Seqrite
Endpoint Protection

SEQRITE

Comprehensive endpoint protection, encompassing enterprise-grade prevention, detection, response, and threat hunting for workstations, laptops, and servers.

www.seqrite.com

Why Securing Endpoints
Is The Future Of Cybersecurity?

As cyberattacks evolve and businesses increasingly adopt cloud services and remote operations, traditional endpoint protection methods fall short of providing adequate security. Despite substantial investments in cybersecurity, organizations often struggle to safeguard their digital assets and data from endpoint-initiated attacks. Hence, securing technologies used by remote workforces is necessary.

To achieve comprehensive endpoint protection, businesses require a network solution that transcends geographical boundaries and encompasses all modern mobile endpoints. Whether in the cloud or on-premises, the choice is yours. We offer an end-to-end security solution designed for optimal performance efficiency, ensuring protection for every endpoint.

Seqrite
Endpoint Protection for Businesses

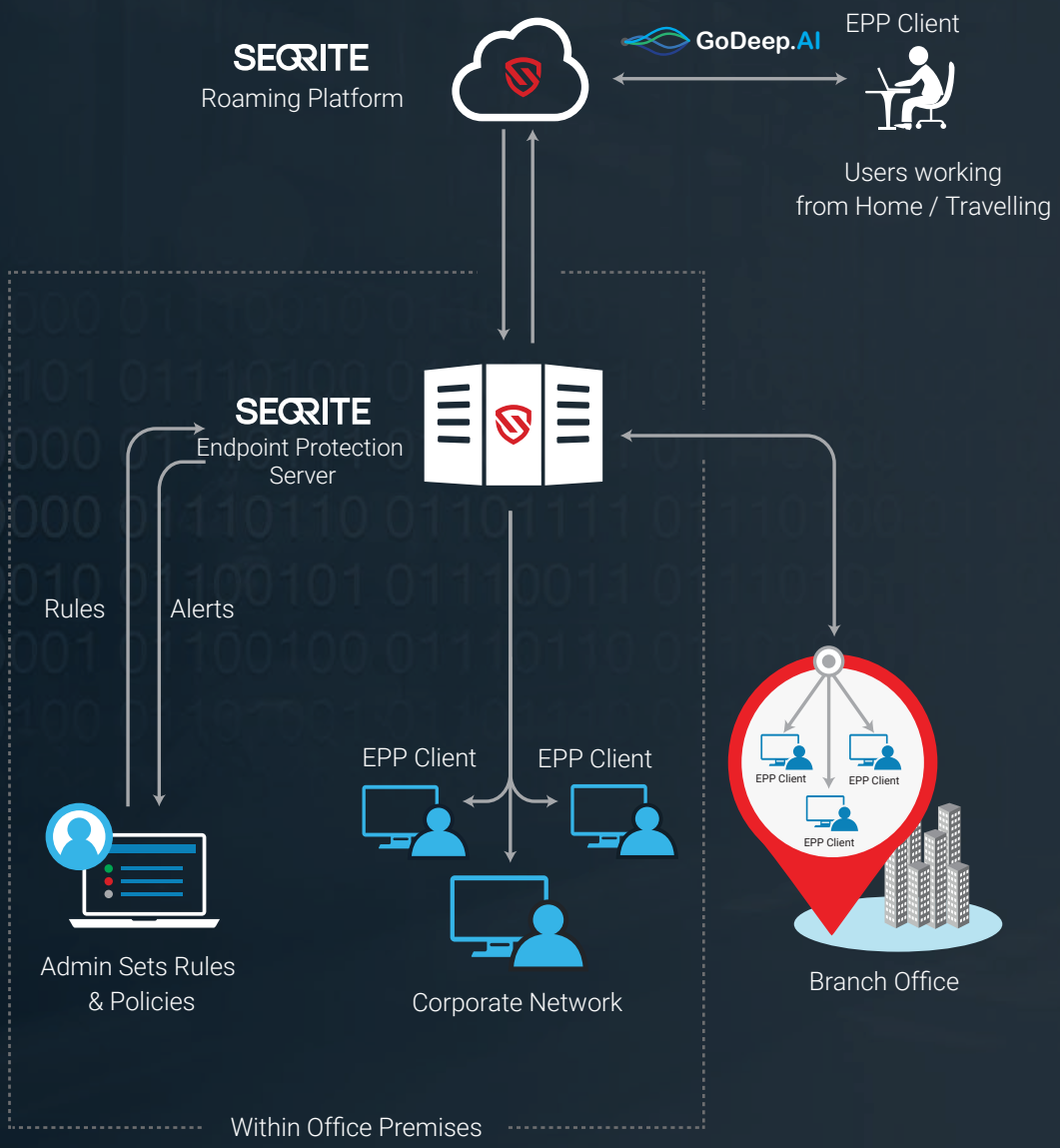
Unified solution to stop threats in their tracks!

