Zombie ZERO

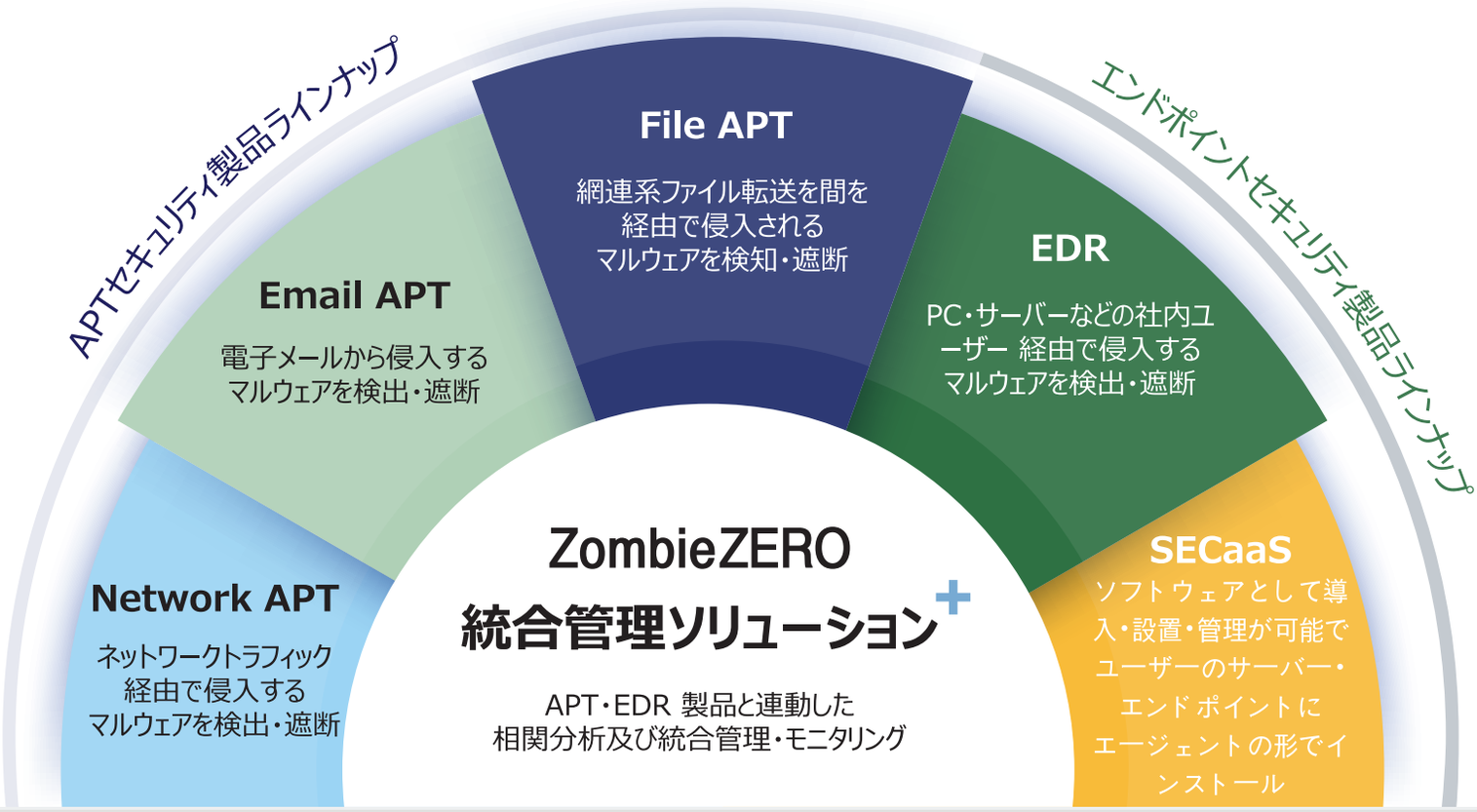
AIベースの新・変種マルウェア及びランサムウェア対応ソリューション



サイバー攻撃の脅威を防ぐ**安全なセキュリティ環境**をご提供致します

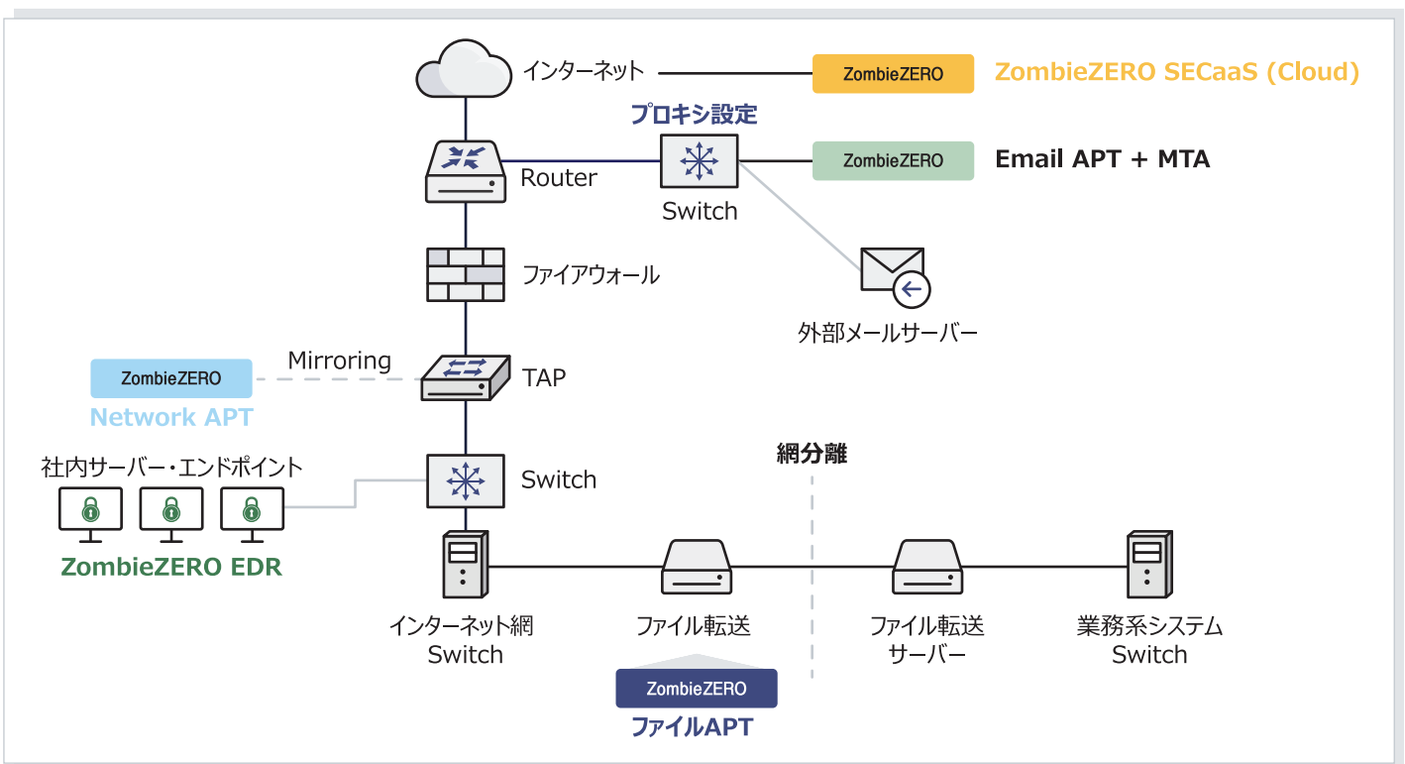
NDCore

ランサムウェア・標的型攻撃（APT）等の新・変種マルウェアを 検知・遮断するAIベースの行動分析セキュリティソリューション



ZombieZERO システム構成図

・マルウェアが侵入する可能性のある様々な経路に対するソリューションの構築が可能



ZombieZERO APT

アプライアンス型の一体型セキュリティソリューション
ネットワーク･電子メール･ファイル（ネットワーク連携区間に構築）



Network APT

行動分析により、従来の シグネチャーベースのシステムが検知できない ゼロデイ攻撃への脆弱性を補完

- ファイルの流入と流出に対する双方向ネットワークトラフィックのモニタリング
- 主要インターネットサービスプロトコルの収集及び分析
- 有害サイトへのアクセス及びC&C通信時の検知・遮断

Email APT

マルウェアに脆弱な既存のシグネチャ-ベースのスパムメールソリューションの限界を補完

- APTとMTA（メッセージ送信エージェント）統合
- スパム・スピアフィッシング・悪性コードが含まれたメールから悪性情報のみ遮断
- メールの添付ファイル及びURLを分析した後、正常なメールのみメールサーバーに送信

