EntrustがZertoのビジネスアプリケーションの統合を支援

2010年に設立されたZertoは、ディザスタリカバリテクノロジーは保険証券ではなく、競争上の強みであるべきだという独自のビジョンを持っています。

ZertoはITレジリエンスを通じて、モダナイゼーションとクラウド採用のリスクと複雑性を排除することによって、顧客のIT変革を加速させています。複数のレガシーソリューションを単一のIT Resilience Platform™に入れ替えることによって、Zertoはディザスタリカバリ、バックアップ、クラウドモビリティを収斂したシンプルなソリューションに統合します。エンタープライズに対応するスケールを持つZertoのソフトウェアプラットフォームは、常に「オン」の顧客エクスペリエンスを継続的に提供しながら、ワークロードのモビリティを合理化し、ハイブリッドクラウドやマルチクラウド環境でアプリケーションを保護、復元、自由に移動します。

ZertoはIT市場に旋風を巻き起こし、ディザスタリカバリの可能性を拡大しました。企業にとって中断されないテクノロジーが不可欠である世界で、Zertoは継続的なデータ保護テクノロジーにおいて革新的な製品を開発し、ディザスタリカバリの単なるツールを超える存在となりました。

> **«他のサプライヤーと比較すると、Entrustの実装およびサポートははるかに優れています。Entrust nShield HSMsは簡単に使用やバックアップができるほか、グラフィカルユーザーインターフェイス（GUI）も気に入っています。»**
>
> – ZertoコーポレートITインフラストラクチャ責任者Nadav Svirsky氏

詳細をチェック：ENTRUST.COM/ja/HSM

Zerto

ビジネスにおけるチャレンジ

ITレジリエンスの主要プロバイダーであるZertoは、自社の業務システムが改竄されるリスクに晒されていないことを確認する必要がありました。そのために最も有効な戦略は、公開鍵基盤（PKI）の信頼性を確認することでした。

PKIとは、デジタル証明書および公開鍵の作成、管理、配信、使用、保管、無効化に必要なハードウェア、ソフトウェア、ポリシー、プロセス、手順のセットです。PKIは、人、デバイス、サービスのアイデンティティを確立し、システムやリソースへの管理されたアクセス、データの保護、トランザクションにおける責任の特定を可能にします。進化するビジネスモデルが、オンライン認証やより厳格なデータセキュリティ規制への準拠を必要とする電子的なやり取りにますます依存するようになるにつれて、次世代のビジネスアプリケーションは、高い保証を確保するためにPKIテクノロジーにさらに依存するようになっています。

公開鍵を関連するユーザー（秘密鍵の所有者）と結び付けるため、PKIはデジタル証明書を使用しています。デジタル証明書とは、トランザクションにおいて、ユーザー間のアイデンティティ確認を容易にする認証です。国民としての個人のアイデンティティを証明するパスポートと同様、デジタル証明書はエコシステム内でユーザーのアイデンティティを確立します。デジタル証明書は、暗号化されたデータの送信先のユーザーを特定する、または情報の署名者のアイデンティティを確認するために使用されるため、システムの信用を維持するためには証明書の信憑性および完全性の保護が欠かせません。これは、信頼されるベンダーとしてのZertoのビジネスモデルにとって不可欠でした。

技術的チャレンジ

認証局（CA）は、ユーザーのアイデンティティを証明するために使用されるデジタル証明書を発行します。CAは、PKIおよびPKIがサポートするサービスを支えているため、ターゲットを絞った高度な攻撃の対象となる可能性があります。CAに対する攻撃のリスクを軽減するために、物理的かつ論理的な制御と、ハードウェアセキュリティモジュール（HSM）などの強化されたメカニズムを使用して、PKIの整合性を確保することが必要になっています。

ZertoはMicrosoftプラットフォームを使用しているため、同社のIT部門はMicrosoftとの協力から、CAをセキュアにするベストプラクティスはHSMを使用することであると知っていました。独立して証明された、改竄に強い環境のHSMは、重要な鍵や業務プロセスの保護に不可欠な部分です。

Zerto

> **Entrust nShield Solo HSMsの実装は当社のCAセキュリティに安心をもたらします。当社経営陣は、リスク削減は十分に投資に値すると感じています。**
>
> – ZertoコーポレートITインフラストラクチャ責任者Nadav Svirsky氏

ソリューション

複数のHSMベンダーの利用経験があるZertoのITチームは、Entrust nShield® Solo HSMの実装を選択しました。ZertoのコーポレートITインフラストラクチャ責任者Nadav Svirsky氏によると、他のベンダーよりもEntrustを選択した理由は、「他のサプライヤーと比較すると、Entrustの実装およびサポートの方が優れており、Entrust nShield Solo HSMsの方が簡単に使用やバックアップができるためです。また、グラフィカル・ユーザー・インターフェイス（GUI）も採用した理由です。」

結果

Zertoは、CAを保護するためにインストールしたEntrust nShield HSMsの測定可能な結果を公表していません。現在プロジェクトの当初目標であったベストプラクティスのCAセキュリティを実現していることについて、Svirsky氏は以下のように述べています。「当社の顧客は当社のシステムが安全で信頼できることに自信を持つ必要があります。残念ながら、何か悪いことが起こり、企業の評判が悪化し、売上高が減少し、株価が下落するまで、データセキュリティの価値はわからないことが多いものです。そのため、Entrust nShield Solo HSMsを実装して当社のCAのセキュリティを維持することは安心をもたらします。当社経営陣は、リスク削減は十分に投資に値すると感じています。」

Zerto

パフォーマンス、信頼性、保護

ビジネスニーズ

- 内部データのセキュリティ問題のリスク低減

技術的ニーズ

- 妥当なコストで、CAサーバの信頼の基点の保護

ソリューション

- Entrust nShield Solo HSM

結果

- リスク削減
- Zerto経営陣の安心感

ENTRUSTについて

Entrust は信頼される認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験がこれまで以上に求められています。Entrust はこうしたインタラクションの要となり、他にはない多様なデジタルセキュリティと認証発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーのネットワーク、150か国以上に顧客を擁するEntrustは、世界で最も信頼されている組織から信頼されています。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

ENTRUST

お問い合わせ：
HSMinfo@entrust.com