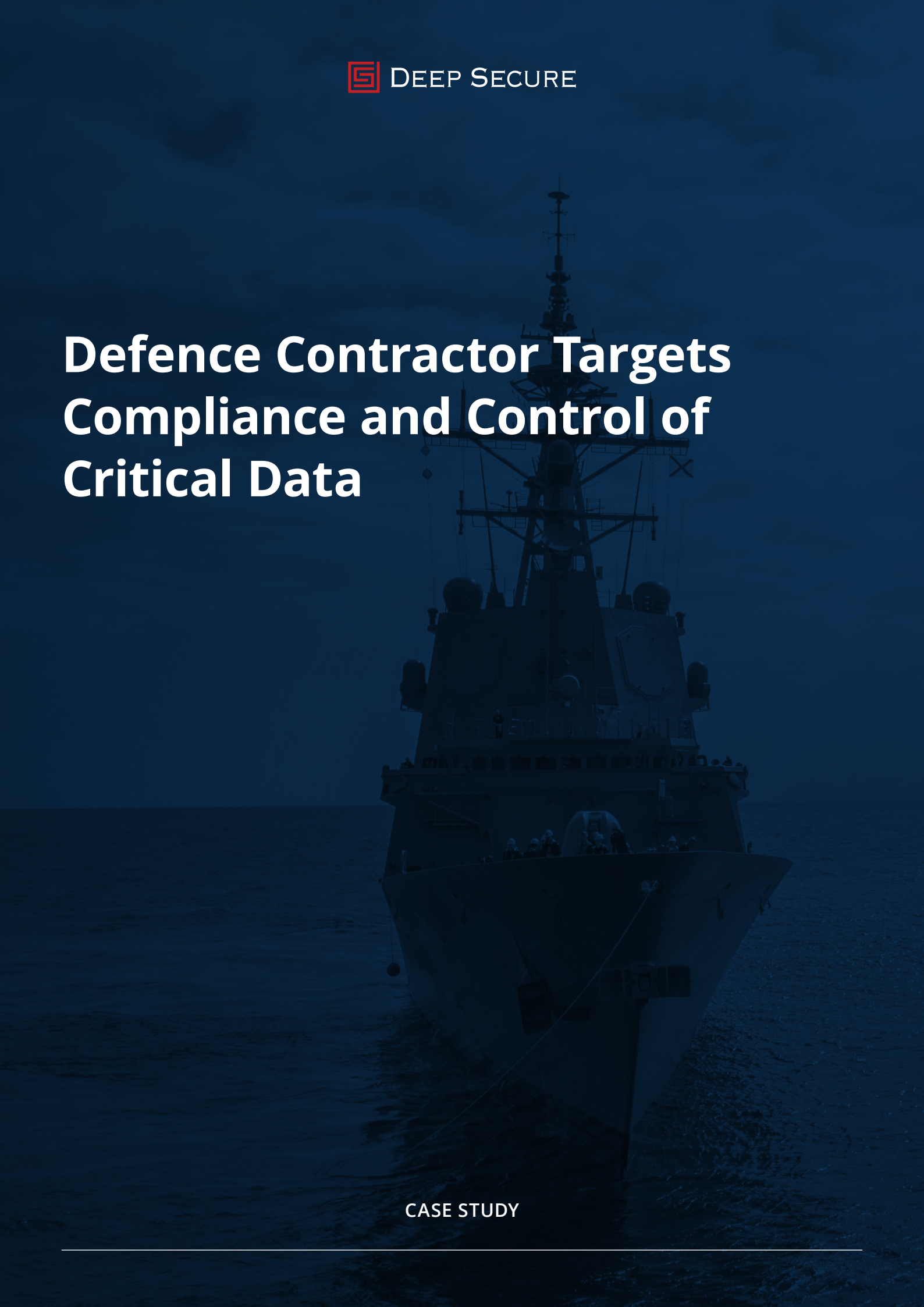
DEEP SECURE

Defence Contractor Targets Compliance and Control of Critical Data



CASE STUDY

Background

International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) are United States regulatory regimes to restrict and control the export of defence and military related technologies.

For any multi-national defence contractor it is essential to be able to demonstrate the appropriate protection of any controlled data covered by these regulations.

When it comes to compliance with ITAR and EAR the stakes are high. A failure to comply has the potential to directly hit the bottom line, resulting in significant fines and ultimately the revocation of the Export Licence.

When a global defence contractor embarked on a project to protect the flow of their business critical data, they chose Deep Secure to provide safe passage.

Challenge

Enforce compliance with International Trade in Arms Regulations (ITAR) export controls

This global defence contractor is responsible for the design of a major new maritime defensive capability, masterminding a complex and challenging multi-million pound engineering project involving several nations and suppliers.

As part of the programme risk and due diligence assessment, the contractor identified a need to both protect the flow of controlled information and enforce compliance with International Trade in Arms Regulations (ITAR) export controls into and out of their domain.

> *"To meet our goals for security and compliance, we needed to introduce a robust, scalable boundary control gateway to sit at the edge of the network and check the content of all outgoing and incoming email and web traffic to ensure that no controlled information was leaving via these protocols,"*

Solution

Deploying Deep Secure's Cross Domain Solutions

The contractor selected Deep Secure cross-domain solutions to provide their boundary control gateway.

The cross domain solutions protect the controlled data handled by the 2000 employees operating in the domain. Controlled data is checked at the boundary. All senders and recipients of email containing ITAR protected information are checked to ensure they are on the contractor's authorised list of people able to handle such data.

Deep Secure worked closely with the team and the contractor's outsourced services supplier. In parallel, the defence contractor ran an internal education and communications campaign to ensure widespread understanding and acceptance of the project goals.

> *"This was a team effort. Together we monitored the boundary traffic, developed the required policy rules and introduced them into the live environment."*

Results

Deep Secure's cross-domain solutions ensure that the contractor can enforce and prove their compliance with ITAR.

In parallel, the cross domain solutions also mitigate the risk of the loss of controlled data over the network boundary, a loss that might otherwise have a potentially devastating impact on both the defence contractor's brand and National Security.

"We chose Deep Secure for a number of reasons. The cross-domain solutions were selected because they provide the most versatile and configurable ruleset for protecting controlled data and delivering compliance with ITAR."

"With Deep Secure's reputation and track record in the Military and Defence markets, we were confident that they would work with us to deliver the levels of assurance and protection we need. As a result, we are able to mitigate the identified risks to an acceptable level, safeguarding our revenues, reputation and workforce."

Head of Information Security, Global Defence Contractor