollback.

It's also important to remove stale links and access control entries. Varonis automatically reports on stale external links. When users share files internally, users receive permissions to relevant files or containers. Varonis reports on permissions that include user ACE's, local groups, and domain groups. Its patented recommendations engine highlights domain group members that can be safely removed.



OUTCOME 3

KEEP THINGS LOCKED DOWN

Without processes and automation to keep permissions up to date, organizations will find that they quickly drift back into chaos. Office 365 makes it easy for users to share links and request access, but it's difficult for owners to see holistic views about the data they manage. Organizations that regularly provide the right information to data owners keep data more secure and improve efficiency at the same time.

Varonis makes it easy for owners stay in control. Varonis identifies and tracks owners, and there's no need to configure or update hundreds of report subscriptions. Data owners can receive any of our out-of-the-box reports about their data, automatically, so they'll know who has access, who uses it, who doesn't use it, what's sensitive and what's stale. Varonis uses analytics to highlight users that have more access than they require. Automate permissions and group changes based on owner feedback via the Varonis commit engine API.

OUTCOME 4

DETECT THREATS – INSIDERS, OUTSIDE ATTACKERS, MALWARE

Detecting access to an unusual amount of data is important; detecting unusual access to sensitive data is critical. Most organizations don't have visibility into what users are doing with which kinds of data or which mailboxes, which devices they're using, and where they connect with them for even a single data store – much less for complex, hybrid environments with many data stores. Even if an organization manages to collect access activity, classify data, or map permissions, that information is almost never correlated or analyzed together.

Without correlating different streams of metadata, security analysts receive many low-fidelity alerts, and must spend hours building context – determining who the user is, whether this is normal behavior, and whether any important data is involved. This increases an organizations "time to detect" a threat, and increases security operations overhead.

For example, if a security analyst receives an alert about unusual access to data, they must answer a series of questions:

- **What is the users' role?**
- **Is the activity coming from their normal work locations, during normal hours?**
- **Was any important data taken?**

Without correlating sensitivity with activity, the analyst must export a list of all files accessed and then cross-reference it with a list of sensitive files in order to answer that question. If classification data is inaccurate or doesn't indicate the amount of sensitive data concerned, the investigation is inconclusive. If an analyst receives several alerts that require this kind of investigation, they lose far too much time.

In another example, many attacks now begin with cloud infrastructure, and then move into on-premises infrastructure, or vice-versa. In these cases, when an analyst receives an alert, they must answer questions to follow a long, complex trail:

- **From where (in the physical world) did the user log in?**
- **How did they authenticate?**
- **Did they authenticate to on-premises Active Directory or Azure AD?**
- **Did they access mailboxes that they don't normally access?**
- **Were attachments sent inside or out?**
- **Are there other alerts or abnormal behaviors associated with the devices or systems they accessed?**
- **Was any sensitive data accessed?**
- **Did the behavior look human or automated?**

Varonis uses machine learning to profile each user's role, what sensitive data they touch and how much, whose mail they normally read, from where they authenticate and more. With "peace-time profiles" that analyze usage over hours, days & weeks, Varonis detects and accurately highlight threats like employees accessing or sharing unusual amounts of sensitive data, accessing unusual mailboxes, or working from abnormal locations, at unusual hours. Varonis detects threats with out-of-the-box threat models.



Varonis customers quickly identify and analyze things like:

- **Service Accounts are accessing sensitive information in Office 365 or on-premises data stores**
- **An unusual amount of sensitive information being accessed right before a large upload to the internet**
- **Attackers accessing sensitive data and then exfiltrating it over DNS**

On Gartner Peer Insights for User & Entity Behavior Analytics, Varonis has more 5-star reviews than any vendor has reviews. Customers can send Varonis alerts to Azure Sentinel or SIEM.

-

OUTCOME 5

INVESTIGATE QUICKLY AND CONCLUSIVELY

When you suspect a threat, there's no time to waste.

