

Security

Benefits for your customers:

- Maintain online services (avoiding disruption) in line with user expectations
- Confidence that online services and information are secure

Benefits for your library:

- Helps prevent hacking attempts
- Avoid potential compromise of services and library data
- Ensure your library is less vulnerable to security threats, minimising potential downtime
- Reduce support overhead based upon tried and tested upgrades

Services Brief

A library's systems and customer-facing applications – and the business-critical data that underpins the quality of service – are a potential target for malicious attacks by hackers. Maintaining a secure online environment, along with the integrity of library services and customer account data, is a fundamental challenge for all concerned. It is important to clarify what possible vulnerabilities exist from the outset and ensure these are eradicated to avoid being the next easy target.

While point-in-time reviews and fixes are an important prerequisite to any security service, the true value is in the continuous monitoring and ongoing updates – providing day-to-day peace of mind.

Maintaining secure library services

Talis Services offer an automated and complementary server and operating system security service, ensuring your core library management systems and data remain intact from external security threats.

This comprehensive service includes an initial audit of all library management system and OPAC servers, followed by the necessary upgrades to the operating system to resolve immediate security concerns. Once complete, an automated monitoring and updating service is rolled out across your servers to maintain a secure library services environment.

Security audit

First and foremost, a full security scan of application server operating systems (including those running Talis Prism and Talis Alto 'Main' and 'MIS' databases) is undertaken which includes over 900 discrete security tests. This detailed scan of servers identifies accessible ports and services, as well as operating system information.

A comprehensive report is generated identifying the servers that responded to the tests, the number of security holes and warnings found, and a summary of security issues and proposed fixes.

Resolve vulnerabilities

Security vulnerabilities identified during the initial scan are resolved using an automated patch client to pull pre-tested patches directly from Talis to your server operating system. At the same time, all available updates held on Talis' software repositories are installed.

Any customised firewall rules are added as well as configuration changes applied to servers to support the standard security mechanisms. In addition, all non-essential services are removed or stopped.

Automated monitoring and updates

Monitoring of server operating systems and security status is fully automated on a daily basis, and any necessary patches or software upgrades applied.

This service is fully maintained during the subscription period, providing ongoing access to a vendor-approved repository of security updates and patches – thereby maintaining the operational and secure status of your library services.

What is included from Talis

Talis Services will provide customers with a comprehensive 'Statement of Work' and ongoing subscription for all application server operating systems identified, including those running Talis Prism and Talis Alto 'Main' and 'MIS' databases.

Maintaining a secure online environment, along with the integrity of library services and customer account data, is a fundamental challenge for all concerned.

Find out more

For more information and a detailed quotation for this service from Talis, please call our Sales Team on 0870 400 5090, visit www.talis.com/services or send an email to sales@talis.com.