File APT

外部網と内部網との間でファイル転送が行われる網連携区間でサーバー保護

- ネットワーク連携ソリューションと連動し、移動待機中のファイルに対する分析・遮断
- 分析されたファイルを分類して正常と判断されたファイルのみ業務系システムに転送
- 共有フォルダ（SMB-NFS-Web APIなど）を利用した分析結果の伝達

導入効果

・弊社APT製品とEDR製品を共に導入した場合

マルウェア・ランサムウェア対応

ワクチンソフトが検出できない 未知の新・変種のマルウェアを検知・遮断し対応が可能

エンドポイントの可視性向上

エンドポイントで発生するサイバー攻撃の具体的な進行状況の確認・可視化を実現

マルウェア侵入防止

マルウェアの侵入経路とシステム間の接続を確認し、内部で脆弱な部分を補完しセキュリティを強化

セキュリティ製品の導入コスト削減

ランサムウェア対応、ファイルのバックアップ機能及びワクチンソフト機能をサポート、別途製品購入が不要

ZombieZERO EDR

PC・サーバーなどのユーザー経由して侵入するマルウェアを検知・遮断します。
オンプレミス又はクラウドでの構築が可能



主な機能

リアルタイムでランサムウェアの検知・遮断

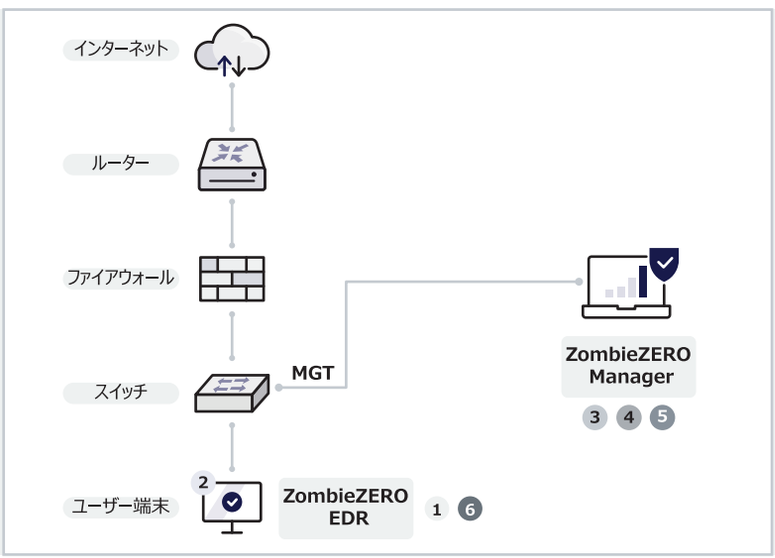
- ランサムウェアのファイル暗号化及び偽造・改ざん対応
- ワクチンソフトBitdefenderのAV機能をサポート

ゼロトラスト対応（実行保留機能）

- 新規ファイルの流入や疑わしいファイルの実行保留を行い分析サーバーに情報をアップロード

IOC ベースのリアルタイム脅威検出

- ユーザー端末の行為に対するIOC検出(ネットワーク、ファイル、プロセス、レジストリなど)



