VARONIS

How Bradshaw International Reined in Permissions and Reduced Their M365 Blast Radius With Varonis

> “In the event of data exfiltration, we could stop the breach, trace back the activity, and identify the exact files that were compromised, regardless of the technology used. That’s the power of Varonis.”

HIGHLIGHTS

Challenges

- Lack of visibility into user activity
- Difficulty identifying overexposed data
- Excessive user permissions
- Noncompliance with the CIS framework

Solution

The Varonis Data Security Platform:

- Provides visibility and control across M365
- Continuously discovers and classifies critical data within M365
- Locks down permissions and prevents exposures
- Proactively detects and helps prevent threats
- Right-sizes permissions to achieve least privilege

Results

- Real-time alerting and increased visibility
- Proactive threat detection and investigation
- Compliance with CIS Critical Security Controls
- Minimized blast radius across the environment

CHALLENGES

Excessive permissions and limited visibility

Since 1905, leading food service equipment manufacturer Bradshaw International built their reputation as a reliable, adaptable partner for retailers. This requires them to stay ahead of trends, anticipate market shifts, and design products with the consumer at the forefront.

The company offers products in over 50,000 retail locations in the U.S. and Canada, including Amazon, Walmart, Target, and Costco. To support their retail partners and ensure data security, the organization aimed to align with the CIS Critical Security Controls framework. However, once they began the initiative, they realized they needed a comprehensive tool for the job.

Brian Foster, the Vice President of Information Technology, said:

> **"There are multiple controls inside of the CIS Standards that you're supposed to have in place, and we didn't have a single tool to achieve those."**

Additionally, over the past several decades, the organization has grown rapidly, leading to increased — and untamed — permissions.

> **"I've been with Bradshaw International for over 25 years and can tell you that we've evolved over time where permissions had been added at the root level, department level, and inside department controls. It was almost impossible to understand who has access to what data."**

The company turned to Varonis to increase their visibility.

> **"We did a Varonis proof of concept, and it opened our eyes to how much data and access was given to the organization as a whole."**

SOLUTION

Establishing role-based access

Bradshaw International began using Varonis to identify and understand the sensitive data stored in the cloud. Upon implementation, Brian soon realized that the Data Security Platform also enabled his team to monitor data access permissions and subsequently restrict access based on roles.

> **"Once we installed Varonis, it allowed my cyber team first to understand who had access to sensitive data and then create roles within Varonis to limit the ability for users to access the data. That way, the access was role-based rather than having individuals assigned to directories and files."**
>
> **"This allowed us to remove the 'all' role, ensuring that data was not accessible to everyone simply through domain user status. With Varonis, if privileged information was present, we locked down access to only the groups who needed it."**

Identifying suspicious user activity

Bradshaw International had a point tool monitoring external data transfers, but it only detected potential PII data loss, not all data types.

In contrast, Varonis' advanced behavioral alerts notify organizations of suspicious activity at every stage of a potential data breach, from reconnaissance to data exfiltration, and identify precisely what data has been accessed.

When an employee leaving the company exfiltrated data outside the organization, Varonis' Proactive Incident Response team identified what data was accessed, by whom, and how the data was handled.

> **"One of our C-level employees gave their notice, and we noticed data being copied from our drives to a Gmail account. We were able to use Varonis to go back in time and see what files were accessed, copied to their computer, or copied directly out to the Gmail account that wasn't caught through our DLP tool."**

Locking down Microsoft 365

Bradshaw International relied on Microsoft Teams to boost collaboration within the organization, Brian said.

> **"When we launched Teams, our goal was to promote Team meetings, teach channel creation and information storage, and highlight the benefits of sharing content in meetings."**

However, with the rise in productivity comes an increase in associated risks.

> **"We empowered users to have the tools for collaboration, not realizing that this setup could inadvertently grant access beyond the intended participants if misconfigured. Varonis identified how much data was open in SharePoint or Teams that we didn't know was open to the world."**
>
> **"Varonis gave us the ability to understand our data in Teams and OneDrive."**

Brian said that despite only having Microsoft Teams for a few years, Bradshaw International had accumulated a massive amount of data and the company needed increased visibility and control of that data.

> **"We have a substantial amount of information left accessible not only to the entire organization but also to any external guests added to our tenant. Within the first couple of days after the Varonis installation, we could lock that data down."**

Additionally, Varonis' automation helps enforce Bradshaw International's data security policies, simplifying the process for Brian's team and significantly reducing their workload.

> **"Without Varonis' automation, manually searching through directory after directory on Teams would have taken us all year."**

“Without Varonis’ automation, manually searching through directory after directory on Teams would have taken us all year.”

RESULTS

Reducing their M365 blast radius

With Varonis' unified Data Security Platform, Bradshaw International can reduce their blast radius, or the amount of damage that can be caused by a single compromised user or device, without disrupting the business.

> **"The less data you have that threat actors can get to, the better off you are. Especially when it comes to stale data, as it often contains old PII and information that must be disclosed in the event of a breach. Varonis identifies stale data by generating reports to examine the last time data was accessed."**

Varonis is an integral partner

Brian relies on Varonis for additional support when his cybersecurity staff is stretched thin.

> **"Varonis is an extension of the team. Knowing you can rely on their dedicated expertise with just one phone call gives you a sense of security that you're not alone in this — that it's not up to you. And when I say dedicated, they're dedicated four to eight hours a day, trying to help understand what happened with no questions asked."**

Varonis' Proactive Incident Response team provides real-time alert monitoring and threat investigation — something Brian finds invaluable.

> **"In the event of data exfiltration, we could stop the breach, trace back the activity, and identify the exact files that were compromised, regardless of the technology they used. This capability can significantly save our organization time and resources. That's the power of Varonis."**

Your Data. Our Mission.

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

Request a demo