How a U.S. Aerospace Contractor Achieves CMMC Compliance with Varonis

CASE STUDY

“Varonis reduces labor for our IT team and cost for our company. It checks so many boxes when it comes to CMMC compliance. It just does so much in one package.”

ABOUT THIS CASE STUDY:

Our client is a U.S.-based aerospace contractor. We have happily accommodated their request for anonymity.

HIGHLIGHTS

CHALLENGES

- Achieving the highest levels of CMMC compliance
- Gaining visibility into Active Directory and on-prem data stores
- Locking down sensitive data including CUI protected under federal regulations

SOLUTION

Varonis Data Security Platform:

- **DatAdvantage** gives complete visibility and control over your critical data and IT infrastructure
- **Data Classification Engine** finds and classifies sensitive data automatically
- **Federal Policy Pack** uses pre-built patterns to identify top secret, secret, and confidential documents
- **Automation Engine** safely automates large-scale permission remediation projects
- **DatAlert** monitors and alerts on abnormal behavior on critical systems
- **Edge** detects and helps prevent threats on the perimeter like DNS exfiltration attempts

RESULTS

Within three hours:

- Open access on sensitive files reduced by 95%
- Total folders with open access reduced by 90%
- Folders with broken permissions reduced by 53%

Challenges

Achieving the highest levels of CMMC compliance

A large U.S.-based aerospace contractor (anonymous by request) with hundreds of employees nationwide is taking steps to protect its data and enforce privacy and compliance.

As a senior systems administrator explains:

> "As a government contractor, we're required to meet new CMMC and NIST 800-171 cybersecurity requirements to continue to do business with the government."

By 2026, CMMC, or Cybersecurity Maturity Model Certification, will be required of all primary contractors who engage directly with the Department of Defense and subcontractors who work through those primary contractors to execute contracts.

This contractor is aiming for the highest levels of cybersecurity maturity—a Level 4 or 5 certification. To achieve that, they need to demonstrate that they have the requisite controls in place, visibility into their data stores, sensitive data locked down, and the ability to stop threats to Controlled Unclassified Information (CUI).

Trying to do all of that manually is a colossal undertaking.

> “CMMC compliance is a big pill to swallow. There are so many controls that you have to adhere to. It’s overwhelming for a small team of systems administrators, especially if it’s being implemented manually.”

So, when the contractor had an opportunity to demo Varonis, they leaped at the chance to check the cyber hygiene of their environment.

> “Before Varonis, we didn’t have a tool in place that would, at a glance, give us an understanding of who had access to what.”

“CMMC compliance is a big pill to swallow. There are so many different controls that you have to adhere to. It’s overwhelming for a small team of system administrators, especially if it’s being implemented manually.”

Solution

NIAP-certified data security platform

The Varonis POC was “eye-opening,” says the SysAdmin. It provided an unprecedented level of visibility into the contractor’s environment that they’d previously lacked.

> “We thought we had a good handle on our file shares, but we were managing them manually. On day one, Varonis showed us that we had a finance directory open to everyone at our corporate office. Then it allowed us to act immediately to get those files secured.”

All of the financial records in that directory, including sensitive information like PII, were open to everyone in the office. Fortunately, Varonis made it easy to discover the exposed data and lock it down with the click of a button.

The POC proved that even the best manual efforts have blind spots and convinced the contractor to fully implement Varonis.

With the **Varonis Data Security Platform**, the contractor has the means to reduce data risk and exposure, protect CUI and other sensitive data, enforce compliance, and alert on threats.

The solutions that make this possible:

1. **DatAdvantage** for Windows and Directory Services provides visibility into Active Directory and monitored platforms—over 1 million folders and 10 million files totaling more than 10 TB of data.
2. **Data Classification Engine + Federal Policy Pack** help the company identify and find sensitive data across data stores in compliance with CMMC, Defense Federal Acquisition Regulation Supplement (DFARS), and International Traffic in Arms Regulations (ITAR) requirements.

For example, the contractor uses a standardized disclaimer at the bottom of every proposal that dictates how the government can use the information. Varonis uses that information in its search parameters to locate and tag contract proposal documentation, locating files even if they have non-standard contract or proposal numbers.

> “Varonis was able to go out and tag every file that contained that disclaimer. It actually found some things that weren’t even in the right directories, which allowed us to clean up those directories and move the data where it belonged. That saved us a lot of time.”

3. **Automation Engine** removes the manual labor from fixing system permission errors and misconfigurations. With it, the contractor can quickly and safely remediate open access en masse.

> “We used Varonis to scan our entire environment and report on the things that were open that we were unaware of. Then Automation Engine helped us immediately start remediating permissions.”

4. **DatAlert** monitors and alerts on critical systems. Fine-tuned alerts separate the noise and surface only the threats that matter, such as anomalous activity indicative of ransomware.
5. **Edge** uses perimeter telemetry to identify difficult-to-detect attacks like DNS tunneling.

> “Varonis went above and beyond and even provided us with a ransomware alert script customized to our environment. If DatAlert sees an indicator of a ransomware attack, it identifies the user that process is being acted upon, blocks their account in Active Directory, and logs off their session automatically. It immediately limits the potential damage. That definitely gives us peace of mind.”

Best of all, in 2020 Varonis achieved NIAP Common Criteria Certification. The Varonis Data Security Platform meets the U.S. National Security System’s strictest security requirements.

> “When Varonis showed off the number of controls that their software would check boxes on, it was incredibly exciting. It’s kind of a one-stop shop for the majority of our CMMC requirements.”

“If DatAlert sees an indicator of a ransomware attack, it immediately limits the potential damage. That definitely gives us peace of mind.”

Results

Data locked down in a fraction of the time

When the contractor adopted Varonis, their first goal was to reduce open access and fix broken permissions using Automation Engine. They targeted three servers for immediate cleanup and remediation.

In just three one-hour sessions, Varonis helped the contractor accomplish what otherwise would have taken months:

- Limiting open access on sensitive files by 95%
- Decreasing total folders with open access by 90%
- Reducing folders with broken permission by 53%

When it comes to compliance, the SysAdmin says that there is now a dramatic difference in visibility, control, and capability versus what their team used to have.

> “Before Varonis, our small team was overwhelmed with the prospect of having to get our entire organization fully compliant. But as a company that does 99% of our business with the government, we couldn’t afford not to be compliant.”

The final ROI is immeasurable. Achieving higher levels of CMMC compliance opens doors to more government contracts. And by locking down their data, they’re minimizing the blast radius of potential ransomware attacks.

> “Varonis reduces labor for our IT team and cost for our company. It checks so many boxes when it comes to CMMC compliance. It just does so much in one package.”

As for the SysAdmin’s experience with Varonis’ support, they say:

> “They’re always available. If we’re ever in trouble, the Incident Response team is quick to respond at no extra cost. And I have an amazing personal relationship with our sales manager. I’ve never worked with a vendor quite like Varonis.”

> “Knowing that Varonis is out there proactively monitoring our contract sites and reporting back without us really having to do anything on a day-to-day basis is super valuable.”

Varonis helps with data risk reduction, compliance, and threat alerting.

REQUEST A DEMO

Learn more about how Varonis helps federal agencies.