Seqrite **EDR on premise**

SEQRITE

In the era of geopolitical instability and economic downturn, government establishments and enterprises have been constant targets of advanced threats. Traditional endpoint security solutions are often ineffective in detecting or preventing these attacks as they fail to fetch the necessary data to expose unusual behavior and respond effectively to stealthy cyber threats.

Seqrite EDR is a robust detection and response solution that solves this issue by providing customers with uninterrupted data visibility and greater control over their system hardware, Operating System, and applications. It allows customers to investigate past alerts and events, query the system for the latest information, and perform manual or real-time automated response and remediation.

MAX

Features of **Seqrite EDR:**

Multi-Phase Verification
Analyzes all system events via multiple layers of behavioral analysis, signature comparisons, and ML-based detection.

Support for offline and air-gapped networks
Seqrite EDR has the most advanced support for air-gapped networks. It can update behavior rules and IOCs and has offline autonomous policy-driven response capabilities for such environments.

Automated and Manual IOC Lookup
Performs automated and manual IOC Lookups on historical data, sourcing IOCs from the latest Threat Intelligence data from the Seqrite Threat Intel team and from government agencies like CERT-IN.

Advanced Notification Systemt
Integrates seamlessly with all SIEM solutions and sends SMS/email alerts.

Dashboard and Widgets
Presents a comprehensive system health overview, including top incidents, overall summary, affected incidents, and false positive rates via intuitive widgets.

Reports
Reports detail alerts summary over time, providing insights aligned with MITRE TTPs.

Rule Builder and Rules
Allows crafting system and custom rules. Leverages rule builder to craft personalized rules for capturing MITRE-related or other unusual or interesting activity on endpoints.

Action Policy Orchestration and Risk-Based Response
Implements real-time and offline response action policies, with defined scopes for risk-based auto-response using generic or custom policies.

Investigative Workbench
Helps investigate incidents and alerts with detailed drill-downs, contextual information, query-based access to live system information, and thorough listing of alerts access to alerts list and alerted tree, enabling centralized alert actions from one location.

Incident Management
Enables incident management through the incident list and information on endpoints and users while formulating remediation actions.

Benefits of Seqrite EDR

Deter advanced attacks

Our Endpoint detection system analyzes each telemetry event generated at the sensors through multiple analysis stages to perform a thorough contextual analysis. If suspicious activity is detected, our EDR system can immediately block it.

Stop Malware before it strikes

By taking automated real-time actions, like isolating the system or stopping the execution, an adversary's chances of executing a successful attack are greatly diminished.

Benefit from thorough investigations

By compiling highly useful information regarding executions, scripts, commands, and process chains, the security analysts' time for triage and response is significantly reduced. This feature expands the capability to meet compliance needs and standards.

Reduce the need to hire outside Incident Response and Forensics Firms

Our Endpoint Detection & Response module allows the security analyst and IT administration teams to conduct detailed investigations of attacks independently, reducing the need to engage external agencies to conduct such investigations.

Look up Historical data for hidden threats

Advanced attacks use stealth technology to remain hidden in the environment for many months. Utilizing our event data storage and Threat Hunting, combined with the latest Threat Intelligence, such hidden threats can be discovered, and immediate response actions can be taken.

System Requirements (for on premise version only)

Windows (64-bit)
(Windows 8.1, 10, 11, 2012, 2016, 2019, 2022).

MacOS - Processor: Intel core or Apple's M1, M2, M3 chip compatible
- macOS 10.14, 10.15, 12 and 14

Linux (64-bit) - Fedora 32, Linux Mint 20, Ubuntu 17.04, 20.04, 22.10, CentOS 8, 8.2, RHEL 8.1, 8.2, 9.1, openSUSE 15.1, Rocky Linux, Boss 8

Minimum System Requirements for Server (On premise version only) - Up to 1000 Endpoints.

Requires 3 Servers –
1) Worker machine: 40 Core, 96 GB Memory, 3.7 TB Disk - Ubuntu 22.04 LTS OS
2) Master machine: 4 Core, 8 GB Memory, 500 GB Disk - Ubuntu 22.04 LTS OS
3) Update Manager – 2 Core, 4 GB Memory, 50 GB Disk (For OS, Click Here)

Strengthen your Endpoint Protection with the ability to detect and block complex malware and support endpoint investigations and analysis through real EDR.

SEQRITE

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