Seqrite

Endpoint Protection 클라우드

릴리즈 노트

Cloud 5.0 | 2024년 8월 31일

www.seqrite.com

저작권 정보

상표

라이센스 조건

Seqrite Endpoint Protection의 설치 및 사용은 사용자가 Seqrite 최종 사용자 라이선스 이용 약관을 무조건적으로 수락하는 것을 전제로 합니다.

라이센스 조건을 읽으려면 http://www.seqrite.com/eula 를 방문하여 제품에 대한 최종 사용자 라이센스 계약을 확인하십시오.

Contents

1. 새로운 소식 6

서버 측: 기능 하이라이트 6

콘솔을 통해 엔드포인트에서 로그 수집 6

Windows Sever 운영 체제를 위한 Windows Server 컨테이너 정책 및 그룹 소개 6

자동 DLP 라이센스 할당 6

엔드포인트 이벤트에 대한 서버 수신 시간 7

타사 바이러스 백신 감지 7

Windows Defender 감지 7

강화된 타사 바이러스 백신 보고 7

Seqrite EPP 10.12 클라이언트 에이전트: Quick Heal 사기 방지 감지 7

전체 호스트 이름 표시 향상 8

사용자 역할 관리 향상 8

새로운 검색 기능 8

데이터 손실 방지 (DLP) 8

부팅 스캔 보호 9

기타 기능 하이라이트 9

클라이언트 측: 기능 하이라이트 10

그룹 및 정책 가시성 향상 10

Windows 10

에이전트 호환성 및 지원 업데이트 10

macOS 10

macOS ARM64 시스템을 위한 고급 장치 제어 지원 10

Linux 10

Mint 21.3 및 RHEL 9.x에 대한 클라이언트 지원 10

2. 시스템 요구 사항 11

3. 버그 수정 15

4. 사용 정보 17

개정 내역

이 문서의 정보는 Quick Heal 연구 개발 및 지원 팀의 단독 사용을 위해 제공됩니다. 이 문서의 일부를 다른 사람에게 게시하거나 배포하는 것은 엄격히 금지되어 있습니다.

문서 버전	날짜	논평
1.0	2024년 8월 31일	Seqrite Endpoint Protection Cloud 5.0 출시된

새로운 소식

이 릴리스에서는 다음 기능이 추가되었습니다. EPP Cloud 5.0.

서버 측: 기능 하이라이트

콘솔을 통해 엔드포인트에서 로그 수집

관리자는 이제 문제 해결을 위한 주요 진단 정보에 필요한 Windows, macOS 및 Linux 클라이언트의 Seqrite EPP 웹 콘솔에서 직접 로그를 수집할 수 있습니다. 로그는 대시보드 > 상태 > 엔드포인트 상태를 통해 다운로드할 수 있습니다.

Windows Sever 운영 체제를 위한 Windows Server 컨테이너 정책 및 그룹 소개

새로운 Windows Server 그룹 및 Windows Server 컨테이너 정책이 도입되었습니다. Seqrite Windows Server 운영 체제에서 실행되는 EPP 클라이언트. 이 업데이트에는 콘솔 > 구성 > 클라이언트 설치 아래에 있는 새로운 구성 설정이 포함되어 있으며, 이 그룹 정책에 클라이언트를 할당합니다.

• 신규 고객의 경우 그룹 정책이 기본적으로 자동으로 적용됩니다.

• 기존 고객의 경우 새로운 설정을 구성하려면 추가 단계가 필요합니다.

자동 DLP 라이센스 할당

관리자가 엔드포인트에 대한 수동 및 자동 라이선스 할당을 선택할 수 있는 DLP 라이선스 할당 모드를 소개합니다. 이 업데이트에는 콘솔 > 구성 > 데이터 손실 방지에 있는 새로운 구성 설정이 포함됩니다.

