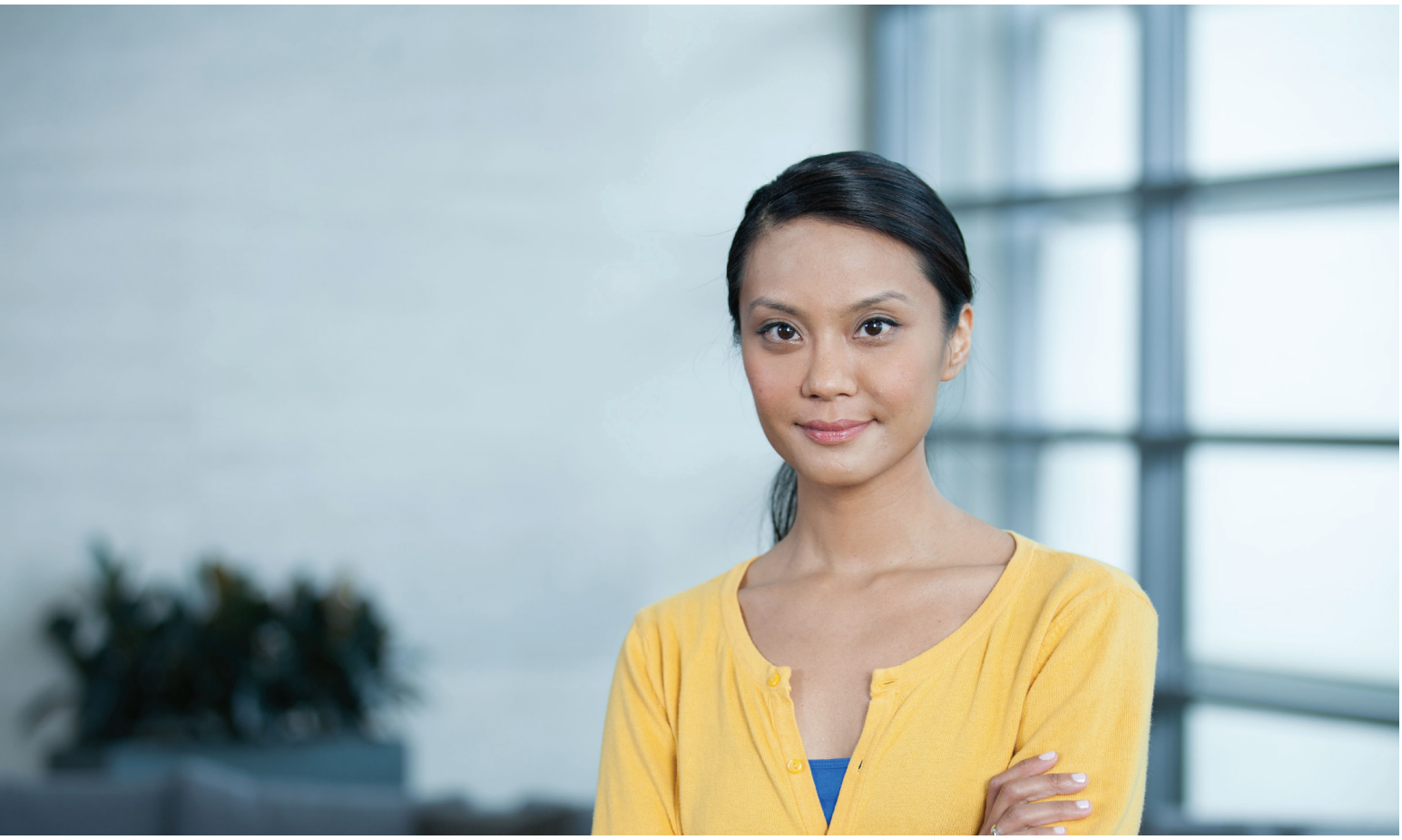
COMMVAULT

モバイル エンドポイントを保護するために絶対に必要な 5 つの機能

企業はユーザーのモバイル エンドポイント デバイスを保護する必要があることを認識しています。
しかしそれはどのようにして行えばいいでしょうか。会社からの厳しい通達は効果がありません。
ユーザーは既に個人用デバイスを会社に持ち込んでいるか、
会社のデバイスに個人データを保存しています。問題を無視することもできません。
保護も暗号化もされていないノート PC に起因するデータ漏洩は広範囲に波及しています。
モバイル デバイスをセキュアなデータセンターの狭い領域内だけに制限しても効果はありません。
第一に、モバイル ユーザーは常に移動しており、
第二に、窃盗犯はノート PC をオフィスから盗み出すことができるためです。



モバイル デバイス、特にノート PC は、不満を抱いている従業員、悪意のある窃盗犯、日和見主義者からの脅威に常にさらされているのが現実です。だれかが自分のノート PC を紛失したときであっても、それを見つけた人に悪意がないとは限りません。もちろんデータ保護には、失われたデータを取り戻すという重要な役割がありますが、最初にやるべきことは、デバイスが紛失しないように保護し、悪意のある窃盗犯がノート PC を持ち出したとしても、そこからデータを盗み出せないようにすることです。

自信を持ってモバイル デバイスを保護し、悪意のある窃盗犯やハッカー (そして忘れっぽい従業員) から守るために必要となる、5 つの重要なセキュリティ機能があります。必要になるのは、1) データ漏洩に対処するためにファイルやフォルダーを暗号化し、2) ユーザーのアクセスを制御し、3) 必要に応じてドライブをリモート消去し、4) 紛失したか盗まれたノート PC の位置を突き止め、5) ポリシーに従ってこれらの操作を自動化することのできるモバイル セキュリティ スイートです。

1: データを暗号化する。

