Essential Cyber Security Bundle

Keep calm and carry norm.

What is it?

Specifically designed for those organisations with between 25 and 75 employees, the **norm.** Essential Cyber Security Bundle helps businesses save the time, money and stress normally associated with traditional cyber security solutions.

Offering comprehensive protection against known and unknown cyber threats, the **norm.** Essential Cyber Security Bundle addresses the three pillars of an effective cyber security defence – process, people and technology. Subscribers gain access to the **norm.** industry leading multi-level reporting and online Visualiser which clearly demonstrates how well a business is protected, and the actions they need to take to improve their cyber security posture.

Available for a single monthly per device fee, the purpose of the **norm.** Essential Cyber Security Bundle is simple:

* To allow organisations to focus on their core business operations by managing their cyber risk

* To deliver enterprise-grade cyber security protection at an affordable price

* To provide a simple and easy to understand picture of an organisation's level of cyber protection and how it can be enhanced

Why now?

Smaller organisations make attractive targets for cyber attackers. They're often constrained by time, finances and a lack of skilled cyber security personnel; and the resources they do have are focused entirely on core business functions. Hackers and cyber criminals know this. And so does the team at **norm.**

But resource constraints shouldn't mean that these organisations are unable to protect their people, data and online assets. **norm.** is committed to helping organisations of all sizes, which is why with the Essential Cyber Security Bundle it's created a comprehensive package of protection that allows smaller companies to benefit from the latest technology advances and the knowledge and expertise of a team of certified cyber security experts - all at a price point that's hard to believe.

A comprehensive cyber security defence is increasingly critical to an organisation's ability to transact, attract new customers and grow. Pressure from suppliers, customers and regulators to demonstrate that their data is adequately protected is only going to intensify, and many businesses today rely on the availability of their online systems in order to deliver products and services.

Regardless of whether a company is mandated to do so or not, managing cyber security risk is now a critical Board-level consideration. Organisations therefore need to ensure that they have full visibility of their cyber risk exposure and the peace of mind that comes from knowing they have the appropriate process, people and technology-related controls in place – without the burden of managing them internally.

The **norm.** Essential Cyber Security Bundle offers:

* Powerful cyber security technology from recognised global industry leaders

* A fully managed service backed by a 24/7 UK Security Operations Centre (SOC)

* Accreditation to industry-recognised cyber security standards

* Ongoing training and awareness for employees

* An affordable monthly fee on a pay-as-you-go basis

What's included?

The **norm.** Essential Cyber Security Bundle is comprised of the following service modules:

Process:
* Cyber Essentials certification

People:
* Continuous Cyber Safety and Phishing Awareness Training endorsed by the NCSC

Technology:
* Vulnerability Management – to provide visibility into vulnerabilities across the core technology estate, whether that is the data centre, the office, the Cloud or the end user device

* Endpoint Threat Detection & Response – founded upon constantly updated Global Threat Intelligence, The **norm.** 24/7 Security Operations Centre continuously monitors an organisation's digital environment for new threats and attacks. When an incident occurs, subscribers are alerted and the suspicious device (and threat) is isolated immediately

* Microsoft Office 365 Cyber Insight – Monitoring the business critical Office365 infrastructure is imperative for any organisation. In addition to 24/7 proactive and preventative monitoring of the platform, the **norm.** team is on hand to guide internal IT teams in ensuring that their environment is securely configured in line with industry guidance

To further enhance your level of cyber resilience **norm.** offers two additonal modules:

* **Patch Management** – remotely correlates identified vulnerabilities with available patches, which are then deployed across an organisation's endpoints, regardless of where and how they are connected to the internet

* **Email Threat Protection** – detects and blocks unwanted and malicious email traffic, including targeted and advanced attacks such as phishing and whaling

Want more detail?

To register your interest and get one of the team to call you <<ClickHere>> or just give us a call on **+44 (0)20 385 55242.**

WESTCOAST CLOUD

Powered by **norm.**
*Reassuringly dull cyber security

In a nutshell…

The **norm.** Essential Cyber Security Bundle addresses process, people and technology to provide comprehensive protection against known and unknown cyber threats. Industry leading multi-level reporting and an online visualiser clearly demonstrate where a business is protected and the action you can take to improve.

FAQs…

We are not a large multinational business, surely we're not a target?

Cyber attackers don't care how big a business is, they care about how easily they can compromise or extract sensitive data or money from them. If there is a prize to be had, they will look for organisations with the weakest defences and target them. It is often easier to extract a couple of thousand pounds from several businesses than a larger sum from a single business that has a comprehensive strategy and protection measures in place.

Could my existing IT provider provide a similar service?

An existing provider may be able to provide certain elements of the service – such as managed endpoint security and support. However they won't be able to offer a service that addresses all elements of a comprehensive cyber security defence. There is also an obvious conflict of interest if a company's IT provider is also asked to assess and improve its cyber resilience, as they are effectively marking their own homework and cannot be truly independent and impartial.

Should we wait until xxx project is completed before subscribing to the service?

Regardless of the status of any internal programmes, the threat of a cyber attack is constant. The flexible nature of the **norm.** service allows customers to protect their technology topology no matter where it resides. If it's on premise, in the Cloud, or somewhere in between, the **norm.** service will adapt as the business transforms. IT projects present numerous risks to a business, the **norm.** Essential Cyber Security Bundle ensures that the cyber risk is one that is effectively mitigated such risk that can be mitigated.

Even if we were attacked, there's nothing of real value the attackers would want, so why do we need this?

That may be true, but can the same be said for your customers and suppliers? Once an attacker gains access to an organisation's environment they can easily find sensitive and confidential data relating to both that organisation, as well as using it as a platform to attack its customers and suppliers – effectively masking their true identity. The direct impact to the organisation may be negligible, but being the cause of a significant loss to its customers could be catastrophic financially as well as legally.

How do I tell if the service is actually providing any value and the protection claimed?

One of the biggest challenges associated with cyber security protection is demonstrating value and proving how the investment is benefitting the business. The Essential Cyber Security Bundle addresses this via its customer Visualiser, which demonstrates how the service processes the millions (yes millions!) of events that pass through an organisation's technology estate on a daily basis. It also delivers insight into the hundreds of alarms and alerts which are analysed in order to identify the one or two real incidents that pose a threat to the business on a constant basis. The Visualiser clearly displays how the **norm.** service eliminates the noise and allows our team of cyber security experts to focus on dealing with the real threats.

norm.