ZombieZERO SECaaS

ZombieZERO EDRのクラウドサービス

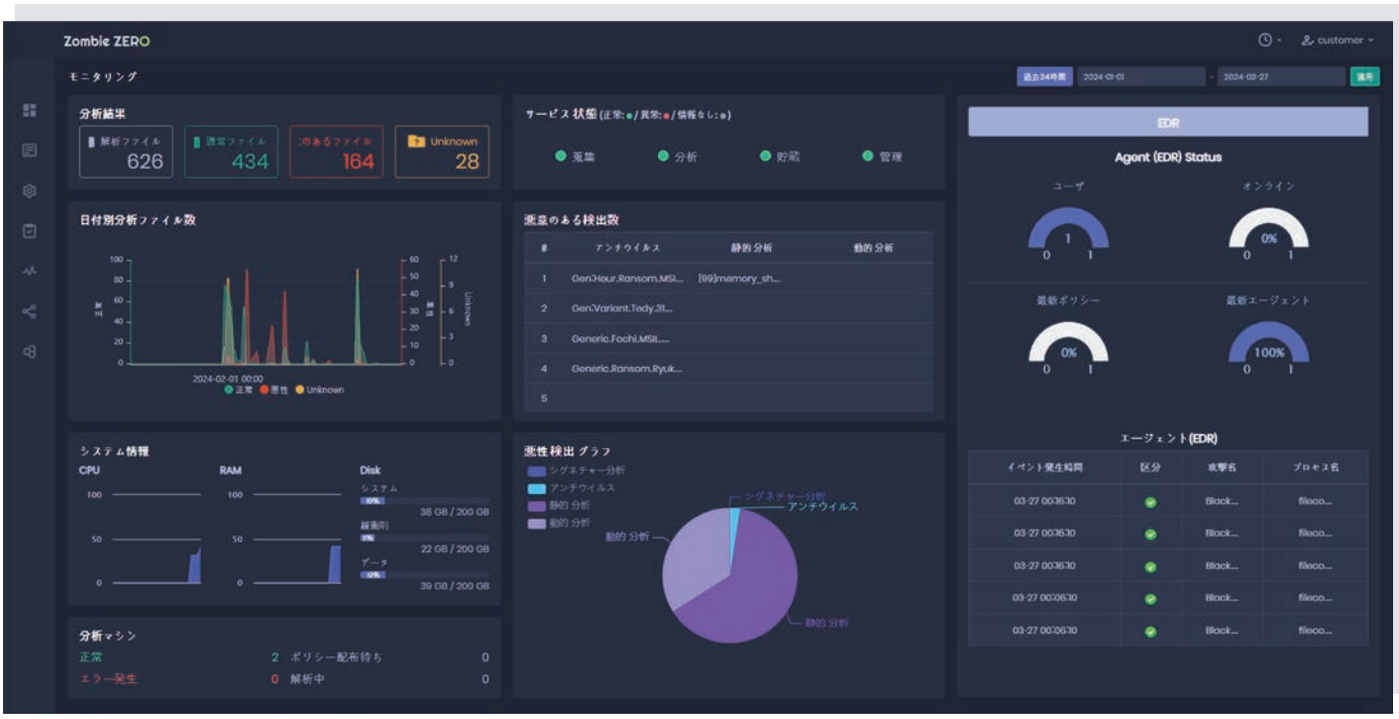
- 専用Webページからエージェントの形でインストール
- Web上で購入・設置・中央管理など全ての機能を提供
- ユーザー管理の高利便性、またハードウェア購入不要
- 中小規模の企業やテレワーク環境に最適

EDR検出・分析機能フローチャート

1. IOCベースの脅威行為の検出 (MITRE ATT&CK 分類)
2. ユーザーPCに新規ファイルの流入と実行
3. 分析サーバーにファイルをアップロード
4. ファイルの分析
5. 分析結果に基づいたポリシーの配布
6. 正常なファイルの場合に実行 疑わしいファイルはブロック・隔離
7. IOCベースの脅威行為の継続的な検出 (MITRE ATT&CK 分類)

ZombieZERO UI

・システム管理者様の利便性を考慮し直感的かつ視覚的に分かり易いレイアウトを採用
・権限を持ったユーザーのみアクセス可能な認証及び権限制御機能でセキュリティを強化



主な共通機能

多次元分析

AV-静的分析-動的分析-評判分析など多次元分析による検出

仮想マシンのバイパス防止

リアルマシンと同じ動的行動分析を提供

MITRE ATT&CK分類

悪質行為 MITRE ATT&CK 基準検出

悪質行為のフローを提供

1011100
0101
1110110

侵害指標（IOC）に応じた攻撃形態の詳細及びモニタリング 機能を提供

ECSCとの連携

韓国教育部 サイバー保全センター Yara Rule と連動

AIベースのマルウェア対策

AIベースの高速かつ正確なマルウェア検出技術

多次元分析

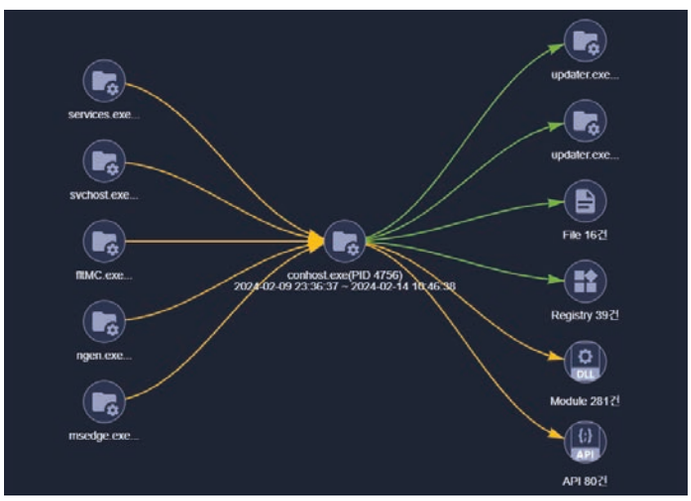
・外部からネットワークを通じてユーザー組織内に流入したトラフィックを多次元で分析、マルウェアを検知・遮断します

