Vision
Statement

WinMagic SecureDoc

ウィンマジックのビジョン – 日々複雑化するデータセキュリティの世界で常に新しい技術をお届けします

AUGUST 2019

WINMAGIC

WinMagic SecureDoc

ウィンマジックは、21年以上にわたり、データ暗号化の分野におけるイノベーターおよびソートリーダーとして高い評価を獲得してきました。これまでウィンマジックは「業界初となる」多くのソリューションを実現および提供し、世界中の企業のセキュリティと管理機能を向上させてきました。独自の強力かつ**インテリジェントな暗号化ソリューション**を提供し、極めて複雑な環境でも簡単に高度なセキュリティを実現することがウィンマジックのこれからの目標です。

ウィンマジックのビジョン – データ保護を最適化するシンプルな方法

現代のデジタル環境におけるデータセキュリティ製品の競争がますます厳しくなる中で、ウィンマジックはエンタープライズ向けのデータセキュリティ製品における重要な一端を担ってきたと自負しています。ウィンマジックのビジョンは、次の3つの重要な領域に焦点を当てています。

1. **暗号技術（暗号化）はデータおよびITセキュリティを推進するための基盤です。**
2. **データの効果的な保護の起点となるのはワークロードを保護することです。**すべてのエンドポイントが保護されていれば、クラウドにデータがある場合でも、攻撃者が重要なデータにアクセスすることは非常に困難となります。しかし、サーバに注力しているセキュリティ戦略が多く、エンドポイントに存在している脆弱性は軽視されています。ウィンマジックの独自のアプローチにより、セキュリティ市場に存在する重大なギャップを解消します。エンドポイントプロテクションに重点を置き、組織全体のデータセキュリティの拡張、向上、統合を推進します。
3. **暗号化と鍵管理はさまざまなプラットフォームに対応する必要があります。**すべてのユーザが使用するプラットフォームに依存しないソリューションを提供するデータセキュリティのリーダー企業が求められています。

データセキュリティ環境における課題とビジネスチャンス

クラウドのような新しいテクノロジによって、攻撃を受ける恐れのある領域が大幅に広がっており、データは新たな脅威にさらされています。これらの新しい脅威に対抗するために、業界ではAIやビッグデータなどの新しいテクノロジを採用しています。しかし、攻撃側もAIとビッグデータを利用できるため、防御側とのせめぎ合いが続いています。そのため、ますます多くのセキュリティベンダーやセキュリティ製品が市場に参入するようになりましたが、最も基盤となるレベルでデータを保護していない製品が多く、短期的な利益のために長期的な効果が軽視されています。

ウィンマジックは**暗号化**に注力しています。暗号化を適切に実装すると、攻撃対象となる領域を大幅に削減して、外部からの攻撃を防止し、データが安全であるという信頼性を高めることができます。攻撃対象となる領域が削減されることにより、保護を簡素化して向上させることができます。必要となる製品の数を削減でき、増大し続ける脅威に対しても確実にデータを保護できます。

a. **多くの暗号化製品は十分に成熟しておらず、補足的に提供されています。**2つの基本的で簡単な質問について考えてみましょう。機密データはいつどこで暗号化すればよいのでしょうか？また、どのような鍵を使用すればよいのでしょうか？たとえば、誰が鍵にアクセスして可読できる平文データにアクセスする必要があるのでしょうか？理想的には、機密データは、処理中の場合（平文のテキストデータを処理するアプリケーションで使用される場合）を除き、常に暗号化する必要があります。理想的には、許可されたユーザだけがデータの暗号化鍵を持っている必要があります。現在のほぼすべての製品は十分に洗練されていません。ネットワーク上にあるアプライアンスは、エンドポイントから送信されるデータを暗号化していない場合があります。さらに重要なのは、アプライアンス、管理者、さらにはサービスプロバイダーが使用できる鍵でデータが暗号化される場合があることです。現在一般的に利用できる製品は、CASBのような製品であっても、簡単に実装できますが、さらに優れたソリューションがあります。

b. **OSに暗号化機能が標準で組み込まれるようになりました。**ウィンマジックが操業を開始した時代とは異なり、多くのOSベンダーが自社のOS環境に暗号化機能を組み込むようになりました。WindowsのBitLocker、Linuxのdm-crypt、MacのFileVault2などの暗号化製品が有名ですが、AWSやVMWareにも暗号化機能が組み込まれています。ただし、プラットフォームベンダーは暗号化のプロフェッショナルではないため、最小限の鍵管理と機能しか提供していません。

