



# How Varonis & Nth Generation Help a Services Company Put Their Data First

---



Varonis is a very powerful solution. When you dig into the reporting, automation, and all of its other capabilities, the sky's the limit.

## About this case study:

Our customer is a services provider. We have happily accommodated their request for anonymity.



## Highlights

### Challenges

- Eliminating overexposed data on-prem and in OneDrive
- Reducing the risk of CCPA regulatory fines
- Detecting and responding to ransomware, insider threats, and APTs

### Solution

#### Nth Generation

- Serves as a key partner, providing strategic advice, expertise, and support

#### Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over critical data and hybrid IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **Policy Pack** enhances Data Classification Engine with CCPA and GDPR patterns
- **Automation Engine** automatically repairs and maintains file system permissions
- **Data Transport Engine** enforces rules for data movement and migration
- **DatAlert** monitors and alerts on abnormal behavior on critical systems

### Results

- Eliminated data leakage in their hybrid environment
- Achieved ISO 27001 certification
- Gained robust alerting to investigate potential threats

## Challenges

### Reducing overexposure of PII and sensitive data

A services provider (anonymous by request) adopted Varonis to mature their data security in three major areas:

#### 1. Data protection

With decades of file shares in unstructured repositories, both on-premises and cloud-based, it had become impossible to manage or hunt down sensitive data manually.

The services provider needed a way to find and classify Personal Identifiable Information (PII), automated clearinghouse (ACH) data, and other sensitive information related to payroll processing.

One Systems Administrator explains:



**“Our first use case was data classification in Windows, NetApp, Microsoft 365, OneDrive, and SharePoint. We needed Varonis to scan those assets and look for sensitive data.”**

#### 2. Privacy and compliance

A lack of visibility into sensitive data increased the risk of non-compliance fines from the California Consumer Privacy Act (CCPA) and other regulations. The company needed to tighten their data security strategy and then enforce data retention and storage best practices.

### 3. Threat detection and response

Protecting data against insider threats and ransomware is always top of mind. One of the company's top priorities was gaining high-fidelity alerting on potential threats and the ability to quickly lock down compromised accounts.

**“With ransomware, damage happens quickly. So you need automated processes to monitor and manage the threat. Human intervention is fantastic but the more you can automate, the better.”**

# Solution

## Reliable support for the first line of defense

The services provider was first introduced to Varonis through its partner, [Nth Generation](#).

Nth Generation is an industry-leading consultative IT and cybersecurity service and solutions provider. Through the [Varonis Partner Program \(VPP\)](#), they're equipped to help the company with any Varonis-related needs. They also can help serve as the first line of support in the event of an attack.



**“Nth Generation is fantastic. They’re always supporting us and always checking in. They brought Varonis to us and any time we have any obstacles or need a new upgrade, they contact Varonis on our behalf.”**

Both Nth Generation and Varonis are committed to helping the company get the most out of every Varonis product.



**“We’ve also dealt with the Varonis support team who have, frankly, all been awesome. Our rep checks in bi-weekly.”**

## 360° visibility into on-prem and cloud file shares

With Varonis in place, the company's first priority was locking down sensitive data on-prem and in Microsoft 365. Three Varonis solutions help them enforce good data governance policies and facilitate compliance.

- **DatAdvantage** for Windows, Directory Services, SharePoint Online, and OneDrive to map data access activity across file and email systems.
- **Data Classification Engine** to find sensitive data stored on-premises and in Microsoft 365.
- **Policy Pack** to enhance Data Classification Engine with CCPA and GDPR patterns.



“The visibility in terms of the sheer amount of data we had and where it lived was eye-opening. It painted a clear picture of where we needed to focus first. And because Varonis ties into Active Directory, it gives us the ability to lock down those file shares based on AD groups.”

## Putting data first via automation

The company wanted to drive digital transformation, so they also purchased solutions to automate permissions clean-up and auto-enforce data governance policies.

- **Automation Engine** to remediate open access across corporate file systems.
- **Data Transport Engine** to create custom automation rules for data retention and other security and privacy policies.



“Automation Engine is critical in the first phase of remediation. It’s very difficult to clean up overexposure without it. There’s so much business use of legacy file shares that if we break something, we break the business.”


## Advanced threat detection and response

The company then made one final purchase to proactively safeguard their data against the growing threat of ransomware. That’s why they purchased:

- **DatAlert** to monitor and alert on file and email systems for abnormal user behavior indicative of a potential threat.



“DatAlert truly complements the other tools we use for monitoring security incidents by monitoring user analytics and behavioral anomalies and tying them to our data. Having high-fidelity alerts that enable us to investigate risks was definitely exciting for stakeholders.”



**“Automation Engine is critical in the first phase of remediation. It is very difficult to clean up overexposure without it ... if we break something, we break the business.”**

# Results

## Sensitive data locked down

With Varonis, the services provider cleaned up their permissions and locked down their sensitive data. Now, Varonis automation enables the company to reinforce best practices as they continue to scale, which is a crucial step for achieving and maintaining compliance.



**“We’re ISO 27001 certified and a big part of that is data classification and governance of sensitive data. That’s where Varonis has been helpful—its reports allow us to show auditors what we’re doing to mature our environment.”**

Varonis helps protect the company’s on-prem and cloud assets. The expert advice of Varonis and Nth Generation is helping them maximize the value of each product.

Next, they plan to explore options like DatAdvantage Cloud, which will help strengthen the security of SaaS data stored in apps like Salesforce, AWS, and Box.




**“The key for us right now is to ensure that we have complete protection on-prem—no data leakage. Varonis is a very powerful solution. When you dig into the reporting, automation, and all of its other capabilities, the sky’s the limit.”**

As for the ever-present threat of ransomware, Varonis’ advanced threat detection and response capabilities have given stakeholders peace of mind.



**“Over the last nine months, our network engineers have gotten much more involved. They’re now writing and leveraging some of the automation toolchains so that when we get an alert, it automatically kicks off a response to disable the account and stop the attack.”**



**“We’re ISO 27001 certified and a big part of that is data classification and governance of sensitive data. That’s where Varonis has been helpful.”**





**Varonis helps you put  
your data first.**

[Request a demo](#)