Varonis Powers Saia's Data Governance Transformation

> The confidence that I have in Varonis' data classification and its ability to recognize sensitive data is outstanding.

HIGHLIGHTS

Challenges

- Legacy data overload
- Remediating overexposed and over-permissive data
- Understanding data ahead of a major cloud migration

Solution

The Varonis Data Security Platform:

- Provides complete visibility and control over critical data in cloud, SaaS, and hybrid environments
- Discovers and classifies sensitive data automatically
- Right-sizes and maintains file system permissions
- Monitors and alerts on abnormal behavior or suspicious activity

Varonis Managed Data Detection and Response (MDDR):

- Provides 24x7x365 service dedicated to stopping threats at the data level

Results

- Risk reduction and cost savings
- Visibility into exposed sensitive data
- Varonis MDDR as a first line of defense
- Automated data security outcomes

CHALLENGES

Tackling legacy data and permissions

Saia is a leading freight and logistics company specializing in less-than-truckload (LTL) shipping. The company manages a significant volume of sensitive data and sought to improve its data governance and security.

Julia Bruce, the Identity and Data Governance Manager at Saia, was brought in to build and lead the company's data governance program. But it would be no easy task: the company faced the challenge of managing decades of legacy data stored on on-prem file servers.

> **"We had over 20 years of legacy data that we had just been holding on to because we thought we might need it for a rainy day. Permissions had never really been managed."**

Like many companies, Saia lacked visibility into their data, and no system was in place to monitor or control access. This posed a significant security risk if a bad actor logged in using stolen credentials.

> **"We had no idea where our sensitive data was, how much of it there was, or who had access to it."**

The company needed to move a large amount of data from on-prem servers to SharePoint Online and OneDrive. The migration was the perfect opportunity to review and clean up their legacy data, reduce their IT storage costs, and improve their data security posture.

> “With other tools, there’s going to be a ton of time that you’ll need to invest tuning it to make sure that a social security number is really a social security number, but with Varonis, you don’t have to do that.”

SOLUTION

Gaining control of data with Varonis

Saia chose Varonis to get a handle on their data. The unified Data Security Platform automatically classifies information, flags sensitive and exposed data, fixes risky misconfigurations, and alerts Saia to suspicious activities.

According to Julia:

> **"Varonis was up and running in no time. We had data and were collecting events. It was a piece of cake."**

Varonis' data classification worked perfectly from the start, Julia said, saving time by flagging millions of sensitive data hits.

> **"With Varonis, we've been able to review over three terabytes of data stored on our on-premise file servers and reduce the risk of around 30 million hits of sensitive data."**
>
> **"We're using Varonis to monitor our on-prem resources and enforce our retention policy. Out of the box, the data classification engine is fantastic — it's incredibly accurate."**
>
> **"With other tools, there's going to be a ton of time that you'll need to invest tuning it to make sure that a social security number is really a social security number, but with Varonis, you don't have to do that."**

Varonis Managed Data Detection and Response

Saia's MDR vendor offered insight into location-based threats but lacked a more comprehensive approach to data. According to Julia:

> **"We had an MDR, but they focused on authentication and geolocation. There wasn't a focus on data. We'd get alerts around 'anyone' links for SharePoint Online, but that's really it as far as the 365 environment goes."**

The company's in-house cybersecurity team turned to Varonis for 24x7x365 support from Varonis' Managed Data Detection and Response (MDDR) team, the managed service dedicated to stopping threats at the data level.

MDDR offers the industry's best SLA, with a 30-minute response for ransomware attacks and a 120-minute response for all other alerts.

> "The visibility that Varonis has given us has empowered the business to make decisions about their data. With Varonis, I know we'll be in a good place."

RESULTS

Improved data access governance

Varonis provided the tools needed to manage data access effectively and enforce retention policies. Saia can also ensure that the sharing links users create don't get out of hand. Julia said:

> **"With Varonis, we were able to create policies to remove any link that hadn't been accessed in over a year, all without impacting the business. That's a big win."**

Unprecedented visibility into enterprise data

Varonis provided the visibility needed to understand where sensitive data was located, who had access to it, and who was using it. Now, Julia and her team can make informed decisions about their data management.

> **"Varonis has come in, and they've given us visibility into where all of our sensitive data is located, who has access to it, and who is using it. They then made recommendations for what we should do with it."**

Varonis enabled Julia's team to save substantial data storage costs for Saia because they didn't have to migrate 20 years of data to the cloud.

> **"We were able to quickly determine what data we needed to keep, what data we'd like to keep, and what data we could get rid of."**
>
> **"The visibility that Varonis has given us has empowered the business to make decisions about their data. With Varonis, I know we'll be able to review permissions and make sure we're in a good place."**

Your data. Our mission.

Varonis right-sizes permissions, finds and remediates exposed sensitive data, and detects abnormal behavior in hybrid environments in cloud, SaaS, and hybrid environments.

Request a demo