ビジネスと IoT の完全性の保護

Symantec Secure App Service: 他に類を見ない IoT のコードサイニングサービスとセキュリティ

Symantec™ Complete Website Security

データシート

モノのインターネット（IoT）によってデジタル業界の状況は急速に変化し、我々が住むこの世界も大きく様変わりしています。インテリジェントデバイスとセンサーによって、スマートカー、ロボット製造設備、スマート医療設備、スマートシティ、工業制御システムなどの多くのものが接続され、人々の生活は便利になり、企業も大幅にコストを削減しています。しかし、いいことばかりではありません。IoT の急速な成長によって、新たな次元のセキュリティ脆弱性が出現し、サイバー犯罪のリスクの悪質さ、深刻さは劇的に増大しているのです。

従来の機密保持に対するサイバーリスクに加え、IoT の脅威には次の攻撃が考えられます。

- スマート電化製品を使用不可にする。
- 都市の送電網を停止する。
- ペースメーカーなどの医療機器をハッキングすること。
- 財務的損害が大きく人命にかかわるような産業事故や危険を引き起こす。
- ボット感染した監視カメラでインターネット全体を不安定にする。
- スマートカーのアクセル、ステアリング、およびブレーキをハイジャックする。

このようなセキュリティの弱点は生命を脅かし、顧客を失望させ、業務の遂行を妨害するだけでなく、IoT 開発者と製造者に、多くのコストと対社会関係の損害を与えます。最近、攻撃者が遠隔操作で車の運転を乗っ取ることができる欠陥が見つかり、140 万台の自動車がリコールされるというケースがありましたが、これなど典型的な例といえるでしょう。

このようなリスクの最大の要因は、ソフトウェアはコードサイニングで保護されていない限り、簡単に改ざんされてしまう可能性があるということです。そしてこれが、IoT デバイスソフトウェアのコードサイニングが必須になった理由です。IoT デバイスでは署名されていないコードを実行すべきではありません。確認されていないデバイスや確認されていないサービスからデータを受け取ることは、とても危険です。

すべての IoT ファームウェアおよびソフトウェアにコードサイニングを行えば、マルウェアの作者が悪意のあるコードをデバイスに埋め込めないようにすることができます。コードサイニングはデジタルによるシュリンクラップのような働きをします。すなわち、ソフトウェアやアップデートが確認済みの発行元から送信されたものであり、署名後に改ざんされていないことを保証します。また、特定の権限者によって署名されたコードだけがファームウェア上で実行できるようにすることもできるようになります。言い換えると、自分が IoT デバイスのコードサイニング権限者となり、自分で署名したコードのみをファームウェアが受け入れるようにすることもできるのです。

サイバーセキュリティの世界的なリーダーとして信頼されるシマンテックの Secure App Service は、必要とされる視認性、敏捷性、安全性を提供することによって、より安全で簡単な IoT のコードサイニングを実現し、ビジネスを重大な財務的損失やブランドダメージから守ります。

