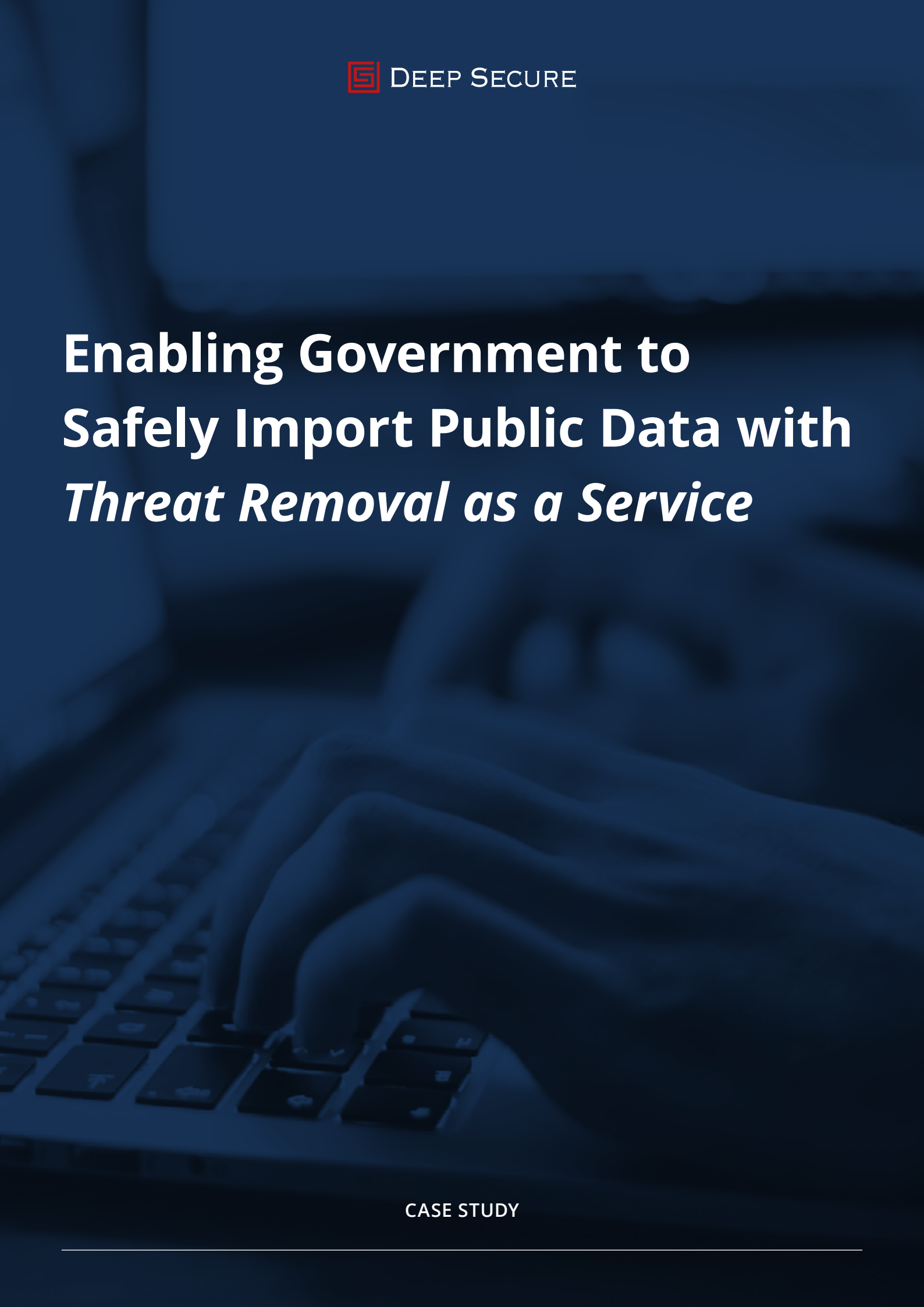

DEEP SECURE

Enabling Government to Safely Import Public Data with *Threat Removal as a Service*

CASE STUDY

Background

Against a backdrop of austerity and ever-reducing budgets, a government authority has implemented a cloud-based portal to cost-effectively and securely import citizen data.

The authority is moving towards an internet-based portal, enabling citizens to upload information in a more expedient way, as part of an initiative to put people and place at the heart of the service. They needed to be certain it couldn't be used as a "backdoor" to import malware into the organisation.

Taking their lead from the NCSC (who have a pattern for the safe import of data to enable this type of solution) they chose Deep Secure's 'Threat Removal as a Service', zero-trust approach to data in the cloud, ensuring documents and images uploaded via their citizen portal are 100% malware-free.

Challenge

Ensure the citizen portal isn't used as a "backdoor" for malware to get into the organisation

The government authority decided to implement their citizen portal in the cloud, taking advantage of the potential cost savings to be gained from having no infrastructure to support and maintain.

However, against the backdrop of many high-profile cyberattacks on government using zero-day malware, the team needed to be certain that the documents and images being uploaded into the portal, in support of benefit claims, were free of malware.

> *"We know that zero-day malware cannot be detected using anti-virus approaches and that it can be concealed in documents and images and uploaded via a portal."*

Mindful of the potential pitfalls, the team asked for advice from the National Cyber Security Centre (NCSC).

Following a consultation, the organisation decided to follow the recommendations laid down in the NCSC "Pattern: For Safely Importing Data", a set of leading practice guidelines for accepting documents and images from untrusted sources.

> *"The citizen portal is a potential vector for the introduction of malware. We needed to be certain we had taken every possible step to ensure we were safely importing citizen data into the organisation and that the portal could not become a "backdoor" for malware to get in."*

Solution

Deploying Deep Secure's 'Threat Removal as a Service' for Risk-free Data Upload

The government authority chose to integrate Deep Secure 'Threat Removal as a Service' (TRaaS) directly into their cloud-based portal application to import, transform and verify uploaded documents and images.

Every time a citizen submits a document or image via the portal TRaaS automatically transforms the file in real time, extracting only the valid business information from it and creating a digitally pure file. The file is verified and the original discarded.

A wholly new risk-free file, formatted to match the original, is placed where it can be accessed and used with confidence.

TRaaS offers a zero-trust, security-as-code, approach to importing data in real-time. Serverless and cloud-native, it is accessed via APIs built into the portal application, enabling the authority to place 100% trust in its data and remove the maintenance and update costs associated with virus scanners.

As the service runs in Amazon AWS, with industry-leading 99.95% reliability levels, the authority can meet its targets for reliability and availability and the team have confidence that uploads are risk-free.

> *"Documents and images allowed in via the portal have all been transformed and verified to ensure they are 100% threat-free."*

Results

Complete confidence and dramatic cost savings

The government authority enjoys complete confidence in a solution that conforms to the NCSC recommendations for safely importing data – transforming, verifying and exchanging it - to render documents and images uploaded by citizens 100% risk-free in real-time.

Integrating 'Threat Removal as a Service' has also proved highly cost and energy efficient. Compared to the on-premise equivalent, the team are seeing savings of over 50% per annum in the management of hardware, power and cooling.

The unique way that 'Threat Removal as a Service' is delivered via the cloud, and built on a serverless model, provides risk-free data import whilst removing the need for updates and maintenance, reducing energy consumption and providing high-availability as the application scales effortlessly to cope with peaks in demand.