2014 年、医療業界では記録的な数の規制されたデータの漏洩がレポートされました。多くの人は、データ漏洩とは悪意のあるデジタル攻撃の結果として生じるものだと考えていますが、実のところ、その 80% 近くは暗号化されていない盗まれたコンピューターや USB ドライブから生じています。[1] 暗号化はファイアウォールの外側のデータを保護するために重要なものです。暗号化により、窃盗犯がデータにアクセスできたとしても、それを読み取って利用できないようにすることができます。FIPS 140-2 などの基準を採用したインテリジェントなセキュリティ ツールは、SOX や HIPAA などの業界や政府の規制に対応します。また、ファイルやフォルダーなどの詳細なレベルで機能する暗号化ソリューションを探す必要があります。

2: ユーザー アクセスを制御する。

理論的には、ユーザーのパスワードは重要なセキュリティ対策です。しかし実際には、ユーザーは脆弱なパスワードを選択し、それをめったに変更せず、できるだけ多くのアプリケーションやサービスで使用できる単純なマスター パスワードを好みます。これらの要因が組み合わさって、非常に多くの人々がパスワードをクラックできるようになっています。強力なパスワードを設定することをユーザーに奨励する一方で、セキュアなシングル サインオン (SSO) や 2 要素認証 (2FA) でセキュリティを強化するように注意を促してください。SSO はマスター パスワードの確認にサード パーティ サービスを使用し、2FA は単純なユーザー ID とパスワードによる認証ではなく 2 層から成るユーザー認証を必要とします。

3: 必要に応じてドライブを消去する。

ノート PC が見つからず、データ漏洩のリスクが高い場合は、ドライブをリモート消去します。従業員が写真データの回復を望む場合もあるので、デフォルトのドライブ全体の消去よりも、保護データを選択的に消去することが推奨されます。ただし、機密性の高い業務データは消去することをお勧めします。必ずしも IT 部門が消去を行う必要はありません。可能であればユーザー自身が必要に応じて消去を行う必要があります。消去とは、単純に削除するだけではありません。ブロックを完全に消去するツールを選択し、窃盗犯がディスクをリカバリできないようにします。

