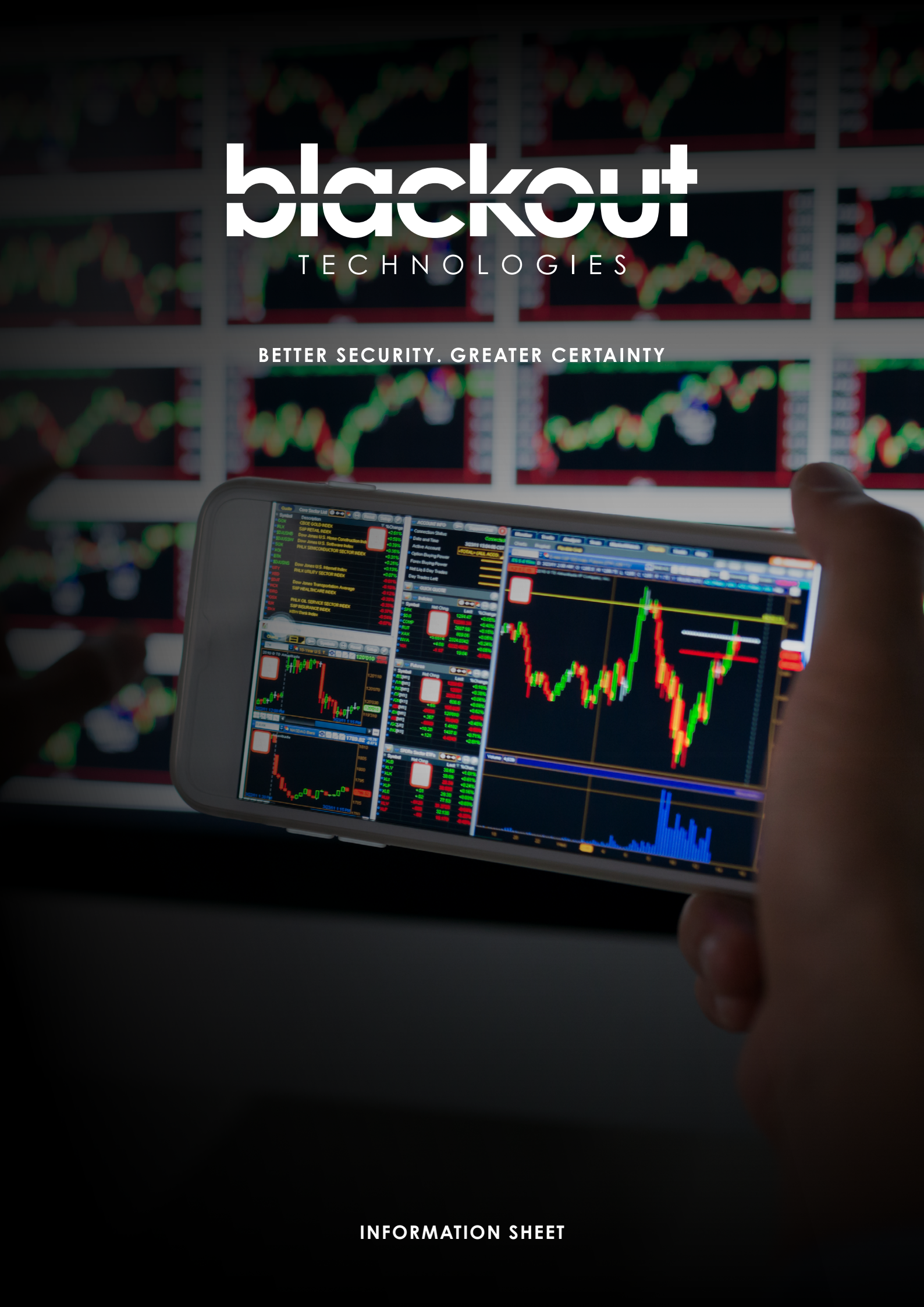
blackout
TECHNOLOGIES

BETTER SECURITY. GREATER CERTAINTY



INFORMATION SHEET

BLACKOUT TECHNOLOGIES

Blackout is a technology company that has developed an innovative system to regulate the use of smart devices in the workplace. It protects sensitive corporate information by restricting unauthorised functionality on smart devices, including encrypted messaging and social media, replicating existing controls on other workplace devices, such as computer terminals. We help companies meet their regulatory obligations to legislation such as MiFID II and the GDPR, limiting unrecordable communications in the workplace, ensuring greater use of authorised channels. By limiting smart device functionality in the workplace, particularly on 4G, our technology also helps to minimise distractions at work and enables employees to improve their productivity.

HOW IT WORKS

Better Security, Greater Certainty

Upon crossing the designated area's threshold, registered devices go 'cold' – losing unauthorised functionality.

