How Varonis Enables a Multinational Defense Contractor to Proactively Meet CMMC Requirements

CASE STUDY

"Having Varonis helps you achieve a higher level of Cybersecurity Maturity Model Certification. It arms you with the evidence you need to prove that you're at the maturity level you claim. Without that certification, you won't be able to bid on the contracts you want."

ABOUT THIS CASE STUDY:

Our client is a large multinational defense contractor. We have happily accommodated their request to anonymize all names & places.

HIGHLIGHTS

CHALLENGES

- Implementing and enforcing controls to maintain advanced cybersecurity maturity
- Undergoing an external security audit to achieve CMMC controls
- Obtaining higher levels of certification to bid on important government DoD contracts

SOLUTION

The most robust data security platform:

- **DatAdvantage** to find and fix overexposed data
- **Data Classification Engine** looks for and flags sensitive federal data, including CUI
- **DataPrivilege** gives access control to department heads
- **Data Transport Engine** enforces rules for data movement and migration
- **Automation Engine** safely automates large-scale remediation projects
- **DatAlert Suite** warns against threats with up-to-date threat models

RESULTS

- Custom rules to protect sensitive data including CUI according to DFARS, ITAR requirements
- Ability to secure data to least privilege and alert to threats
- Technical capabilities to implement and enforce CMMC controls

Challenge

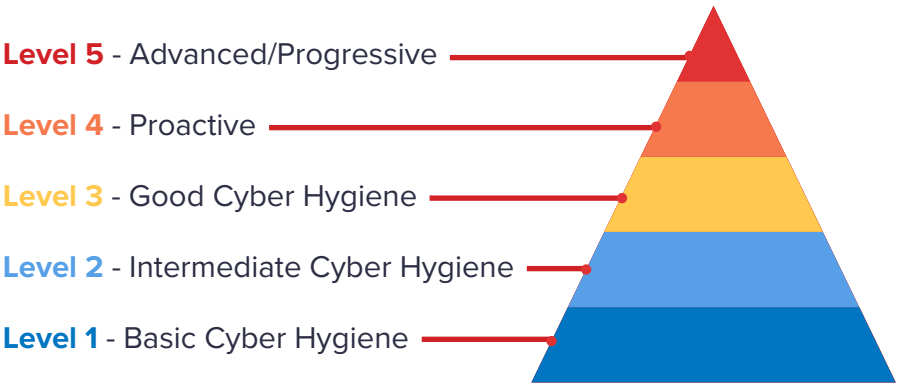
Achieving high-level CMMC controls

The introduction of the Cybersecurity Maturity Model Certification (CMMC) is changing the game for DoD contractors, including one Varonis client (anonymous by request).

While defense contractors have always had to comply with various compliance processes (including NIST SP 800-171, NIST SP 800-52, ISO 27001, ISO 27032, and AIA NA9933), CMMC ties these discrete processes together into one unified framework.

Under the new model, all contractors need to achieve some level of CMMC to work on DoD contracts, either as a prime or a subcontractor, and prove compliance via an **external security audit.**

Cybersecurity Maturity Model Certification Levels



Understanding that their ability to win government contracts hinged on having controls in place to protect sensitive data and reach higher CMMC levels, this Varonis client was striving to reach level four — if not level five — before CMMC came into full effect.

As their system admin explains, “We’re doing internal assessments to prepare for CMMC. With Varonis, we have an easy way to pull records and export compliance reports.”

Level four replicates a lot of existing requirements of DFARs and ITAR. In most cases, it’s the bare minimum requirement for prime contractors, and it requires the ability to proactively measure, detect, and defeat threats, including advanced persistent threats (APTs).

Satisfying these technical requirements is impossible without advanced software solutions. That’s why the company reached out to Varonis. The sys admin says:

> “If you want to advance your CMMC, you need insights that are not natively built into your Windows Server and Active Directory. You wouldn’t be able to identify potential spillage issues or find data when people move it out of designated files.”

To achieve level five, the company would have to implement additional security controls. On top of solid technical capabilities, their auditing and managerial processes needed to be airtight.

“If you want to advance your CMMC, you need insights that are not natively built into your Windows Server and Active Directory.”

Solution

An easy way to identify, remediate, and safeguard sensitive federal data

Varonis gave the company visibility into the state of their servers' security at the outset and helped them prioritize remediation tasks.

