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

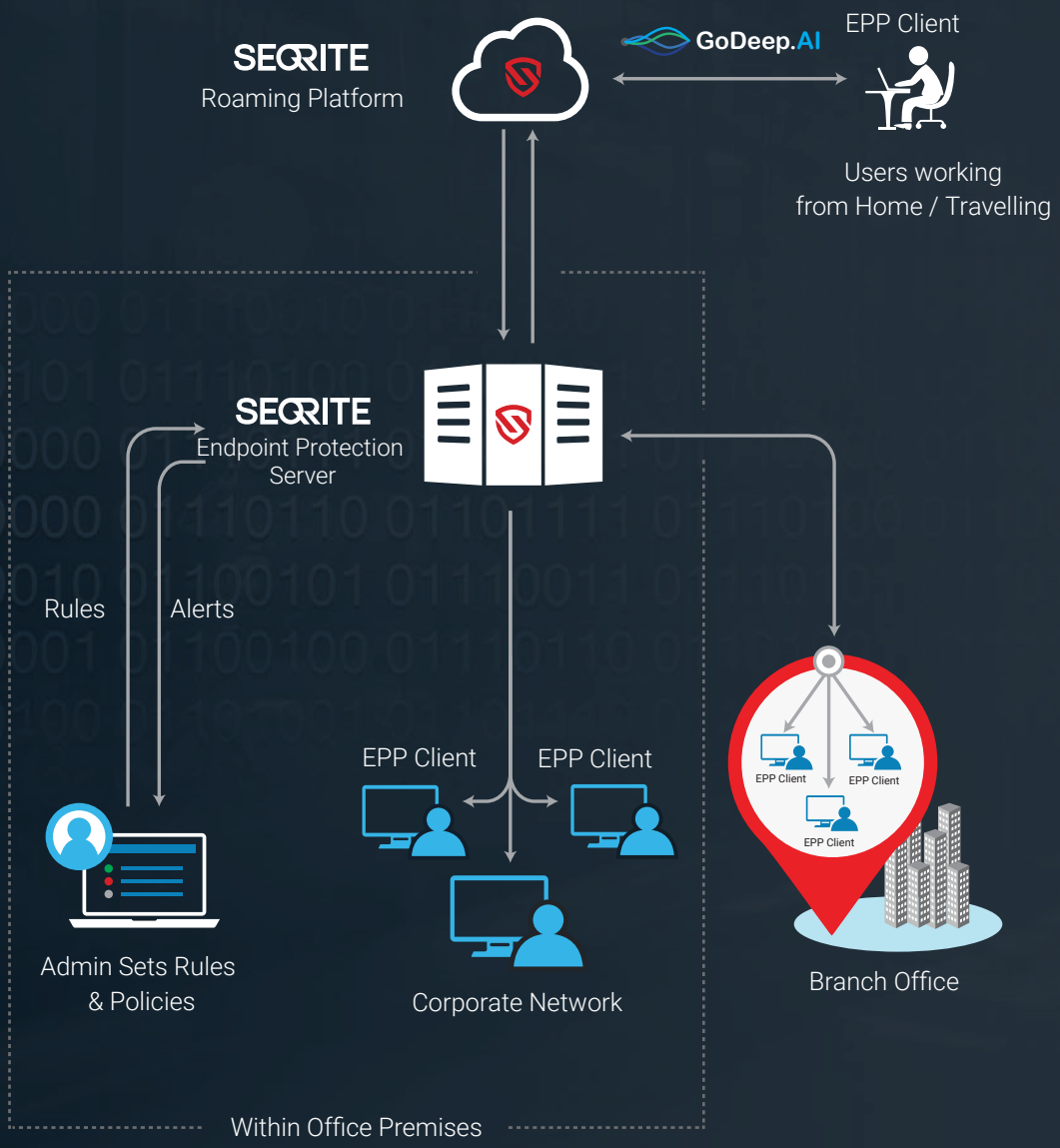
Unified solution to stop threats in their tracks!

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, Enterprise File Search, 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

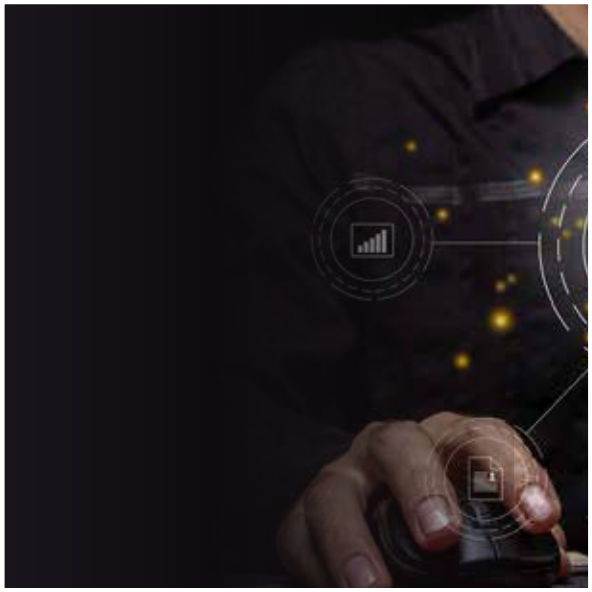
Certified by various industry certifications, it integrates innovative technologies like Advanced DNA Scan, Behaviour Detection, Enterprise File Search, and Anti-Ransomware to protect your system from malware and advanced threats at different levels.