さらに、暗号化ソリューションの中には、マネージドサービスプロバイダ（MSP）に暗号鍵の使用を許可しなければならないものがあり、この場合システムに重大な脆弱性が生じます。たとえば、「BYOK（Bring Your Own Key）」を促進する一方で、MSPはシステムを実行するために鍵を必要とし、最終的に鍵を所有することになります。ノートPCの所有者は、ベンダーがデータにアクセスすることを想定していませんが、クラウドはこのような望んでいない妥協案を受け入れざるを得ず、クラウドのすべてのデータにアクセス可能な鍵をMSPに手渡すしか方策はありませんでした。現在、ウィンマジックは別の方法を提供しています。ここで説明しているサービスプロバイダーに公開される暗号鍵の概念は、（a）で説明した鍵管理の問題とは異なります。（a）では鍵管理の問題を、ここでは暗号化の方法について説明しています。暗号化はMSPによって実行されるため、鍵が必要となり、どのような鍵管理ソリューションもこの状況を変更することはできません。

c. **ITセキュリティ市場は優れた暗号化ソリューションから利益を得ることができます。** 優れた暗号化ソリューションは、ベンダーと顧客の両方を含めたすべてのユーザの利益のために、セキュリティエコシステムとの互換性を確保します。具体的には、データが存在する場所を保護する統合型でプラットフォームに依存しないソリューションがセキュリティ業界で求められています。つまり、IoT、データセンター、クラウドにいたるまで、すべてのプラットフォームで完全な相互運用性を実現するユニバーサルなソリューションです。ウィンマジックは、これから求められる暗号化製品を提供できる理想的なポジションにあるのです。

d. **仮想化とクラウドの重要性。** 十分なセキュリティを確保できるのであれば、すべての企業は移行を推進するべきです。物理的なエンドポイントには脆弱性があり、ワークロードはオンプレミスではなくクラウドで実行されるようになっており、自社による管理が困難であるため、セキュリティの確保が格段に困難になっています。エンドポイントとクラウド間、オンプレミスからクラウド間、さらにはクラウド間で移動するデータにはすべて、完全な保護が必要です。

   ウィンマジックは、これまで培ってきたエンドポイント暗号化の基盤をクラウドに移行し、セキュリティ業界のデータセキュリティの在り方を大きく変えることに注力してきました。ウィンマジックは、新しいクラウドの時代のために従来の製品の焼き直しではなく、長年培ってきたオフラインでのナレッジと専門知識を基盤としたソリューションを構築しています。

e. **法令順守とポリシー。** GDPRやHIPAAなどの新しい法律が施行されたことにより、暗号化はほぼすべての企業や政府機関にとって、「あることが望ましいもの」から「なければならないもの」に変わりました。ウィンマジックは、リソースを投入し暗号化などの高度な技術を活用した優れたテクノロジソリューションによって、政策立案者を支援していきます。

ウィンマジックのビジョンの重要性

ウィンマジックのビジョンの中核は「Techno-logical（技術的かつ論理的）」と呼ばれる、先端技術に根差した明確で論理的な思考から成っています。

ウィンマジックは、短期的および長期的な利用が可能な「Everything Encryption（全方位の暗号化）」のためのインテリジェントなソリューションを提供でき、グローバルな暗号化市場で重要な役割を果たします。

