HARMONY

2024年5月29日

ENDPOINT SECURITY CLIENTS FOR WINDOWS

E88.X

リリース ノート

CHECK POINT™

Check Point Copyright Notice

権利の制限

商標

重要な情報

最新版ソフトウェア
最新版ソフトウェアには、機能や安定性の向上、セキュリティの拡張、新たな脅威や進化する攻撃に対処する最新の保護機能が備えられています。常に最新版をインストールすることをお勧めします。

認定資格
サードパーティによるCheck Pointの認定資格については、Check Point Certificationsページを参照してください。

Check Point E88.x Endpoint Security Clients for Windows リリースノート
このバージョンのリリースに関する詳細は、Endpoint Securityホームページを参照してください。

最新版ドキュメント(英語版)
Webブラウザでこのドキュメントの最新バージョンを参照してください。
PDF形式のドキュメントの最新バージョンをダウンロードしてください。

ドキュメントに関するご意見
チェック・ポイントは、わかりやすいマニュアルの作成に日々取り組んでいます。
ご意見やご要望がありましたら、ぜひ弊社までお送りください。

目次

Endpoint Security Client for Windows E88.xの紹介

Check Point Endpoint Securityクライアントは、Windowsを実行するエンドポイントを保護するセキュリティソリューションです。エンドポイントを保護する機能には、以下が含まれています。

- アンチマルウェア
- アンチボットとURLフィルタリング
- アンチランサムウェア、Behavioral Guard、フォレンジック
- Threat Emulation およびアンチエクスプロイト
- リモート アクセス VPN
- コンプライアンス
- ファイアウォール & アプリケーション コントロール
- Media Encryption & Port Protection
- Full Disk Encryption

リモートアクセスVPNの情報については、*E88.x Remote Access VPN Clients for Windows Release Notes* を参照してください。

本リリースでの新機能

新しい機能と強化

E88.30 - 2024年4月17日リリース

新機能:SAとOFRのオフラインアップデート機能を追加しました。オフライン アップデートを実行するにはsk180690を参照してください。

新機能:高度な機能に、検出/阻止/オフモードを次のセンサーに追加しました。

- ThreatCloudレピュテーション
- オフライン レピュテーション
- オフィスファイルのスタティック分析、
- 実行ファイルのスタティック分析、
- DDLファイルのスタティック分析。

モードの設定詳細については、『Harmony Endpoint EPMaaS Administration Guide』の、「Configuring the Endpoint Policy」>「Configuring the Threat Prevention Policy」>「Web & Files Protection」を参照してください。

強化:Endpoint Securityクライアントで、CPInfoをAmazon S3 (Simple Storage Service) にプッシュ操作、およびS3アプリケーションで手動アップロードできるようになりました。

強化:管理者は、クライアント設定の一般セクションにある無効機能に対して、タイムアウトとパスワードを設定できるようになりました。パスワードプロンプトは現在英語でのみ利用可能で、任意のWindowsクライアントで機能を無効に設定できる人を管理でき、クライアントUIの機能を無効にする画面にアクセスする前に、パスワード認証を要求できます。機能を一度無効にすると、指定したタイムアウト間隔で、無効になった機能が自動的に稼働状態に戻るまでの時間が決まります。

強化:クライアントUIのThreat Emulation Bladeがファイル保護で表示されるようになりました。

強化:Anti-Bot Bladeに、Check Point ThreatCloudを活用するDNSインスペクション サポートが加わりました。この保護により、DNS解決プロセスにおいてアンチボットで悪質なドメインへのアクセスをブロックできます。

強化:Anti-Malware E1 Bladeで、マルウェアのスキャンやモニタリングから除外すべき、信頼されたプロセスから発生するプロセス (派生したものなど) を指定することができるようになりました。不要なリソース活用と潜在的な誤検知を最小限にします。

強化:Threat Emulation Bladeのインストールとは別に、Anti-Malware E2 Bladeのみをインストールすることができるようになりました。

