



Matrix42 とのパートナー シップによる最適なエン ドポイントセキュリティ の説明および探究

MATRIX42

#KingstonIsWithYou

Matrix42 とのパートナーシップによる最適な エンドポイントセキュリティの説明および探究



はじめに

データ保護は、今日の世界の企業、政府、そして個人にとって根本的な要件です。

データの侵害、ハッキング、そして人的要素は、世界中の脅威とリスクを常に彷彿とさせます。データの侵害に伴う金銭的損害や企業イメージへのダメージは天文学的な数字となる場合もあります。データ保護のための高度なサイバーセキュリティと、エンドポイントの DLP（データ損失防止）戦略の要件はすべて、信頼性が高く、効率的なストレージとメモリに依存します。

成功事例、標準、およびポリシーと組み合わせた暗号化、高速ストレージ、およびメモリの使用は、大きなステップになります。紛失したノートパソコンや USB ドライブは、個人や企業が個人情報や私的な情報を暴露して、脆弱な状態にします。Kingstonは、既存または開発中のセキュリティ計画を補完しながら、リスク軽減に役立つ脅威防止のソリューションを提供します。



Matrix42 とのパートナーシップによる最適な エンドポイントセキュリティの説明および探究

内容

この短い eBook では、エンドポイントソリューションについて触れ、Kingston の暗号化 USB ドライブ、そのカスタマイズプログラムおよび Matrix42 EgoSecure Data Protection ソフトウェアが、どのような場面で6つの異なる業界セクターの課題解決に役立ち、ビジネスニーズに合ったソリューションを提供するかについて述べます。

これらの6つのセクターについて詳しく説明し、エンドポイントセキュリティの課題にどのように対処したかを見ていきます。

目次

セクション 1	業界事例 - 公共セクター	4
セクション 2	業界事例 - 医療	5
セクション 3	業界事例 - 金融	6
セクション 4	業界事例 - 自動車	7
セクション 5	業界事例 - 電気通信	8
セクション 6	業界事例 - 製造	9
セクション 7	Kingston および Matrix42 のソリューション	10
	まとめ	11
	Kingston について	12



セクション1：業界事例

公共セクター



状況：

公共セクターでは、USB デバイスの使用が非常に一般的です。たとえば、治安局では駐車違反者や管理規程違反者によって撮影された写真は、デジタルカメラから USB ケーブルを介して当局のシステムへコピーしなければなりません。警察当局は、外部データストレージデバイスに入った捜査データを受領します。このデータは書き換えの必要があり、不正なアクセスを防止しなければなりません。

課題：

USB デバイスの需要が高いため、従業員は定期的に USB を要求します。個人用および未認可のデータストレージデバイスは、セキュリティ上の理由で排除しなければなりません。ある従業員が新しい USB ストレージデバイスを必要としている場合、その従業員の仕事の支障にならないように、ユーザーヘルプデスクを通じて迅速に利用可能にしなければなりません。適切な USB デバイスを使用して、セキュリティ問題を発生させないことも重要です。

ソリューション：

デバイス管理、データフィルタリングおよび暗号化を組み合わせ、次のシナリオを可能にできます。

未知のデバイスは通常、コンピュータのエンドポイントでブロックされます。デジタルカメラなどのデータストレージデバイスは、画像ファイルの読み込みなど特定の機能のみ許可されます。書き込み操作は通常暗号化され、認可された USB デバイスでのみ許可されます。すべてのデータアクセスは記録されます。認可済みデバイスの管理は、シリアル番号およびハードウェア ID のカスタマイズによって簡素化できます。このようにして Matrix42 Service Management では、ユーザーがセルフサービスポータルでパーソナライズされた Kingston Technology USB Drive を要求することができます。承認プロセス後、USB デバイスは自動的に EgoSecure Data Protection で使用可能になります。

“ 当社の従業員は、短い承認プロセスの後に新しい USB デバイスが簡単にすばやく提供されることにたいへん喜んでいました。Kingston Technology のカスタマイズプログラムと、Matrix42 の簡単な管理機能を組み合わせたサービス管理およびエンドポイントセキュリティに非常に満足しています。 ”

公共セクター、ヘルプデスク責任者

セクション 2：業界事例 医療



状況：

外部ストレージデバイスは、従業員と他の医療機関とのデータ交換の手段として、頻繁に使用されています。

たとえば、ドイツの病院では、現在のがん症例とその進行についての情報を、がんレジストリに提供しなければなりません。手続きを簡単にするため、このデータはモバイルデータストレージデバイスを介して移行されます。

