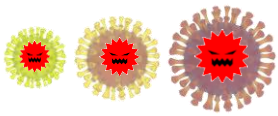
ランサムウェア、もはや100%の防御は不可能です!!

従来のサイバーセキュリティ産業の限界

回顧的	サイロ型	遅れ
従来型ツールは、これまでに見られたことのあるテクニックを検知し、攻撃に反応することしかできない	Eメール/クラウド/ネットワーク/エンドポイント/OTに対するセキュリティソリューションは別々に進化してきた	これまでマシンスピードの脅威に対処するためにも人間に頼ってきた

サイバー犯罪者はEメールゲートウェイ、アンチウィルスツール、エンドポイントソリューションが使用する**回顧的な拒否リストを回避できる**ことを知った



攻撃インフラを更に**獰猛なものに更新し進化**させた

新型コロナのように変異し巧妙化

攻撃の範囲を拡大し、Eメールや SaaS 環境から**クラウドインフラ、IoT、産業用制御装置（ICS）**まで、デジタルエンタープライズ内のさまざまなエリアを標的とするようになった

脅威の新時代（５つのトレンド）

1. ランサムウェアの台頭 — 産業用ICSを標的としたランサムウェアは増えつつあり、2018年以降500%増加している
2. ステルス&先行性APT* — 大手の多国籍企業や政府機関だけでなく、より広範囲な企業が標的
3. クラウドベースの攻撃 — デバイスではなくID を狙う: SaaSアカウントの乗っとり（Zoom/Teams/Microsoft365等）
4. ゼロディ攻撃 — マイクロソフト Exchange サーバーのゼロデイを悪用した攻撃が発生中であることを発表
5. 攻撃型AIの出現 — AIはサイバー犯罪者の攻撃力を増し、よりステルス的な、より高速な、より効果的な攻撃を可能にする

*ATP(Advanced Persistent Threat)：脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃のこと（IPA）

出典:ダークトレース社ホワイトペーパー

確実な復旧こそ最終対策、安全安心のバックアップは最後の砦!!

データプロテクションで新しい脅威の対策を

攻撃を受けたデータの格納場所の6割がパブリッククラウド*という事実に対し

*出典：IT Leaders 2020.5.28

▶ Windowsが直接アクセスできない環境を提供します

▶ 圧縮/暗号化/ブロック分割でマルウェアを封じ込めます

CrossLinks データプロテクション 製品ラインアップ

製品名 ＼ 機能	クラウドバックアップ		エンドポイントセキュリティ	
	デバイスデータ バックアップ	クラウドデータ バックアップ	盗難データ保全 (遠隔データロック/削除)	マルウェア検知/駆除 URL脅威検知
データプロテクションスイート	○		○	○
データプロテクション	○		○	
MS365バックアップ		○		

<システム要件>
対応OS PC：Microsoft Windows 8.1/10, macOS Sierra(10.12) 以降、サーバー：Windows Server 2012/2012 R2/2016/2019

販売代理店：	株式会社グローバル・アドバンス	販売元：	株式会社クロスリンクス

スイート製品のうちバックアップ製品は米国Carbonite社の"Carbonite Endpoint"です。Carbonite社は2006年に創業し、2020年6月現在世界で2万4千社のパートナー企業を含む45万人の顧客に利用され、7000億のファイル(250ペタバイト)を管理しています。またセキュリティ製品は米国Webroot社の"Webroot® Business Endpoint Protection"です。Webroot社は1997年に創業し、2020年6月現在1万5千社のパートナーを含む20万社の法人に利用され、3,000万以上の契約数を持っています。