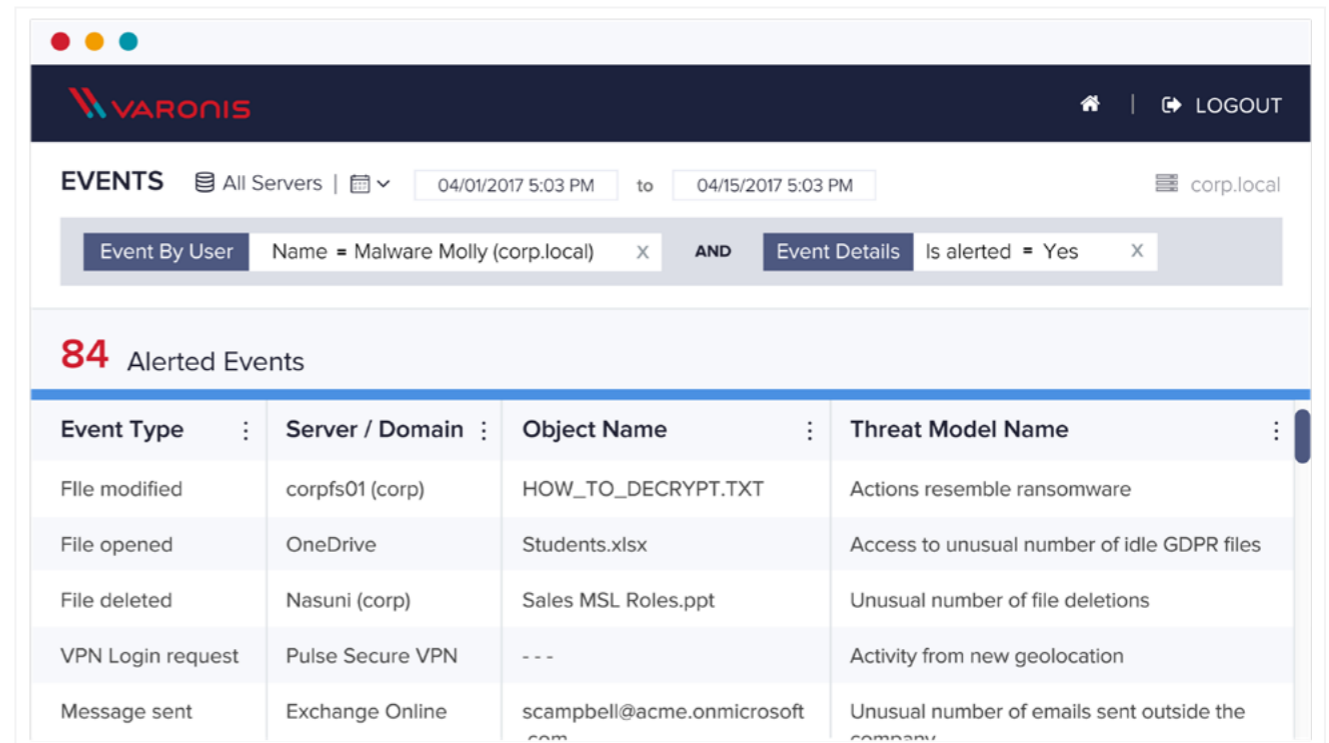
Varonis automatically compiles what security analysts need to investigate, highlights the users role and whether sensitive data is involved, and what's normal or not.

- **Is this their normal device?**
- **Their normal data patterns, their normal location, normal working hours?**
- **Any other alerts associated with the user or device?**
- **Is the user a privileged account?**
- **Are they already on a watch list?**

Other auditing solutions lack flexible search, query and export functionality, hampering investigations. Analysts struggle to combine information from cloud and on-premises data stores, Active Directory and perimeter devices. Without correlating access patterns and sensitivity, it is very difficult to determine whether important data was accessed inappropriately, and uncover the phases of an attack.

Varonis allows security analysts to perform advanced reporting and search activity by any user through cloud and on-premises data stores and in Active Directory, see what queries and connections their device made, and filter on data sensitivity and other dimensions.

The events in Varonis Data Security Platform are automatically resolved and cleaned up: a user accessing a file over several hours (because they have it open on their desktop) is one row, VPN login is one row, a modification to a GPO in Active Directory shows the settings both before and after the change. The Varonis UI has powerful query, search and drill down functions that make investigations fast and conclusive. There's no quicker way to understand if, when and how an insider or attacker that got in accessed and stole sensitive data.



The screenshot displays the Varonis Events management interface. At the top, there's a navigation bar with the Varonis logo and a 'LOGOUT' button. Below this, the 'EVENTS' section shows filters for 'All Servers', a date range from '04/01/2017 5:03 PM' to '04/15/2017 5:03 PM', and a domain filter 'corp.local'. A search bar contains two filters: 'Event By User' with 'Name = Malware Molly (corp.local)' and 'Event Details' with 'Is alerted = Yes'. Below the filters, a summary indicates '84 Alerted Events'. The main content is a table with the following columns: Event Type, Server / Domain, Object Name, and Threat Model Name. The table lists several events, including file modifications, file openings, file deletions, VPN login requests, and message sends, each with associated server/domain, object name, and a descriptive threat model name.

Event Type	Server / Domain	Object Name	Threat Model Name
File modified	corpfs01 (corp)	HOW_TO_DECRYPT.TXT	Actions resemble ransomware
File opened	OneDrive	Students.xlsx	Access to unusual number of idle GDPR files
File deleted	Nasuni (corp)	Sales MSL Roles.ppt	Unusual number of file deletions
VPN Login request	Pulse Secure VPN	- - -	Activity from new geolocation
Message sent	Exchange Online	scampbell@acme.onmicrosoft.com	Unusual number of emails sent outside the company

