Article

Avecto

National Institute of Standards and Technology

Achieving Defense Federal Acquisition Regulation Supplement (DFARS) compliance

Avecto has assisted many global clients to meet the requirements of DFARS NIST 800-171. Read on to find out how Avecto's Defendpoint software secures your endpoints through integrated privilege management and application control technology.

About DFARS

Department of Defense (DoD) contractors and subcontractors must meet Defense Federal Acquisition Regulation Supplement (DFARS) compliance rules before the end of 2017.

Changes to DFARS requires contractors to meet the mandatory security standards outlined in National Institute of Standards and Technology (NIST) Special Publication 800-171: Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations.

The US government legislation intends to safeguard 'controlled unclassified information' (CUI) against the growing cyber security threats, requiring affected organizations will need to act to adequately protect their processes, systems and contracts.

CUI is classified as "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies".

What will happen to those who fail to comply?

Those who fail to comply will likely lose government contracts, whereas organizations able to demonstrate compliance at an early stage may be in a better position to secure additional wins.

DFARS controls

Government contractors and subcontractors are required by DFARS 252.204-7008 to comply with the 14 control families of the NIST SP 800-171 by December 2017:

Access control*

Awareness and training

Audit and accountability*

Configuration management*

Identification and authentication

Incident response

Maintenance*

Media protection

Personnel security

Physical protection

Risk assessment

Security assessment

System and communications protection

System and information integrity*

*Mapped to by Defendpoint

Avecto

How Defendpoint helps with notable controls

By December 2017, companies must, at a minimum, meet the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 standards or have an alternative security system approved.

Below are some key aspects of the compliance your organization will need to deal with, and an explanation of how Defendpoint can help.

Requirement	How Defendpoint helps
NIST 800-171 **Access control** 3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). 3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. 3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts. 3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions. 3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions. 3.1.9 Provide privacy and security notices consistent with applicable CUI rules. 3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Defendpoint can help with a number of Access Control requirements. Administrative privileges can be taken away from end users and unauthorized applications blocked, all while ensuring they still have the flexibility needed to do their job. IT can assign rights to individual processes, applications, scripts, batch files and control panel applets, etc. As a result, if the removal of administrative privileges from users' accounts causes a legacy application to stop functioning correctly, or users can no longer perform a maintenance task, the required rights are transparently added to the required process according to centralized policy set by the IT department. Message handling can play a part in organizations meeting privacy and security notice requirements.
Audit and accountability 3.3.1 Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. 3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. 3.3.3 Review and update audited events. 3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. 3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting. 3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion. 3.3.9 Limit management of audit functionality to a subset of privileged users.	PCs, Macs and servers can be monitored, giving you details of applications and processes being used and the privileges required to run them. Having access to this data can also prove useful in reducing the likelihood of user issues when administrative rights are removed. This is done by ensuring application and process compatibility with standard user accounts is known before least privilege is deployed. Anti-tamper on logs ensures audit information and tools are protected and access restricted to approved users only.

Avecto

Requirement	How Defendpoint helps
Configuration management 3.4.1 Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. 3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational information systems. 3.4.3 Track, review, approve/disapprove, and audit changes to information systems. 3.4.6 Employ the principle of least functionality by configuring the information system to provide only essential capabilities. 3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. 3.4.9 Control and monitor user-installed software.	Application control allows you to set a handful of broad rules based on trusted application types, automatically stopping unapproved applications from running. Workstyles, message handling, Challenge/Response messaging and Insights can assist in meeting requirement 3.4.3. Intelligent yet simple rules allow you to achieve whitelisting very easily, with unknown applications managed via dynamic exception handling. Defendpoint Insights allows you to discover, monitor and manage user activity across the entire business.
3.7 Maintenance 3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	A targeted workstyle that focuses on PMAC, around which maintenance tools/software can be executed even as a standard user, can help you meet this requirement.
3.14 System and information integrity 3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems. 3.14.4 Update malicious code protection mechanisms when new releases are available.	Defendpoint helps with 3.14.2 through privilege management and application control, with the additional benefit that we proactively protect against malicious mode.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.