- 자동 할당:
  - 라이센스는 사용 가능한 경우 자동으로 할당됩니다.
  - 사용 가능한 라이센스가 없는 경우 알림이 표시됩니다.
  - 신규 고객 온보딩의 경우 DLP 라이선스 수가 총 라이선스 수와 일치하면 자동 모드가 사용됩니다. 그렇지 않으면 수동 모드가 적용됩니다.
- 수동 할당: 그대로 유지됩니다.

- 자동 모드로 전환할 때 사용 가능한 라이선스가 없으면 EPP 콘솔에 알림이 나타납니다. 이러한 알림은 수동 모드로 돌아갈 때까지 모든 새 등록에 대해 계속 표시됩니다.

엔드포인트 이벤트에 대한 서버 수신 시간

향상된 이벤트 추적: 엔드포인트에서 서버로의 흐름을 정확하게 매핑하기 위해 엔드포인트에서 이벤트에 대한 서버 수신 시간을 추가했습니다. 이 향상에는 서버 콘솔 보고서와 CSV 내보내기에 서버 날짜 및 시간 열이 추가되었습니다.

타사 바이러스 백신 감지

콘솔 > 구성 > 클라이언트 설치 > 다른 바이러스 백신 애플리케이션 감지에 새 설정을 추가했습니다. 이 기능은 Seqrite EPP 클라이언트 설치 중에 타사 바이러스 백신 소프트웨어를 식별하고 관리하는 데 도움이 됩니다. 기존 바이러스 백신 프로그램을 감지하고 충돌을 방지하려면 이 옵션을 선택해야 합니다. 다른 바이러스 백신 애플리케이션이 설치되지 않았다고 확신하는 경우에만 이 옵션을 선택 취소하세요.

참고: 이 설정은 Seqrite EPP 웹 콘솔에서 변경 후 배포된 새 클라이언트 패키저 또는 클라이언트 에이전트에만 적용됩니다. 변경 전에 배포된 클라이언트 또는 패키저에는 영향을 미치지 않습니다.

Windows Defender 감지

서버 운영 체제와 Quick Heal Retail AV 제품의 Windows Defender는 '다른 바이러스 백신 애플리케이션 감지' 설정과 관계없이 계속 감지됩니다. 그러나 이러한 제품은 자동으로 제거되지 않습니다.

강화된 타사 바이러스 백신 보고

클라이언트 설치 프로세스에는 이제 설치 충돌을 일으키는 타사 바이러스 백신 소프트웨어의 이름을 Seqrite EPP 웹 콘솔로 직접 보내는 기능이 포함됩니다. 타사 바이러스 백신의 이름은 Seqrite EPP 웹 콘솔 대시보드 > 알림에 표시됩니다.

Seqrite EPP 10.12 클라이언트 에이전트: Quick Heal 사기 방지 감지

Quick Heal 사기 방지 감지 기능이 추가되었습니다.

전체 호스트 이름 표시 향상

호스트 이름 길이 증가: 호스트 이름의 최대 허용 길이가 15자에서 25자로 늘어났습니다. 이를 통해 호스트 이름이 표시되는 모든 곳에서 전체 호스트 이름이 완전히 표시됩니다. Seqrite EPP 웹 콘솔.

사용자 역할 관리 향상

이제 사용자 역할을 다음에서 직접 수정할 수 있습니다. Seqrite EPP 웹 콘솔. 또한, "역할 이름"이 이제 참조를 위해 사용자 페이지에 표시됩니다.

새로운 검색 기능

- 애플리케이션 제어
  - 구성 > 애플리케이션 제어 > 모든 애플리케이션 허용에 검색 기능이 추가되어 애플리케이션 이름이나 프로세스 이름으로 검색할 수 있습니다.
- 정책
  - 정책 > 세부정보 보기 > 보류 중인 엔드포인트에서 엔드포인트 이름으로 검색을 활성화했습니다.
  - 정책 편집 > 애플리케이션 제어 > 모든 애플리케이션 허용에서 애플리케이션 이름으로 검색을 활성화했습니다.

