SecureAge

SecureAgeの透過暗号使用により防御可能な情報漏洩12事例

SecureAge ホワイトペーパー2020年

サイバーセキュリティの新たな境界

ネットワーク境界の保護が不十分であることは、かなり以前から認識されてきました。今日のローカルネットワーク、ネットワークデバイス、クラウドアプリケーションの環境において、組織が使用するセキュリティ技術には、ゼロトラスト等のSDP（ソフトウエア・デファインド・ペリメタ）、マイクロセグメンテーションなどがあります。これらのアプローチと関連技術は、ファイルなどのデータコンテナへの不正なアクセスをブロックするよう設計されています。ファイルへのアクセス制御が、セキュリティの新たな境界です。

制御しても無くなることのない情報漏洩

しかしながら、2019年の情報漏洩は123億件と報告されており、データ盗難が依然として一般的な問題であることが明らかです。オペレーティングシステム、ネットワークハードウェア、その他のデバイスにはサイバーセキュリティ制御を回避できる欠陥が常に伴い、悪用されてファイルへの不正アクセスを提供する可能性があります。

> MS SMBv3の脆弱性により、不正な攻撃者によるターゲットサーバーやクライアントマシン上でのコード実行が可能となり、特権的アクセスを即時に付与してしまう恐れがある。

また人的要因も非常に重要です。外部の不正者以上に、内部者と関係者である第三者がデータ損失の最も深刻な原因と見られていますが、これは偶発的か意図的かに関係なく、情報へのアクセス権限があるためです。

前述の技術では、これが大きな問題となります。なぜなら、データへの承認されたアクセスとデータの不正使用の区別が不可能であるからです。そして一番の問題は、これらのシステムがファイル内のデータ自体を保護しないという点にあります。そのためアクセス許可を持つ正当なユーザーによって、ファイル（ファイル内に保持される重要な情報）が流出する可能性があるのです。

情報漏洩—4つのパス

データの流出や盗難は、以下4つのパスのいずれかによるものです。

A. 内部者によるデータ窃取

この場合は、少なくとも正当なユーザーのように見える個人がデータを盗みます。

B. 特権ユーザーによるデータ窃取

特権ユーザーはデータへの広範なアクセス権を持ち、データを流出させることのできる立場にあります。

C. ハッカーの侵入によるデータ流出

盗むか買い取ったユーザーの資格情報、マルウェア、ネットワークの脆弱性は、すべてハッキングに利用されます。

D. 人為的なエラー

誰にでもミスをする可能性があります。その結果、ある段階でデータが脆弱になることがあります。

本書の構成

情報漏洩の4つのパスの構造から、さまざまなデータ流出と盗難のシナリオを検証していきます。いずれも、不正なデータアクセスをブロックするはずであった既存のサイバーセキュリティツールを回避する手法を利用したシナリオです。それらの環境でどのようにデータが流出したのか、その脅威をSecureAgeのアプローチであれば、いかに防御できるかを、各シナリオごとに説明していきます。

データ自体がセキュリティを纏うアプローチ

情報はファイル内に（保護されずに）含まれています。しかし、機密情報や知的財産はもちろん、毎年何十億というデータレコードが盗まれたり紛失しています。そしてその全てが、組織外では完全に非保護となるファイル内に含まれています。

SecureAgeのSecureDataは、情報を最も基本レベルであるファイル単位で暗号化により保護を行い、データ自体がセキュリティを纏うアプローチを採用しています。ファイルへの不正アクセスをブロックしたり、保護対象データを選択したりするような他のサイバーセキュリティ製品とは異なり、SecureDataは暗号化により、ファイル内の全データを本質的に保護します。

仮に盗まれても、SecureDataを使用して暗号化されたファイルは復号化が不可能なため、だれ一人ファイルにアクセスすることは出来ません。データアクセス権限のある内部者に盗まれた場合でも、盗難データを確実にアクセス不能にするためには、このアプローチしかありません。

情報漏洩のシナリオA
内部者によるデータ窃取

1. ユーザーアカウントへの不正アクセス

あるユーザーのログインIDとパスワードが不正にアクセスされています。犯人は侵害したユーザーのラップトップ操作、リモート操作、または仮想デスクトップを介して企業アカウントへのアクセスを得ました。内部者と見られるこの犯人は、侵害したユーザーアカウントで利用可能な全情報にアクセスすることができます。それらのデータには、個人情報、知的財産、その他の機密資料が含まれている可能性があります。このユーザーの担当業務を考えると、明らかにそうした情報へのアクセスが可能なアカウントです。

