Policy Monitor

Measure, manage and monitor cyber risk

About Policy Monitor

Policy Monitor provides security policy management solutions and services to measure, manage and monitor cyber risk and guard against cyber-attacks. Its flagship product, Cyber Security Policy Monitor (CSPM) guides you to achieve compliance with a cyber policy.

CSPM ensures you know what to do, when to do it and how to maintain a secure state and avoid:

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

Taking Policy Monitor's automated and phased approach provides businesses with the tools to visualise their risk and create a security strategy. CSPM helps companies to deliver an externally recognised security posture and supporting certification at the fraction of the cost of retaining in-house cyber security expertise.

CSPM

Measure

Manage

Monitor

Cyber security has become a fundamental component of business operations. As cyber criminals become more sophisticated and threats continue to evolve, it is vital that companies protect themselves and invest in security policies, procedures and products. No organisation, regardless of size, sector or location, is immune to cyber-attacks and the risk of a data breach.

To maintain a foundation of good cyber hygiene, organisations require a consistent set of policies and processes, backed up by continual employee training. Starting the journey can seem like a daunting task when security expertise and resources are limited. That's where Cyber Security Policy Monitor (CSPM) from Policy Monitor can help.

CYBER ESSENTIALS

IASME Consortium®

Cyber Security Policy Monitor (CSPM)

The cyber security workflow and compliance solution for SMEs

Cyber Security Policy Monitor (CSPM) delivers a clear path for small and medium enterprises (SMEs) to create a security strategy in easy to manage steps. The solution simplifies the process of developing security policies and procedures, guiding you at every stage. CSPM has been designed to ensure SMEs can guard their organisation against cyber-attacks without needing expensive staff or external consultants.

Policy Monitor's flagship solution, Cyber Security Policy Monitor (CSPM), is a policy management system that embraces cyber security policy standards. It guides organisations through data and technology safety procedures and protocols, improving their online security and reducing the risk of cyber threats.

CSPM is a simple to use cloud-based solution to help provide structured cyber awareness education to employees including monitoring various technical activities to establish a sound cyber defence posture, such as patching, access controls and firewalls. With dashboards to display compliance progress against the target cyber policy as well as online security training videos for continual staff training.

Costing from £1 per user per month, CSPM:

- reduces the complexity of cyber security
- removes the need for costly full-time security consultants or compliance officers
- mitigates the risk of lawsuits and regulatory fines
- ensures employees are trained regularly and kept up to date with the latest cyber security updates
- allows an organisation to bid for work where a cyber accreditation is required.

Cyber Security Policy Monitor (CSPM) incorporates Cyber Essentials from the NCSC and IASME Governance cyber policies to guide organisations through data security procedures and protocols. By using CSPM, companies can improve their online security posture and protect against the vast majority of common cyber-attacks.

SMEs are as much at risk from data breaches as large organisations. If you are struggling with the complexity and cost of cyber defence solutions or confused as what to do first, let CSPM be your low-cost guide to establishing a sound cyber defence based on a recognised Cyber policy.

CSPM Core

The first line of defence in any organisation is its people. CSPM Core, Policy Monitor'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. CSPM Core is an affordable low-cost solution that will put your organisation on the path to improving your online security and reducing your risk of cyber threats.

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

Security Policy Levels

CSPM Core

CSPM Cyber Essentials

CSPM IASME Governance

CSPM Cyber Essentials (CE)

CSPM CE guides your organisation on the next stage of the cyber security journey.

Cyber Essentials (CE) is a policy guidance from the UK's National Cyber Security Centre (NCSC), 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 cyberattacks. Cyber Security Policy Monitor guides 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 online cyber-attacks.

This phased approach then progresses at your pace onto the governance processes and procedures. These ensure you can evaluate and prioritise your risks and can implement effective cyber security measures to manage them. The goal is to ensure that the security of your company and its data is maintained and compliant with corporate and regulatory requirements.

At this stage, CSPM 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 Policy Levels

CSPM Core

CSPM Cyber Essentials

CSPM IASME Governance

CSPM IASME Governance (IASME)

CSPM IASME provides process and policies – ISO27001 for SMEs.

IASME Governance (Information Assurance for SMEs) is aligned to the UK Government's 10 Steps to Cyber Security and embraces CE, adding controls around people and processes to deliver a more robust cyber posture. It also covers General Data Protection Regulation (GDPR) requirements. It is aligned to the much more complex and rigorous ISO27001 but is more affordable and achievable for SMEs.

CSPM IASME includes pro-forma policies and processes to allow you to quickly establish compliance with IASME Governance, reducing the time and cost to achieve certification.

Security Policy Levels

CSPM Core

CSPM Cyber Essentials

CSPM IASME Governance

CSPM is your route to building secure foundations

Cyber Security Policy Monitor provides the foundation required for organisations to remain safe and secure in the online world. Using the NCSC's Cyber Essentials and IASME Governance standard, CSPM guides organisations through the necessary actions and has a workflow system to ensure important tasks are completed at regular intervals and then curates those activities.

CSPM helps to:

- Educate employees on common cyber scams, such as phishing emails with rogue web links, that open-up the organisation to cyberattacks. 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. CSPM 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.

CSPM cuts through the complexity and provides the perfect place to start when it comes to managing your cyber security strategy.