HASH ▶ Bitdefender ▶ yara ▶ vmware ▶ VirusTotal

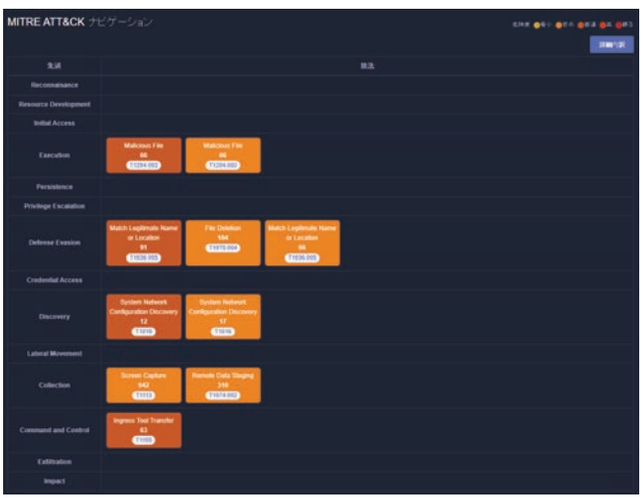
User Black　AV Engine　Yara 静的解析　仮想マシンの動作分析　評判分析

MITRE ATT&CK・悪質行為フローチャート

・進行中の攻撃に対する技術及び方法の形態を監視



プロセス分析情報（悪質行為フローチャート）



プロセス分析情報（悪質行為フローチャート）

リアルタイム・バックアップ

・ファイルが改ざんされる直前に，通常プロセスではアクセス出来ないフォルダに文書ファイルをバックアップ
・カーネルドライバ側でのバックアップ実行により アプリケーション間の競合と性能低下を回避

ファイルの
モニタリング ▶ ファイルオープンと
プログラム作成 ▶ ドライバのセキュリティ
フォルダにリアルタイム・
バックアップを実行 ▶ 保存したバックアップ
ファイルの復元
（破損のないオリジナルファイル） ▶ 完璧な二重保護

導入実績

韓国トップの 標的型攻撃ソリューションベンダーであるエヌピーコアは、国内外累計
１５０社以上の導入実績がございます

Korean National Police Agency
Prosecution Office
Ministry Of National Defense
Korea Post
Seoul Guarantee Insurance
National Fire Agency
Korea Inclusive Finance Agency
The Korean Teachers' Credit Union
Gyeongsangnam-do
Gyeongsangbuk-do
Seoul Metropolitan Office Of Education
Gyeonggido Office Of Education
BUSAN Metropolitan City Office Of Education
INCHEON Metropolitan City Office Of Education
Gyeongsangbuk-do Office Of Education
JEOLLANAMDO Office Of Education
DAEGU Metropolitan Office Of Education
Korea Student Aid Foundation
KYONG GI University
Dongduk Women's University
OSB Savings Bank
BNK Kyongnam Bank
Financial Services Commission
Posco
JTBC Broadcast Stations
Ls Mtron Industrial Machinery Company
VHS Medical Center
Seoul Medical Center
Jeju National University Hospital
Indosat Ooredoo
Kamisu City Hall, Japan
Royal Malaysia Police
Vietnam Posts And Telecom Group
Vietnam Cryptography University
Ministry Of Transport
Skylake Golf Resort

認証・特許

GS認証1等級セキュリティ機能確認書革新製品認証ISO認証など、
米国と日本の特許を含む15件のセキュリティ関連認証及び特許を保有しています。



Security Functionality Certificate



ISO 9001 : 2015



GS認証登録



米国特許登録



革新技術製品認定

NPCore

ソウル特別市永登浦区唐山路171ㆍ701号(唐山洞4街錦江ペンテリウムITタワー)
T. +82-2-1544-5317 | E. marketing@npcore.com