> 外国籍の3人組が、ニューヨークの法律事務所2か所のネットワーク侵入に成功し、内部情報（保留中のM&A情報）を窃盗・売却した。不正利益は400万ドル以上。

既存のサイバーセキュリティツールは、ログインしたユーザーのIDに基づいて機密のデータファイルへのアクセスを可能にしますが、意図の正当性や悪意があるかどうかの判断は不可能です。盗まれたファイルはもはや何の保護もなく、その情報へのアクセスは簡単です。

ソリューション

SecureAgeのSecureDataを利用すれば、ファイルはあらゆる記憶域メディア上で常に暗号化されたままとなります。SecureDataは常に操作を必要とせず機能するため、決してユーザーの妨げにならず、バックグラウンドでファイルの暗号化が処理されていても気がつきません。

犯人がユーザーアカウントにログインして、ファイル表示できる可能性があっても、SecureDataであれば、新しい保存場所（USBスティックなど）にコピーされてもファイルは暗号化されたままなので、組織外に出ると利用することができなくなります。トークンベース認証が使用され、暗号化キーがトークンに保存されている場合、盗んだ資格情報を使用する犯人は、トークンへのアクセスなしにファイル内容を表示することはできないのです。

2. ユーザーがアプリケーションからデータを抽出

正当なユーザーが、アプリケーションデータをローカルファイルにコピーまたはエクスポートします。これで、このアプリケーション自体のセキュリティはもはや適用されなくなり、保護されてないこの新ファイル内のデータを簡単に盗むことができます。

> Morrisons Supermarketのある上席監査役が、会社への恨みから同社に損害を与えようと、約10万人分の従業員の給与データを漏洩。

ソリューション

SecureDataのファイルレベルでの本質的な暗号化により、エクスポートされたデータはローカルファイル作成時に静かに暗号化され、その保護はファイルのライフサイクルを通して維持されます。データがアプリケーションから新しいファイルまたは既存のファイルにコピーまたはエクスポートされると、ソースで暗号化され、その権限あるユーザーがファイルを自宅に持ち帰っても暗号化が続きます。もっとも、組織外ではそのファイルを復号することはできません。

他のファイル暗号化製品は、暗号化するかどうかの主体的な決定がユーザーにより行われています。これらには、指定されたステータスに基づいてファイルを暗号化するデータ分類の場合もあれば、Microsoft EFSのようにファイルまたはフォルダを直接暗号化するものもあります。どちらにしても、ユーザーに判断を委ねるのは当事者に(a)選択によるプライバシーとセキュリティへの影響に対する認識がない可能性、(b)セキュリティよりも利便性だけで選択する可能性が考えられるため、問題があります。

3. データベースログと一時ファイルの盗難

データベースログや機密情報を含む一時ファイルが、USBストレージにコピーされました。ログおよび一時ファイルは、アクセス権管理ソフトウェアが「重要」に分類しなかったため、保護されていません。さらに、ログおよび一時ファイルとともに構造化されていないファイルは、データベースの透過的データ暗号化（TDE）製品によって保護されないため、この技術では情報の盗難を防止できません。

> Peekaboo Momentsアプリを開発したBithouse Inc.が、電子メールアドレス、地理的位置データ、詳細なデバイスデータ、写真やビデオへのリンク等の情報を含む、7,000万以上のログファイルの保護に失敗。

ソリューション

SecureDataは、すべての保存場所にある全ファイルを暗号化するため、確実にすべての情報を保護します。

そのため、盗まれたログや一時ファイルも暗号化されたままとなり、利用することは不可能です。データベースだけでなく、多くのアプリケーションも機密性のある情報の要素を含む一時ファイルを生成します。Microsoft Officeアプリケーションはそうしたグループの一例にすぎません。

アクセス権管理や分類ソリューションにおいては、一時ファイルとログファイルは重要なものではないとして無視されます。しかし、しばしばその中に、プライマリファイルに保持されているデータの多くが含まれています。SecureDataのシームレスなファイル暗号化のアプローチは、ユーザーとアプリケーションの双方に透過的であり、暗号化エンジンを経由してメモリを出入りするデータが「ストリーム処理」されることでパフォーマンスに影響しません。さらに、CPUのAES-NIを使用することで、暗号化処理がI/Oよりも確実に高速化されます。