데이터 손실 방지 (DLP)

- 사용자 정의 작업 추가

  이 옵션을 사용하면 신고 또는 차단에 대한 자유도가 더 높아집니다. (예를 들어, 이제 PDF만 차단할 수 있고 Word, Excel 등의 다른 파일 형식은 자유롭게 작동할 수 있으며 그 반대의 경우도 마찬가지입니다.)

- 사용자 정의 앱
  - 사용자 정의 애플리케이션: 이 기능을 사용하면 모니터링하거나 DLP에서 제외해야 하는 애플리케이션을 추가할 수 있습니다.
  - 이제 사용자는 여러 데이터 유형에 대한 블록 보고서 작업을 사용자 정의할 수 있습니다.
  - 사용자는 여러 데이터 유형을 차단하고 보고할 수 있으며, 모두 차단 및 보고만 파일 설정을 각각 사용자 정의할 수 있습니다.

- 사용자 정의 분류기

  사용자 지정 분류자 목록은 채널을 통한 데이터 전송을 모니터링하기 위한 것입니다. 이는 네트워크 내의 통신 채널을 통해 이동하는 특정 유형의 데이터를 식별하고 분류하는 데 사용되는 맞춤화된 규칙 또는 기준 집합입니다.

부팅 스캔 보호

부팅 검사 건너뛰기에 대한 암호 보호 기능을 추가하여 보안 조치를 강화했습니다.

기타 기능 하이라이트

- 기존 저장 버튼 옆에 정책 페이지에 취소 버튼이 추가되었습니다.
- 클라이언트 측의 비밀번호 관리와 관련된 취약점을 해결했습니다.
- "제조업체 이름" 열이 추가되었습니다. 고급의 향상된 장치 식별을 위한 장치 제어 기능.
- 더욱 자세한 네트워크 정보를 제공하기 위해 보고서에 "MAC 주소" 및 "IP 주소" 열이 추가되었습니다.
- 타사 바이러스 백신 감지: 다음에 대한 지원이 추가되었습니다.
  - HP Wolf Security 11.x.
  - Sophos Endpoint Agent 2023.2.x.
  - ESET에 대한 지원이 추가되었습니다. Endpoint Security 11.x.

클라이언트 측: 기능 하이라이트

그룹 및 정책 가시성 향상

- Windows, macOS, Linux 클라이언트에 새로운 기능이 추가되어 사용자가 연관된 그룹과 정책을 볼 수 있습니다. 클라이언트 콘솔에서 도움말 > 정보 페이지의 서버 세부 정보 버튼을 클릭하여 이 정보에 액세스합니다. 이 섹션에는 다음이 표시됩니다.
- 서버 : IP 주소 또는 도메인 이름 Seqrite Endpoint Protection 서버.
- 그룹: Seqrite Endpoint Protection 클라이언트에 할당된 그룹입니다.
- 정책: Seqrite Endpoint Protection 클라이언트에게 적용되는 정책입니다.
- 연결 상태: 클라이언트와 서버 간의 연결이 활성 상태인지 비활성 상태인지를 나타냅니다.
- 마지막 연결 시간: 가장 최근에 성공한 연결 시간을 보여줍니다.
- 오류 메시지: 연결 문제에 대한 세부 정보를 제공하거나, 오류가 없으면 '오류 없음'을 표시합니다.

Windows

에이전트 호환성 및 지원 업데이트

최신 업데이트 에이전트는 Windows, macOS, Linux 플랫폼 전반에서 클라이언트 에이전트 버전 10.8 이상에서 클라이언트에 대한 업데이트 다운로드를 지원합니다.

macOS

macOS ARM64 시스템을 위한 고급 장치 제어 지원

최신 업데이트는 macOS ARM64 기반 시스템에서 고급 장치 제어에 대한 지원을 도입하여 ARM64 아키텍처 환경에 대한 장치 관리 기능을 개선합니다.

Linux

Mint 21.3 및 RHEL 9.x에 대한 클라이언트 지원

Seqrite EPP Cloud 5.0 클라이언트는 이제 Linux Mint 21.3, RHEL 9.0, 9.1, 9.2, 9.3에서 지원됩니다.

