A product sheet from O$_2$

O$_2$ business

Capsule – Secure Mobile from O$_2$

For organisations looking to surround their mobile devices with next generation Cyber Security Protection.

Secure your mobile devices…

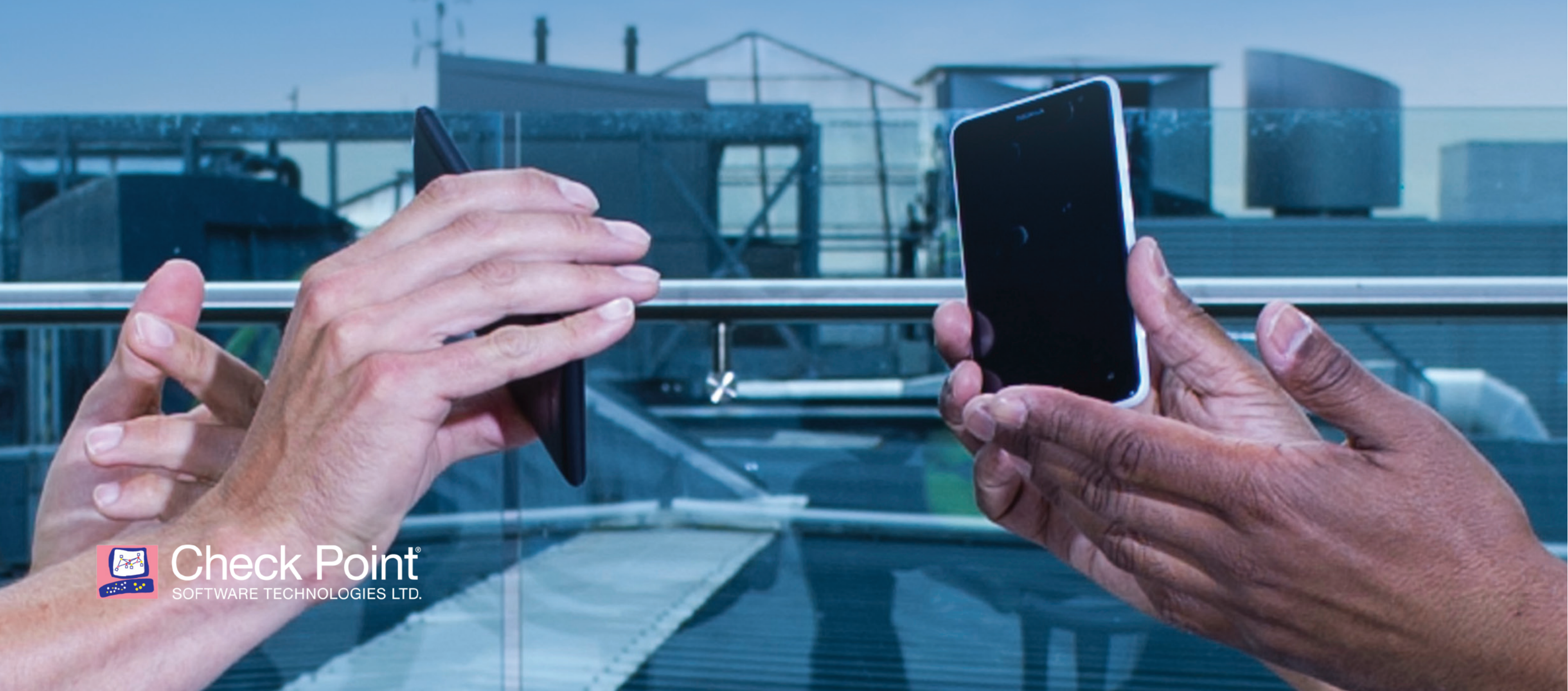
Cyber Security threats no longer only threaten networks, laptops and servers. Organisations increasingly rely on smartphone and tablet technology to ensure their users can be productive, where ever they are and however they connect. Organisations are providing mobile and remote users with increased access to applications and data required for them to do their job via these devices.

Until now, security levels for smartphone and Tablet users have been relatively low, with few of the security policies in place within corporate networks being able to be applied to users outside of the network.