4. 効果のないサードパーティのセキュリティ

機密データを処理するサードパーティのパートナー企業やコンサルタントが、情報に十分なセキュリティを維持していない場合があります。貴社の管理外かつ常時監視外のサードパーティは、潜在的なデータ損失の典型例です。

> Nedbankの顧客170万件が対象となったセキュリティ侵害は、サードパーティ サービスプロバイダーで生じた。データはサードパーティにSSL/TLSで暗号化送信されたが、保管時には非暗号化のままだった。

ソリューション

サードパーティにSecureDataの使用を義務付けることで、この問題を解決できます。サードパーティやコンサルタントから盗まれたデータは、すべて暗号化されているため利用できません。

SecureData展開の利点はそれだけでなく、その特殊なファイル暗号化技術によりサードパーティの業務にも影響を与えません。貴社のデータは暗号化されたままで、しかも必要に応じてアクセス、変更、管理が可能です。

セキュリティ管理サーバー（SMS）を使用すると、サードパーティのエンドポイントデータの使用に対する制御を維持できます。さらに、貴社の暗号化キーの使用により、自社データをそのまま管理下におけます。そのデータへのアクセスは、SMS経由で対応するポリシーを変更することで失効させることができます。

情報漏洩のシナリオB
特権ユーザーによるデータ窃取

5. 特権ユーザーによる未許可ファイルへのアクセス

特権ユーザーが自分のアクセス権を使用し、見ることを想定されてないデータが含まれたファイルを持ち出しました。個人がファイルへの正当なアクセス権（業務上必要なアクセス）を持っていれば、ファイルを盗むことが可能です。

> Edward Snowdenは管理者としての立場を利用し、米国のNSAから約170万のドキュメントを窃盗。

管理者はその立場上、ファイル管理が可能でなければなりません。例えばサーバー間の移動や、バックアップの復元などです。

それが可能ということは、つまりそのファイルの内容を見ることも可能になります。監査ログと監視では何があったのかがイベント後に判りますが、それではデータ盗難を予防できません 。

ソリューション

SecureDataなら、ユーザーごとにファイルレベルでの暗号化を行い、許可されたユーザーだけが各ファイルを復号できます。管理者によるファイル移動や権限管理はそのまま可能ですが、ファイルの内容を復号してアクセスすることはできません。このシナリオでは、特権ユーザーは自分の職務の実行は可能ですが、自分が管理するファイルの内容を表示することまではできません。さらにSecureAge SMSは、ファイルを復号しようとして失敗した場合にそのすべてを記録します。

6. 管理者によるバックアップからのファイル窃盗

ある特権ユーザーがバックアップメディアにアクセスし、知的財産を含むファイルを持ち出しました。管理者は、必要なときにファイルを復元できるよう、バックアップメディアの内容にアクセスできる必要があります。多くの場合、バックアップは暗号化され保護されていますが、バックアップの復号キーにアクセスする必要がある管理者は、バックアップされたファイルを復元できます。

> Uberのユーザーデータ数百万件が盗難。ハッカーは、GitHubリポジトリに誤って残された資格情報を使用し、Amazonウェブサーバーへのアクセス権を入手。ファイルには、顧客データを含むバックアップが含まれていた。

ソリューション

SecureDataのユーザーごとのファイルレベルの暗号化により、バックアップに個別に暗号化されたファイルが含まれるようになります。

管理者は引き続き、これらのファイルをバックアップメディアから復元できますが、復号してファイルの内容にアクセスすることはできません。

情報漏洩のシナリオC
ハッカーの侵入によるデータ流出

7. マルウェア

> Travelexはランサムウェア攻撃を受けた結果、数週間のあいだ手動処理で業務をするはめに。取引先は外貨両替をできず、一般客は自己負担を強いられた。顧客情報が盗まれたとの情報もある。

内部者がネットワーク上でマルウェアを展開することに成功、あるいはあるユーザーがフィッシング攻撃の被害を受けました。マルウェアはしばらくの間休止してから、検出したデータを流出させます。最後にすべて暗号化してから、復号のために身代金を要求します。ソーシャルエンジニアリング、スピアフィッシング、ディープフェイク等はますます高度になり、ユーザー教育だけでは、多忙な担当者が有害なリンクをクリックしないように、あるいは悪意あるドキュメントを開かないように徹底させることはできません。マルウェアは、企業の境界管理と内部セキュリティの回避を許し、技術的・人的脆弱性を悪用するように設計されています。アクセスさえ得れば、ファイルを流出させるのは簡単です。また、ハッカー側は数千あるいは数百万回の攻撃を実行できる立場にあり、その中の1つが成功するだけで良いのです。一方の組織側は、攻撃をすべて防御する必要があります。