(Linux 클라이언트는 영어를 지원합니다.)

특징과 기능에 대한 자세한 내용은 온라인 도움말이나 매뉴얼을 참조하세요.

시스템 요구 사항

EPP 클라이언트를 위한 시스템 요구 사항

클라이언트 설치 유틸리티를 통해 Seqrite Endpoint Protection 클라이언트를 설치하는 경우 시스템 요구 사항은 다음과 같습니다.

다음 운영 체제 중 하나:

Windows 운영 체제

- Microsoft Windows 2008 Server R2 Web/Standard/Enterprise/Datacenter (64비트)
- Microsoft Windows 7 Home Basic/Premium/Professional/Enterprise/Ultimate (32비트/64비트)
- Microsoft Windows SBS 2011 Standard/ Essentials
- Microsoft Windows Server 2012 R2 Standard/Datacenter(64비트)
- Microsoft Windows Server 2012 Standard/Essentials/Foundation/Storage Server/Datacenter (64비트)
- Microsoft Windows 8.1 Professional/Enterprise (32비트/64비트))
- Microsoft Windows 10 Home/Pro/Enterprise/Education (32비트/64비트)
- Microsoft Windows 11
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019(64비트)
- Windows 10 2019년 11월 업데이트
- Microsoft Windows Server 2022 표준/데이터 시작/필수 요소

Mac

프로세서

- Intel core or Apple’s M1, M2, M3 chip compatible

Mac 운영 체제

- MacOS X 10.12, 10.13, 10.14, 10.15, 11, 12, 13 and 14

Linux 32비트

- GNU C Library 2.5 이상
- SAMBA 버전 4.16 이하

EPP 클라이언트 지원 배포판

- Debian 9, 10
- Ubuntu 14.04,16.04
- Boss 6.0
- Linux Mint 19.3

Linux 64 비트

- GNU C Library 2.5 이상
- SAMBA 버전 4.16 이전

EPP 클라이언트 지원 배포판:

- Fedora 30, 32, 35
- Linux Mint 19.3, 20
- Ubuntu 16.04, 18.04, 20.4, 22.04
- Debian 9, 10
- CentOS 7.8, 8.2
- RHEL 7.5, 7.8, 8.2, 8.6, 8.8 Enterprise
- SUSE Linux 12. SP4/Enterprise Desktop 15
- Rocky Linux 8.4
- Boss 6.0, 8.0, 9.0(데스크탑), 8.0(서버)
- Oracle Linux 7.1, 7.9 및 8.1

암호화 정책 구성을 위한 시스템 요구 사항

클라이언트 전제 조건:

- 클라이언트 버전: 10.11
- 라이센스 버전: 프리미엄

하드웨어:

- TPM 2.0
- • UEFI 모드가 있는 BIOS

OS:

- Windows 10 64비트
- Windows 11

일반적인 요구 사항

Windows

프로세서

- 최소: 1 GHz 32비트(x86) 또는 64비트(x64) 프로세서
- 추천: 2 GHz 32비트(x86) 또는 64비트(x64) 프로세서

RAM

- 최소: 1 GB
- 추천: 2 GB free RAM

하드 디스크 공간

- 3200 MB free space

웹 브라우저

- Internet Explorer 7또는 나중에

네트워크 프로토콜:

- TLS 1.2

Mac

프로세서

- Intel core 또는Apple’s M1, M2, M3 chip 호환 가능

RAM

- 최소: 512 MB
- 추천: 2 GB 무료RAM

하드 디스크 공간

- 1200 MB 자유 공간

Linux

프로세서

- Intel 또는 호환 가능

RAM

- 최소: 512 MB
- 추천: 1 GB 무료RAM

하드 디스크 공간

- 1200 MB 자유 공간

참고: Linux Seqrite 클라이언트 프로그램에만 안티 바이러스 설정이 포함되어 있습니다.