Seqrite Endpoint Protection is a simple and comprehensive platform that integrates innovative technologies like Anti Ransomware, and Behavioural Detection System to protect your network from today's advanced threats.

It offers a wide range of cutting-edge features like Advanced Device Control, DLP, Vulnerability Scan, Patch Management, Web Filtering, Asset Management, Endpoint Threat Hunting, etc., to ensure complete protection for enterprises' digital assets.

One Platform
Solving Many Problems

Seqrite Endpoint Protection



Why choose Seqrite **Endpoint Protection?**

1 Comprehensive Endpoint Protection and Control

A simple yet powerful platform enforcing control over data, applications, and web access through a comprehensive suite of features, including Advanced Device Control, DLP, Asset Management, Application Control, and more.

2 Multilayered Protection

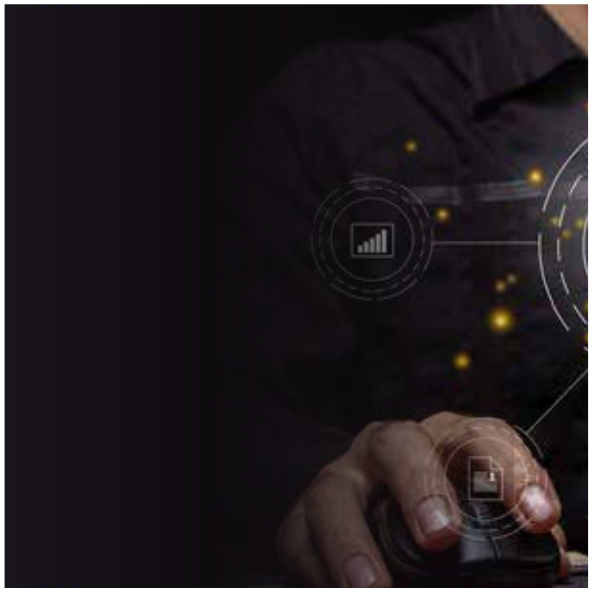
Certified by various industry certifications, it integrates innovative technologies like Advanced DNA Scan, Behaviour Detection, Endpoint Threat Hunting, and Anti-Ransomware to protect your system from malware and advanced threats at different levels.

3 Scan and Patch Application Vulnerabilities

It helps detect application and operating system vulnerabilities and fixes those by installing missing patches. Regular updating of applications makes the network less vulnerable to malware attacks.

4 Centralized Management and Control

User-friendly interface for monitoring, configuring, and managing systems in the network with the detailed report and graphical dashboards.



Feature Description

Core Protection

Antivirus
Offers malware protection that is certified by leading industry certifications

Anti Ransomware
Protection from ransomware attacks and automatically takes back-up of selected files types.

File Sandboxing
Integrate with Seqrite Cloud Sandbox to analyse suspicious files for malwares. No reason to buy and operate hardware or software for Malware Analysis.

Device Control and DLP

Advanced Device Control
Enforce policies regarding the use of storage devices, mobile and portable devices, wireless devices, network interfaces connected to endpoints.

Data Loss Prevention
Prevents data loss by monitoring confidential and user defined data shared through removable drives, network or various applications.

Web Protection

Browsing Protection
Blocks malicious sites.

Phishing Protection
Blocks phishing sites.

Web Filtering
Blocks sites as per its categories.

Scheduled Internet Access
Schedule time based internet access.

Google and YouTube Access Controller
Blocks Personal and allows Corporate Google Access based on the administrator's chosen account domains. Blocks YouTube Videos depending on the Content Category, Publisher Name, etc.

