CASE STUDY

CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press Protects its In-House
Database Content with Seqrite Data Loss Prevention (DLP)

> " A minor leak of our in-house content can be disastrous to our publication business. Thanks to Seqrite for providing us with a strong security solution with easy maintenance. "

The publication arm of University of Cambridge provides educational and academic materials to readers all over the world. With over 50 offices around the globe, Cambridge University Press has a major publishing presence in diverse academic fields. In India, Cambridge University Press caters to millions of readers in India and South Asia. Their books are perfectly positioned in the market channel to reach out to their primary audience, major global web portals and electronic and searchable databases.

Cambridge University Press was looking for an effective solution to protect its work stations from frequent virus and malware attacks. It develops and publishes content that are global in presentation, approach and recognition and thus wanted a robust security solution to protect its intellectual property. After a thorough assessment of the options available, Cambridge University Press went for Seqrite Endpoint Security (EPS) with the DLP Solution.

Key Challenges:

➢ No means to regulate all data transfer channels
➢ Lack of a centralized point of view over all network systems and their security status
➢ Frequent virus and malware attacks were disrupting operations

Solutions by Seqrite:

➢ **Data Loss Prevention** to regulate all data transfer channels
➢ **Unified Console** allows centralized management of security and makes information access easier
➢ **Web Security**, Spam Protection and Vulnerability Scan protect all networked systems

Business Challenge

Over the years, Cambridge University Press has defined innovative ways of delivering content and embraced digital information technology to serve the needs of readers at all levels. Content development forms one of the core competencies of Cambridge University Press and it did not have a strong enterprise security solution to safeguard its intellectual property from theft and loss.

The publication house was finding it challenging to proactively monitor the activities of network systems and was looking for an integrated solution, across its network and endpoints, to provide a centralized view of its infrastructure. The network systems were also prone to virus and malware attacks and Cambridge University Press wanted a powerful and flexible security solution that deploys antivirus and malware protection.

The Seqrite Solution

Cambridge University Press wanted to take strong security preventive measures to safeguard its in-house developed content. After considering options, the publication house went for Seqrite EPS with DLP Solution. Seqrite DLP allows enterprises to detect and protect sensitive content across communication channels. With DLP Solution, Cambridge University Press was able to avoid the risk related to misuse and loss of data. By regulating and monitoring all transfer channels, it was primarily able to secure all in-house and unpublished content and critical information.

With Seqrite EPS, the publication house was able to have greater visibility and control of its office network and security status. The IT team had holistic insights of each and every system within the network and received critical information on major threats and attacks. With advanced threat protection and web security approach of EPS, Cambridge University Press could detect and block viruses and thwart infected and malicious websites from affecting the network systems.

Business Benefits

Seqrite EPS with DLP Solution is developed specifically for organizations like Cambridge University Press looking to further protect its security infrastructure and intellectual property. The publication house has significantly improved its security infrastructure with Seqrite. The changeover to a strong enterprise solution has enabled it to manage risks effectively and protect network systems from security threats. This has significantly affected the publication house's commitment in delivering high quality content to its readers.

With centralized visibility into its network systems, Cambridge University Press now has greater management control and is able to secure its in-house content from theft and loss.

Seqrite
Endpoint Security

A comprehensive approach to endpoint security with host based content aware Data Loss Prevention.

Enterprise security solutions SEQRITE, though relatively new in the market, is backed by a large global company Quick Heal Technologies with vast experience in many aspects of information security.

Seqrite Endpoint Security 6 consists of comprehensive endpoint security features to secure and mange endpoints. It also includes Advanced Device Control and Content Aware DLP. All of these functions are integrated into a single endpoint management console. It is compatible with a wide variety of operating environments like all flavors and versions of Windows desktops, servers, and also supports Apple Mac and Linux at endpoints. With a wide range of endpoint protection features like anti-malware, distributed firewall, content filter, asset management, application control and vulnerability scanner Seqrite Endpoint Security is a solid product for enterprise security.

Seqrite
Mobile Device Managment

Cloud based, centrally managed mobile management solution for enterprise environment.

Seqrite Mobile Device Management is an easy-to-use enterprise mobility solution that is cloud-based and includes all the vital security features. It simplifies the end-to-end management of Android, iOS and Windows mobile devices within your enterprise network. With Seqrite MDM you have control over the app repository and can set restrictions on the use of applications. The solution streamlines device configuration and provides complete visibility and control of all devices from a single console. Seqrite MDM offers enterprises the advantage of an economical on-demand solution.

Seqrite
TERMINATOR

Single, high-performance platform for all your network security needs.

Seqrite offers the Terminator series of gateway appliances for small and midsize businesses and remote offices. The appliance provides firewall, antivirus, content and email filter, intrusion prevention and application control in a single package. This offering also includes additional features like bandwidth management, link failover management and VPN connectivity. Terminator with its excellent performance and well-designed features backed by excellent support has been winning good clients.