REMOTE WORKING Covid-19

With the recent outbreak of Covid-19 many businesses are implementing remote working policies. During this period of uncertainty, it is more important than ever to ensure you have the correct solutions in place to secure your workforce when working from home.

Censornet have compiled a simple remote working checklist which highlights the key areas you should consider, to ensure your business can continue to operate effectively and securely at this time.

Remote Working Checklist:

- Ensure all users devices have endpoint antivirus installed and are up to date.
- Review existing VPN settings and policies to ensure users only have access to the things they are meant to.
- Be wary of allowing VPN access from untrusted devices, if however, you are allowing users to work from personal devices and VPN into the office, then ensure you're posture checking these devices on your VPN solution – for example, checking they are running up to date AV.
- Consider enabling split tunnelling for users to access the internet and applications like Office 365 directly from home and only send specific traffic over a VPN to applications that need it i.e. on-premises applications.
- Re-instrument gateway protection directly on the endpoint using agents to provide web and cloud application security and ensure head office protection is not sacrificed or bypassed for users working from home.
- If your VPN environment cannot cope with the increase in user capacity, then consider the other options you have for providing remote access to internal applications – such as Remote Desktop Services (RDS), or Virtual Desktop Infrastructure (VDI).
- Review your authentication process to ensure you have adaptive Multi-Factor Authentication (MFA) in front of your cloud applications and any connections back to your corporate environment.
- Resist short term changes to firewall rules which could weaken your security posture.

To help during this period of uncertainty we would like to offer all of our existing customers 60 days of Multi-Factor Authentication (MFA) for free; and if you are already an MFA customer, we will provide you with any additional licenses you might need for a 60-day period.

How can Censornet help?

M. MFA

Enable MFA anywhere it's available
Censornet MFA has support for the broadest range of systems applications and services including all major VPNs, VDI environments and cloud applications

The Censornet agent provides visibility and control to:

- Prevent access to malicious websites, inappropriate content and manage time spent on websites that impact productivity
- Stop users downloading unsanctioned applications, such as executable files
- Restrict specific actions within cloud applications, such as sharing sensitive information over Dropbox

Leveraging cloud security can expedite a secure remote working environment, and with Censornet everything is consolidated into one platform, allowing you to monitor and secure your workforce wherever they may be.

censornet.com

To discuss enabling your remote workforce contact us today.

sales@censornet.com
+44 (0) 845 230 9590

censornet.