CONCLUSION

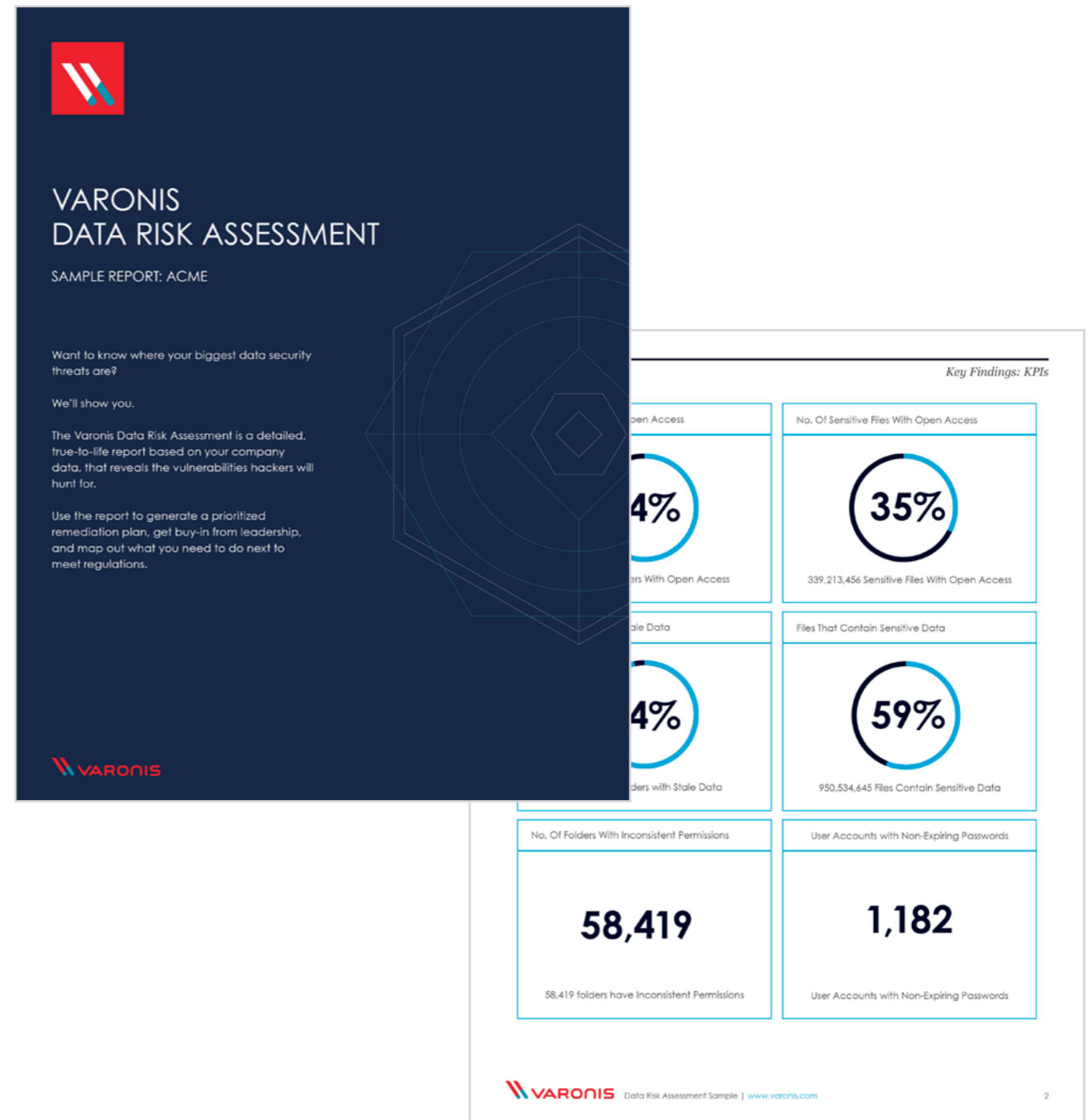
Thousands of customers rely on Varonis to protect their on-premises and cloud data in Microsoft environments. Organizations are free to choose where to store their data without losing control. They get the benefits and flexibility of cloud and hybrid infrastructures without settling for disconnected security solutions.

Varonis has a proven, outcome-focused methodology that starts with helping organizations see and prioritize their risk through a free data risk assessment. Varonis deploys within hours on physical or virtual servers, in the cloud or on premises.

With visibility into on-premises and cloud data stores, Active Directory and perimeter devices, Varonis helps initiate and automate remediation and transformation projects to get data under control quickly. At the same time, Varonis automatically begins to build a baseline, or “peace-time profiles” over hours, days and weeks for every user and device, so when they start behaving strangely they get noticed.

START A FREE RISK ASSESSMENT TODAY, AND SEE HOW QUICKLY YOU CAN

- Prioritize risk on files and containers by analyzing permissions exposure, and content
- Classify data accurately with very few false positives or false negatives
- Remediate risk quickly and safely with automation that simulates changes, measures their impact and commits them
- Keep risk levels low with easily scheduled reports for data owners and automated cleanup
- Detect threats quickly with best-of-breed, behavior-based threat models that analyze activity, classification, Active Directory, and much more
- Investigate threats quickly and conclusively with pre-built context and advanced event search that answers the most important questions.



ABOUT VARONIS

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and, as of December 31, 2018, had approximately 6,600 customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.

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