

CASE STUDY



**NATIONAL STEEL  
AND AGRO INDUSTRIES LTD.**

National Steel & Agro Industries Ltd. (NSAIL) Prevents Data Loss and Data Leak through USB Drives and Insecure Mails with Seqrite Data Loss Prevention (DLP)

“ Seqrite has helped us protect our critical and sensitive data from insider and outsider threats. We can now easily customize access policies for every single device type and model. Thanks to Seqrite, we can now prevent the leakage of sensitive data through numerous transfer channels. ”



National Steel and Agro Industries Ltd. (NSAIL), a public limited company, is the largest steel producer in Central India and one of the leading manufacturers and exporters in agriculture, power and metals since 1985. Having achieved the status of “Star Trading House” in exports, NSAIL products are well established in the USA, EU, UAE and African markets. The global market player has a PAN India presence through its 25 branches and warehouses with an annual turnover of over Rs.2300 crore/23 billion. NSAIL decided to move away from its existing security solutions as it did not live up to its commitment of blocking websites and providing effective storage security solutions. In June 2015, the company went for Seqrite End Point Security (EPS) with Seqrite Data Loss Prevention (DLP) to prevent data loss and leakage within or outside the organization by regulating data transfer channels.

## Key Challenges:

- The existing IT security solution of NSAIL was proving ineffective resulting in major operational hurdles
- There were instances of ex-employees siphoning off data through emails, USB drives and other external devices
- IT compliance was routinely being breached because of various storage and transfer devices that employees had access to.
- NSAIL was losing a lot of company data and had no means to track and control data theft

## Solutions by Seqrite:

- **Data Loss Prevention** to regulate all data transfer channels
- **Email Scan** to filter out spam mails and phishing attacks
- **Advanced Device Control** to configure access for every device type

## Business Challenge

NSAIL was continuously making efforts to safeguard its confidential data and prevent unauthorized disclosure of data across the enterprise. It had to secure some of its most important non-financial confidential business information, typically stored as unstructured data. In addition, business customer information and other intellectual property related data had to be preserved.

NSAIL’s then existing security solution did not meet the data privacy requirements. They failed to regulate data transfer channels and provide an effective remedy to data leakage. Ex-employees had easily siphoned off data most by emails and external hard disks.



## The Seqrite Solution

NSAIL was looking for an alternative to its existing security solution. Initially, the company had two major requirements. The security solutions should be easy to use and deploy and second, it should have a comprehensive Data Loss Prevention (DLP) feature. The feature should prevent data leakage within or outside the organization by regulating data transfer channels. Second, NSAIL wanted an adequate mail server security for incoming/outgoing emails. Moreover, it wanted greater device control over employee owned devices and configure separate access policies for USB drives and other storage devices.

After considering different security solutions provider, NSAIL finalized on Seqrite Endpoint Security (EPS) with Seqrite Data Loss Prevention (DLP). Seqrite DLP feature stops data leakage within or outside the organization by regulating data transfer channels such as removable devices, network sharing, and web applications amongst others. Office files, programming files, confidential data, personal data and other sensitive files can be regulated using the Seqrite DLP feature.

Email Scan feature of EPS enables a client to effectively scan user-end inboxes and separately set up whitelists and blacklists for certain email addresses and domains. In addition, Advanced Device Control allows a client to configure separate access policies for USB drives and other storage devices. The company has control over the devices employees use and hence protect the network from unverified devices.

## Business Benefits

Since the deployment of Seqrite Endpoint Security with DLP solution, NSAIL has advanced control over all its networked systems. The company found a lot of features useful for improved system performance and less network downtime resulting in operational efficiency. NSAIL has gained greater visibility on the outgoing and incoming traffic across its networked systems. There was a significant decrease in security policy violations by employees via emails and other storage devices. The DLP solution proved vital in securing NSAIL's sensitive data and maintaining an edge in the market.

## 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 manage 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 Management

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.