

Customer profile



Region: global
Sector: Oilfield Services
Employees: 1,200

The company

The Linz company VAOS Ltd. assumes all responsibilities, from the planning of oilfields to the construction and operation of the plants, and is in charge of all services for pipelines and refineries. The main branches are located in Malta, Austria and Libya and a number of smaller branches in the Sahara are also connected.

The initial situation

Up to now, the main branches and the smaller VAOS locations were protected by Check Point solutions. The increased demands made on company IT make it necessary to find new approaches to enterprise security.

The solution

SecureGUARD TMG950 appliances based on the MS Forefront Threat Management Gateway 2010 connect all locations via VPNs, with VoIP and access to SAP applications. Central management is located in Linz and so is IT security. Microsoft offers a one-stop solution consisting of a firewall, AV scanning, URL filtering and HTTPS inspection.

The benefits

The SecureGUARD solution in conjunction with the Forefront Threat Management Gateway 2010 provides cost advantages in comparison with the Check Point systems it replaces. The licenses provide the same performance at more reasonable cost. The SecureGUARD solution guarantees further savings of time and money through faster rollout and central management for all locations. SecureGUARD provides VAOS with a one-stop solution for hardware and software maintenance.

Microsoft Forefront
Threat Management Gateway 2010: Security Solutions

Security oasis in the desert

“We have a reliable, efficient security solution in the Forefront Threat Management Gateway 2010 (TMG) from Microsoft and an outstanding service and technology partner in SecureGUARD.”

Stefan Tomek, IT manager of VAOS Beteiligungs- und Handelsgesellschaft

VAOS Ltd. is a company which specializes in oilfield projects in the desert. Being the project leader, it assumes all responsibilities, from the planning of oilfields to the construction and operation of the plants, and is in charge of services for pipelines and refineries. The main branches are located at Portomaso (Malta), Linz (Austria) and Tripoli (Libya) and a number of smaller branches are also connected. These are usually located in the middle of the Sahara Desert and some of them are hundreds of kilometres apart, so their IT infrastructure has to be able to withstand extreme climatic conditions.

At the main branches of VAOS and at a few of the smaller locations, company IT has up to now been protected by Check Point firewalls.

These have now been replaced by SecureGUARD appliances based on the Forefront Threat Management Gateway 2010 from Microsoft. The joint SecureGUARD-Microsoft solution guarantees VAOS the secure and reliable connection of all branches via satellite, including stable Internet telephony and SAP access.

"The SecureGUARD TMG950 appliance with the Microsoft TMG 2010 provides the security level we require at a much lower price than other products of competitors."

Stefan Tomek, IT manager of VAOS
Beteiligungs- und Handelsgesellschaft

Location: the Sahara desert. For the IT infrastructure of the oilfield projector VAOS, this means extreme demands at all levels. With maximum temperatures of 58° C, the Libyan desert region is considered to be the place with the highest temperatures ever measured worldwide. In addition, the branches are often hundreds of kilometres apart and there is usually no electricity supply, let alone telephone or Internet connections. In spite of all the adversities, the secure connection of all branches must be guaranteed. Up to now VAOS ensured this via large Check Point solutions at the three main company branches and Check Point VPN-1 Edge devices at the smaller branches.

The expectations which VAOS has with regard to reliable modern company communication via the Internet made higher demands on IT security too. For example, access to SAP applications was to be possible from the outside and via site-to-site VPNs in future. A request was also made for a reliable VoIP connection, central management from the Linz location and access to the distributed Microsoft systems at various locations. "The monitoring of the users is becoming increasingly important for a company too: for security reasons, it should always know where its users are in the Internet and who is logging in where and when," explains Helmut Otto, the manager of SecureGUARD GmbH. As a result, the existing Check Point solution had to be tested in order to show whether it could live up to the increased expectations of VAOS.

Too many features we don't need

It was decided to introduce a new solution: the security software Forefront Threat Management Gateway 2010 (TMG) from Microsoft, which is integrated into the optimized hardware of a SecureGUARD

TMG950 appliance. Stefan Tomek, IT manager of VAOS Beteiligungs- und Handelsgesellschaft, sums up as follows: "Check Point is a tried and tested solution which has given us good service. When we compared the benefits with the costs, however, we realized that the new licensed model was not suitable for our demands - it was simply too expensive, that is." Otto also confirms that Check Point offers a wide range of functions, "but our customer does not use them, and consequently he does not benefit from them either." This is especially true considering that the number of users connected to the many smaller branches of VAOS often only amounts to three or four.

Tomek describes the complicated or non-existent Linux support of the new Check Point software as a disadvantage too: "For us this would have meant purchasing additional new appliances from another supplier. The choice was between paying about 30 to 50% more or looking around for a new solution."

Alone in terms of the necessary licenses, the decision to use the SecureGUARD TMG series means cost savings of around 30% in comparison with the Check Point products. "The Microsoft TMG 2010 allows us to save nearly € 20,000 on licensing fees for ten locations compared with Check Point. Tomek concludes that it would be irresponsible to make any other decision here as the more economical product of the competitors does the necessary job too."