医師はまた、それぞれが講義をする際に研究データなどの文書を USB ドライブに入れて持ち運ぶことを好みます。

課題：

患者データは非常に機密性が高く、権限のない人の手に渡ることがあってはなりません。したがって、データ保護を増強する必要があります。データ記憶媒体の紛失は、GDPR 違反という点だけでなく、患者の福祉という点でも大きな問題となる場合があります。このため、USB データストレージへのアクセスを管理、モニターおよび暗号化することが重要です。

ソリューション：

EgoSecure Data Protection では、管理、データ監査、フィルタリング、暗号化などの各種の保護手段をひとつのソリューションに組み合わせています。IT 管理者は、どの従業員にどのデバイスへのアクセスを許可するかを決定することができます。例外は、たとえばシリアル番号やハードウェア ID などによって設定することができます。これらの ID は、Kingston Technology のカスタマイズプログラムによって設定できますので、EgoSecure Data Protection 管理機能にひとつの値を構成するだけで、会社の承認したデバイスのみを使用可能にできます。これにより、管理作業が大幅に最小化されます。また、アクセスが暗号化およびモニタリングされるため、データセキュリティ（GDPR、CCPA、HIPAA など）が向上します。

“ 当社ではすでに Kingston の USB ドライブを使用することがあります。今度は、EgoSecure Data Protection によって、患者データのデータ移送でも、EU-GDPR に沿ったトレーサビリティを実現できるようになりました。 ”

大学病院CISO



セクション 3：業界事例

金融



状況：

銀行は、各種のコンプライアンス要件の対象とされています。これらの要件のひとつに、PCI-DSS（Payment Card Industry Data Security Standard）への準拠があります。PCI-DSS 要件には、データ暗号化、脆弱性分析およびデータフィルタリングの必要性が含まれます。最終目標は、脅威および IT セキュリティリスクの最小化または完全防止です。

課題：

エンドポイントには、IT セキュリティの面で多くのリスクが存在します。従業員は毎日、消費者や企業からのペイメントカード情報を取り扱い、金融機関からの機密データを処理する必要があります。そのため、クラウド、電子メール、USB およびウェブからのデータを適切に保護しない場合、それらのデータがマルウェアによって侵害される脅威や、データが誤って第三者の手に渡る脅威にさらされています。このような事故は銀行にとって、GDPR や PCI-DSS だけでなくサーベンス・オクスリー法の面からも、金銭的影響を伴うリスクとなる場合があります。さらにサイバー犯罪者はさまざまな方法で、銀行システムに影響や改ざんを加えようとし、その

手口はますます巧妙化しています。最近では、たとえば ATM 関連で、金を盗むために電源を停止させ、ブータブル USB デバイスによってシステムを始動するというサイバー犯罪がありました。

ソリューション：

IT システムは、複数のレイヤーに分かれた保護手段で守る必要があります。これは、アプリケーション制御、デバイス制御、異常検知、UEBA（ユーザーおよびエンティティ行動分析）、モニタリング、プリブート認証によるフルディスク暗号化によって達成できます。Matrix42 では、これを自動化された統合エコシステムに実装できますので、許可されたアプリケーションおよび暗号化された USB デバイスのみが可能になります。その上で、不審なアクティビティや悪意あるアクティビティが検出され、さらに対策が自動的に開始されます。USB ドライブの使用については、カスタマイズされた Kingston Technology 製 USB ドライブを組み合わせることで、最小の労力で確実にデバイスがホワイトリストに入れられ、追跡可能な方法でデータが暗号化されます。これにより、追加作業なしにコンプライアンスが大幅に向上します。



“EgoSecure Data Protection およびホワイトリスト機能によって、当社では Kingston 暗号化 USB ドライブにのみ承認を許可しています。当社では、パーソナライズされたハードウェア ID の付いた Kingston 暗号化 USB ドライブをホワイトリストに入れました。他のドライブは許可されません。これによって、管理作業が大幅に削減され、セキュリティが向上しました。”

金融機関 IT 管理者

セクション 4：業界事例 自動車

状況：

自動車業界では、さまざまな分野で USB デバイスが使用されています。たとえば、研究データが外部ストレージデバイスに保存され、社内の各エンジニアの間で交換されます。生産機械を構成するため、ファイルが IT 環境から OT 環境へ運ばれます。これらのデータはすべて機密性が高く、産業スパイやデータ窃盗から保護する必要があります。保護しない場合、蓄積したノウハウが犯罪者の手に渡ります。

