VOSO™

Be safe in the online world

CySure

About CySure

CySure provides information security management solutions and services to businesses so they can reduce their cyber risk and be safe in the online, connected world.

CySure's Virtual Online Security Officer (VOSO) means you know what, when and how to maintain a secure state. Rely on VOSO to avoid:

- Business interruption
- Regulatory fines
- Loss of customer data
- Theft of intellectual property
- Damage to reputation and trust

Taking CySure's automated and phased approach provides organisations with the tools to visualise their risk and create a security strategy to keep them safe. VOSO helps companies to deliver an externally recognised security posture and supporting certification at the fraction of the cost of its human counterpart.

VOSO

Cyber security has become a fundamental component of business operations.
As cyber criminals get more sophisticated and threats continue to evolve, it is vital that companies invest in security policies, procedures and products regardless of their size, market or location.

To protect themselves organisations require a consistent set of policies and processes, backed up by continued employee training. Starting the journey can seem like a daunting task when security resources are limited. That's where CySure's Virtual Online Security Officer (VOSO) can help.

CYBER ESSENTIALS

IASME Consortium®

VOSO™

The cyber security workflow and compliance solution for SMEs

CySure's flagship solution, Virtual Online Security Officer (VOSO), is an information security management system. VOSO incorporates cyber security standards to guide organisations through data and technology safety procedures and protocols, improve their online security and reduce the risk of cyber threats. VOSO is a simple to use web-based solution that helps monitor various technical defences such as the configuration of all networked device, asset mapping, vulnerability scanning and patching. With dashboards to display compliance progress against selected standards as well as online security training videos for continual staff training. Costing from £1 per user per month, VOSO reduces the requirement for full-time cyber security consultants or compliance officers, mitigates the risk of lawsuits and regulatory fines and ensures employees are trained regularly and kept informed of the latest cyber security updates.

VOSO, the information security management system incorporates Cyber Essentials and IASME cyber security standards to guide organisations through data security procedures and protocols. By using VOSO, companies can improve their online security posture and reduce the risk of cyber threats, avoiding the majority of cyber-attacks.

Small and medium-sized enterprises (SMEs) are as much at risk from data breaches as large organisations. Whatever the size of your organisation, CySure has a solution to meet your needs.

Security Levels

VOSO

VOSO Lite

VOSO™ Lite

The first line of defence in any organisation is its people and processes. VOSO Lite, CySure's entry point solution, provides the staff training, information risk and general data protection policies to ensure your employees are aware of their cyber risks and responsibilities.

With 90%* of security incidents being traced back to human error, it is clear to see why many government and industry standards state the importance of continuously training employees. By upskilling teams in basic cyber hygiene, companies can prevent unauthorised disclosure of protected personal information and avoid negligently allowing cyber criminals access to corporate systems via social engineering. VOSO Lite is an affordable low-cost solution that will put your organisation on the path to improving online security and reduce the risk of cyber threats.

*National Cyber Security Centre (NCSC) www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020

Security Levels

VOSO

VOSO Lite

VOSO™

VOSO helps to guide your organisation on the next stage of the cyber secure journey.

Cyber Essentials (CE) is a policy guidance from the UK's National Cyber Security Centre, to help all organisations protect themselves against common cyber-attacks. Cyber Essentials aims to provide businesses with a structured framework and a continuous process that implements the minimum standards to deflect most cyber-attacks. Your dedicated Virtual Online Security Officer (VOSO) will initiate and guide you through the required polices, processes and events in an easy to understand way.

Being fully Cyber Essentials compliant mitigates many of the risks faced by businesses, such as malware infections, social engineering attacks and hacking. By achieving and maintaining a certified standard such as CE, your organisation will be able to verify that you have implemented the basic technical controls towards protecting your business and your data from internet based cyber-attacks.

This phased approach then progresses at your pace onto the governance processes and procedures that ensure executive oversight that the security of the company and its data is maintained and compliant with corporate and regulatory requirements. It adds several actions such as assessing business risks, incident response planning and handling operations issues. By completing this stage, your organisation will be able to demonstrate that it has implemented a wider governance system for management of the controls protecting personal data.

Security Levels

VOSO

VOSO
Lite

VOSO™ is your Virtual Online Security Officer

VOSO is an information security management system (ISMS) that provides the foundation required for organisations to remain safe and secure in the online world. Using the NCSC's Cyber Essentials standard, VOSO acts as a virtual guide which takes organisations through the necessary tasks and has a workflow system to ensure important tasks are completed at regular intervals and then curates those activities.