Another serious advantage which was crucial for the decision to purchase this solution was the convenient connection of the VAOS back office, which is based on Microsoft infrastructure throughout. The SecureGUARD appliance allows access to distributed Microsoft systems at the various main locations. The Threat

The technology in a nutshell

The Microsoft Forefront Threat Management Gateway (TMG) is the next generation of network security solutions from Microsoft and is based on the tried and tested processes and technologies of ISA Server (Internet Security and Acceleration Server). As an integrated security gateway for the company network, TMG offers a secure connection, simplified administration and protection from numerous Internet-based threats. It functions as a Web gateway security solution which protects the company and its employees from Web-based threats and consists of a firewall, VPN, intrusion prevention, antivirus scanning and URL filtering. All functionalities of the powerful Microsoft Gateway TMG 2010 are "rolled up" into one optimized hardware appliance from SecureGUARD: for the customer, this means guaranteed fault-free operation of his security solution and no possible collisions with BIOS, network components or RAID controller during updating as well as simple and convenient maintenance and administration.

Photo: VAOS



The desert makes high demands on IT.

Management Gateway 2010 communicates smoothly with the Microsoft infrastructure such as the Exchange mail system and update and client deployment (Microsoft Windows Deployment Server). It fetches the user and access information from the Active Directory, thus protecting the company network in an optimum way.

"The decision was made easier still for us by the fact that Microsoft had already announced the TMG and that SecureGUARD as a long-standing partner of ours had been so committed to developing the hardware and optimizing management," Tomek explains. As "proof of concept", the company used Microsoft ISA Server 2006 appliances from SecureGUARD at smaller locations at an early stage: "This worked well and saved costs."

Successfully replaced

A virtualized Microsoft Enterprise Management Server (EMS) has now been installed

at the main IT location in Linz in addition to a cluster with two nodes. Two SecureGUARD TMG950 appliances are used for the two nodes. Each of the other two larger locations at Portomaso and Tripoli are connected via a TMG950 appliance.

The SecureGUARD Starter Edition was sufficient for the desert branches, which do not have many users: this is an economical alternative for connecting locations with a small number of users as it uses a modified version of the TMG Workgroup Edition. The price is very reasonable due to the limitation to 25 simultaneous users.

All branches are connected via site-to-site VPN and are administered centrally from Linz. This is made possible by the "Branch Office Deployment" function of SecureGUARD appliance management in conjunction with the new functionality of the Microsoft Enterprise Management Server in Linz, which permits the central administration of the branches.

Further information

Reference customer

VAOS Ltd.
Portomaso Business Tower Level 18
Portomaso STJ 4011, Malta,
Tel.: +356 23165000
Fax: +356 23165600
E-mail: info@vaos.com
www.vaos.com

Microsoft-Partner

SecureGUARD GmbH
Helmut Otto
Industriezeile 35
4021 Linz
Austria
Tel.: +43 732 601440
E-Mail: office@secureguard.at
www.secureguard.at

Business Customer Support

Microsoft Deutschland GmbH
Konrad-Zuse-Straße 1
85716 Unterschleißheim
Tel.: 0180 5 672330*
Fax: 0180 5 229554*
E-Mail: btob@microsoft.com

*0.12 Euro/min. throughout Germany

For other customer references
please go to:

www.microsoft.com/germany/kundenreferenzen

The programmers at SecureGUARD ensured the communication of customers and suppliers via the enterprise software SAP by using a self-developed NAT driver specially designed for the Microsoft TGM 2010. The centralized temperature monitoring of the individual branches is not possible without this development. Comprehensive company security is provided for by the functionalities of the new Microsoft Threat Management Gateway 2010: all branches are protected by a firewall, antivirus scanning, URL filtering and HTTPS inspection.

Clean error-free communication via satellite

Many locations are connected to the company network via satellite and Internet as a result of their problematic geographical location. As a partner for this task, VAOS chose the German supplier ATREXX, which also developed and installed a Quality of Services solution on the satellite modems. The satellite connections made high demands on data transmission: in comparison with a connection via under-sea cable in a conventional transatlantic connection operating at a transmission rate of 20 milliseconds, for example, the satellite connection requires 500 milliseconds. This is a problem for any software connection, but SecureGUARD has mastered it extremely well: "Thanks to the optimized functionality of the appliance, a good, clean VoIP connection via satellite has been achieved," says Tomek full of praise. The same is true of central management and the SAP applications.

Successful liaison: Microsoft and SecureGUARD

"This project shows once again that SecureGUARD has the serious advantage of being able to offer the customer a one-stop solution consisting of design, software, hardware, implementation and support," stresses Karl Lehner, Solution Specialist – Management & Security for Microsoft Austria. As for the customer, the benefits of the SecureGUARD appliance based on the new Microsoft solution are obvious: with the new security functions, the entire administration can be carried out from one location and downtimes are minimized as a result of the improved disaster recovery, in which Microsoft integrates a firewall and a malware and content protection system into one unit. On the part of VAOS, this saves personnel resources and a considerable amount of time during operation, thus reducing the costs required for implementing IT security. This is also contributed to by the benefits of the faster software rollout ensured by the SecureGUARD Appliance Management System as well as by wizards such as the Branch Office Deployment Wizard.

The Linz company has been the ideal partner for Tomek for a long time now: "With SecureGUARD, we can completely count on reliable around-the-clock support for hardware and software and on well-designed solutions which function in an optimum way." In conjunction with the technology partner Microsoft, SecureGUARD will continue to be the principal partner in future too.

Software and Services

■ Microsoft Forefront
Threat Management Gateway 2010

Partner

■ SecureGUARD GmbH