

Commerzbank

HP Enterprise Security Customer Case Study

“The high quality of ArcSight technology, along with the excellent service received during implementation, allowed an extremely fast deployment, exceeding our needs and expectations of a SIM solution.”

—Uwe Tacke, IT Production and CERT, Commerzbank

COMMERZBANK 

Customer Brief

Commerzbank offers tailor-made services in retail and corporate banking to its customers across the globe. Germany’s second largest bank is represented in over 40 countries, employing 35,000 staff, with over eight million customers worldwide. Its partnership with ArcSight has enabled Commerzbank to provide high standards of security to its global customer base.

Product(s)

- ArcSight ESM

Business Benefits

- ArcSight ESM provides Commerzbank with the ability to filter and correlate millions of security events received each day
- Commerzbank technicians are released from hours of low-level analysis, allowing them to concentrate on improving IT security
- The solution enabled Commerzbank to achieve a strong ROI, exceeding needs and expectations



HP Enterprise Security Customer Case Study:

ArcSight provides this global retail and corporate bank with a clear overview of its IT infrastructure and security environment, with automated reporting and correlation.

Industry: Banking

The Commerzbank Challenge

Whilst dealing with the increasing threat environment of the financial sector, Commerzbank also faced a challenge common in any global organisation – keeping track of the millions of security events occurring everyday. With more than 700 security devices to monitor, Commerzbank estimates that it receives between seven million and 15 million security events each day from devices including firewalls, proxy servers, IDS and anti-virus.

“Log files were checked manually before the deployment of ArcSight ESM, and with 15 million logged events every day and no automated correlation capabilities it was not possible to cover every eventuality,” says Uwe Tacke, IT Production and CERT, Commerzbank.

Commerzbank was finding it hard to manage the huge volumes of security data, and as a growing multi-national organisation, the complexity was only going to increase. Therefore, it was necessary for Commerzbank to implement a security information and event management (SIEM) solution.



The ArcSight Solution

Commerzbank carried out a full market assessment and following a comprehensive evaluation with five vendors, it selected ArcSight ESM. "ArcSight was the only vendor to fulfill all the necessary requirements in the trial phase, meeting all our specific selection criteria as it integrated well into our environment, supported existing products and provided us with automated correlation capabilities that we had not had before," says Uwe Tacke.

The defining feature that attracted Commerzbank to ArcSight was its comprehensive correlation and reporting capabilities, allowing it to process and correlate millions of security events, enabling effective threat prioritisation, reporting and remediation. Other product functionality benefits included extensive reporting and breadth of device support which allowed for easy integration in the bank's existing infrastructure.

"We began working with ArcSight ESM in January 2005 and implementation was completed within the month, with a seamless integration into our existing systems," adds Uwe Tacke. "The high quality of ArcSight technology, along with the excellent service received during implementation, allowed an extremely fast deployment, exceeding our needs and expectations of a SIEM solution."

The scalability of ArcSight ESM was also an important feature to Commerzbank. As an ever-growing global organisation, its infrastructure will continue to grow in size and complexity. Indeed, a recent acquisition by Commerzbank requires a further 150 security devices to be monitored, all of which are seamlessly supported by ArcSight ESM.

The ArcSight Impact

ArcSight ESM made an immediate impact on Commerzbank business, providing a clear overview of its IT infrastructure and security environment that was not previously possible. The automatic correlation functionality has seen great improvements in the organisation's ability to manage its huge volume of security information, allowing Commerzbank to better prioritise threats, eliminate false positives and take swift remedial action when required. This has also freed Commerzbank technicians from a great deal of low-level analysis that was previously necessary with the manual monitoring of security log files.

"The oversight that ArcSight ESM has provided us, along with the automated correlation capability, has created great business benefit since its deployment last year. Rather than being carried out across many disparate departments, log analysis is now taken care of by the Computer Emergency Response Team. The automation ArcSight ESM brings allows them to spend their time accurately gauging threat exposure and taking the necessary action, rather than spending hours on low-level analysis," says Uwe Tacke.

Since the deployment, ArcSight ESM has also enabled Commerzbank to identify servers and network applications that were misconfigured, such as identification on non-existent users and highlighting machines trying to make unauthorised connections with other machines. With an ongoing support relationship with ArcSight, Commerzbank estimates that it has achieved a strong ROI since implementation.

Originally deployed solely for its security requirements, Commerzbank is now working with ArcSight to achieve deeper integration and to meet compliance standards such as Sarbanes-Oxley in the United States and Basel II in Europe, for which it must have systems and procedures in place by the start of 2007.