Yet with increased connectivity comes increased risk. As the demand from employees to remotely access corporate data grows, so do the gaps that inevitably open within your infrastructure. The result is a series of security 'blind spots' that expose organisations to new avenues of attack.

Capsule - Secure Mobile from O2, powered by Check Point's Capsule, enables organisations to provide a powerful and continuous level of security across their entire business operation. The solution provides always-on, always up-to-date protection for Smartphone and Tablet users outside your security perimeter – to prevent suspicious file downloads, block malicious activity, and stop bot attacks before they cause any damage.

Static policies, containers, PINs and passwords provide little protection against today's sophisticated cyber threats, and they can't tell you when an attack is underway. Capsule's intelligent threat detection technology monitors more than just one attack vector. It looks at a whole device in context, including its environment – a key component of any successful mobile device security strategy.



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Bringing the threat to life…

According to the latest insights from Dimensional Research[1]:
Device usage continues to grow:
72% of companies more than doubled the number of connected mobile devices in the past two years, while
75% allow personal devices to connect to their corporate network.

And so does the threat:
82% of security professionals expect mobile security incidents to increase this year with
64% say the cost of remediating such incidents is increasing.
In 2014 over 11.6 million mobile devices were infected by malware.

The benefits of capsule…

A complement to your existing MDM

Mobile Device Management (MDM) helps you to manage, configure and monitor mobile devices – Capsule enables you to protect them. This means adding the capabilities needed to ensure effective malware protection, and greater protection against malicious data going in and out of any device.

It offers real-time protection

Capsule calculates the responses to known and unknown threats to prevent compromised devices from gaining access to your organisation's network. Should a threat be identified, all mobile devices traffic is directed through a secure tunnel to the cloud, where extended protection is enforced on all traffic to and from the device. In addition, Capsule offers the flexibility to create unique security and compliance policies for different thresholds, or for different individuals or groups of users.

Maintain full visibility with a single, integrated platform

The Capsule threat analysis creates real-time intelligence about the security posture of the mobile devices you support. This can be fed into existing enterprise systems like your security information and event management (SIEM) platform. Detailed logs and other indicators of compromise can be filtered to trigger response actions that help your security team take action quickly to control and eliminate risk.

Deploy advance mobile security with ease

Whether you support 30 or 300,000 devices, integrating Capsule with your MDM is fast and easy. Capsule is also designed to be non-intrusive, making it easy for users to keep work data secure – maintaining device performance while respecting end user privacy.

Why O_2?

We are a trusted adviser with years of unrivalled business mobile experience. Whilst others may offer a single product or solution, we have a substantial portfolio of Enterprise Mobility solutions which can be integrated, including platforms, devices, applications and even on-premise, hybrid and cloud-based solutions. Supported by O2's CAS(T) Security accreditation on our network.

What you get with Capsule

- Cloud-based Behavioural Risk Engine (BRE) determines a device's true risk level and calculates an appropriate response to keep data protected
- Advanced App analysis to check if user installed apps could be malicious
- Advanced Cloud Based attack protection when threat identified
- Seamless integration with your existing infrastructure and MDM solutions
- Easily manage policy and access

Features

- On Device protection against Malware and Cyber Threats
- Cloud Protection for Data Including Anti-Bot protection
- Data centres located across the globe
- Supported on tablets and smartphones running iOS and Android
- Logs are made available for instant analysis online or can be pushed out to local servers or SIEM Solutions
- Cloud based Management Portal with detailed reporting
- Clear user alerts with remediation recommendations
- MDM integration for seamless deployments and compromised device control

We'll support you all the way

To find out more, talk to your Account Manager, call us on **01235 433507** or visit **o2.co.uk/enterprise**

[1] The impact of mobile devices on information security, Dimensional Research, October 2014

[2] Source: Kindsight Security Labs Malware Report, February 2014

Published in July 2015. All information is correct at time of going to print.
Telefónica UK Limited Registered in England no. 1743099.
Registered Office: 260 Bath Road, Slough, SL1 4DX