IoT デバイスおよびビジネスの完全性の保護

Symantec Secure App Service のコードサイニングによって、IoT デバイスで次のことを実現できます。

- 信頼できる発行元からのコードのみを受け入れる
- 署名されて認証されたコードのみを実行する
- 実行するようプログラムされたことのみを実行する

Symantec

ビジネスと IoT の完全性の保護

Symantec Secure App Service: 他に類を見ない
IoT のコードサイニングサービスとセキュリティ

Symantec™ Complete Website Security

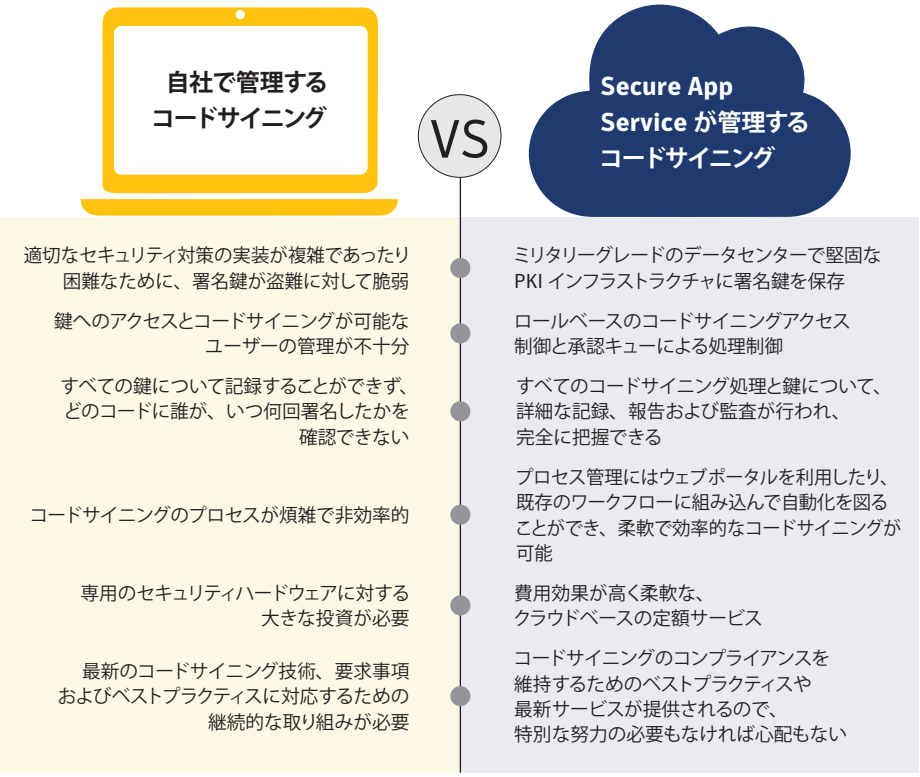
迅速で簡素化されたコードサイニングによる鍵の保護

IoT デバイスに埋め込まれたソフトウェアがサイバー犯罪者によって改ざんされないよう防止するには、コードサイニングだけでは不十分です。コードサイニングの秘密鍵を安全に保つ必要があります。コードサイニングは、認証局 (CA) から発行されたデジタル証明書によってソフトウェアにデジタル署名することで成り立ちます。これらの証明書の安全は、公開鍵と秘密鍵という鍵のペアに依存します。何者かによって秘密鍵が盗まれた場合、その人物はその秘密鍵を使用してマルウェアに署名し、それをすべての IoT デバイスに合法的に配布することができるようになってしまいます。

鍵の保護に失敗すると、サイバー犯罪者に IoT ソリューションの完全な制御を許してしまいます。Secure App Service を利用すれば、幅広く奥深い機能によって鍵の保護を実現できます。しかも、IoT ソフトウェアのコードサイニングの労力が軽減され、不安も払拭されます。

企業独自の IoT コードサイニングに苦労して取り組む必要はありません。Secure App Service はプロセスが簡単なので、シンプルで安全な IoT コードサイニングを実現できます。

- シマンテックの安全なクラウドサービスにソフトウェアまたはファイルハッシュをアップロードしていただき、シマンテックが署名を行います。
- シマンテックの管理ダッシュボードを使用できます。または、シマンテックが提供する API を使用して管理サービスをお客様独自のビルド処理に組み込むこともできます。
- クラウド上のミリタリーグレードのデータセンターに、証明書および鍵を安全に保存することができます。
- 鍵を社内環境に保存する場合に生じるセキュリティリスク、管理の複雑さ、ハードウェアセキュリティへの投資などについて心配する必要がなくなります。



全面的な IoT セキュリティ

コードサイニングによる IoT デバイスのソフトウェアの完全性の保護に加え、シマンテックは幾層にも重なるさまざまなセキュリティのソリューションを提供し、さらに包括的な IoT 保護を実現します。

- ユーザーとデバイス、サービスとデバイス、およびデバイス間の通信における強力な相互認証
- 無線通信データや保存データを保護する、強力でチップ効率のよい暗号化
- ホスト上での鍵の保護や保護機能の強化により、高度な脅威を緩和
- 動的 IoT セキュリティ管理

Symantec

ビジネスと IoT の完全性の保護

Symantec Secure App Service: 他に類を見ない
IoT のコードサイニングサービスとセキュリティ

Symantec™ Complete Website Security

柔軟なコードサイニングオプションによる IoT ソフトウェアの保護

IoT は極めて革新的で幅が広く、絶えず変化しています。したがって、その開発環境は多様であり、サポートすべきソフトウェアのファイルタイプも多岐に渡ります。こうした IoT ソフトウェアの多様性に対応するため、Secure App Service では Open SSL、GPG、RPM の 3 つの署名オプションをサポートし、柔軟なコードサイニングを実現しています。これらの署名オプションはいずれも、IoT のファームウェアや OS イメージへの署名が可能です。また、ファイルサイズの大きさによらず、さまざまな特性のソフトウェアへの署名も可能です。

Secure App Service の IoT コードサイニングオプション

	Open SSL	GPG	RPM
鍵モデル	固定証明書プール（オンデマンド鍵）固有鍵モデル	新規の鍵固定証明書プール	新規の鍵固定証明書プール
ファイルタイプ	すべて	すべて	.rpm
全ファイルアップロードとハッシュベース署名	ハッシュベースおよび全ファイルアップロード	全ファイルアップロードのみ	全ファイルアップロードのみ
ダイジェストアルゴリズム	SHA1 SHA256	SHA1 SHA256	SHA1 SHA256
サイニングオプション	rsautl dgst	sign（バイナリ） clearsign detach-sign	addsign resign

コードサイニングのすべての処理を完全に制御し、またすべての情報を把握することによって、ビジネスと IoT の完全性を保護しましょう。サイバーセキュリティの世界的なリーダーとして信頼されるシマンテックの Secure App Service は、視認性、敏捷性、安全性を提供することによって、シンプルで安心して利用できる IoT のコードサイニングを実現し、ビジネスを重大な財務的損失やブランドダメージから守ります。

Symantec