強化:脅威ハンティングへのイベントアップロードにかかる時間が改善されました。

強化:ランサムウェアの検出がより高速になりました。初期の攻撃時など特定の状況で、ランサムウェアの暗号化を一時停止および防止できる可能性のある、新しいメカニズムを採用しました。

強化:シグネチャの機能が強化されました。

強化:シグネチャの正確性が強化されました。

強化:プロセスへのセンサーの可視性が強化されました。

強化:修復が強化されました。

強化:PIVスマートカード ドライバで、IDEmia Cosmo 8.1カードと圧縮証明書がサポートされるようになりました。

強化:FDEの従来の起動前認証とSmart Pre-bootのフローがさらに改良され、視覚障害者ユーザにとってよりスムーズなフローになりました。

強化:Endpoint Securityクライアント言語をManagement UI(ポリシー>クライアント設定>ユーザインタフェース) から変更できる機能を追加しました。

E88.20 - 2024年3月13日リリース

新しい機能と強化

強化:ソフトウェアコンポーネント検証のセキュリティ対策を実装し、未確認のコードからのリスクを軽減します。これにより、Endpointクライアントセキュリティポスチャーの向上と、より強化されたコンピュータ環境を実現します。

強化:Anti-Bot、URL Filtering、Threat Emulation、Anti-Malware E2 DHS Bladeにおいて、特定のプロセスと関連サブプロセスが除外され、分析力とプロセス監視のストリームラインがより強化されました。

強化:インストールしたホットフィックスをEndpoint Securityクライアント UIで確認できるようになりました。

強化:マッチング動作の指標のための"*SameFile*"ルールパラメータのサポートを追加しました。

強化:Eメールからの攻撃実行を検出するセンサーを追加しました。

強化:ファイルワイパーのみを検出するランキングアルゴリズムを変更しました。

強化:Endpoint Securityクライアントの安定性が向上しました。

強化:ファイルがインシデントの一部としてすでに処理されている場合、修復(Remediation)で新しいステータス("*FileAlreadyQuarantined*")を返すようになりました。以前までは、ファイルが隔離されるとRemediationマネージャに"*File already deleted*"(ファイルは削除済み)と表示されていました。

強化:Harmony Endpointで、ポリシーで設定されるPosture Automatic Deployment(ポスチャー自動展開)をサポートするようになりました。

強化:インストーラで、FDE起動前認証タイプからFDEスマート起動前認証(EA機能)にデフォルトで切り替わらず、インストールの前に特定のポリシーを適用する必要があります。インストール時、起動前認証タイプの切り替えが通常操作時のポリシー設定で行えるようになり、これまでのバージョンで切り替えに必要だったアップグレードが不要になりました。

強化:FDEデータベースのメンテナンスが強化され、長時間実行するインストール時のメモリ割り当ての問題を防ぎます。

E88.10 - 2024年2月19日リリース

強化:Endpoint Securityクライアントのインストーラで、チェコ語、ギリシャ語、ウクライナ語、ポルトガル語がサポートされるようになりました。

強化:クライアントUIで、ロケールID(LCID)が正式にサポートされていない言語の場合、デフォルトで英語に設定されるようになりました。

強化:ユーザがアクセスするネットワークドライブの改ざん防止メカニズムの性能が強化されました。

強化:永続化メカニズムのマルウェアに対する修復が強化されました。

強化:マルウェアなりすましの検出が強化されました。

強化:回避手法の検出が強化されました。

強化:ワイパー検出の正確性が強化されました。

強化:検出したDLLに対する修復プロセスが強化されました。

強化:認証情報の盗難の検出が強化されました。

強化:高度な署名のサポートを追加しました。

強化:Harmony Endpoint管理で、変更があった場合は新たなグローバルポリシーを実行し、Endpoint SecurityクライアントにURLS変更を再起動せずに反映することができます。