Network Protection

IDS/IPS
Detects malicious network activities which exploit application vulnerabilities and blocks intruder attempts.

Firewall
Monitors inbound and outbound network traffic based on rules.

Port Scan Attack Prevention
Alerts about port scanning attack.

DDOS Attack Prevention
Alerts about DDOS attacks.

Monitoring and Control

Vulnerability Scan
Provides summarized view of vulnerabilities as per severity

Patch Management
Centralized patch management solution to patch vulnerabilities of Microsoft and Non-Microsoft application.

File Activity Monitor
Monitors confidential company files and notifies administrators when such files are copied, renamed or deleted.

Management and Control

Centralized Administration
Web-based console with graphical dashboard, group and policy management, email and sms notification, easy deployment.

Roaming Platform
Manage clients even if they move out of the corporate network.

Migration from EPS v7.6
Facilitates migration of Endpoints, Users, Groups, and Policies to the new EPS Server setup. It also allows migration in batches/groups of endpoints.

High Availability (HA)
High Availability ensures uninterrupted user access to services, applications, and data even during hardware failures and software glitches, thus minimizing the system's downtime.

Feature Description

Management and Control

BitLocker Encryption Management for Data Security

Allows central management of BitLocker encryption policies, keys, and recovery options, ensuring robust data security and compliance with regulatory requirements.

Endpoint Detection and Response (EDR)

Rapid Query to Endpoints

Fetches endpoints in real-time to gather information from pre-defined data sources on the Endpoints.

Automated IoC Search

Integrates with MISP server for Threat Feeds. These File Hashes from MISP will be searched regularly (daily/weekly), and results will be populated on the reports.

Real-time IoC Blocking

Submit File Hashes for continued investigation of malicious content and real-time blocking.

Endpoint Threat Hunting

Endpoint Threat Hunting (ETH) is an effective way to search for files that match malicious hashes across your endpoints. ETH detects hidden attacks based on the hashes provided by a user and helps hunt them down before they cause any harm to the system.

Application and Asset Management

Application Control Safelist

Restricts application access based on Zero Trust methodology. Allows defining application permissions depending on the Operating System, including default OS and Seqrite applications. Offers a 'Monitoring Only' mode to record application access for administrative viewing without blocking it.

Asset Management

Gives total visibility of hardware and software running on endpoints and also helps to track software / hardware changes happening on endpoints.

Product Comparison

Features	SME	Business	Total	Enterprise Suite	EDR
Antivirus	✓	✓	✓	✓	✓
Anti Ransomware	✓	✓	✓	✓	✓
Email Protection	✓	✓	✓	✓	✓
IDS/IPS Protection	✓	✓	✓	✓	✓
Firewall Protection	✓	✓	✓	✓	✓
Phishing Protection	✓	✓	✓	✓	✓
Browsing Protection	✓	✓	✓	✓	✓
SMS Notification*	✓	✓	✓	✓	✓
Vulnerability Scan	✓	✓	✓	✓	✓
Roaming Platform	✓	✓	✓	✓	✓
GoDeep.AI*	✓	✓	✓	✓	✓
Asset Management		✓	✓	✓	✓
Spam Protection		✓	✓	✓	✓
Web Filtering		✓	✓	✓	✓
Advanced Device Control		✓	✓	✓	✓
SIEM Integration		✓	✓	✓	✓
Application Control - Blocklist			✓	✓	✓
Application Control - Safelist			✓	✓	✓
Tuneup*			✓	✓	✓
File Activity Monitor			✓	✓	✓
Patch Management			✓	✓	✓
YouTube Access Controller				✓	✓
Google Access Controller				✓	✓
Disk Encryption Management				✓	✓
Rapid Query to Endpoints					✓
Automated IoC Search					✓
Realtime IoC Blocking					✓
Endpoint Threat Hunting		Add-on	Add-on	Add-on	✓
Data Loss Prevention		Add-on	Add-on	✓	✓
File Sandboxing		Add-on	Add-on	Add-on	Add-on

