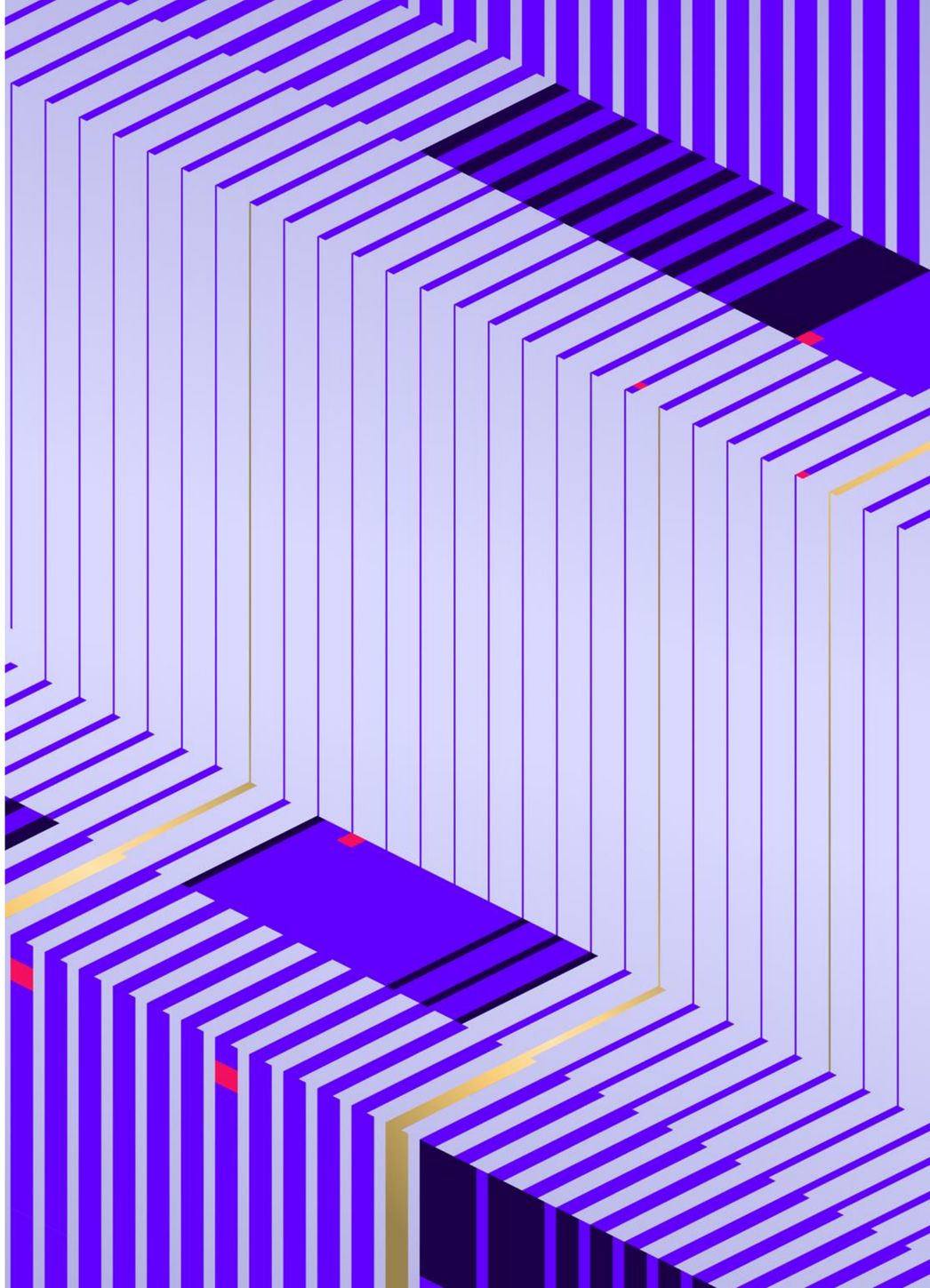
# SentinelOne エージェントのアップデート方式について

2024年7月22日
SentinelOne Japan 株式会社

SentinelOne
Secure Tomorrow



# SentinelOne エージェントのアップデート方式

## ライブ
## アップデート

検出および保護機能を
強化するための小規模な
セキュリティアップデート

## エージェント
## アップグレード

エージェントの全体的な
機能やセキュリティ機能の
大規模なアップグレード

# ライブアップデートとエージェントアップグレードの違い

| | ライブ<br>アップデート | エージェント<br>アップグレード |
|---|---|---|
| 目的 | 検出および保護機能を強化するための<br>小規模なセキュリティアップデート | エージェントの全体的な機能や<br>セキュリティ機能の大規模なアップグレード |
| 内容 | 静的・動的検出エンジンの更新や<br>ルールの追加 | 追加された新機能や修正を施すための<br>エージェントモジュール全体の更新 |
| カーネルコンポーネント<br>（ドライバや.sysファイル<br>など）の有無 | なし<br>（ユーザーモードのみ） | あり<br>（カーネルドライバを含む） |
| 自動更新 | あり<br>（ユーザーにて自動更新の有効・無効の選択が可能） | なし<br>（ユーザーが指定したバージョンに更新） |
| 展開方法 | 環境へのリスクを最小限に抑えるため<br>段階的な展開を実施<br>（一斉同時更新は実施されない） | 環境へのリスクを最小限に抑えるため<br>段階的な配布を実施<br>（管理者が設定したエリア、バージョン、<br>スケジュールに従って展開の実行が可能） |
| 公開頻度 | 不定期 | GA：定期（1回/四半期）<br>パッチ（軽微な更新を含む）：不定期 |