強化:シャドウコピー作成の検出が強化されました。

強化:VSMONプロセスで、ネットワークの高負荷(DNSサーバで発生する負荷など)の処理時に、接続待ちソケットを開くスピードが20%早くなりました。

強化:Lenovo L14 Gen 3のWi-FiカードがFDEスマート起動前認証(EA機能)でサポートされるようになりました。

強化:*TESvc*サービスの名前が*CPFileAnlyz*(Check Point Endpoint SecurityFile Analyzer)に変わりました。

新しい機能と強化

E88.00 - 2024年1月22日リリース

新機能:Harmony Endpointで、Microsoft Entra ID (旧Azure Active Directory)ドメインサービスをサポートするようになりました。

強化:Harmony Endpointからサーバにハードウェア情報を送信するようになりました。

強化:Harmony Endpointで、Trellixのアンインストール(McAfee製品の一部)をサポートするようになりました。"REMOVEPRODUCTS"パラメータを使用して実行できます。

Enhancement: Harmony Endpointで、外部のサーバAPIによる隔離管理 (Quarantine Management) がサポートされるようになりました。

強化:日付形式が、3文字のMonth(月)、Day(曜日)、Year(年)、Time(時刻)になりました。例: Oct 5, 2023 2:47 PM(2023年10月5日2:47PM)

強化:Endpointクライアントで、マシンがオフラインでもSmart App ControlがオンになったWindows 11をサポートするようになりました。

強化:Anti-Malware E1ライセンスが、VDIおよびスーパーノード環境において自動アップデートされるようになりました。

強化:Anti-Malware E2 Bladeで、クリティカル領域のスキャンをサポートするようになりました。

強化:Windowsコンポーネント モニタリングの拡大により、保護が強化されます。

強化:検出が発生したときのThreat Hunting(脅威ハンティング)へのレポート送信が早くなりました。

強化:高度な署名のパフォーマンスが向上しました。

強化:悪質な操作の検出を向上させるための、インジェクション ロジックが強化されました。

強化:高度なマルウェアに対する保護が強化されました。

強化:リードのサイレント署名は、ユーザが実際の攻撃と混同してしまうリスクを最小限に抑えるため、脅威ハンティング(Threat Hunting)へ転送されることはなくなりました。

強化:AMSI除外メカニズムが強化されました。

強化:Exchange ServerのAMSIパフォーマンスが強化されました。

強化:Behavioral GuardおよびForensic Bladeにおいて、特定のプロセスと関連サブプロセスが除外され、分析力とプロセス監視のストリームラインがより強化されました。注:この機能はSmart Exclusions(スマート除外)を使用するお客様のみご利用いただけます。

強化:データブロックに関するイベントをスキャンすることによる行動解析が強化されました。

強化:ポスチャー管理のインストール率が改善されました。

強化:Application Controlカスタム ルール評価がパフォーマンスに最適化されています。

強化:Full Disk Encryptionのスマート起動前認証Wi-Fiドライバがアップデートされました。

強化:Full Disk Encryption Bladeで、Microsoft Entra ID (旧Azure Active Directory) からのユーザがサポートされるようになりました。既知の制限事項セクションを参照してください。

強化:Full Disk Encryption起動前認証で、これまでの31文字制限をなくし、長いユーザ名 (64文字まで) とパスワード (256文字まで) をサポートするようになりました。この変更は、FDE起動前認証とFDEリカバリツールでのユーザ認証情報フィールドに適用されます。

新しい機能と強化

強化:ブラウザベースのDLP(データ漏えい防止) 機能をEA(Early Availability) のお客様向けに追加しました。初期フェーズでブラウザ拡張が有効な場合、セキュリティはアップロード/ダウンロードされたファイルのスキャンを通して強化されます。

リリースマップ

ダウンロードパッケージの場合、新しい機能、強化、修正された問題、既知の制限の全一覧は、専用のSKを参照してください。

バージョン	SK記事	公開日
E88.30	sk182109	2024年4月17日
E88.20	sk182044	2024年3月13日
E88.10	sk181927	2024年2月19日
E88.00	sk181675	2024年1月22日

管理サーバの要件

- E88.xクライアントを管理できるEndpoint Security Management Serverは次のとおりです。R81.20、R81.10、R81、R80.40、R80.30、R80.20、R80.20.M2、R80.10です。

