SME STREET

Quick Heal Introduces Seqrite NOVA for Data Privacy Compliance

At the core of Seqrite NOVA is advanced AI-powered intelligence engineered to minimize manual effort and automate the heaviest lifts of data privacy compliance.

Quick Heal Technologies Limited, through its enterprise cybersecurity brand Seqrite, today announced **Seqrite NOVA Data Privacy**, an AI-powered offering designed to simplify and accelerate the DPDP compliance journey for small office/home office (SOHO) businesses, small and medium businesses (SMBs), and mid-enterprises. NOVA brings enterprise-grade privacy technology into defined packs, helping organizations get started in days with minimal manual intervention and limited reliance on specialist IT skills, while managing personal data as their operations grow.

With India's digital economy expanding rapidly, businesses face an urgent mandate to establish robust data governance, identify personal data across fragmented repositories, respect Data Principal rights and manage explicit consent. However, navigating the compliance landscape of the DPDP Act often poses severe operational challenges, ranging from resource constraints and limited in-house IT expertise in smaller businesses to high compliance complexity in growing mid-sized enterprises.

Seqrite NOVA bridges this critical gap by transforming a complex regulatory mandate into a smooth, AI-powered and automated compliance journey. Delivered across three scalable tiers:

- **Lite**
- **Essentials**
- **Professional**

Seqrite NOVA is purpose-built to cater to all segments of businesses, right from SOHO setups to SMBs and Mid-Enterprises.

AI-powered discovery, classification and multilingual intelligence

At the core of Seqrite NOVA is advanced AI-powered intelligence engineered to minimize manual effort and automate the heaviest lifts of data privacy compliance. The platform leverages AI to continuously discover and classify personal data across endpoints, cloud applications, databases, and unstructured files. NOVA's intelligent engine can even recognize text embedded within scanned documents and images, allowing security and privacy teams to quickly identify sensitive information requiring protection. This AI-led automation reduces repetitive data review, helping teams act faster with less specialist IT effort.

Furthermore, to help organizations fulfill DPDP mandates requiring privacy notices to be accessible in Indian languages, Seqrite NOVA features a built-in AI language translation engine. This capability automatically translates customer consent experiences, privacy notices, and cookie preference menus into 22 officially recognized Indian languages, enabling businesses to engage customers transparently in their preferred language, reducing manual translation work while maintaining human-in-the-loop review controls.

"Navigating India's DPDP compliance shouldn't be a complex, resource-heavy ordeal for growing businesses," said **Harish Kumar GS, Chief Executive Officer, Quick Heal Technologies Limited.** *"With Seqrite NOVA, we have democratized enterprise-grade privacy technology. Whether you are a SOHO operating a few systems, an SMB scaling up, or a Mid-Enterprise managing large volumes of customer data, NOVA offers a tailored, AI-powered path to accelerate DPDP compliance with minimal manual intervention, limited reliance on specialist IT skills, and an investment matched to your needs."*

Comprehensive data privacy capabilities for growing operations

Seqrite NOVA allows organizations to match their investment to their exact stage of growth and privacy complexity without taking on unnecessary operational hurdles. The tiered packs are designed to minimize upfront investment by allowing businesses to start with the capabilities they need and expand as their operations grow. Across its offering, NOVA delivers a unified suite of enterprise-grade privacy and protection capabilities:

- **Endpoint Visibility and Data Leakage Prevention:** Provides clear visibility into sensitive personal files across devices while enforcing controls to prevent accidental or unauthorized data exposure, integrated alongside robust cybersecurity defense.

- **Consent and Preference Management:** Automates web cookie preferences and captures, tracks, and manages explicit customer consent across digital touchpoints.
- **Data Subject Request (DSR) Workflows**: Streamlines rights management by providing automated workflows to fulfill Data Principal requests for data access, correction, and erasure.
- **Advanced Privacy Operations:** Offers modular support for structured privacy impact assessments and rapid data breach notification response workflows to satisfy stringent regulatory timelines.