暗号化製品は、暗号化コンポーネント(EC: Encryption Component)と鍵管理コンポーネント(KMC: Key Management Cpmponent)の2つの異なる部分から構成されます。 プラットフォームベンダーは、そのプラットフォーム環境向けの堅牢で透過的な暗号化ソリューションを作成できる最適な立場にありますが、鍵管理コンポーネントについては全く異なるアプローチが求められます。優れたKMCであればさまざまなプラットフォームで動作させることができ、組織のデータがどこにあっても安全に保護できます。

ウィンマジックにとって重要な理由

それぞれのオペレーティングシステムに付属する独自の暗号化機能が広く利用できるようになるにつれて、プラットフォームベンダーの暗号化ソリューションはベストオブブリードの鍵管理ソリューションによって管理されるようになっています。ウィンマジックは、プラットフォームベンダーと競合するECを開発するのではなく、BitLocker、FileVault2、dm-crypt、SEDなどのソフトウェア製品と連携するソリューションを今後も開発していきます。ウィンマジックのKMCは他の製品と同じような簡易方法でBitLockerを管理するだけではなく、プリブート認証（PBA）を今後も実装します。このPBAを継続することは、強力なKMCを実行するために必要となります。

OSに組み込まれている暗号化よりも優れた機能を提供：自己暗号化ドライブ（SED: Self-Encrypting Drive）。 最高のテクノロジーイノベーションは、スマートで、シンプルで効率的であるべきです。これこそがウィンマジックのSEDの特長です。OSの暗号化機能では競合する多数のカーネルドライバとの互換性が必要となり、CPUも消耗します。ドライブベースの暗号化はシンプルで安全です。多くの点でSEDがディスク暗号化の基盤となるソリューションになるとウィンマジックは考えています。最新の仮想化テクノロジとセキュアワークロードにより、ストレージの暗号化は変わりつつあり、一部の分野ではSEDは最適なソリューションではなくなっていますが、依然としてITシステムで保存されるデータについては、SEDを基盤として活用する必要があります。

ウィンマジックにとって重要な理由

OSに暗号化機能が組み込まれているのにもかかわらず、企業はFDEに多額の投資を続けています。SEDは、解決が必要な多くの初期的な問題（BIOSなどの互換性）を抱えていますが、この状況は、この分野の先駆者となる機会をウィンマジックにもたらします。ウィンマジックの市場での評価と実績、これまで築き上げてきたSEDベンダーやPCベンダーとの素晴らしいパートナーシップも、ウィンマジックの今後の戦略にとって有用となります。

セキュアワークロード - 市場を大きく変えるテクノロジ。 企業は、データの機密性、データの露出、クラウドサービスプロバイダによるアクセス、インフラストラクチャの脆弱性、政府によるアクセスの可能性などの懸念が存在するために、機密データをクラウドに移行することを躊躇しています。同じように、クラウドサービスプロバイダも、顧客のデータにアクセスしてしまい、露出させてしまうという懸念を抱えています。

これらの懸念を解決するための方法の1つは、Secure Encrypted Virtualization（SEV）のようなメモリ暗号化テクノロジで使用中のデータを保護することです。SEVでは、暗号化されていないデータ、平文テキスト、メモリへのアクセスは、顧客（つまりゲスト）の仮想マシンのみに限られ、CSPのハイパーバイザー、管理ソフトウェア、または管理者はアクセスできません。

ウィンマジックにとって重要な理由
保管中のデータを保護せず、使用中のデータの機密性だけを保護することは、完全な解決策にはなりません。一般に、ワークロードはディスクから開始されます。次に、メモリ内のデータ（使用中のデータ）が処理され、ディスクに書き込まれます（保存中のデータ）。ゲスト内のFDE暗号化では、CPUとメモリを使用して保存中のデータを保護し、SEVが提供する保護機能も活用できます。

これは、ウィンマジックのアプローチが重要な意味を持つ領域です。顧客（ゲスト所有者）は、ディスクに保存されている機密データをロック解除してワークロードをロードする前に、ゲスト仮想ワークロードがSEVで保護されていることを確認できます。ウィンマジックのFDEおよびエンタープライズクラスの鍵管理機能とSEVを併用するセキュアワークロードテクノロジは、クラウドサービスプロバイダやSaaSプロバイダのデータセキュリティ戦略を大きく変えることになるでしょう。

