

> SMB SNAPSHOT Maxim Employee Benefits Ltd.



South Africa-based Maxim Employee Benefits is an independent provider of solutions to retirement funds, via umbrella and free-standing fund arrangements. The company specializes in administration services to freestanding, employer specific funds, and its independent approach means that Maxim can use and administer any underwriter's products.

THE CHALLENGE

Two months after he joined Maxim in the role of IT manager, Jerome du Toit faced a daunting crisis: a serious, potentially damaging virus outbreak that threatened the company's files, servers, and endpoints. His company had been hit by the W32.Changeup.C worm that spreads through removable and mapped drives, as well as through certain file-sharing programs, and downloads threats and misleading applications to the compromised endpoints. The virus protection provided by Maxim's outsourced IT provider had failed to prevent the malware attack.

"The virus quickly spread off the desktops to the servers," says du Toit. "It hid the main files, so when you went to look for them, all you could see were the shortcuts. When we went into the server, we saw the files hidden in Windows, but five minutes after 'unhiding' them, they disappeared again. We couldn't operate under these conditions."

At the height of the outbreak, when staff arrived for work in the morning, it took them 15 minutes just to login. This was the case for about a week until the gravity of the situation was understood and action sought. That 15 minutes was the equivalent of a total of 27 hours of lost productivity—time when staff could have been managing clients' retirement enquiries; not waiting for their endpoint to login to the network. In total, Maxim's network was so badly compromised by the virus outbreak that the entire business environment was eventually down for three consecutive days.

THE SOLUTION

One of Du Toit's immediate calls was to Infoprotect, one of South Africa's leading cyber security service providers. Infoprotect immediately recommended the deployment of Symantec Endpoint Protection 12.1. In their opinion, it offered a reliable, best practice approach to eliminating with the immediate virus outbreak and safeguarding the systems. Endpoint Protection, they said to du Toit, also offered best-in-class performance, comprehensive protection for Maxim's KVM Linux-based virtual servers, and was very easy to use.

Du Toit was inclined to agree with that recommendation. "I had used other well-known endpoint security solutions in the past, but was never impressed by their capability," he explains. "Compared with Symantec Endpoint Protection, the tools I had experience of are

relatively complex and not very easy to use. For example, it can be quite a complicated process to set rules and policies. You really need to be an expert before you can use either of them. Endpoint Protection is so intuitive, we created the policies in about 90 seconds!"

That same evening, a team from Infoprotect lived up to their name: immediately protecting Maxim's information and removing the virus from the network. Since that attack more than one year ago, the South African financial services provider has not experienced a single virus outbreak.

THE BENEFITS

Specifically deployed to provide antivirus protection, firewall protection, antispyware, and device and access control, Endpoint Protection 12.1 is transforming Maxim's antivirus security, performance, and management. For example, the SONAR program in Symantec Insight™ examines Maxim's programs 'on the fly', as they run, identifying and stopping malicious behavior of emerging threats.

Endpoint Protection 12.1 is also optimized to support the company's KVM servers—the performance is so good, there's barely any noticeable scan overhead, according to du Toit. "The performance is in a league of its own compared with the other tools I have used," he comments. Moreover, the solution is great for Maxim's KVM servers, automatically identifying and managing the virtual clients, and whitelisting baseline images.

Best of all from du Toit's point of view is that the endpoint security solution is so easy to use. "We save a lot of time using Endpoint Protection," he says. "We get real-time, detailed automatic email notifications about what has or hasn't updated. From my experience with the other leading solutions, half my time was spent checking whether they were working properly."

He also has a lot of respect for the work done by Infoprotect. "They came to our rescue," says du Toit. "They identified the virus problem from the start and worked non-stop to resolve it. They have worked like that ever since. They are always on station, ready to support and advise us."

"We save a lot of time using Endpoint Protection. We get real-time, detailed automatic email notifications about what has or hasn't updated. From my experience with the other leading solutions, half my time was spent checking whether they were working properly."

Jerome du Toit

IT Manager, Maxim Employee Benefits

THE ORGANISATION

WEBSITE: www.maximeb.co.za

EMPLOYEES: 80

HEADQUARTERS: Johannesburg, South Africa

THE SOLUTION

- Symantec Partner
Infoprotect
(www.infoprotect.co.za)
- Symantec™ Endpoint Protection 12.1

WHY SYMANTEC?

- Recommendation of partner Infoprotect
- Ease of use compared with experience using other security tools
- Confidence and respect for Symantec brand

THE INFRASTRUCTURE

- Users: 80
- Servers: 5 production servers, virtualized under Linux KVM
- Operating systems: Microsoft Windows, Mac OS
- Applications: Exchange, SQL, file/server, Active Directory, among others