



## Wüstenrot Gruppe

### Customer Profile

- Large Austrian financial services company with building society and insurance branches

### Industry

- Financial Services

### IT environment

- 3,500 employees

### Challenge

- Previous SIEM solution did not effectively support company's evolving needs

### McAfee solution

- McAfee Enterprise Security Manager

### Results

- Implementation in only 15 days
- High-performance, accurate logging of data from 100 sources
- Handling of more than 1,000 events per minute
- Robust log archiving and encryption capabilities
- Configurable dashboards to support a full range of data types and reporting

# McAfee ESM Strengthens Banking and Insurance Company's Security Visibility

Wüstenrot Gruppe is one of Austria's largest financial services companies, with more than 3,500 employees and 3.5 million customers. The company has two divisions: a building society offering banking and mortgage lending for residential construction projects, and the Wüstenrot Insurance group. Wüstenrot has subsidiaries in the Czech Republic, Slovakia, Hungary, Slovenia, and Croatia.

### Business Challenge: Secure Banking and Insurance

Data and network security is a critical success factor for any company operating in the banking and insurance sectors. In order to preserve its reputation and the trust of its clients, Wüstenrot is committed to maintaining the highest levels of security -- especially in regard to sensitive client data and the management of banking systems and networks.

Wüstenrot previously used IBM Tivoli Compliance Insight Manager for processing and analyzing security event logs, but that solution could not keep pace with the company's growth and evolution. Therefore, Wüstenrot identified several requirements for a new security information and event management (SIEM) solution. The company was looking for a complete turnkey solution including hardware and operating system with simplified reporting, no-agent log collection, and support of monitoring metrics including BASEL II, PCI-DSS, and ISO 27002. In addition, Wüstenrot sought a solution that could provide immediate availability of all events occurring over the last five days and logging of data from Oracle HPUX, Windows Server, Microsoft SQL Server, CheckPoint, and McAfee ePolicy Orchestrator (ePO). Wüstenrot looked for a SIEM vendor that would not place license restrictions on the number of log sources, with a guarantee on maintenance costs.

### Why McAfee: High-Performance SIEM

Based on these requirements, McAfee Enterprise Security Manager (ESM) became Wüstenrot's top candidate – but the company decided to put the SIEM solution to the test with a proof-of-concept (PoC) implementation before making a final decision. In PoC mode, McAfee ESM was required to log data from each source in its own environment and then verify that outputs and performance corresponded to Wüstenrot's internal specifications. Systems integrators Auriga Systems and COMGUARD were able to deploy McAfee ESM in less than a day, which also included a short workshop on the solution's advanced capabilities and mutual approval of metrics for a successful PoC. After operating for a month, the McAfee ESM proved its ability to link to all required log sources.

### The McAfee Solution

Based on the successful PoC and a favorable pricing model from McAfee, Wüstenrot selected McAfee ESM model ETM-4600-ELM. With the ability to log at least 1,000 events per second (EPS), McAfee ESM was the ideal choice to meet Wüstenrot's requirements.

Working with the systems integrators, the Wüstenrot IT team was able to implement McAfee ESM in only 15 working days. Pulling from 100 different log sources, the solution demonstrated very high log parsing accuracy and performance.

---

*“McAfee Enterprise Security Manager is a very agile and effective solution that enables us to handle events over several months in a matter of seconds and get immediately to the relevant information. The dashboards are very intuitive and readily usable by our security team and myself, and I’m able to easily identify problems and then to respond to them in time.”*

— Bc. Jiří Dolejš,  
Security Manager,  
Wüstenrot

---

After the full implementation of log sources, the implementation team configured dashboards and reports according to pre-agreed specifications in several key areas. These included changes in the permission levels for Active Directory, crashes and restarts of servers, crashes and restarts of services, antivirus events across the infrastructure, and newly detected devices on the network.

McAfee technical support provided a prompt and effective solution for the single issue that popped up during implementation, an incompatible time stamp format for the Oracle database audit log. McAfee was able to devise a special timestamp format within the native Oracle environment.

#### **Future Plans**

McAfee ESM far exceeds Wüstenrot’s initial requirement to provide immediate availability of events over the last five days, with aggregated log information now available for immediate processing for up to one year.

Phase one of the implementation involved launching the SIEM and filling it with data, and now Wüstenrot is working to add analytical dashboards for selected areas that need to be visible to the security department. In addition, Wüstenrot is focusing on tuning correlation rules so as to eliminate false positives for default rules.

Archiving of logs in their original form is limited only by the amount of storage space. Wüstenrot has high standards for the integrity and confidentiality of its archived logs; therefore, the company has allocated dedicated storage array hardware for the logs that makes use of the certified cryptographic functions in McAfee ELM. With an initial goal to archive logs for one year, Wüstenrot is currently preparing the storage arrays. The next step will be to activate the log archive function with indexing for full-text searching using McAfee Enterprise Log Manager.