ブロックチェーンベースのDPKIを活用した安全なデータ共有 – 社内および社外のパートナーと安全かつ簡単にデータを共有することは難しく、高い管理コストが伴います。既存のソリューションは、課題の多いパスワードに依存しており、ユーザが自分でアカウントを作成するか、電子メールやDropboxなどの特定の方法を転送媒体として使用する必要があります。

ウィンマジックにとって重要な理由
この問題は、既存のウィンマジックのファイル暗号化と対称鍵管理のノウハウを新しいブロックチェーンベースの分散型公開鍵インフラストラクチャ（DPKI）テクノロジと組み合わせることで解決できます。ユーザ（管理者）が共有グループを作成および管理できるようにすることが、ウィンマジックのビジョンです。これらのグループは、社内共有のための対称鍵の暗号化鍵と外部共有のための公開鍵の暗号化を組み合わせます。ブロックチェーンベースのDPKIは、従来の集中型PKIシステムに存在していた多くの欠陥を解決する公開鍵のリポジトリです。暗号化されたファイルは任意の方法（USB、電子メール、Boxなど）で共有でき、受信者はデータにアクセスするためにパスワードを必要としません。また、ファイルが本来の送信先ではないユーザに渡ったとしても、鍵がないためこれらのユーザはファイルの内容を読み取ることができません。

統合型のインテリジェントな鍵管理 - 現在のデータセキュリティの諸問題への解決策。 ウィンマジックは、通常は安全な鍵の保管場所として機能する従来型の鍵管理とは異なる、コンテキストアウェア（コンテキストを意識した）な鍵管理アプリケーションを提唱しています。ウィンマジックのインテリジェントな鍵管理ソリューションは、鍵を要求したユーザにアクセス権限を付与する必要があるかどうかを判断するために、ユーザ、デバイス、認証方法などの多くの要素を考慮します。また、エンドポイントでの安全な鍵の保管（デバイスが盗まれて攻撃される恐れがありますが、安全性は確保されます）と安全な鍵の配信（OSの起動前でも）を可能にします。アプリケーションベンダーは、ウィンマジックの鍵管理の専門知識から恩恵を受けることができ、最終的に安全で優れた製品を顧客に提供できます。

ウィンマジックにとって重要な理由
WinMagic SecureDocは、Windows、Linux、Mac をサポートし、エンドポイント、IoT、データセンターやクラウドにあるサーバーのディスク暗号、ファイル暗号、コンテナ暗号とその鍵を一元的に管理する唯一の製品です。鍵の管理は複雑であるため、共通で使用できるツールキットがあれば、他のベンダーもウィンマジックの鍵管理の恩恵を受けることができます。暗号化は本質的に難しいものですが、ツールキットがあれば暗号化を「容易に」することができます。同じことが鍵管理にも当てはまります。

WinMagic SecureDoc

今後について

21年以上にわたり、暗号化の優れた機能を提供し、使いやすいソリューションを生み出してきたことにウィンマジックは誇りを持っています。ウィンマジックはユーザの利便性とコンピュータサイエンスに関するナレッジを組み合わせるという製品設計哲学をもとに製品を市場に提供し、さまざまな組織のデータセキュリティを向上させ、合理化してきました。ウィンマジックの製品ポートフォリオは、競合ベンダーにはない包括的なデータセキュリティソリューションを企業に提供します。お客様のためにこの分野の研究に注力し、努力を重ねることで、ウィンマジックはこのミッションステートメントに忠実に業務を遂行していきます。高い基準と倫理を元にグローバルにデータを保護します。

このミッションステートメントから、ウィンマジックがUnified Intelligent Encryption Solutionsの世界的リーダーになると確信している理由をご理解いただければ幸いです。ウィンマジックの今後の戦略に皆様のご理解とご協力を今後ともどうぞよろしくお願いいたします。

Thi Nguyen-Huu
ウインマジック、創設者/CEO