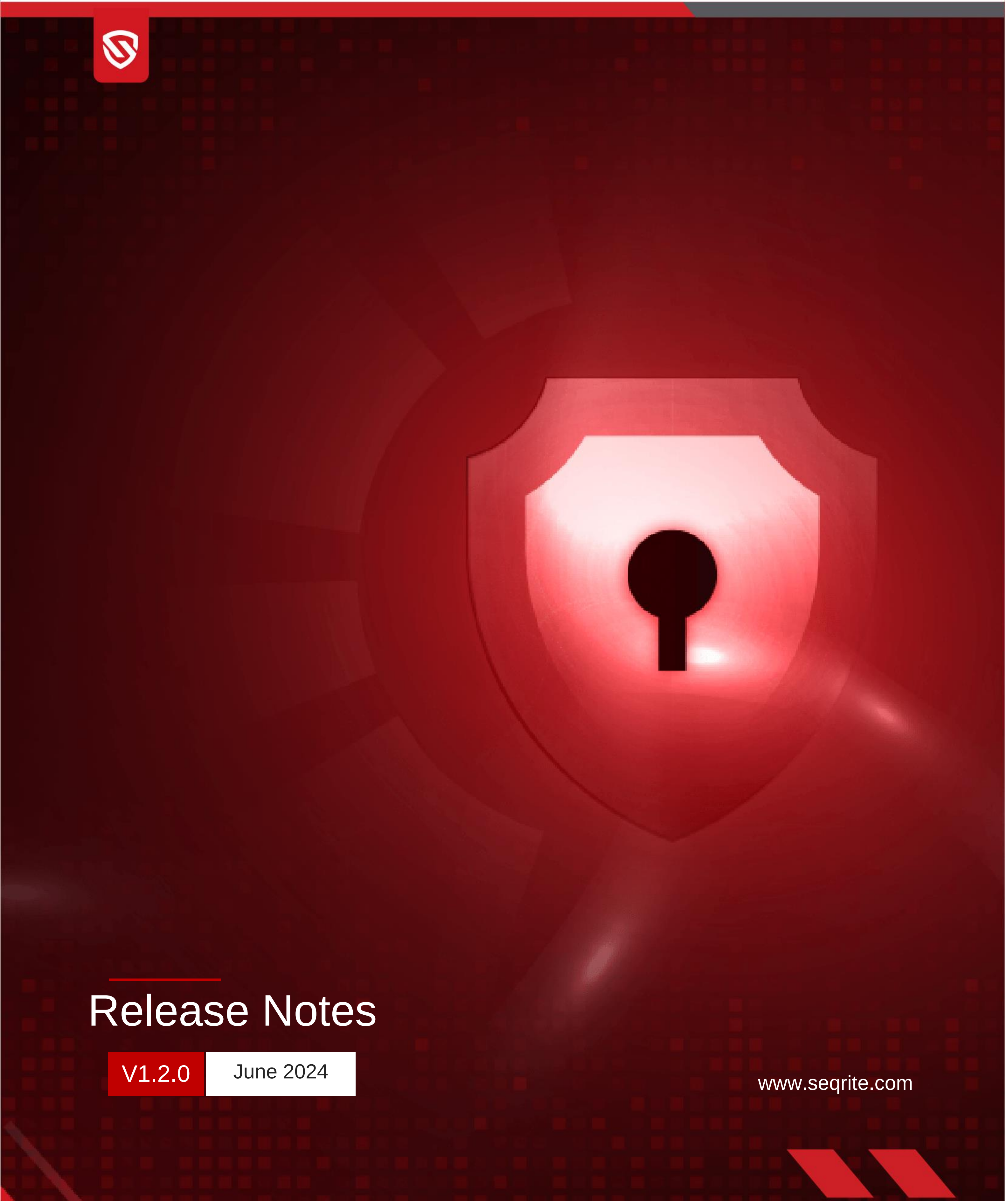
Seqrite
Endpoint Protection **EDR**



Release Notes

V1.2.0 June 2024

www.seqrite.com

Copyright Information

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

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 Released

Features and Enhancements

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.

- 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 for 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 wide distributed deployments.

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

System Requirements

System Requirements for EDR Server

EDR Server Supported OS

- EDR Server only supports the Linux OS with Ubuntu 22.04 LTS server edition.

EDR Endpoint Supported OS

- Windows
  - Windows Server 2012, Core 2016 and 2019
  - Windows Server 2022, 2019, 2016
  - Windows 7, 8 (EPP), 10, 11
- Linux
  - CentOS 7.0+,
  - Red Hat Enterprise Linux (RHEL) 8.1 and later,
  - Mint 18.1 SUSE Linux 11.4+,
  - Ubuntu 18.04+,
  - BOSS 6,7,8
- Mac
  - Latest versions from and after Mac 10.15

System Requirements for EPS Server

Server that supports up to 0 to 5000 endpoints

- Ubuntu 22.04
- Available Disk Space: 60 GBs or above
- Available RAM: 8 GBs or above
- Processer: 4 Core(x86-64), 2.60GHz or above

Server that supports up to 5001 to 15000 endpoints

- Ubuntu 22.04
- Available Disk Space: 100 GBs or above
- Available RAM: 16 GBs or above
- Processer: 8 Core(x86-64), 2.60GHz or above

Server that supports up to 15001 to 25000 endpoints

- Ubuntu 22.04
- Available Disk Space: 150 GBs or above
- Available RAM: 32 GBs or above
- Processer: 16 Core(x86-64),2.60GHz or above

System Requirements for EPS Client

- **Windows**

  Supportability matrix remains the same as 8.1.

- **Mac**
  - **Processor**: Intel core or Apple's M1, M2 chip compatible
  - **OS**: X 10.12, 10.13, 10.14, 10.15, 11, 12, and 13

  Note: No support for Mac OS 10.11 and below.

- **Linux**

  Supportability matrix remains the same as 8.1.

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.