# How a U.S. Government Agency Uses Varonis to Secure CUI in a Large Hybrid Environment

> “Sometimes you get an application, deploy it, and then come back to it a few years later and realize it’s not doing what you think it’s doing. I don’t see that at all with the support we get from the Varonis team.”

**About this case study:**

Our customer is a U.S. government agency. We have happily accommodated their request to anonymize all names and places.

# HIGHLIGHTS

## Challenges

- Protecting sensitive PII and mission-critical data from nefarious insiders and external actors
- Complying with Controlled Unclassified Information (CUI) mandates
- Expanding protection from an on-prem system to a hybrid environment

## Solution

**The Varonis Data Security Platform:**

- Discovers and locks down sensitive data in Microsoft 365 and on-prem automatically
- Monitors and notifies of abnormal behavior in critical systems
- Makes ongoing compliance with CUI mandates easy

## Results

- Days saved with every security incident
- Better security at lower costs
- Confidence to take on more sensitive projects in a hybrid environment

# CHALLENGES

## Protecting mission-critical data from exposure, alteration, and exfiltration

The cybersecurity manager at a U.S. government agency worried about users inadvertently opening the door to nefarious internal or external actors.

> **“Sooner or later, a user is going to click on a link and unknowingly launch something that’s going to propagate throughout your network.”**

The agency is responsible for protecting its PII and sensitive mission-critical data. An insider with bad intentions or external actors could potentially expose, alter, or exfiltrate this information.

The agency is also subject to the federal government’s Controlled Unclassified Information (CUI) mandate. This mandate standardizes the protections and practices of unclassified information (information that requires safeguarding or dissemination controls but is not classified across departments and agencies.

At first, the agency created PowerShell scripts in-house in an effort to automate security checks.

They soon realized they needed more visibility into where their sensitive information was located, especially as they moved to the cloud.

According to the cybersecurity manager:

> **“We were blind in a couple of areas, especially when it came to SharePoint.”**

The PowerShell scripts were also time-intensive to create and difficult to keep up to date.

> **“Policy changes would immediately trigger more development work and the time we needed to spend doing that work.”**

The more the agency moved beyond its on-prem Windows system to Microsoft 365 (including SharePoint Online, Exchange Online, and OneDrive), the clearer it became that they needed a different approach.

That’s when they turned to Varonis.

# SOLUTION

## Automatically classify and lock down data in a hybrid environment

Once the agency installed Varonis, the Data Security Posture Management (DSPM) solution started to automatically inventory all data and identify where sensitive information was overexposed in Microsoft 365. Varonis also uncovered and flagged risky misconfigurations in Active Directory and Entra ID.

The cybersecurity manager was surprised at how easily and quickly Varonis uncovered risk — with little human intervention.

> **“I didn’t think that Varonis could pick up on our CUI tagging and labeling — it was a nice bonus that I didn’t expect.”**

## Automatic CUI compliance

Varonis worked closely with the cybersecurity manager to help the agency with the CUI mandate. Varonis has hundreds of auto-updating policies to discover and lock down CUI and PII information automatically.

> **“The Varonis team walked us through the product to help us understand how the policies work, where the policies come from and what they mean, and how we can carve out the stuff that wasn’t of value to us and focus on what we actually needed for our information and alerting.”**

When mandates are updated or new regulations are applied, Varonis makes it easy to maintain compliance.

> **“CUI mandates change and evolve through time. Varonis already did the legwork to develop policies based on the mandates and laws. That accelerated things quite a bit.**
>
> **When you use Varonis, it’s just a matter of adding the policy to the alert system. That saves us quite a bit of time and effort.”**

## Flagging suspicious activity

With these protections in place, suspicious activity is automatically detected and flagged to the cybersecurity manager. In a recent example, someone tried to log in and access files from 10 different IPs within a few minutes. Varonis automatically notified the cybersecurity manager of the suspicious activity.

As it turns out, it was an authorized user struggling with their VPN.

> **“Fortunately, it wasn’t a security incident, and Varonis helped us figure out how to help the end user.”**

Varonis also flags overexposed data. The cybersecurity manager provides an example:

> **“When someone publishes a paper, they may put it in SharePoint and share it with everybody. When Varonis alerts us, we can take a look and see if it should be shared with everyone or if we can trim the sharing list to a domain or something like that.”**
>
> **“Varonis tells us when anything weird or unsual happens. If someone is compromised, we get alerts about accessing stale files or an abnormal amount of files. Or if they are trying to access to something that they shouldn’t. That alerting has benefited us.”**

# RESULTS

## Saving days per security incident

With Varonis, the cybersecurity manager’s team saves days with every security incident.

> **“Without Varonis, we would probably have to dedicate a full-time equivalent to keep up with alerts. We’d also lose days nailing down the blast radius of an attack if something did happen — as opposed to Varonis saying, ‘Here’s what they accessed in SharePoint.’”**

## Better security at lower costs

The cybersecurity manager notes that if the agency had stayed with their in-house PowerShell scripts, the costs would have been higher — and the level of security lower.

> **“The money we put toward Varonis saves us in other areas. We’re not rolling out our own product or sticking in another monitoring tool that may or may not be as broad or deep as Varonis.”**

## Ongoing commitment and support

The cybersecurity manager has been particularly impressed with Varonis’ commitment to ensuring the agency gets everything it needs from the DSPM solution. The manager explains:

> **“In my experience, sometimes you get an application, you deploy it, and everybody goes home. You don’t touch it for a couple years, and then when you come back to it, you realize it’s not doing what you think it’s doing for you.”**

Fortunately, that is not the case with Varonis.

> **“We’re using the Varonis platform and getting the support we need from the Varonis team. It’s worth it to try to get a sense of what the Varonis platform can bring to the table — in addition to the support you receive from the team itself.”**

## Confidence for the future

Today, the cybersecurity manager feels good about the security of the agency’s large hybrid environment, which is important as they embark on advanced projects.

The cybersecurity manager is also leading an initiative to implement Zero-Trust architecture at the agency, and they see Varonis playing an important role in that implementation.

> **“We’re looking forward to Varonis giving us the capacity for enhanced monitoring without having to buy a case of TUMS® every day.**
>
> **I expect to use Varonis heavily to support the security requirements surrounding the data pillar of Zero Trust.”**

**“Without Varonis, we would probably have to dedicate a full-time equivalent to keep up with alerts.”**

“We’re looking forward to Varonis giving us the capacity for enhanced monitoring without having to buy a case of TUMS® every day.”

# Your Data. Our Mission.

Varonis protects your mission-critical data wherever it lives.

Request a demo