

Mission impossible?

Securing today's hybrid work environments is a headache for companies, but the right mix of products can help.



Henk Olivier, Managing Director at Ozone Information Distribution

One of the enduring legacies of the Covid-19 lockdowns is the emergence of hybrid work styles, in terms of which employees work for at least part of the time from home. While time will tell, it does seem clear that many, especially in professional services, will continue to work at least partly from home; one global survey showed that 86% of managers and decision-makers expect employees to work remotely one to two days a week (53%) or three to four days a week (33%).

Key drivers of the move to hybrid working, with the majority of time spent in-office, are

the productivity challenges for anyone who has to work in teams, especially as demand picks up, and the impact on induction and training.

"As a distributor of cybersecurity products, I can say that we are seeing an increase in cybersecurity issues associated with the work-from-home (WFH) phenomenon, including ransomware and the use of phishing to obtain network access," says Henk Olivier, MD, Ozone IT Distribution. "The big issue for companies is how to control the proliferating number of devices being used outside of the corporate network."

The risk is particularly acute for those companies that need to transmit financial and personal data between the company and clients or remote workers. Given South Africa's persistent loadshedding, during which connectivity can be an issue, many companies have had to allow remote workers to download data in order to maintain productivity.

Olivier says that key issues are patch and security updates, as well as password management.

Managing the unmanageable

Products from established CyberSecurity solution provider, GFI Software can help in several ways. GFI LanGuard can help secure these hybrid work environments via patch management and vulnerability scans. It's a surprising fact that many of the most devastating cyber-attacks –remember WannaCry? – were made possible because so many companies simply had not implemented a routine patch. GFI LanGuard also ensures

that end-user devices' anti-virus software is up to date, and it provides a useful dashboard that allows IT administrators visibility of the whole network as well as individual devices.

Another key item in the cybersecurity armoury is GFI KerioControl, a next-generation firewall for small and medium-sized businesses. Olivier says it is easy to use, and allows companies that don't have dedicated security or IT departments to monitor internet traffic to detect threats and neutralise viruses, as well as block dangerous website or applications. It has the important additional functionality of allowing administrators to prioritise and shape internet traffic to improve the user experience.

GFI KerioControl also offers a virtual private network to ensure safe data transfer. Finally, it offers automated reporting so that administrators are alerted to any security issues.

Larger companies should consider Exinda Network Orchestrator to optimise wide-area networks. Exinda allows the company to manage network traffic between sites in order to ensure that even the most complex networks work smoothly.

"Today's and tomorrow's hybrid work styles present a significant security challenge for IT administrators, particularly within smaller companies with constrained IT resources," concludes Olivier. "These products, implemented by Ozone's highly skilled channel partners, provide the tools needed to overcome the challenges cost-effectively." ■

Embed security, easily, with Ozone Distributed Information Technology [\[ozone.co.za\]](https://ozone.co.za)