Note: * Feature(s) included only in v7.x

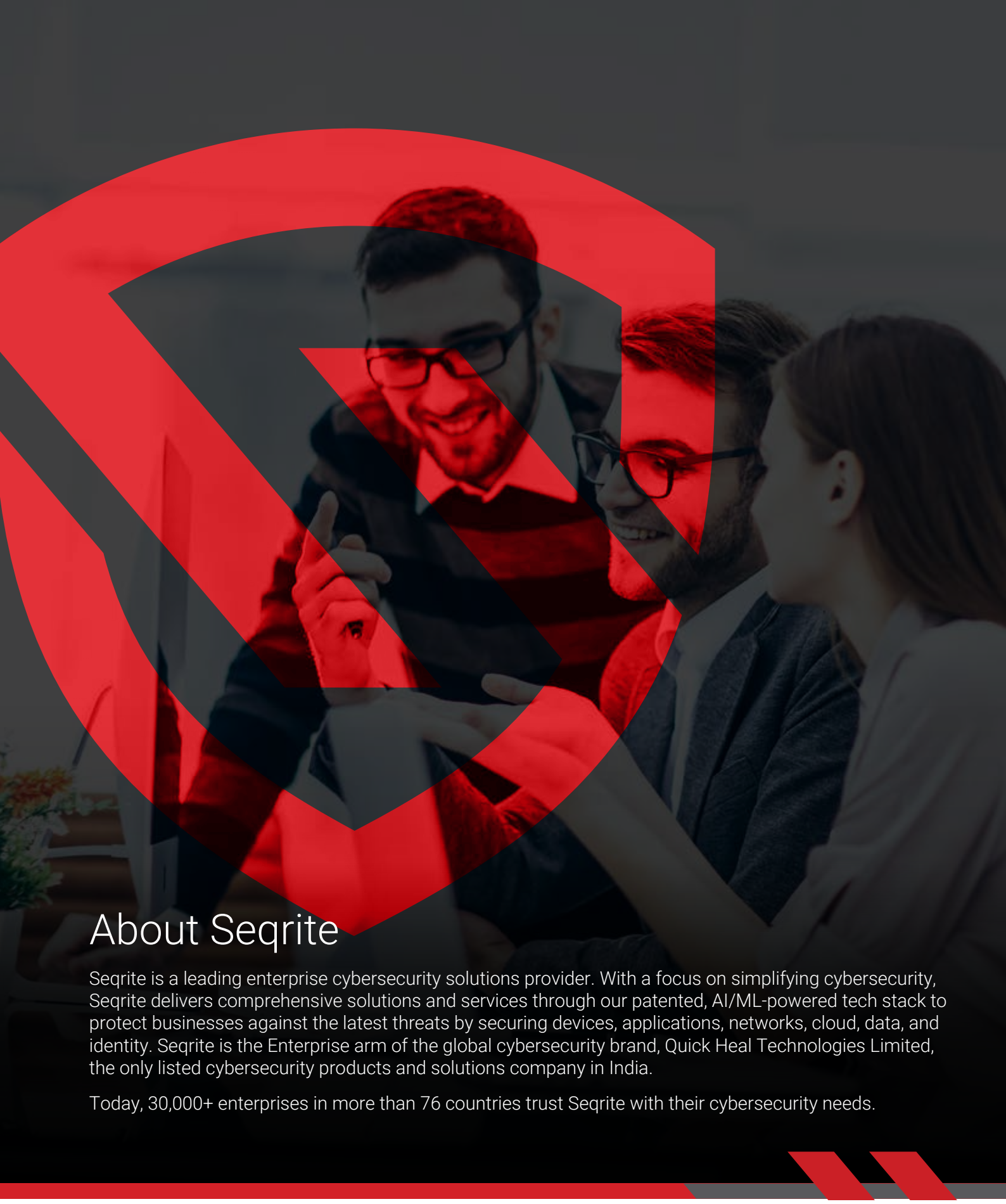
Certifications

Seqrite Endpoint Protection certified as 'Approved Corporate Endpoint Protection' for Windows by 'AV-Test'

Ready for a trial?

Click Here

or scan



About Seqrite

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

Today, 30,000+ enterprises in more than 76 countries trust Seqrite with their cybersecurity needs.

SEQRITE | Quick Heal Technologies Limited
Phone: 1800-212-7377 | info@seqrite.com | www.seqrite.com | /seqrite