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
Detects, blocks, and removes malware using real-time scanning, signatures, and behavioral analysis.

Anti Ransomware
Prevents unauthorized encryption attempts and blocks ransomware processes.

Behavior Detection System
Uses behavioral patterns to detect unknown, zero-day, or evolving threats.

DNA Scan
Uses DNA-level pattern analysis to identify new, mutated, and hard-to-detect malware variants.

Device & Autorun Protection
Prevents malicious autorun execution and scans USB and external devices to stop infection sprea

Rogueware Protection
Identifies and blocks fake antivirus and deceptive applications.

Network Protection

Firewall
Monitors and controls inbound and outbound network traffic based on policies.

IDS/IPS
Detects and blocks network intrusion attempts and exploits.

DDoS Detection
Identifies abnormal traffic patterns and potential denial-of-service attacks.

Port Scan Detection
Detects and blocks port-scanning activity.

Endpoint Isolation
Automatically isolates compromised endpoints from the network.

Wi-Fi Security Monitoring
Detects insecure or rogue wireless networks.

Web Protection

Browsing Protection
Blocks access to unsafe or compromised websites.

Web Filtering
Filters malicious, inappropriate, or harmful web content by category.

Phishing Protection
Blocks phishing websites and unsafe URLs.

Safe Banking Browser
Launches a protected browser environment for financial transactions.

Secure Browser Mode
Opens an isolated browsing environment for high-risk activity.

Scheduled Internet Access
Restricts internet usage according to time-based policies.

Google Access Controller
Restricts access to Google services based on administrator policies.

YouTube Access Controller
Controls YouTube access by category and restriction.

Email Protection

Email Threat Protection
Scans emails, attachments, and URLs for malicious content.

Anti-Spam
Filters spam and malicious emails.

Trusted Mail Client Protection
Secures supported email applications against threats.

Feature Description

Endpoint Management & Control

Centralized Endpoint Log Collection
Allows administrators to collect debugging logs directly from endpoints.

Advanced Device Control
Enforces policies for USB, storage, mobile, and wireless devices.

Temporary Device Access
Provides controlled temporary access for troubleshooting.

Shadow IT Detection
Identifies unapproved or unauthorized applications.

Multi-Site Management
Allows centralized control over geographically dispersed locations, ensuring security and efficiency.

External Device Control

Application Control
Allows only approved applications to run while blocking unauthorized ones

Camera Protection
Blocks unauthorized use of endpoint cameras.

Printer Control
Restricts access to printers to prevent data leakage.

Network Share Control
Controls access to shared network folders.

Security & Compliance

Vulnerability Scan
Identifies system vulnerabilities and missing patches.

Patch Management
Deploys patches for operating systems and applications.

Virtual Patching
Blocks exploitation attempts before official patches are applied.

Asset Management
Provides visibility into hardware and software inventory.

Data Loss Prevention

Data Loss Prevention Suite
Monitors and controls sensitive data across devices, networks, and applications.

OCR Image DLP
Detects sensitive information embedded within images using OCR.

Watermarking
Applies visible watermarks to documents to ensure traceability.

Data Discovery
Identifies sensitive data stored on endpoints.

Secure File Backup & Recovery
Provides centralized or endpoint-level file backup and recovery.

Disk Encryption Management
Manages encryption policies, keys, and recovery workflows.

Centralized Management & Deployment

Centralized Unified Web Control
Provides a graphical dashboard for monitoring, policy management, notifications, and deployment and automates patch and signature updates.

3rd-Party AV Remover
Automatically removes conflicting antivirus solutions during agent installation.

Unprotected Endpoint Discovery
Identifies unmanaged or unprotected devices on the network.

Seamless Migration from On-Prem
Enables smooth transition from legacy endpoint deployments to the cloud.

Feature Description

Advanced Threat Defense

Centralized Quarantine Management

Manages quarantined files from a single console.

File Sandbox

Runs suspicious files in isolation to determine malicious behavior.

AI-Powered Threat Detection with GoDeep.AI

Uses deep learning to predict and block zero-day and advanced malware by analyzing behavior and global threat patterns in real time.

System Optimization & Rescue Tool

System Tune-up

Cleans junk files and optimizes endpoint performance

Emergency Rescue Disk

Bootable tool to clean infected systems offline

Advanced Protection

Enterprise File Search (EFS)

EFS is an effective way to find files that match malicious hashes across your endpoints. Based on the hashes provided by a user, EFS detects hidden attacks and helps hunt them down before they harm the system.

Security, Compliance & Insights

Executive Dashboard

Displays endpoint security posture and status, tracks compliance metrics and policy violations, and monitors DLP events to ensure comprehensive security and data protection oversight.

