

# The Cologne Bonn Airport Optimizes IT security with the McAfee SIEM Solution



## Airport Cologne Bonn

### Customer profile

The Cologne Bonn Airport is one of the largest commercial airports in Germany with more than nine million passengers and over 740,000 tons of air freight.

### Industry

Aviation.

### IT environment

More than 1,800 employees, multiple central management consoles within a heterogeneous environment.

### Challenges

- Heterogeneous IT landscape.
- Strict compliance and IT security requirements.
- Legal administration and access controls.
- Aggregation and correlation of existing data.

### McAfee solution

- Enterprise Security Manager
- Advanced Correlation Engine
- Enterprise Log Manager
- Vulnerability Manager

### Results

- Extended options for security incident response and forensic processes.
- Results-based analyses.
- Improved options for auditing and compliance tasks.
- Automatic and targeted handling of threats and faults.

The Cologne Bonn Airport is an economic power center in Germany and ensures a high number of business travelers, due to several exhibitions, conventions, and multinational corporations seated in the region. In contrast to many other airports that are already experiencing bottlenecks, Cologne Bonn has a considerable reserve for take-off and landing strip capacities. Airlines can therefore select their slots freely for an optimal flight plan. The modern take-off and landing strip system, with the longest strip measuring 3,815 m, also allows nonstop flights with fully loaded and fueled jets throughout the world; only one of the reasons why, for instance, UPS operates its European hub at Cologne Bonn and why FedEx has also set up its hub for central and western Europe there.

## Business Trigger: Security and Compliance in a Heterogeneous IT Environment

A company this complex and with the special demands of an airport must make especially certain that all of the requirements pertaining to IT security and IT compliance are fulfilled. In the case of the Cologne Bonn Airport, verifying IT security has not always been easy; the IT infrastructure had grown heterogeneously in several large networks over the years, different system architectures had to be harmonized and evaluated centrally.

Until recently, this complicated, decentralized analyses at different management consoles resulted in what, in the eyes of René Koch, the IT Security Manager at the Cologne Bonn Airport, considers an excessively high use of resources. To generate a risk analysis and process security incidents, an IT organization must be able to easily, quickly and reliably track information about events in conjunction with the legal administration, access controls as well as data on threats and vulnerabilities.

René Koch says, "This information was generated locally here and recorded at different times. Correlating already existing information was virtually impossible." The IT team had to identify potential vulnerable areas and manually assign them to the relevant information systems. A statement regarding the degree of the vulnerability wasn't always possible on short notice, so complying with the requirements of IT security and compliance could not always be definitively ensured. A new solution was necessary in order to improve the situation.

## Solution Focus: Integrated Control Cockpit for Security.

It was mandatory that the new solution fulfill two objectives: increase transparency and make the IT landscape centrally controllable. The security specialists working with René Koch wanted to be able to determine the status of their security posture in close to real-time. All information pertaining to IT security should also be able to be partially controlled, influenced and documented via an integrated "control cockpit".

Documented information must be complete, secure against forgery, and incapable of being revised afterwards to ensure the probative value of the reports. In addition, the solution had to be capable of normalizing the heterogeneous information to create an overall picture and allow the team to easily filter out individually prioritized processes from the multitude of overall results. Also, with regard to access rights, the solution should allow granular control.

The Cologne Bonn Airport ultimately chose McAfee Enterprise Security Manager for their security information and event management (SIEM) needs. McAfee Enterprise Security Manager not only fulfills the requirements for robust reporting, it also offers the

---

*“Security is the highest priority at an airport and McAfee is an important partner for us in this regard. [McAfee Enterprise Security Manager] ESM helps us in particular to create transparency and to control our IT according to the requirements. Thanks to the central management capabilities of [McAfee] ePO, we can now utilize our resources in an extremely targeted manner.”*

—René Koch, IT Security Manager, Cologne Bonn Airport

---

security specialists the ability to react to security incidents quickly and on a founded basis. Because the system allows for a risk-based prioritization, tasks for combating vulnerabilities and threats can be intelligently controlled and sustained.

### Why McAfee? **SIEM Individualization for Tailor-Made Security**

Today, the Cologne Bonn Airport information technology department can observe relevant events independent of the product and adapted to the respective needs of the different specialist teams. “That saves us not only time during ongoing operations, but we can also focus training on one solution,” explains René Koch. “Our analyses deliver comprehensive results, detached from the architecture-dependent event reports from the respective competence center. By also integrating McAfee Vulnerability Manager and McAfee ePolicy Orchestrator® (McAfee ePO™), we are now in a position to identify vulnerabilities, and combat threats and faults in our IT landscape in a targeted manner, while managing everything in a central location.”

Thus, the penetration tests supplement a constant vulnerability analysis of potential hazards and vulnerabilities. The results and information of active and passive components are continuously evaluated and centrally prepared in an integrated view. Deviations from and violations to the defined rules automatically

trigger notifications. Thus, the administrators are always informed about potential security-related incidents.

The security specialists immediately started developing their own measuring criteria based on the analyses and fault notifications and storing them in the SIEM system, for instance, with regard to changes in the volume of data processed in the network landscape. If measurement values are conspicuous, the responsible system administrators automatically receive notifications. The multitude rule books within McAfee Advanced Correlation Engine can be individually adapted by the team. “The opportunity for integrated alarm notification and reporting created by this offers an advantage in comparison to other solutions on the market,” explains René Koch.

A comprehensive solution for managing security information and events significantly simplifies the control of complex IT infrastructures. The more integrated and intelligent the solution, the more control it offers the responsible persons. René Koch concludes, “Security is the highest priority at an airport and McAfee is an important partner for us in this regard. [McAfee Enterprise Security Manager] ESM helps us in particular to create transparency and to control our IT according to the requirements. Thanks to the central management capabilities of [McAfee] ePO, we can now utilize our resources in an extremely targeted manner.”