  注:
  - BitLocker Managementでは、R80.40およびそれ以降、またはホットフィックスを持つR80.30バージョンが必要です。*BitLocker Management Release Notes*を参照してください。
  - HarmonyEndpointとCapsule Docsを管理できるEndpoint Security Management Serverは、R81.10、R81、R80.40、R80.30、R80.20、R80.20.M2です。お使いのサーババージョンのリリースノートに記載されているサーバ要件を参照してください。

- 新しいThreat Emulationレポートフォーマットは、E80.90クライアント以降で使用できます。Endpoint Security Management R80.30より古いバージョンでこの機能を利用するには、sk152752を参照してください。

- E80.89以降のクライアントのアンチマルウェアでは、Endpoint Security Management Serverからシグネチャアップデートを受け取るためのManagement Serverアップデートが必要です。sk141033を参照してください。

- E88.xをEndpoint Security Management Serverにアップロードする際にエラーが発生した場合、Full Disk EncryptionユーザはSmartConsoleをEndpoint Security Clients for Windowsリリースページから利用できるバージョンで置き換える必要があります。リリースの一覧の*リリースマップ (10ページ)*セクションを参照してください。

- E80.87およびそれ以降のバージョンでは、Endpoint Security Management Serverバージョン R80.20以前のSmartLogでログを表示するためにManagement Serverのアップデートが必要です。sk106662を参照してください。

クライアント要件

このセクションでは、Endpoint Securityクライアントの要件について説明します。

サポートされているクライアントのオペレーティングシステム

Microsoft Windows

バージョン	エディション	サポート開始
11 23H2	Enterprise Pro	Endpoint Securityクライアント E87.62
11 22H2	Enterprise Pro	Endpoint Securityクライアント E86.70
11 21H2	Enterprise Pro	Endpoint Securityクライアント E85.40
10 22H2	Enterprise Pro	EAサポート : Endpoint Securityクライアント E86.80 GAサポート : Endpoint Securityクライアント E87.00
10 LTSC (バージョン21H2)	Enterprise Pro	Endpoint Securityクライアント E86.00
10 21H2	Enterprise Pro	Endpoint Securityクライアント E86.00
10 21H1 (バージョン2103)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 20H2 (バージョン2009)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 20H1 (バージョン2004)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 19H2 (バージョン1909)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 19H1 (バージョン1903)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 LTSC (バージョン1809)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 (バージョン1809)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 (バージョン1803)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 (バージョン1709)	Enterprise Pro	Endpoint Securityクライアント E85.00
10 LTSB (バージョン1607)	Enterprise Pro	Endpoint Securityクライアント E85.00
8.1 アップデート 1	Enterprise Pro	Endpoint Securityクライアント E85.00
7 SP1 Microsoft更新プログラム KB3033929	Enterprise Professional	Endpoint Securityクライアント E85.00

注:

- 既存のEndpoint Security導入において、OSバージョンのアップグレード前に、上記の表で希望するOSバージョンをサポートするEndpoint Securityクライアントのバージョンにアップグレードする必要があります。
- Windows 7のサポートに関する追加情報は、sk164006を参照してください。
- Windowsオペレーティング システムが、Check Pointクライアント サポートのライフサイクルに基づきサポートされ、またバーチャル マシンでもサポートされるようになりました。ただし、Windowsの異なるバージョンすべてに対する専用QAプロセスは設けていません。サポート バージョンのうち、いずれかのWindows OSバージョンに関連する特定の問題が発生した場合、Check Pointでは開発部門の支援を得ながら、最大限の努力とサポートを提供していきます。