悪者を完全に阻止する : モバイル データを保護する[1]

モバイル デバイスは、その性質上、紛失や盗難のリスクにさらされています。そのリスクを管理することはモバイル セキュリティの中核を成すものですが、適切なツールなくしてそれはうまくいきません。悪者を完全に阻止する強力なセキュリティおよびデータ消失回避機能によってモバイル データを保護する方法についてお読みください。

今すぐ読む

4: ノート PC を追跡する。

IP アドレスのログと位置情報を使用して、紛失したノート PC を追跡します。エンドポイント セキュリティ ソフトウェアはノート PC がサーバーにアクセスするたびに IP アドレスをログに記録し、位置情報ツールはノート PC の地理的な位置を突き止めます。ベスト プラクティスは、郵便番号ではなく、番地までノート PC を追跡できる位置情報検索ソフトウェアに投資することです。ノート PC が紛失した場合、このようなソフトウェアでは最後に判明していた位置を特定し、国、都道府県、市町村、郵便番号、番地によってマークされた地図を表示します。ユーザーの住所がその番地である場合、ノート PC はソファのクッションの下に隠れているかもしれません。紛失したノート PC が移動中であり、空港から 15 キロ離れた場所が位置情報によって示されている場合は、リモート消去を開始する必要があるかもしれません。

5: セキュリティを自動化する。

ポリシーに基づく自動化はモバイル デバイスの保護にとって重要であり、デバイスの数と、企業ネットワークの外部に保管されている企業データの量が多いほど、重要度が急速に増します。一般的なセキュリティの自動化には、サーバーのアクセス時間に基づいた基本応答の設定、選択的または完全なリモート消去、きめ細かな暗号化、ユーザーや役割ごとの強力なアクセス制御などのオプションが含まれます。変更を行う必要が生じた場合、IT 部門では管理対象のポリシーにのみ変更を行います。自動化では、しきい値イベントに対応してリモート消去やアラートなどのセキュリティ対策も実施します。自動化されたデバイス検出も非常に便利で、数百台以上のリモート デバイスを保護する必要のある中規模の企業にも対応します。

強力なセキュリティ、バックアップとリカバリ、セキュアなコラボレーション、e ディスカバリーとコンプライアンス、データ分析などの包括的なモバイル エンドポイント管理および制御によってモバイル エンドポイントを保護してください。これにより、紛失したノート PC による不確実性やデータ漏洩による大きな被害から企業を保護できます。悪者は常に存在しますが、適切な保護により、彼らの被害者とならずに済みます。

データ漏洩の 80% 近くは暗号化されているコンピューターや USB サム ドライブの盗難から生じています。

PRECYSESOURCE、
"The Cause of a Data Breach – Lost/Stolen Laptops or a Security Design Flaw" 2014

リソース

1 http://commvau.lt/1M1pSA0

Commvault® ソフトウェアでエンドポイントおよびモバイル デバイスを保護する方法の詳細については、commvault.com/solutions/endpoint-data-protection をご覧ください。

© 2017 Commvault Systems, Inc. All rights reserved. Commvault、Commvault とロゴ、「六角形の C」のロゴ、Commvault Systems、Commvault OnePass、CommServe、CommCell、IntelliSnap、Commvault Edge、および Edge Drive は、Commvault Systems, Inc. の商標または登録商標です。その他すべてのサード パーティのブランド、製品、サービス名、商標、または登録サービス マークは、それぞれの所有者の所有物であり、これらの所有者の製品またはサービスを識別するために使用されます。すべての記載は通知なしに変更される場合があります。

COMMVAULT

Commvault Systems Japan 株式会社　〒141-6008 東京都品川区大崎 2-1-1 ThinkPark Tower 8F

www.commvault.com | PHONE: 03-5747-9610 | jpsales@commvault.com
© 2017 Commvault Systems, Inc. All rights reserved.