Reporting & Analytics

Provides customizable security and compliance reports.

SIEM Integration

Sends endpoint security logs to SIEM platforms for correlation.

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.

Product Comparison

Features	SME	Business	Total	Enterprise Suite	EDR
Antivirus	✓	✓	✓	✓	✓
Anti Ransomware	✓	✓	✓	✓	✓
Email Protection	✓	✓	✓	✓	✓
IDS/IPS Protection	✓	✓	✓	✓	✓
Firewall Protection	✓	✓	✓	✓	✓
Phishing Protection	✓	✓	✓	✓	✓
Browsing Protection	✓	✓	✓	✓	✓
Vulnerability Scan	✓	✓	✓	✓	✓
Roaming Platform	✓	✓	✓	✓	✓
Multi-Site Management	✓	✓	✓	✓	✓
Centralized Quarantine Management	✓	✓	✓	✓	✓
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					✓
Enterprise File Search(EFS)					✓
Data Loss Prevention		Add-on	Add-on	✓	✓
File Sandboxing		Add-on	Add-on	Add-on	Add-on

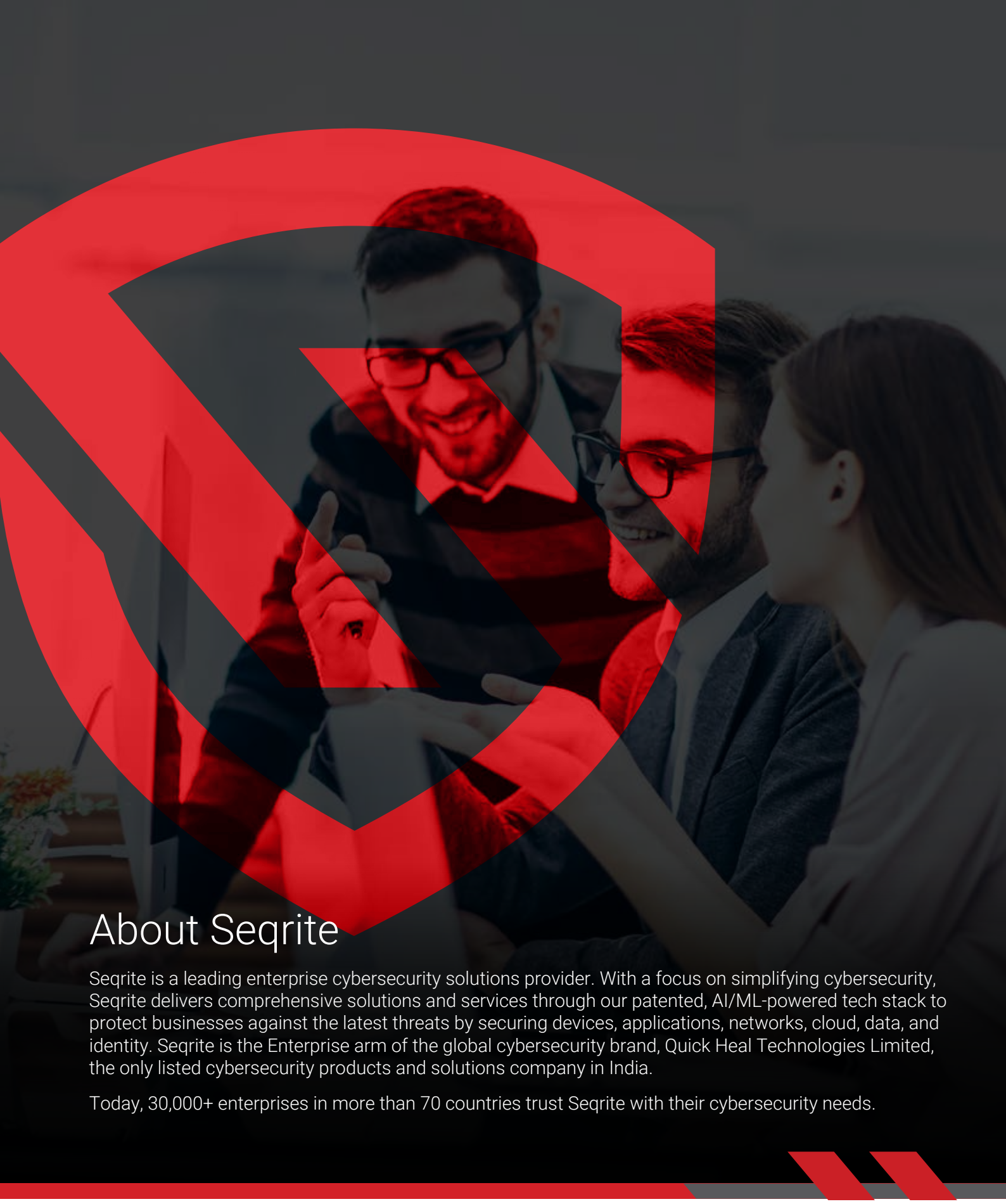
Certifications

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 70 countries trust Seqrite with their cybersecurity needs.

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