ソリューション

不正な処理、すなわちマルウェアがネットワーク上で動作することは最も避けたい事態です。SecureDataなら、盗まれたファイルがすべて暗号化されたままであることが保証されています。攻撃者は、盗んだファイルが自分たちには無用の長物であることに気付くでしょう。さらに、SecureAgeのSecureAPlusは、承認された処理のみ実行を許可するアプリケーションコントロールとホワイトリスト機能を備えています。許可されたユーザーでもマルウェアの実行は不可能です。ユーザーが有害なリンクやファイルを誤ってクリックしても、関連するマルウェア（実行可能ファイル、ファイルレス攻撃、スクリプト、マクロなど）が承認された処理リストにないため、その実行が遮断されることが判るでしょう。このシナリオでは、SecureAge製品の使用によって、データ窃取、身代金の要求、そして組織の撹乱全てが失敗に終わるでしょう。

8. ユーザーアカウントの侵害

> ケベック州の教員約36万人の個人情報が漏洩。ハッカーは、ユーザーコードとパスワードを盗んでデータへのアクセスを可能にし、容易に情報を窃取。

外部の犯人が、盗んだユーザーの認証情報を使用して、自身のマシンからリモートでターゲットネットワークにアクセスします。この事例では、犯人が侵害したユーザーアカウントで利用可能な全ファイルにアクセスできます。ファイルは、企業ネットワークから外部の犯人のデスクトップに簡単にコピーされます。

ソリューション

SecureDataを使用すると、侵害されたユーザーアカウントにアクセスできた外部の犯人も、そのユーザーの暗号化キーにはアクセスできません。SecureDataでは、すべてのファイルが常に暗号化され保護されていますから、犯人はどのファイルも復号できません。SecureAgeセキュリティ管理サーバー（SMS）は監査データを収集するため、外部にコピーされた（暗号化済み）ファイルのログ情報を記録します。これは、データ盗難の試みが失敗した証拠として、以降のフォレンジック分析に使用できます。

9. 誤分類されたファイル

ユーザーが機密文書を誤分類した結果、データ保護レベルが低下したものです。ユーザーが情報を分類できるということは、彼らがプライバシーと情報セキュリティの重大性を読み違えて、誤った決定をする可能性があります。自動分類ツールにより、ファイルをスキャンし、内容に基づきファイル分類を行うこともできます。ただし、これらのシステムの効果は構成により決まります。すべてのデータストアがスキャンされなかったり、フィルターに一致するデータに漏れがあれば、やはり誤分類が問題になります。

> 欧州最大手のホテル予約プラットフォームGekko Groupは、セキュリティ保護のないデータベースが原因で、顧客、クライアント、パートナーに関する1TB超のデータを漏洩し、被害者を口座盗取詐欺、なりすまし詐欺、金融詐欺の危険にさらした。

現在の「普通」データが明日には機密情報になる可能性を認識し、重要には思えない情報も悪用され得ることを認識することが大切です。そのため、サイバーセキュリティを目的とした分類ルールの構成は特に難しくなります。

たとえば、Facebookの5千万アカウント流出の際、ほぼ無害と思われたデータが、セキュリティ質問の解読や偽アカウント作成、あるいはユーザーへの詐取に使用される可能性があるのです。多くの目的に役立つ分類も、セキュリティ手段の機能として依存するのには疑問があります。

ソリューション

SecureDataのファイルレベルの透過暗号であれば、全ファイルが保護され、しかもユーザーやアプリケーションに干渉しないよう設計されています。全ファイルが暗号化されるため、誤分類や未分類によりデータの一部が保護されないという懸念もなくなります。

情報漏洩のシナリオD
人為的なエラー

10. クラウドデータベースが保護されていない

クラウドサービスに保持されているデータベースが、ミスにより安全に構成されていませんでした。こうした保護されていないクラウドデータベースについてのメディア記事は多く見られます。データベースがライブシステムの一部であるか開発環境の一部であるかを問わずに、この種の人的エラーは発生するものです。いずれの場合も、機密情報がこの不確かな方法で保存されており、盗難に対して脆弱な場合が考えられます。