버그 수정

다음은 수정된 버그 목록입니다. EPP Cloud 5.0 릴리스:

서버	
1	"공급업체 ID" 및 "제품 ID" 필드가 16진수 값을 올바르게 허용하도록 장치 제어 구성을 업데이트했습니다.
2	EPS 클라우드에서 패치 스캔 보고서가 반영되는 데 지연이 발생하는 문제가 해결되었습니다..
3	클라이언트 상태 페이지를 내보내는 동안 발생하는 오류가 해결되었습니다.
4	이벤트 식별자 대신 이벤트 설명을 표시하도록 SIEM 서버에서 내보내기 세부 정보를 수정했습니다.
5	보고서가 생성되고 있는데도 바이러스 보고 그래프가 비어 있는 문제가 해결되었습니다.
6	클라이언트 상태 내보내기 보고서에 "레코드가 없습니다"라고 표시되는 문제가 해결되었습니다.
클라이언트	
Windows/Mac/Linux	
1	qhwebsec 서비스 – EPS Cloud로 인해 Linux 시스템에서 웹사이트 탐색이 불가능하고 네트워크 아이콘에 느낌표가 나타나는 문제를 해결했습니다.
2	IntelliJ 소프트웨어 - EPS Cloud 11을 사용할 때 catflt.sys와 관련된 Windows 4.0 머신의 BSOD 문제가 해결되었습니다.
3	Application Control Scan이 검사를 수행하지 않고 종료되는 문제를 해결했습니다.
4	대시보드 포털에 일정 스캔 시간이 올바르게 표시되지 않는 문제가 해결되었습니다.
5	최근 설치한 자산에 대한 세부 정보가 표시되지 않는 문제를 수정했습니다.led Linux 클라이언트 – UEM 10.8
6	확장자가 활성화되지 않은 경우에도 DLP가 Outlook 메일의 Excel, CSV 및 PDF 첨부 파일을 기밀 데이터로 차단하는 문제가 해결되었습니다.

7	UEM 4.0 대시보드에서 마지막 일정 클라이언트 스캔 날짜가 업데이트되지 않는 문제가 해결되었습니다.
8	탐색 및 피싱 보호가 활성화된 경우 인터넷 접속이 중단되는 문제를 해결했습니다.
9	ARM64 아키텍처를 사용하는 macOS Ventura에서 사용자가 macOS 클라이언트 대시보드를 열 수 없는 문제를 해결했습니다.
10	macOS Sonoma에서 특정 애플리케이션을 사용할 때 발생하는 Sonoma 성능 문제가 해결되었습니다.

사용 정보

1. Windows 2016, Windows 2019 Server 및 Windows 2022 Server의 경우 EPP 4.0 클라이언트를 설치하기 전에 Windows Defender를 제거하세요.
2. Windows 7 및 Windows 2008 R2에 EPP 4.0 클라이언트를 설치하려면 SHA2 호환성을 위한 다음 Windows 패치를 설치해야 합니다.
   Windows 7의 경우: KB4474419 및 KB4490628.
   Windows 2008 R2의 경우: KB4474419 및 KB4490628
3. Windows 7 32비트 클라이언트에 패치를 설치하려면 다음으로 업그레이드해야 합니다. Internet Explorer 버전 11.
4. 관리자가 엔드포인트에 대한 튜닝 알림을 시작하고 엔드포인트가 로그인되어 있지 않으면 튜닝 알림이 실패합니다.
5. 고급 장치 제어: 승인되고 암호화된 장치가 포맷되면 해당 장치는 승인되지 않은 장치로 처리됩니다. 이 경우 관리자는 장치 제어에서 장치를 다시 추가하고 그에 따라 정책을 구성해야 합니다.
6. 브라우저 샌드박스를 사용하려면 BIOS 구성에서 시스템의 보안 부팅 기능을 끕니다.
7. 기본적으로 스팸 보호는 비활성화되어 있습니다. 따라서 클라이언트 대시보드에 빨간색 느낌표가 나타납니다.
8. 안티멀웨어 검사 보고서에는 이전 브랜드 이름인 'Endpoint Security'가 포함되어 있습니다.