

# SEQRITE Endpoint Security (EPS)

---

Simple and Comprehensive  
Endpoint Security for workstations,  
laptops and servers.

Maximize the performance of the security  
posture for enterprise-grade prevention,  
detection, response, and threat hunting  
with advanced technologies.





# Why Securing Endpoints Is The Future Of Cybersecurity?

## Are you thinking, "Do I need endpoint protection?"

With evolving cyberattacks, the drastic rise of cloud adoption, and businesses leaning towards remote operations – traditional endpoint security methods are no longer sufficient.

It's becoming challenging for security to protect the assets and data from cyber-attacks that start at the endpoint, despite enterprises spending a lot on cyber protection. Securing the technology your remote workforce uses can help mitigate risks and protect the organization.

For adequate endpoint security, businesses must have a network that doesn't have geographical limits and covers all modern mobile endpoints. In the cloud or on-premise? You decide! We have an end-to-end security solution optimized for performance efficiency, helping you protect every endpoint.





# SEQRITE Endpoint Security (EPS) for Business

## Unified solution to stop threats in their tracks!

Seqrite Endpoint Security 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.

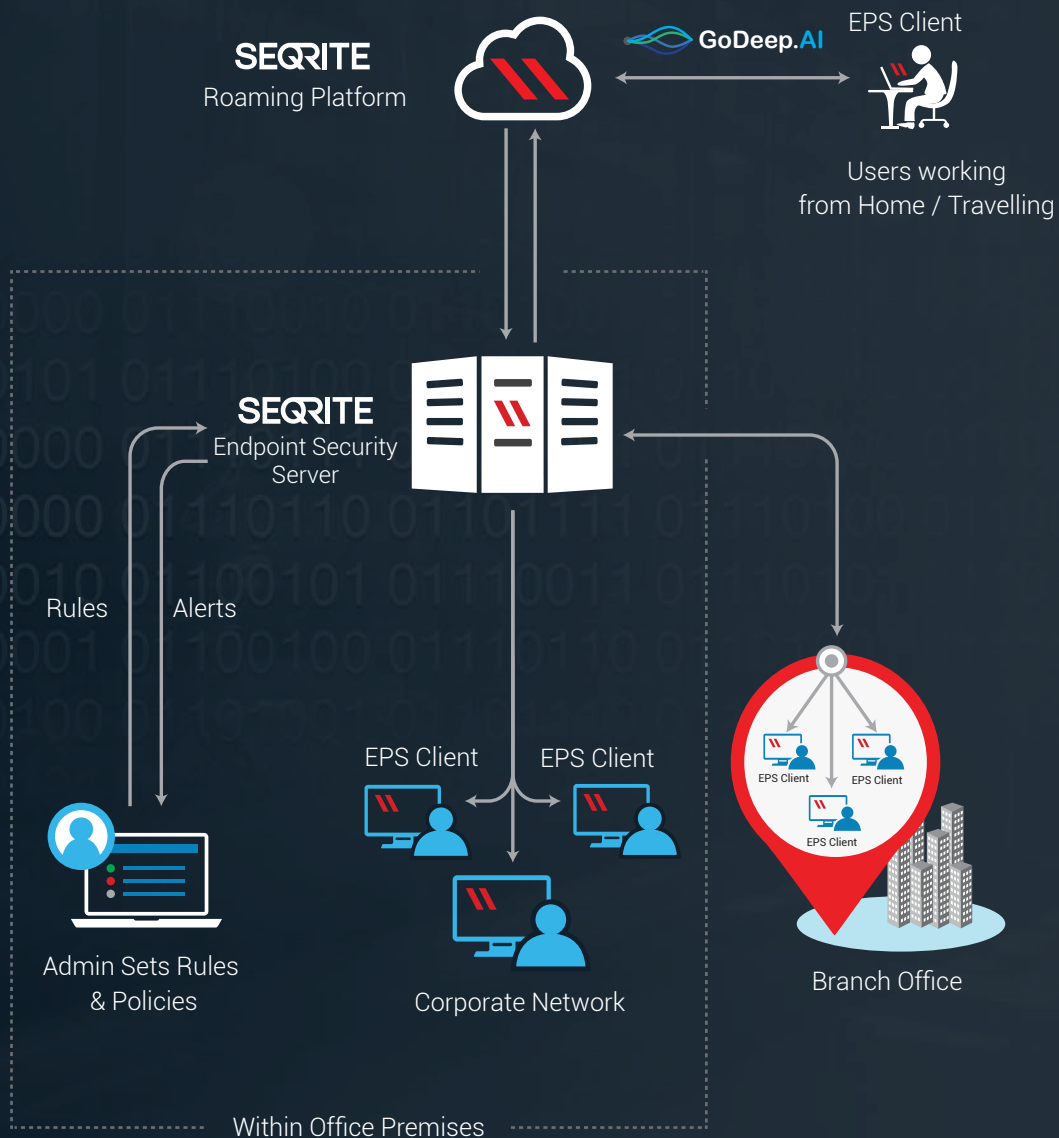
It offers a wide range of advanced features like Advanced Device Control, DLP, Vulnerability Scan, Patch Management, Web Filtering, Asset Management, etc., under a single platform to enable organizations to ensure complete security and enforce control. SEQRITE Endpoint Security (EPS) also comes with Endpoint Threat Hunting capabilities.





# One Platform Solving More Problems

## Seqrite Endpoint Security (EPS)





# Why SEQRITE Endpoint Security?

1

## Comprehensive Endpoint Security and Control

Seqrite Endpoint Security is a simple yet powerful platform for managing security. It helps enforce control over data, applications, and web access with a wide range of features such as Advanced Device Control, DLP, Asset Management, Application Control, etc.

2

## Multilayered Protection

Certified by various industry certifications, Seqrite EPS integrates innovative technologies like Advanced DNA Scan, Behaviour Detection, and Anti-Ransomware to protect your system from malware and advanced threats at different levels. Endpoint threat hunting involves the use of detection and IoC data collection from each of the endpoints.

3

## Scan and Patch Application Vulnerabilities

It helps detect application and operating system vulnerabilities and fix 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 file 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 Seqrte 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 Security certified as 'Approved Corporate Endpoint Protection' for Windows by 'AV-Test'

**Register here for a free demo**

<https://www.seqrite.com/endpoint-security/seqrite-endpoint-security>



**SEQRITE**

Quick Heal Technologies Limited

Phone: 1800-212-7377 | [info@seqrite.com](mailto:info@seqrite.com) | [www.seqrite.com](http://www.seqrite.com)