Avecto Whitepaper

Compliance series

Guide to meeting requirements of the Defence Cyber Protection Partnership

The Ministry of Defence will require all suppliers to adhere to the requirements set out in the Defence Cyber Protection Partnership's (DCPP) Cyber Security Model (CSM), which builds on the UK Government's Cyber Essentials Scheme, starting April 2016. In this paper, Avecto looks at the new regulation and how you can prepare for it.

The Defence Cyber Protection Partnership is a joint industry and Government response to the threat to Defence from malicious actors, including terrorists and foreign intelligence services. Officially launched in 2013 by the Ministry of Defence (MOD), government departments, and industry suppliers, the scheme allows the above parties to work together to improve the resilience of the sector to attack. DCPP is divided into three core strands: information sharing, measurements and standards, and supply chain awareness - of which measurements and standards is responsible for establishing CSM security controls.

> "The Defence Cyber Protection Partnership is a joint industry and Government response to the threat to Defence from malicious actors."

Cyber Essentials Scheme

Developed primarily with SMEs in mind, the Cyber Essentials Scheme is aimed at reducing the risks associated with cyberattacks by improving a company's overall security position while bearing in mind the lack of resources and expertise available to small organizations. A reduced version of the government's 10 Steps to Cyber Security document, Cyber Essentials provides five key controls that both small and large businesses should implement to secure their IT systems.

The five goals set out in the Cyber Essentials Scheme are as follows:

1. **Boundary firewalls and internet gateways**
2. **Secure configuration**
3. **Access control**
4. **Malware protection**
5. **Patch management**

Excluding contracts that fall into the 'Not Applicable' Cyber Risk Profile category, all MoD suppliers must achieve Cyber Essentials certification, or Cyber Essentials Plus if the assessed Cyber Risk Profile is 'Low' or higher. This offers greater assurance over the base Cyber Essentials certification via external testing of the implemented controls, and a completed questionnaire that's approved by a company executive, and then verified by an independent certification body.

DCPP Cyber Security Model (CSM)

The controls set out in Cyber Essentials were considered by DCPP, in most cases, to be inadequate for securing MoD suppliers. As such, DCPP developed its own standard, the Cyber Security Model (CSM), which aims to extend the existing Cyber Essentials Scheme to provide the necessary level of security for suppliers.

CSM is divided into three stages. Stage 1 is a risk assessment based on a questionnaire completed by the contractor, and the outcome determines the contract's Cyber Risk Profile. The second stage involves the contracting authority deciding on a Cyber Risk Profile and the supplier implementing the requirements. Finally, the third stage requires the supplier to evidence that the controls have been applied as required.

> "This is an issue which demands a concerted and co-ordinated approach between government and industry, and the DCPP is a critical component of this."

Vic Leverett, DCPP Chair

Cyber Risk Profiles

MoD contracts are assessed and assigned to a Cyber Risk Profile. The higher risk the contract is considered, the more controls that need to be observed. This five Cyber Risk Profiles are outlined in Table 1 below.

Not Applicable	Contracts assessed as no or negligible risk
Very Low	Contracts assessed as a basic threat. E.g. where attacks are likely to be opportunistic and non-persistent. This profile often applies to commodity suppliers.
Low	Contracts where attacks might be targeted but not persistent, such as social engineering attacks aimed at management and carried out by semi-skilled malicious actors. This profile usually applies to contracts dealing with classified information but not linked to military activity.
Moderate	Contracts that might be subject to advanced threats aiming to gain access to specific information or launching a denial of service attack. This profile might apply to organizations processing large amounts of information deemed OFFICIAL – SENSITIVE.
High	Contracts that might be targeted by highly sophisticated attackers using Advanced Persistent Threats (APTs). This profile usually applies to contracts dealing with information classified as SECRET or higher.

CSM requires additional technical controls over those set out in the Cyber Essentials Scheme. For example, contracts assessed as 'Moderate' and higher must also define and implement a policy for Data Loss Prevention (DLP), control the use of authorised software, implement a policy to monitor user account usage and manage changes of access rights.

> "This is a clear demonstration that government and industry can work together – sharing information, experience and expertise."
>
> Philip Dunne, Minister for Defence Equipment, Support and Technology

Avecto Defendpoint

Avecto Defendpoint can help organizations meet the access control requirements of the Cyber Essentials Scheme and CSM, of which removing administrative privileges from users is a key control. In turn, the use of standard user accounts helps maintain secure configuration and prevent malware, as also required by the Cyber Essentials Scheme.

Defendpoint's Privilege Management and Application Control modules can be used to meet some of CSM's technical controls, such as:

L.12 Define and implement a policy to manage the access rights of user accounts
M.09 Define and implement a policy to monitor user account usage and to manage changes of access rights
M.11 Define and implement a policy to control the use of authorised software
H.06 Define and implement a policy to control installations of and changes to software on any systems on the network

Privilege Management

User Account Control (UAC) Protected Administrator accounts, a consumer technology that helps users run without administrative privileges most of the time, don't provide the same protection as standard users, and Protected Administrators can elevate privileges any time at the user's discretion.

Defendpoint solves this problem using a policy-driven privilege management engine that improves on UAC by allowing enterprises to remove administrative privileges and assign processes additional privileges as required, rather than user accounts. Defendpoint enables IT to remove administrative privileges from users without impacting productivity.

> "90% of large organisations and 74% of small businesses have had a security breach."

2015 Information Security Breaches Survey

Application Control

While Windows 7 Enterprise has a built-in application control feature in AppLocker, Defendpoint's Application Control module supports all Windows editions, tightly integrates with the privilege management and sandboxing modules, and also permits organizations to configure advanced exception handling with customizable messages and prompts.

Defendpoint's combined Privilege Management and Application Control features help organizations meet the demands of Cyber Essentials and CSM across the full range of Cyber Risk Profiles, where the built-in Windows tools fall short of providing a complete solution.

About Avecto

Avecto is an innovator in endpoint security.

Founded in 2008, the company was established to challenge the status quo that effective security leads to user lockdown. This philosophy of security + freedom promotes a positive user experience across every software implementation, allowing organizations to strike just the right balance.

Its unique Defendpoint software makes prevention possible, integrating three proactive technologies to stop malware at the endpoint. This innovative software has been implemented at many of the world's most recognizable brands, with over 8 million licenses deployed.

Attention to detail is paramount, with a team of qualified and experienced technology consultants to guide clients through a robust implementation methodology. This consultative approach provides clients with a clearly mapped journey against measurable objectives to ensure project success.

The company has placed in the top four of the Deloitte Fast 50 for the last two consecutive years, making it one of the UK's fastest growing software companies as well on the global stage.

Deloitte. Technology Fast50 UK 2014

UKtech awards 2015

winner Cyber Security Awards

intel Security Innovation Alliance

Microsoft Partner Gold Application Development