Seqrite

Endpoint Protection **EDR**

SEQRITE

Release Notes

V1.2.1 | Aug 2024

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to the user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Version History

The information in this document is provided for the sole use of Quick Heal Research and Development, and Support Team. It is strictly forbidden to publish or distribute any part of this document to any other party.

Doc Version	Date	Comment
1.0	June 2024	Seqrite Endpoint Protection EDR 1.2.0 Released
2.0	Aug 2024	Seqrite Endpoint Protection EDR 1.2.1 Released

Overview

Seqrite EDR is a comprehensive detection and response solution. This resolves the user's data visibility and control over the system hardware, operating system, and applications.

Seqrite EDR also allows the user to review past alerts, access the latest information, and perform manual or automated responses on the affected endpoints.

The EPP 8.3 release introduces the EDR edition with Endpoint Protection. Here are a few benefits of EDR edition.

What's New in Version 1.2.0

- **Multi-Phase Verification**
  - Enables the system to analyze all events through multiple layers of behavioral analysis.
- **Immediate Remediation action**
  - Helps the system to restrict potentially infected hosts and perform automated actions automatically or manually.
- **Automated and Manual IOC Lookup**
  - Enables the system for IOC lookups on previous data generated by the Seqrite Threat Intel team and other sources.
- **Advanced Notification System**
  - Integrates seamlessly with the system with all the SIEM solutions and sends notifications.
- **Dashboard and Widgets**
  - Provides comprehensive system health overview via intuitive widgets.
- **Reports**
  - Summarizes insightful reports aligned with alerts and MITRE TTPs.
- **Rule Builder and Rules**
  - Enables the crafting system and custom rules.
  - Leverages rule builder to create personalized rules for monitoring MITRE-related or odd activity on endpoints.
- **Action Policy Orchestration and Risk-Based Response**
  - Supports real-time and offline response policies with a defined scope for risk-based auto-response using generic or custom policies.

- **Investigative Workbench**
    - The feature provides deep drill downs, contextual information, and query-based access to current system information.
    - It also allows for centralized alarm actions from a single location.
- **Support air-gapped network**
    - Comprehensive air-gap network support, ensuring offline updates of rules, policies, signatures, and other components.
- **Multi-site support**
    - Effectively provide support to multiple satellite sites and central aggregation for widely distributed deployments.

What’s New in Version 1.2.1

- **FQDN (Fully Qualified Domain Name) Installation Support**
  - The installation process has been improved to allow configuration of the EDR server using Fully Qualified Domain Names (FQDN).
- **No resource limits on Live Query**
  - Live Query now operates without any resource limits.

For more details on the Features and functionalities, refer to the respective guide/help.

System requirements for EDR

- Machine requirements: 2 Nodes for EDR + 1 Node for Update Manager
- Data Retention: 30 days
- High Availability : No

System requirements for EDR Nodes

EDR	Node 1 (Master)				Node 2 (Worker)		
Operating Sys	Ubuntu 22.04 LTS				Ubuntu 22.04 LTS		
Endpoints	**CPU**	**Memory**	**Disk**		**CPU**	**Memory**	**Disk**
<= 20	4 Core	8 GB	200 GB		12 Core	42 GB	500 GB
<1000	4 Core	8 GB	500 GB		40 Core	96 GB	3.7 TB
1000 - 2000	4 Core	8 GB	500 GB		40 Core	96 GB	7 TB
2000- 4000	4 Core	8 GB	500 GB		48 Core	96 GB	12 TB
4000-5000	4 Core	8 GB	500 GB		48 Core	112 GB	15 TB

System requirements for EDR Update Manager

CPU	Memory	Disk	Supported Platforms
2 Core	4 GB	50 GB	• Linux Mint 19.2 • Linux Mint 20 64bit • Ubuntu 22 • openSUSE 42.3 64bit • openSUSE 15.2 64bit • Ubuntu 20.04 64bit • Red Hat Enterprise Linux 9.1 • BOSS 6 32bit • BOSS 8 64bit • Rocky Linux

Supported platforms for EDR Clients

Windows (64 bit)	Linux (64 bit)	Mac OS
Windows 10	Red Hat Enterprise Linux (RHEL) 8.1	Mac OS Monterey
Windows 8.1	Red Hat Enterprise Linux (RHEL) 9.1	macOS Catalina
Windows server 2019	Ubuntu 20.04	macOS Monterey 12.5 M2
Windows server 2016	Ubuntu 22.10	macOS 14.1.2 (Sonoma) M3
Windows server 2022	openSUSE 15.1	macOS Mojave 10.14.6
Windows Server 2012 R2 Datacenter	Linux Mint 20 Ulyana	
Windows Server 2012 Datacenter	Red Hat Enterprise Linux (RHEL) 8.2	
Windows 11	Rocky Linux	
	Ubuntu 17.04 64bit	
	Linux Mint 20 64bit	
	CentOS 8 64bit	
	CentOS 8.2 64bit	
	Fedora 32 64bit	
	BOSS 8 64bit	

Known Issues

- Mac
  Multiple psassword prompts appear on the system for remote uninstallation multiple times.
  Workaround: A series of pop-up windows appear where the user needs to enter the password multiple for successful uninstallation.

Usage Information

1. For Windows 2016, Windows 2019 Server and Windows 2022 Server, uninstall Windows Defender before installing EPS 8.2 client.
2. To install EPS 8.2 client on windows 7 and windows 2008 R2, you need to install these windows Patches for SHA2 compatibility:
   - For Windows 7: KB4474419 and KB4490628.
   - For Windows 2008 R2: KB-4474419 and KB-4490628
3. To install patches on Windows 7 32-Bit client, you must upgrade to Internet Explorer version 11.
4. If the administrator initiates tuneup notification for the endpoint and if the endpoint is not logged in, then the tuneup notification will fail.
5. Advanced Device Control: If an authorized and encrypted device is formatted, the device will be treated as an unauthorized device. In this case, Administrator will need to add the device again in Device Control and configure the policies accordingly.
6. To use Browser Sandbox, turn off the Secure Boot feature of the system from BIOS Configuration.
7. By default, Spam Protection is disabled. So, a red exclamation mark appears on the client Dashboard.
8. Linux
   - It is recommended to disable SELinux for RHEL-based distribution stream.
   - Remote Support tool cannot be executed with ‘sudo’ command. The tool can be executed with super user (su) command.
   - On selecting migration option for a group with one Linux and another Windows client machines, warning message **Linux client migration is not supported** is displayed.