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

Security Policy Levels

CSPM Core

CSPM Cyber Essentials

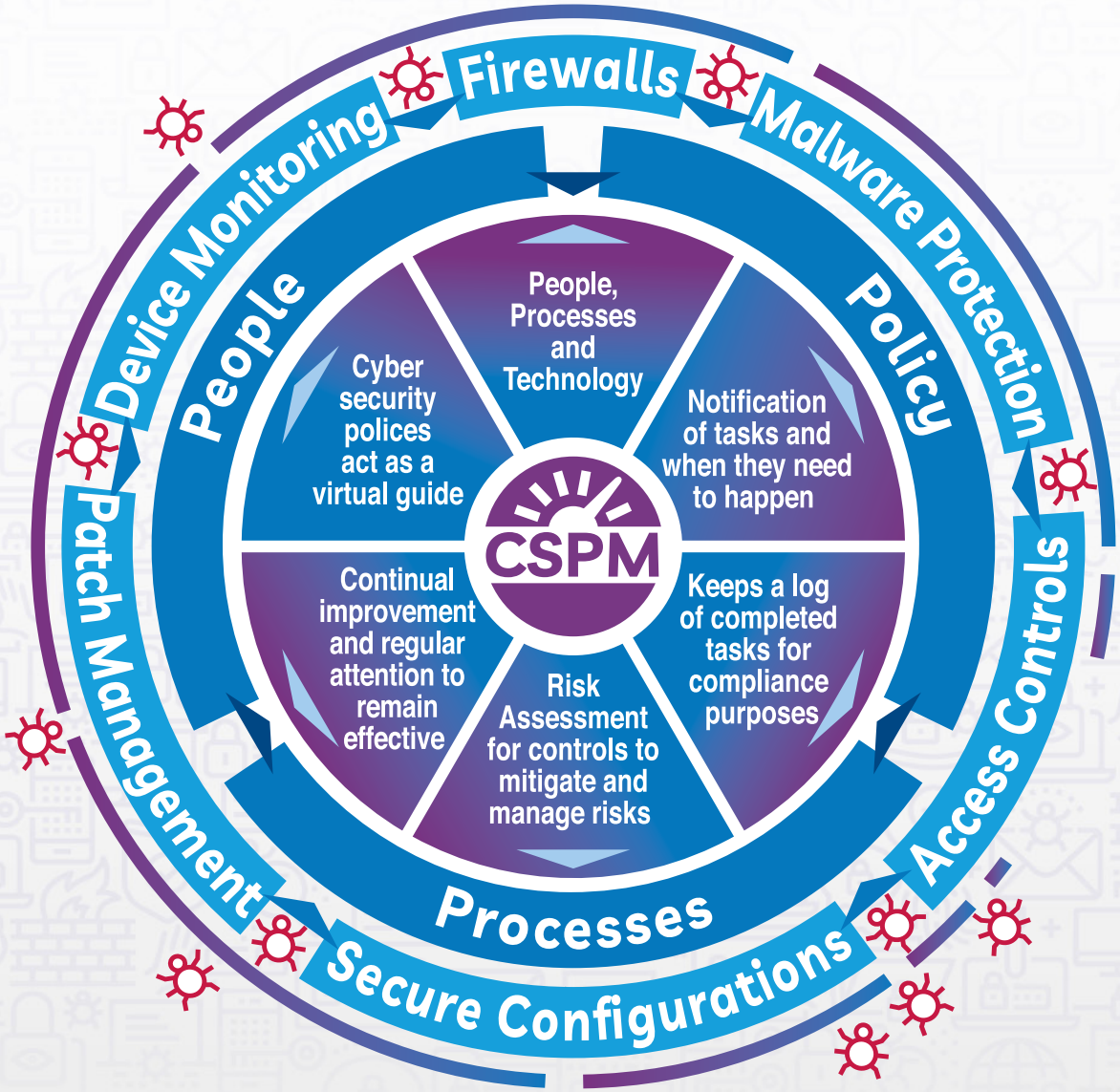
CSPM IASME Governance

Where does CSPM fit?

Cyber Security Policy Monitor

identify, measure and manage your cyber risk

- **90%* of security breaches** are as a result of user mistakes, by way of social engineering attacks
- **80%** of attacks** can be defeated with good cyber hygiene



CSPM provides an end-to-end view, guidance and oversight for cyber-security. It records the actions taken to ensure employees are aware of the dangers and therelevant security technology products are deployed to keep an organisation secure.

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

* National Cyber Security Centre (NCSC) www.ncsc.gov.uk/report/weekly-threat-report-7th-february-2020
** 80% reference www.ico.org.uk/action-weve-taken/data-security-incident-trends/

CSPM

Three steps to a good security posture and compliance

Measure 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 and measuring their awareness and training 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. CSPM 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. CSPM keeps track of training progress - so you don't have to!

Manage Data Security

In the event of a breach your organisation will need to inform the relevant authorities and demonstrate that you ensured appropriate security was in place to protect your own and other people's data. That extends to all third-party 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.

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

Governance

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

- CSPM maintains a library of policies and documents an organisation would need to implement the standards it selects to follow
- Events and tasks are at the heart of how CSPM 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 help monitor governance and keep management updated CSPM incorporates a dashboard and automatically generates 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

Removing cost and complexity

CSPM is a simple and cost-effective way to manage the organisation's cyber security workflow and compliance needs to achieve certification.

Why CSPM?

- **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 common cyber threats 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 your firewalls set up correctly? Are they functioning effectively and regularly scanning for threats to your systems?
9.	Can your IT providers show you how they are protecting your information?

Extra printed page

Extra printed page

Cyber Security Policy Monitor

Measure, manage and monitor cyber risk

Contact Us:

UK +44 (0)808 189 3226

US +1 (1) 844 258 2001

Visit us online: **www.policymonitor.co.uk**