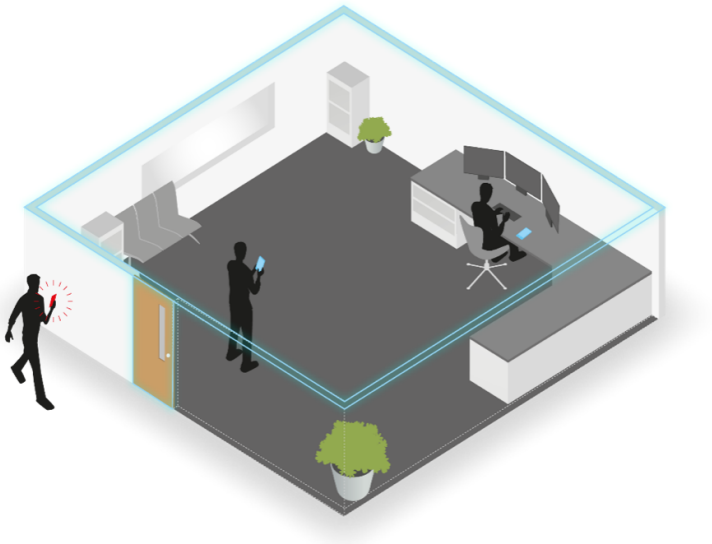
Monitoring and Enforcement

Employees within the designated area are limited to regulated and monitored channels of communication.

Improved Productivity

Removing unwarranted distractions in the workplace helps employees to focus on tasks and enables them to be more productive.

CREATING A DESIGNATED AREA



Regulates accessible sites and apps

Disables camera functionality

Controls smart device use

Unregulated

Regulated

Utilising a non-invasive combination of proprietary cutting-edge technologies, Blackout provides Mobile Device and App Management software to define restricted areas of the workplace and regulate the smart devices within them.

Blackout's system locates and identifies smart devices in defined areas, ensuring they adhere to the employer's security and compliance policies. The technology can also have a beneficial impact on workplace productivity by removing the ability for employees to access unauthorised functionality on their smart devices.

HOW CAN WORKPLACES BE SECURED FROM THE RISKS CREATED BY SMART DEVICES?

Do you really know how secure your workplace is? With the ubiquity of smart devices and encrypted messaging at work, how is your company protecting itself from the regulatory and security risks created by smart devices in the workplace?

Blackout Technologies believes the risks created by smart devices are only beginning to be properly understood. Its innovative blocking technology enables companies to regulate the use of smart devices in the workplace, enhancing information security, preventing data loss, ensuring greater regulatory compliance and improving productivity.

Our primary aim is to reduce the risk that smart devices pose to clients. The business was set-up because our founders, Mark Hadley and Charles Watson, saw first-hand how the saturation of smart devices in the workplace created significant security and regulatory challenges for employers - photographing screens, drudging through Facebook or pinging sensitive information through encrypted channels at the flick of a thumb.

The last 10 years have shown how easily smart devices can be used to compromise corporate security. At the same time as the developmental pace of new technology has accelerated, productivity remains stubbornly unchanged but mental health issues associated with new technologies - especially smart devices - have increased. Unauthorised encrypted messaging in the workplace has aided market abuse and the negative impacts of excessive smart device use on mental health and productivity are well documented. Mark and Charles built Blackout to combat these effects and mitigate risks to companies and employees alike.

Blackout's mobile device and app management software protects its clients' sensitive corporate information by restricting unauthorised functionality on smart devices, including encrypted messaging, social media, voice recording and camera use, replicating existing controls on other workplace devices.

The technology also aids regulatory compliance, ever more vital since GDPR and MIFID II have increased the regulatory burden on companies to hold and protect data. As unrecorded and encrypted communications threaten to bypass existing company security and compliance measures for regulated workspaces, Blackout limits unrecordable communications and ensures greater use of authorised channels - securing the workplace and preventing data loss.

Beyond security, smart devices have impacted the productivity of the workplace. Whilst providing greater certainty, security and compliance, Blackout enables employees to focus and minimise distractions from the relentless and addictive apps on mobile devices.

The system itself works by using a non-invasive combination of cutting-edge proprietary technologies that provide mobile device and app management software to define restricted areas of the workplace and regulate the smart devices within them.

Blackout’s system locates and identifies smart devices in defined areas, ensuring they conform to the employer’s security and compliance policies. It does not have access to personal or private data within users’ smart devices and is only active when users enter workspaces controlled by the system.

As companies continue to allow smart devices within their walls they have a duty to protect their data and maintain security integrity. Blackout is the solution to these growing challenges.

FOR FURTHER INFORMATION:

info@blackout-technologies.com

www.blackout-technologies.com

www.linkedin.com/company/blackout-technologies-ltd

KEY FEATURES

- ✓ Two-step installation
- ✓ Internal directory integration
- ✓ Location-based regulation
- ✓ Time-based regulation
- ✓ Comprehensive administration platform
- ✓ Real time reporting options
- ✓ 4G regulation
- ✓ Policy violation response system
- ✓ Fleet management and push messaging
- ✓ Device policy settings and management
- ✓ 24/7 customer support

INFORMATION SECURITY

- Data leakage prevention
- IP protection
- PCI DSS compliance
- GDPR & MiFID II compliance
- FCA compliance
- IS policy compliance
- IT SOC direct controls
- Risk management for BYODs
- ISO27001 CyberEssentials strategy

PRODUCTIVITY

- Reduced distractions
- Increased productivity
- Optimised workforce efficiency
- Financial benefits for the company