# SentinelOne エージェントと更新プロセスの特徴

## ✓ お客様にて設定可能な更新管理

- ライブアップデートおよびエージェントアップグレードいずれにおいても、お客様にて自動更新の有効・無効の選択が可能な方式（オプトイン方式）を採用しております。
- 特にカーネルや重要なコンポーネントを更新するエージェントアップグレードにおいては、手動または設定したポリシー（エリアと時間帯を指定）に従い更新を実行できるため、お客様の組織や環境のニーズに合わせることが可能です。

## ✓ 慎重な段階的展開プロセス

- ライブアップデートに関しては、一斉での全システムへ適用は行われず、複数の段階を経て慎重に展開されます。
- 各段階で問題を監視し、影響範囲を最小限に抑えながら安全に更新を進めることが可能です。

## ✓ 安全性重視のエージェント

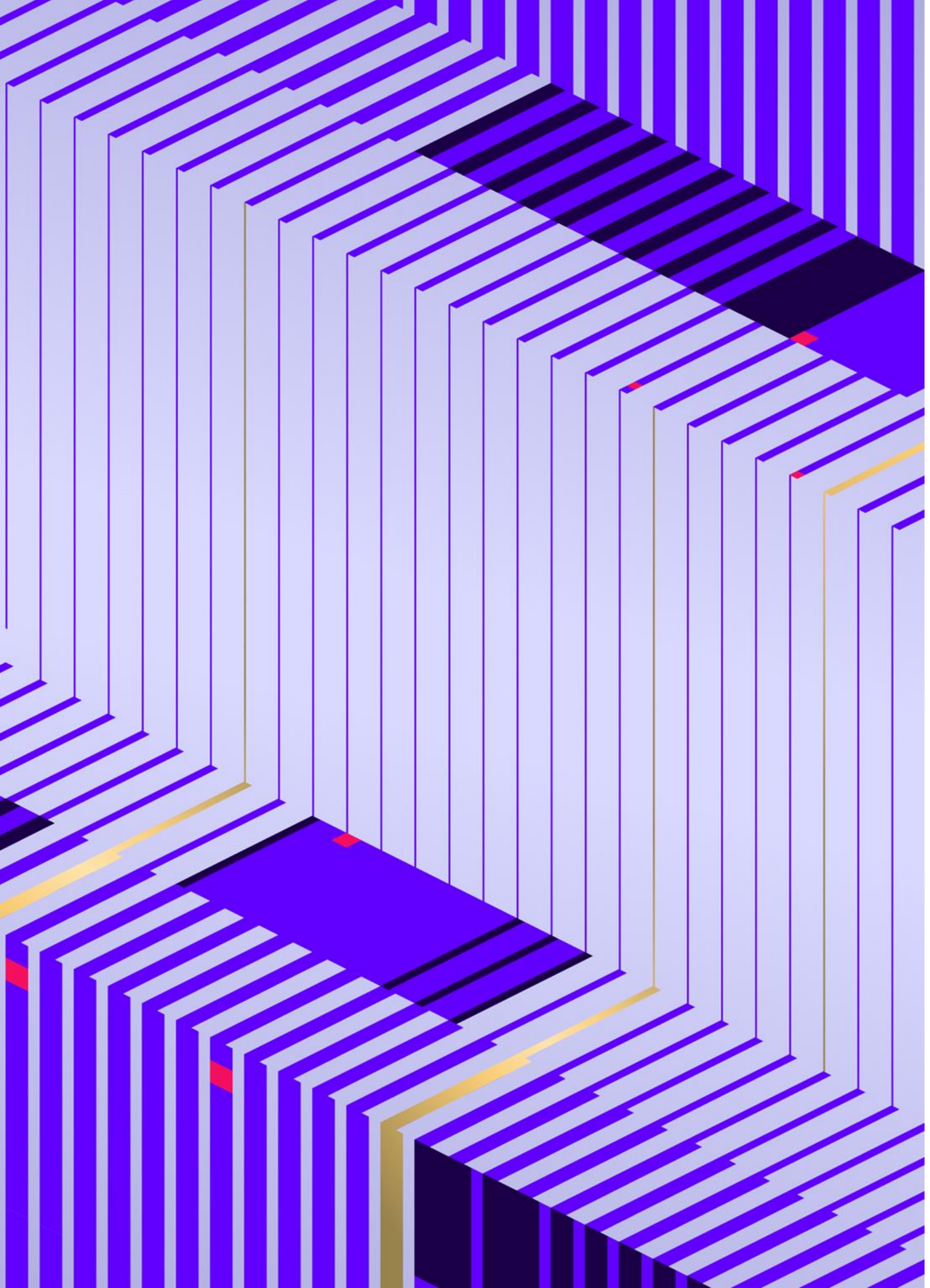
- ライブアップデートでは、システムの安定性に直接影響を与えるカーネルモジュールや重要なコンポーネントを更新しておりません。
- 殆どのエージェント機能はユーザーモードで動作しています。一部カーネルモードで動作している機能もありますが、非常にシンプルな機能であるため、影響を与える可能性は低いものとなっています。

## ✓ 徹底した事前テストと検証

- カーネルや重要なコンポーネントが含まれるエージェントアップグレードにおいては、リリース前に多段階のテストプロセスと約60万のエージェントによる事前テストを実施しております。
- これにより、本番環境での予期せぬ問題のリスクを大幅に低減し、高い信頼性を確保しています。

## ✓ 透明性の高い更新情報提供

- 各更新には詳細なリリースノートと変更内容の説明をご案内しております。
- お客様は更新の目的と影響をあらかじめ理解し、情報に基づいた展開の判断が可能となります。



SentinelOne
Secure Tomorrow

# Thank You

Sentinelone.com