課題：

自動車業界は、TISAX、プロトタイプ保護、ENX、ISO27001、「第三者接続」、GDPRなどのコンプライアンス要件の対象です。TISAX では、Control 9.1、9.5 および 10.1 条で、データアクセスを管理、モニター、フィルターおよび暗号化しなければならないと規定しています。これらの措置は、すべての分野の自動車会社において、GDPR や ISO27001 などの他のコンプライアンス要件にも適合していなければなりません。

ソリューション：

Kingston Technology 暗号化 USB ドライブは、ハードウェアベースの暗号化でデータを保護します。これらのデバイスには、パーソナライズされたシリアル番号およびハードウェア ID を付けることができ、それらは EgoSecure Data Protection の中で、特定の用途用のホワイトリストに自動的に入れるために使用できます。さらに、不審なアクティビティがあった場合、データ移動のモニターおよび分析ができます。

“ Matrix42 および Kingston Technology によって、ユーザーの行動を大きく変えずに、Control 9.5（情報およびアプリケーションへのアクセス）や Control 10.1（暗号化）などの TISAX 要件を実装できました。 ”

自動車サプライヤ CTO



セクション 5：業界事例 電気通信



状況：

電気通信プロバイダには、顧客に関する多くの情報があります。この情報は、特に GDPR 関連の機密性が高いです。したがって、データ損失やデータ窃盗を防止するために、十分な対策を取る必要があります。

課題：

電気通信会社の従業員は、顧客データを毎日取り扱っています。データの多くは、業務アプリケーションに保存されています。しかし、それらに接続するエンドポイントおよび外部デバイスに、顧客の契約どころかデータベースのエクスポートまで保存されるリスクがあります。ユーザーはデータ交換に外部ストレージをよく使用します。したがって、誤ったデータストレージ手順を検知し、修正または防止することが非常に重要です。

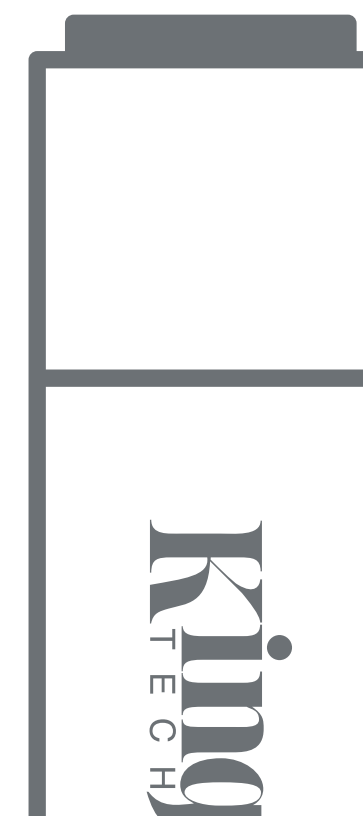
ソリューション：

調達プロセスを簡素化するため、パーソナライズされた製品 ID 付きの Kingston Technology 暗号化 USB ドライブは、EgoSecure Data Protection 中に

事前定義されたホワイトリストを通じて迅速に購入でき、Matrix42 Service Catalog を通じて納入できます。機密情報を含んでいる可能性のあるデータストレージおよびエクスポートを、「使用中データ」および「保存データ」のスキャンに基づいたディープコンテンツインスペクションにより自動的に識別し修正できます。データの移動は集中ロギングされます。したがって従業員は、データストレージ用の新しいハードウェアを要求し承認されるとすぐに、受け取ることができます。このため、確実に GDPR に準拠したものが使われます。

“ Matrix42 のセルフサービスポータルによって、ユーザーは必要なストレージメディアを要求できます。注文の承認および納品が完了すると、デバイスは EgoSecure のデバイス管理によって認可されます。Matrix42 と Kingston Technology の組み合わせによって、当社の生産性とセキュリティが向上します。 ”

電気通信プロバイダ CTO



セクション 6：業界事例

製造業界



状況：

デジタルデータには、将来大きな利益を生む可能性があります。製造業界の場合、この貴重なデータには、生産計画、顧客およびサプライヤの情報、企業ノウハウなどが含まれます。このデータを損失した場合、GDPR の観点から非常に厳しいペナルティが課されるだけでなく、多額の損害や企業イメージの低下などの問題となる可能性があります。残念なことに、USB の落とし物は毎日タクシー、ランドリー、空港、駅、駐車場などで見つかります。