An initial audit uncovered **14,617 files containing sensitive data,** including SSNs, PCI, and HIPAA. Over half of those files were stale (not modified in 3+ years) and many were alarmingly overexposed. Over 96,000 Social Security Numbers and an additional 97,000 plain-text passwords were open to every employee.

According to the CMMC controls, locking down access is a required step in achieving compliance:

- **AC.1.001** Limit information system access to authorized users, processes action on behalf of authorized user, or devices (including other information systems)
- **AC.1.002** Limit information system to the types of transactions and functions that authorized users are permitted to execute
- **AC.2.007** Employ the principle of least privilege, including for specific security functions and privileged accounts

"Varonis opened our eyes to the problem. With Varonis, it's not hard to disable inheritance or turn permissions off. But without Varonis, you'd just have no idea."

Data Classification Engine looks for and flags sensitive data. Varonis enabled custom rules to identify highly sensitive and confidential federal data, including DFARS, ITAR, Controlled Unclassified Information (CUI), and FOUO data (Varonis also offers Federal Policy Pack for out-of-the-box support).

Once sensitive data has been identified, **DatAdvantage** for Windows, Exchange, and Directory Services simplifies remediation by mapping permissions. The sys admin knows at a glance who can access the data and who is accessing the data. If a file is ever altered or relocated, remediation only takes seconds.

With **DataPrivilege,** department heads can grant and revoke access and directly manage authorization workflows without IT assistance. Generating reports and reviewing who can access what is as simple as clicking a button, which streamlines compliance processes.

When it comes to large-scale remediation, **Data Transport Engine** and **Automation Engine** help the company move toward least privilege while mitigating risk and minimizing workflow interruptions. These systems automatically enforce the 'rules of the road' for properly storing data and safely remove global group access en masse.

"After more than fifteen years of sprawl and a Wild West mentality to global group access, you can't make sweeping changes because you'll break permissions.

I use Automation Engine to automatically fix broken permissions in the company. Then I set it up to repeatedly fix new global access issues that crop up. I leave it with the 72-hour wait period so that I don't kick users out of the files they need.

It's hugely beneficial to be able to automatically parse through and remove authenticated users and only give access to the people who are actually using the information."

Finally, **DatAlert Suite** equips the company to detect and defeat even the most insidious threats. With its advanced insights and 24/7 monitoring for anomalous behavior, DatAlert enables the sys admin to assess and kill threats before they have a chance to escalate.

> “We had an alert come in today of a possible cross-site scripting attack. I sent that off to our cybersecurity team for immediate investigation. With DatAlert, I’m able to review alerts and act on them in real-time.”

“It’s hugely beneficial to be able to automatically parse through and remove authenticated users and only give access to the people who are actually using the information.”

Results

Controls in place to achieve CMMC

With Varonis, this DoD contractor has critical technical systems in place to help proactively meet CMMC requirements.

They have the means to identify and mitigate risk associated with CUI, in addition to automatically enforced rules that meet DFARS and ITAR requirements.

> “CMMC Assessors want proof of compliance, like records of who has admin access and how those accounts are being used. With Varonis, we have those records.”

Between DatAdvantage, Data Transport Engine, and Automation Engine, they have a robust combination of manual and automated real-time response capabilities to quickly and decisively deal with issues like overexposed sensitive data.

Varonis also acts as an advanced warning system. It’s always monitoring critical folders and it automatically catalogs and updates threat profiles and adversary TTPs for up-to-date risk management and threat intelligence.

When it comes time to prove that CMMC controls are in place, the sys admin can easily audit their systems, generate comprehensive reports, and review audit reports in detail.

> “Having an easily exportable report that I can just hand to decision-makers or CMMC Assessors whenever they ask for it is hugely beneficial.”

> “Having Varonis helps you achieve a higher level of CMMC. It arms you with the evidence you need to prove that you’re at the maturity level you claim. Without that certification, you won’t be able to bid on the contracts you want.”

The value of Varonis for this defense contractor cannot be overstated. For them, having that high level of visibility and control is the difference between landing an important government contract and watching it fall in the hands of a competitor.

“CMMC Assessors want proof of compliance, like records of who has admin access and how those accounts are being used. With Varonis, we have those records.”

Level up your CMMC preparedness.

Varonis helps you safeguard sensitive federal data and achieve the certification you need to bid on DoD contracts.

REQUEST A DEMO