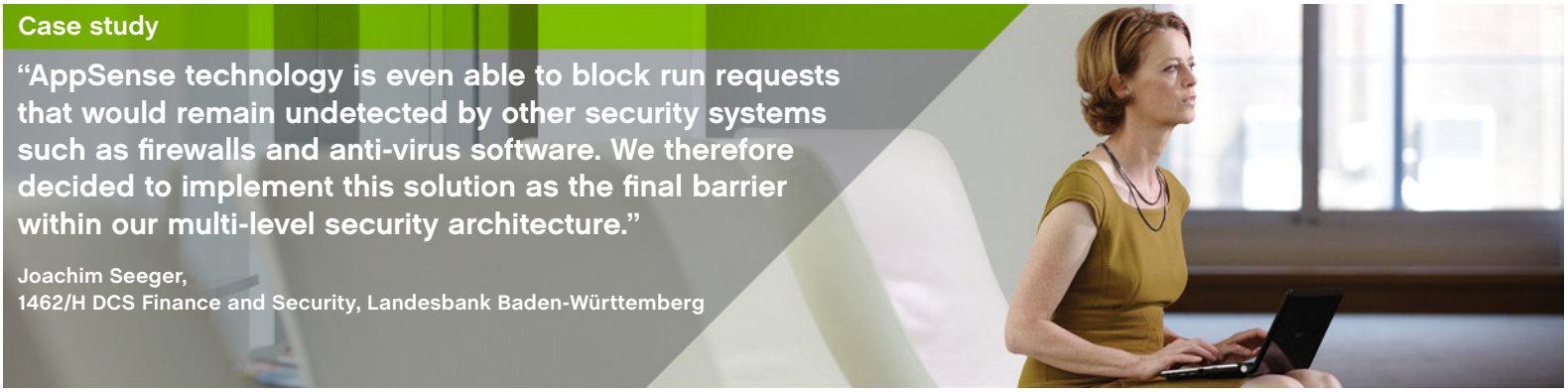
Financial services

Landesbank Baden-Württemberg

AppSense

Case study



"AppSense technology is even able to block run requests that would remain undetected by other security systems such as firewalls and anti-virus software. We therefore decided to implement this solution as the final barrier within our multi-level security architecture."

Joachim Seeger,
1462/H DCS Finance and Security, Landesbank Baden-Württemberg

LBBW
Landesbank Baden-Württemberg

AppSense solution protects 1,500 XenApp servers from unauthorised software

The challenges

- To protect the central XenApp environment
- User and group-specific access requirements
- Robust compliance and audit policies

Solution

- AppSense User Virtualization Platform
- 13,000 users

Benefits

- Maximum system security by blocking all non-authorised applications at kernel level
- Proactive protection against executable and script-based viruses, spyware, peer-to-peer tools and hacker tools
- Optimal system stability and integrity for 1,500 XenApp servers
- Simple, rules-based configuration for users and groups
- Efficient systems analysis thanks to passive monitoring
- Automatic logging of all security-related events

The company

Landesbank Baden-Württemberg (LBBW) is one of the largest commercial banks in Germany and is also the central bank for the savings banks in the German states of Baden-Württemberg, Saxony and Rhineland Palatinate. LBBW's core activities include retail banking and corporate banking, particularly for small and medium-sized businesses, as well as services for savings banks. It also focuses on real estate financing and customer-driven capital market business with banks, savings banks and institutional investors. Subsidiaries specialising in leasing, factoring or asset management round off the LBBW Group's own range of services.

In recent years, LBBW has systematically centralised its entire IT applications infrastructure with the aim of reducing administration work required for the bank's 13,000 IT workstations. Today, most of the business applications for the bank's four main locations in Stuttgart, Karlsruhe, Mannheim and Mainz, as well as some 200 nationwide branches are provided via a central Citrix XenApp environment. In the large majority of cases, workstation PCs have been replaced by thin clients on which no applications – other than a few system applications – are installed.

User virtualization as part of the security architecture

The changeover to the central applications infrastructure had to be accompanied by an appropriately robust security concept: "We needed to put in place multi-level security that would prevent the execution of unauthorized software on the XenApp server farms," explains Joachim Seeger, project manager from the DCS Finance and Security department at LBBW. It was particularly important to protect the environment against malware that could potentially be embedded within e-mail attachments, web browsers or removable storage devices.

After evaluating the various security options available, the IT organisation finally opted for the AppSense User Virtualization Platform. According to Joachim Seeger: "AppSense technology is even able to block run requests that would remain undetected by other security systems such as firewalls and anti-virus software. We therefore decided to implement this solution as the final barrier within our multi-level security architecture."

The AppSense User Virtualization Platform uses secure capture mechanisms at kernel level to identify and automatically block unwanted software applications on servers or terminals, meaning that it is able to protect against script-based and executable viruses, trojans and spyware. The AppSense User Virtualization Platform also offers control over software content, such as ActiveX, VBScripts, batch files, Windows Installer packages and configuration files for registration.

Financial services
Landesbank Baden-Württemberg

❝ Within our current XenApp environment of 1,500 servers, stability and security take top priority. That is why it is vital for us to effectively rule out any risk presented by authorised applications. AppSense technology is ideal for this. Thanks to its extensive control functionality, the solution allows us to implement internal security policies across the entire company in a highly efficient, user-friendly manner. ❞

Joachim Seeger,
1462/H DCS Finance and Security,
Landesbank Baden-Württemberg

Proven trusted owner concept

"In our daily work, we particularly appreciate the comprehensive control functionality offered by AppSense technology, which allow us to define rules-based policies for application execution for individual groups or users," explains Joachim Seeger. As standard, the XenApp environment of LBBW only permits the execution of applications that have been installed by a trusted owner; that is, system administrators who have the required permissions for central installation software. Web applications can only be launched on the XenApp servers if an administrator has already added them to a white list containing permitted applications that is stored on the AppSense system. The compilation of black lists allows the IT department to block known malware and problem applications across the entire system.

The AppSense solution logs all security-related events in a log file that can be used for auditing purposes. A clear error message appears for the user if an application is prevented from running. They can then quote this message when contacting the help desk to identify the cause. All major security events are forwarded automatically to the LBBW security specialists.

Passive monitoring supports security configuration

"One AppSense function that has proven highly useful for our day-to-day work is passive monitoring mode," reports Joachim Seeger. This mode allows unauthorised execution attempts to be monitored without preventing user execution. Passive monitoring is a useful tool in allowing LBBW to observe user behaviour before a planned new implementation: "With every update of the XenApp environment, we are therefore able to investigate in advance how the changes will impact our security configurations. We can then adapt the application execution rules accordingly before the server update goes live," Joachim Seeger adds.

The project manager is keen to stress that the AppSense User Virtualization Platform has become a key strategic component of LBBW's IT infrastructure: "Within our current XenApp environment of 1,500 servers, stability and security take top priority. That is why it is vital for us to effectively rule out any risk presented by authorised applications. AppSense technology is ideal for this. Thanks to its extensive control functionality, the solution allows us to implement internal security policies across the entire company in a highly efficient, user-friendly manner."

About AppSense

AppSense is the global leader in User Environment Management (UEM) with over 3,000 enterprise customers worldwide that have deployed to over 7 million desktops. AppSense DesktopNow and DataNow enable IT teams to deliver the ultimate user experience and productivity across physical and virtual desktops while optimizing security and reducing operational and infrastructure costs. The company is headquartered in Sunnyvale, CA with offices around the world.