> Desjardins Groupの悪質な社員が、自分の正当なユーザー資格情報を悪用して、約290万件の顧客アカウントデータの記録を窃取。DLP(情報漏洩対策)があったと推定されるが、なぜか機密データエクスポートの検出には失敗。

ソリューション

SecureDataでは、データベースを構成する全ファイルが暗号化されます。これらのファイルは仮に盗まれても、ファイルは暗号化されたままで役に立たないため、データを失うことになりません。

TDEなどのデータベース暗号化ソリューションもデータベースファイルの盗難を軽減しますが、これらのシステムは関連付けられた非構造化ファイルやログファイル、一時ファイル、レポートファイルまでは暗号化しません。SecureDataなら、これらのファイルすべてを自動的に暗号化します。

11. クラウドストレージの間違った構成/誤用

ドキュメントの保存と管理に、クラウドサービスが使用されていますが、クラウドインフラストラクチャの構成が正しくないため、セキュリティに脆弱性が生じていました。この場合、ハッカーあるいは悪意ある内部者は、インフラストラクチャの構成ミスを悪用してファイルに簡単にアクセスし、データを盗むことができます。

さらに、クラウドサービスプロバイダー側にも独自のシステム管理者がおり、貴社のファイルへのアクセス権をもつ可能性が高いことも問題です。データ保護規制のGDPRやCCPAでは、個人を特定できる情報(PII)にアクセスできるのは、決められた特定者のみと指図しています。クラウド管理者が、貴社のデータを見る必要はないのです。

> AWSに保存されていたCapital One顧客レコード1億件を、Amazonエンジニアが盗む。誤構成されたファイアウォールを利用し、700以上のデータフォルダにリモートアクセスした手口による。継続的な犯行は4か月もの間未発覚。

ソリューション

SecureDataのユーザーごとのファイルレベルの暗号化なら、全データが暗号化されます。SecureDataに、OneDriveやG-Driveなどのデータ複製サービスを併用する場合は、ファイルは暗号化されてローカルシステムドライブに保存され、複製されたクラウドコピーも暗号化されます。SecureDataのファイル暗号化により、暗号化されていない唯一のデータは、アプリケーションの動作中にメモリに存在する必要があるデータだけになります。

つまり内部者、クラウド管理者または外部者が盗んだファイルは暗号化されたままで、役立たないことを意味します。さらに、クラウド管理者もそのファイル内容を表示できません。

12. BitLockerで保護された仮想デスクトップサーバーからのファイル盗難

仮想デスクトップサービスを提供するサーバーでは、ディスク上の全データが確実に暗号化されるようにBitLockerが有効化されていますが、ファイルが内部者によって持ち出されました。

BitLockerなどのフルディスク暗号化（FDE）機能は、実行中でないシステムでのみ有効です。BitLockerを備えた実行中のシステムでは、データの内容を問わず、要求されるすべてのプロセスに暗号化されていない形式でデータを受け渡ししています。

> MGMホテル客1,060万人の詳細がハッキングフォーラムに投稿。このデータは、明らかにFDE（フルディスク暗号化）が有効化されたクラウドサーバーへの不正アクセスにより収集された。

つまり、FDEは紛失したラップトップのデータ保護には最適ですし、コンプライアンス対策のため「データは暗号化されていますか？」と問われれば、簡単にチェックボックスにチェックマークを入れることができます。しかし、FDEは常時稼働しているサーバーでは役に立ちません。

ファイルは暗号化されずにシステム上を動いていますので、悪質な社員、ユーザーアカウントや特権ユーザーの侵害者は、見つけたデータを簡単に盗むことができます。

ソリューション

SecureDataの本質的なファイルレベルの暗号化は永続的な暗号化を維持し、データは許可された個人が暗号化キーを使用してアクセスした場合にのみ復号されます。さらに複合後も、ディスク上のデータは暗号化された状態を保ち、他の場所にコピーされた場合も同様です。暗号／復号プロセスは透過的であるため、ユーザー（およびアプリケーション）はこのアクティビティを意識することがありません。ファイルレベルの暗号化を、実用的なセキュリティソリューションとして実現する鍵がここにあります。