VOSO helps to:

- Educate employees to prevent them from taking actions that open-up the organisation to cyber attacks. People are the weakest link with 90%* of security breaches due to mistakes by users.
- Notifies of the tasks required to stay safe and when they need to happen. Good cyber security requires regular attention.
- Keeps a log of completed tasks to help to provide proof of compliance in the event of an attack.

While organisations might think they have cyber-security covered they rarely have. VOSO provides an end-to-end view, guidance and oversight. It records the actions taken to ensure the relevant security technology products are deployed to keep an organisation secure.

VOSO cuts through the complexity and provides the perfect place to start when it comes cyber security.

*National Cyber Security Centre (NCSC) www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020

Security Levels

VOSO

VOSO Lite

VOSO™:

Three steps to a good security posture and compliance

The Human Element

The human firewall is perhaps the most significant element of cyber security system because people are the weakest link. Reports show that 90%* of security breaches are due to mistakes by users. Ensuring employees are aware of their cyber risks and responsibilities is a vital part of mitigating the risk of cyber threats. Employees will often click on websites and links without realising these represent a security risk.

VOSO provides the information risk and general data protection policies that informs employees of their responsibilities and maintains a library of awareness training videos that are sent out regularly to continually remind them of the risks. VOSO keeps track of training progress - so you don't have to!

Data Security

In the event of a breach your organisation will need to demonstrate that it ensured appropriate security was in place to protect its and other people's data. That extends to suppliers and contractors to your business. All of the data security standards start off with the essential infrastructure requirements.

Including:

- Firewalls
- Secure configuration
- User Access Control
- Malware protection
- Vulnerability Patch management

VOSO guides organisations through the required implementation of these five requirements to achieve the relevant standard or certification. By following these procedures you will avoid the majority of the attacks that take place, and demonstrate you ensured the appropriate security to a recognised standard, such as Cyber Essentials and IASME.

Governance

Along with continual training and data security, an organisation will need to demonstrate that there was governance in place to ensure proper oversight of its policies and controls.

- VOSO maintains a library of policies and documents, a small and medium sized enterprise (SME) would need to implement the standards it selects to follow.
- Events and tasks are at the heart of how VOSO works. It has defined workflows with events to ensure tasks are assigned and completed in line with the defined cyber security policies and regulatory standards. The tasks are colour coded as red tasks for unassigned, yellow for tasks in progress and green for tasks completed.
- To keep management updated VOSO incorporates a dashboard and automatically creates an audit trail of all activities. The audit trail provides executive oversight to ensure that standards are being maintained so that executives can immediately see how compliant and safe the organisation is at any point.

*National Cyber Security Centre (NCSC) www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020

VOSO™, Your Most Valuable Employee Working 24/7

VOSO is your organisation’s personal virtual online security officer, it doesn’t need breaks, never takes holiday and works 24x7. VOSO is focused on managing the organisation’s cyber security workflow and compliance needs.

Why VOSO?

- Simple to use and easy to manage
- At a glance dashboard with full status overview
- Incorporates government and industry backed regulatory standards
- Comprehensive reporting on tasks over time, progress and status updates
- Provides support at every stage of the cyber security compliance process
- Flexible product and SME pricing options

A Simple Checklist

How do you currently manage your company's cyber security requirements? Here is a checklist to help answer that tricky question:

1 Do you hold regular reminder training for all staff on the cyber threats that they are likely to be exposed to?

2 Do all new starters receive awareness training on your security policies as part of onboarding?

3 When someone leaves, is the IT function informed so system access is immediately removed and shared passwords changed?

4 Do you have guidelines and policies that describe the obligations of employees when interacting with company systems?

5 Is there a policy for reporting security breaches?

6 What happens if you have a breach – is there a documented disaster recovery policy?

7 Do you know what hardware is in use and the software running on it – what vulnerabilities need patching?

8 Are firewalls effective and are you regularly scanning for threats to your systems?

9 Can your IT providers show you how they are protecting your information?

VOSO

Be safe in the online world

Contact Us:

🇬🇧 +44 (0)808 189 3226

🇺🇸 +1 (1) 844 258 2001

Visit us online: www.cysure.ltd

CySure