課題：

ストレージデバイスには、機密性の高いデータが入れられることが多いですが、残念なことに、このデータが暗号化されていないことがよくあります。また、保守技術員が生産機械にアップデートをインストールする際に、外部のデータ記憶媒体を使用するリスクもあります。これらの外部デバイスには、ネットワークにマルウェアを入り込ませるリスクがあります。

ソリューション：

Kingston Technology 暗号化 USB ドライブは、ハードウェアベースの暗号化でデータを保護します。これらのデバイスには、パーソナライズされたシリアル番号およびハードウェア ID を付けて納入でき、それらは EgoSecure Data Protection の中で特定の用途用のホワイトリストに自動的に入れるために使用できます。さらに、不審なアクティビティがあった場合、データ移動のモニターおよび分析ができます。

“生産データの暗号化は、当社がデータ窃盗に対して自衛する上で、非常に重要です。このような機密性の高いデータは、EgoSecure Data Protection によるファイルフィルタリングを介して、承認済みの Kingston 暗号化 USB ドライブにのみ入れることが許可されます。他の USB デバイスではすべて、データがブロックされます。外部データストレージへの書き込みアクセスは、EgoSecure のオンザフライ暗号化およびロギングによって保護されます。”

製造業界、ITセキュリティ担当者





セクション 7：Kingston Technology および Matrix42 のソリューション



成功事例、標準、およびポリシーと組み合わせた暗号化、高速ストレージ、およびメモリの使用は、大きなステップになります。紛失したノートパソコンや USB ドライブは、個人や企業が個人情報や私的な情報を暴露して、脆弱な状態にします。Kingston Technology は、既存または開発中のセキュリティ計画を補完しながら、リスク軽減に役立つ脅威防止のソリューションを提供します。

Kingston Technology 暗号化 USB ドライブ

Kingston Technology のハードウェアベースの暗号化 USB ドライブは、組織のファイアウォール内外のモバイルデータ用のデータ保護ソリューションを備えています。機密性の高いセキュリティが必要なデータを保護するよう設計されたこれらのドライブは、特定の業界標準、指令、規制を満たすのに役立ちます。製品は TAA 準拠、FIPS 認証取得済みで、最大 128GB の容量をご用意していますので、企業ユーザーおよび政府機関の両方に最適です。



安全なカスタマイズ プログラム

Kingston Technology の暗号化 USB ドライブは、企業ニーズに合わせてさまざまな方法でカスタマイズできます。さらに機能を追加すれば、独自のドライブになります。Kingston Technology では、ご希望の再販業者か販売業者を経由して、カスタマイズ暗号化 USB ドライブを簡単に、そして便利な方法で発注できます。Kingston Technology の暗号化 USB 製品には、DTVP30、DT4000G2、および IKD300S シリーズがあります。このプログラムでは、シリアル番号の付与、デュアルパスワード、カスタムロゴなど、お客様からのリクエストが特に多いオプションを提供しています。プログラムの最大発注数は 50 個、再発注数は 25 個で、お客様の会社がまさに必要とするものをお届けします。

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection では、デバイス、システムおよびデータの保護のため、企業に 360° のセキュリティ管理を提供します。ソリューションは、予防および検知から損害時の対策まで、生産性を低下させずに全プロセスを自動化します。

データ保護およびサイバーセキュリティは、非常に困難な責任のように思えるかもしれません。従業員がいつでもどのデバイスを使って働くかを自分で決められるようになったことで、デジタルワークの要件は大幅に変化しました。ハードウェアベースの暗号化 USB ドライブとエンドポイントソフトウェア管理を適切に組み合わせることにより、企業は社内のデバイスをコントロールできるようになります。それにより、データ侵害のリスクを軽減し、実施中の GDPR コンプライアンス戦略をサポートします。





Kingston について

Kingston Technology には 30 年以上の経験があり、お客様の企業に不正な侵入を許さず、エンドポイントセキュリティの課題を識別し解決する知識があります。

©2021 Kingston Technology Far East Corp. (Asia Headquarters), No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan.
すべての商標および登録商標は、各所有者に帰属します。

#KingstonIsWithYou