Microsoft Windows Server

バージョン	エディション	サポート開始	サポートされている機能
2022 64ビット	すべて	E85.40	Compliance、Anti-Malware、Firewall、Application Control、Forensics、Anti-Ransomware、Anti-Bot、Threat Emulation、Capsule Docs (スタンドアロン クライアント)、Media Encryption & Port Protection
2019 64ビット	すべて	E85.00	Compliance、Anti-Malware、Firewall、Application Control、Forensics、Anti-Ransomware、Anti-Bot、Threat Emulation、Capsule Docs (スタンドアロン クライアント)、Media Encryption & Port Protection
2016 64ビット	すべて	E85.00	Compliance、Anti-Malware、Firewall、Application Control、Forensics、Anti-Ransomware、Anti-Bot、Threat Emulation、Capsule Docs (スタンドアロン クライアント)
2012 R2 64ビット	すべて	E85.00	Compliance、Anti-Malware、Firewall、Application Control、Forensics、Anti-Ransomware、Anti-Bot、Threat Emulation、Capsule Docs (スタンドアロン クライアント)
2012 64ビット	すべて	E85.00	Compliance、Anti-Malware、Firewall、Application Control、Forensics、Anti-Ransomware、Anti-Bot、Threat Emulation、Capsule Docs (スタンドアロン クライアント)
2008 R2 32/64ビット	すべて	E85.00	Compliance、Anti-Malware、Firewall、Application Control、Forensics、Anti-Ransomware、Anti-Bot、Threat Emulation、Capsule Docs (スタンドアロン クライアント)

注:

- Windows Server 2016向けのEndpoint Complianceルールを R80.20より古いバージョンでサポートするには、sk122136を参照してください。
- Windows Server COREはサポートされていません。
- サーバでサポートされていない機能が含まれたクライアント パッケージをインストールすると、インストール自体は成功しますが、サポートされている機能だけが実際にインストールされます。

サポートされるHarmony Endpoint Browser Extension for Windows

Harmony Endpoint Browser Extension for Windowsクライアントの対応ブラウザ

	Chrome	Microsoft Edge (Chromium)	Firefox	Internet Explorer
ファイルダウンロード時の保護	✓	✓	✓	✓
ゼロフィッシングや企業のパスワードの再使用保護などを含む認証情報の盗難保護	✓	✓	✓	✓
URLフィルタリング (Web Managementユーザのみ)	✓	✓	✓	–

注 - Firefox ESRでの拡張機能を有効にするには、ユーザが手動で許可する必要があります。

Endpoint Securityクライアントの対応言語

Endpoint Securityクライアントでは以下の言語を利用できます。

- 英語
- イタリア語
- ポルトガル語
- ドイツ語
- ロシア語
- ウクライナ語
- ポーランド語
- フランス語
- チェコ語
- 日本語
- ギリシャ語
- スペイン語

クライアントのハードウェア要件

Total Endpoint Security Packageを実行するためのクライアントコンピュータのハードウェアの最小要件は次のとおりです。

- 2 GB RAM
- 2 GBディスク空き領域

Total Endpoint Security Packageを実行するためのクライアントコンピュータのハードウェアの推奨要件は次のとおりです。

- 8 GB RAM
- 6 GBディスク空き領域

Full Disk Encryption要件

ここではCheck Point Full Disk Encryptionについて説明します(BitLocker Managementは対象外) 。

Full Disk Encryptionクライアントには以下が必要です。

- クライアントのシステムボリュームに512MBの連続した空き領域

注 - Full Disk Encryptionをクライアントに導入する際、512MBの連続したディスク領域を確保するためにFull Disk Encryptionサービスで自動的に最適化が行われます。ディスクの暗号化実行中は、Windowsのハイバネーション機能を一時的に停止します。

クライアントに以下が**ないようにして**ください。

- RAID。
- ストライプセットまたはボリュームセットの一部となっているパーティション。
- ハイブリッドドライブまたは同様のドライブキャッシュ技術。sk107381を参照してください。
- 圧縮されたルートディレクトリ(ルートディレクトリの圧縮されたサブディレクトリはサポート) 。

UEFI(Unified Extensible Firmware Interface) の要件

一部のコンピュータ上のBIOSを置き換える新しいUEFIファームウェアには、Full Disk Encryptionで使われる新たな機能があります。

UEFIモードのFull Disk Encryptionの要件は、以下のとおりです。

- Windows 11
- Windows 10(32/64ビット)
- Windows 8.1アップデート1(32/64ビット)
- Windows 7(64ビット)