結論

報告された事例とともに、12のデータ盗難シナリオについて検証してきました。いずれのケースでも、一度データが盗まれて組織の制御構造外に出ると、流出したファイル内の情報は非保護になり、データの悪用が可能になります。

しかしファイルが盗まれても、SecureAgeのSecureDataが実装されている場合にはデータへのアクセスが完全に不可能です。盗難されたデータを組織外では利用不能にすることで、情報漏洩による損害が、規制、ブランドダメージ、訴訟、業務復旧などの面で軽減されます。このSecureAgeのアプローチにより、知的財産、機微情報や機密情報を確実に侵害から守る事ができるのです。すべてのファイルがいつでもどこでも暗号化され、何らかの方法でファイルが操作されても、常に保護が維持されたままであるからです。

SecureAge Technology

SecureAge Technologyはシンガポールに本社を置く、真のセキュリティと使いやすさを両立させるデータセキュリティ企業です。SecureDataは、改良されたPKIセキュリティ技術をベースに、2003年にシンガポール政府のためにまず着手されました。SecureAgeは自社特許であるPKIベースの暗号化を、固有の透過的なデータ保護コンポーネントとしてまとめ上げたもので、すぐさま後続の政府機関や公共機関に推奨されるデータ暗号化パートナーになりました。こうした長期的な深い統合関係から、SecureAgeには大規模かつ複雑な組織のデータを保護する広範な経験が備わっています。

SecureAgeのデータセキュリティソリューションは、公共機関や民間企業がそのネットワーク内のデータ移動を完全に制御できるようにします。すべてのファイルを、いつでも、どこでも。

SecureAgeのセキュリティ製品は、最高レベルのデータ保護を必要とする組織にお選びいただいています。顧客には、シンガポール、香港、および日本政府のさまざまな機関や、ブリティッシュ・アメリカン・タバコ、ソニー、成田エアポートテクノ、タイ政府貯蓄銀行、GRGバンキングなどが含まれます。

SecureAge Technology:
データセキュリティへのアプローチ

プロアクティブな保護

データセキュリティ

データセキュリティとは、遍在的な暗号を意味します。データは、最も基本的な自己完結単位であるファイルで保護する必要があります。競合する他のソリューションでは、一部のデータを一定期間だけ保護したり、セキュリティよりもコンプライアンスを重視したり、複雑化したりして逆にリスクをもたらします。また内部で働くユーザー（どのシステムでも最も脆弱な部分）に対しては、境界の防御を施すだけでは不十分です。

アプリケーション インテグリティ

アプリケーションの整合性とは、ホワイトリストそしてデータのアプリケーションへの結び付けによる制御を意味します。承認されたプロセスのみが、特定の目的で特定のデータにアクセスすべきと考えるからです。従来のマルウェア対策システムはパッシブ保護の代表的なものですが、それでは手遅れです。これらのシステムの焦点は、既知のマルウェアに置かれているため、常にアクティブで悪意のあるプロセスを阻止しようとするだけのものです。

ユーザビリティ

ユーザビリティとは、本質的で意識されない透過的テクノロジーを意味します。ソリューションにおいて人的要素は、構成の一部にしたり変えようしたりとするのではなく、完全に排除する必要があります。なぜなら、トレーニングやモニタリングは常に機能するわけではなく、ソリューションが自然でないと、人は独自の（セキュアでない）メソッドを編み出してしまうからです。ユーザーは、追加トレーニングや教育を必要とせず、思い通りに作業できる環境が必要です。

トレードオフなし

SecureAgeのこれらの原則の間には、トレードオフがありません。特にユーザビリティ面で、データセキュリティ強化のために妥協することはありません。「適切な」方法が難しいものであれば、人は何かを達成するために他の方法を見つけるもの、そう認識することがSecureAgeの製品設計の基本原則です。

詳細はこちら

SecureAgeのエンタープライズデータ セキュリティソリューションの詳細は、当社までお問い合わせください。SecureAgeの使用で貴社のデータセキュリティがどう改善されるかについて、また無料トライアルなどについてもお気軽にご連絡ください。

ウェブサイト www.secureage.com

SecureAge

シンガポール 3 Fusionopolis Way, 05-21 Symbiosis, Singapore 138633
英国 74 Mackie Avenue, Brigton, BNI 8RB, Company No. 11734665
日本 105-0001 東京都港区虎ノ門1-16-6 UCF7F
北米 1801 Old Reston Ave Suite 301 Reston, VA 20190, USA