LANでのロック解除の要件

- **macOS** - macOSでは、LANでのロック解除をOS X Lionおよびそれ以降を標準装備しているコンピュータで使用できます。LANでのロック解除は、コンピュータのファームウェアがアップデートされている場合は一部の古いコンピュータ上でも利用できます。
- **Windows** - Windowsでは、LANでのロック解除をUEFIネットワークプロトコルをサポートしているコンピュータで使用できます。UEFIネットワークプロトコルは、ビルトインのイーサネットポートを持つWindows 8、Windows 10、またはWindows 11ロゴ認定コンピュータ上にあります。コンピュータは、UEFI Nativeモードで Windows 8、Windows 10、またはWindows 11を実行していて、Compatibility Support Module(CSM) が無効になっている必要があります。一部のコンピュータでは、UEFIネットワークのサポートはBIOSセットアップで手動により有効にする必要があります。

UEFIネットワーク接続問題に関するトラブルシューティングは、sk93709を参照してください。

UEFI「Absolute Pointer」キーボードレスタブレットタッチの要件

タブレット(64ビット) の起動前タッチ入力のサポートには以下の要件があります。

- Windows 8、Windows 10、Windows 11ロゴ認証のコンピュータ
- UEFIファームウェアはUEFI Absolute Pointerプロトコルを実装している必要あり

デバイスのタッチサポートに関する情報は、sk93032を参照してください。

自己暗号化ドライブ(SED)

Full Disk Encryption対応の自己暗号化ドライブを使用できます。

要件は以下のとおりです。

- UEFIモードをサポートしているWindowsバージョン
- UEFI ATAパススループロトコルまたはUEFI Security Commandプロトコルを実装しているUEFIファームウェア
- TCG Opal準拠ドライブ(バージョン1.0.または2.0)

チェック・ポイントでテストしたデバイスの一覧についてはsk108092を参照してください。

SED Opal暗号化を備えたUEFIコンピュータのCheck Point Full Disk Encryptionとの互換性に関する情報は、sk93345を参照してください。

TPMのサポート

TPMは起動前コンポーネントの整合性を確認するセキュリティを強化するために使われます。TPMを使用するには、Full Disk Encryptionポリシーで有効にする必要があります。

システム要件は以下のとおりです。

- 1.2または2.0の仕様のTPMハードウェア

Media Encryption & Port Protection

ストレージデバイス:

- USBデバイス
- eSATAデバイス
- CD/DVDデバイス
- SDカード

クライアント導入

1. Endpoint Security Clients for Windowsを*リリースマップ (10ページ)*セクションからダウンロードしてください。
2. インストールおよびアップグレードの手順については、*Endpoint Security Clients for Windows ユーザガイド* > はじめに > クライアントのインストールとアップグレードを参照してください。

サポートされるアップグレードパス

Endpoint Securityクライアントのサポート対象アップグレード

E88.x Endpoint Securityクライアントへアップグレードできるのは、E81.00以降のバージョンです。

ATM向けEndpoint Securityクライアントのサポート対象アップグレード

最新のATM向けEndpoint Securityクライアントへアップグレードできるバージョン:

- E80.86およびそれ以降のATM向けEndpoint Securityクライアント
- E75.30およびそれ以降のATM向けリモートアクセスVPNクライアント

詳細とダウンロードについては、sk133174を参照してください。

レガシークライアントのアップグレード

- **レガシーMedia Encryptionクライアント**

  レガシーMedia Encryptionのサポートされているアップグレードについては、sk99116を参照してください。

- **レガシーFull Disk Encryptionクライアント**

  レガシーFull Disk Encryptionクライアントのサポートされているアップグレード パスは、7.5.1からE80.82、およびE80.82からE88.xのアップグレードです。

  重要 - E80.82 ~ E81.10およびそれ以降からE88.xにアップグレードする前に、sk110420を参考にしてください。