Fuva Brain

Press Release

報道関係者各位

2025 年 5 月 26 日

株式会社フーバーブレイン

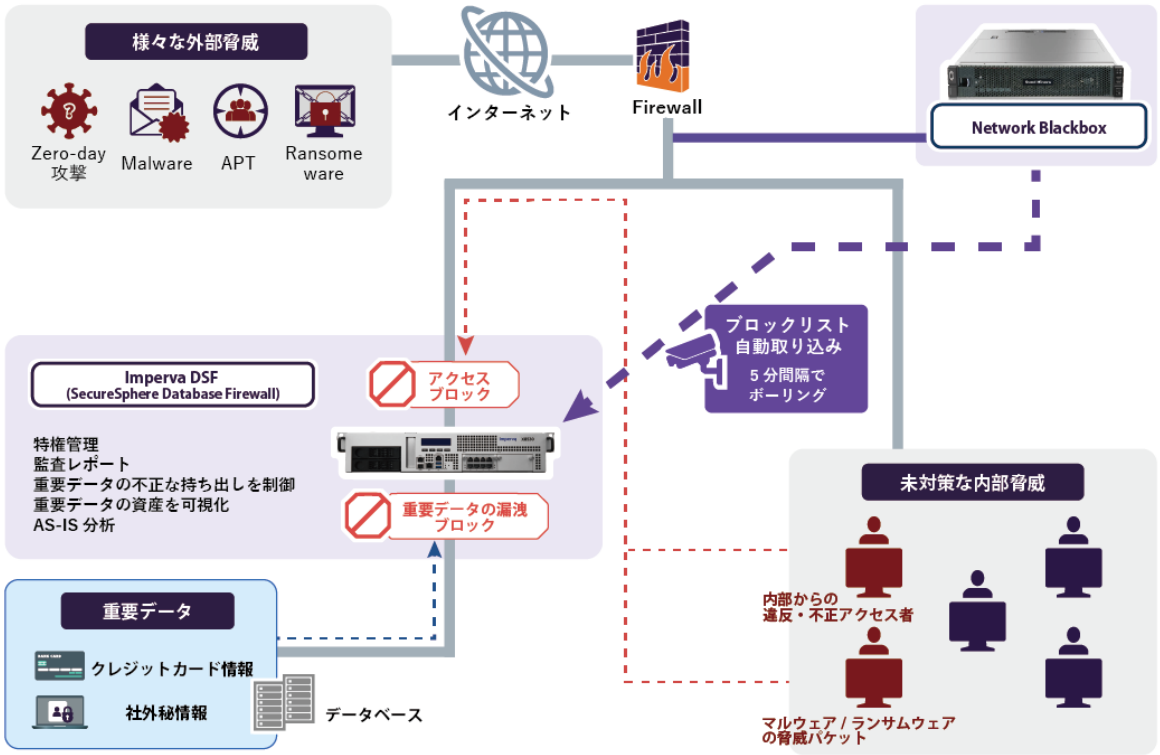
セキュリティ脅威を自動的に可視化・検知・防御する 世界初*1 ソリューション「L3to7 Auto-response」を提供開始

Web/データベースセキュリティの先駆製品 Imperva (SecureSphere) と フルパケットキャプチャの先進 NDR 製品 Network Blackbox の技術連携を実現

サイバーセキュリティカンパニーの株式会社フーバーブレイン(本社:東京都千代田区、代表取締役社長:輿水 英行、東証グロース 3927、以下、当社)は、Web/データベースセキュリティの先駆製品 Imperva (SecureSphere) と、フルパケットキャプチャの先進 NDR 製品 Network Blackbox を当社独自ノウハウで技術連携し、ネットワーク層～アプリケーション層を横断するセキュリティ脅威に対し、可視化・検知・防御を一気通貫で実現する世界初*1 のセキュリティ連携ソリューション「L3to7 Auto-response (エル スリー トゥ セブン オートレスポンス)」を新たにリリースします。

詳細 URL:https://www.fuva-brain.co.jp/products_services/l3to7autoresponse/

*1: 自社調べ



今回、当社が提供する「L3to7 Auto-response」は、法人組織内のネットワーク層に侵入するランサムウェアなどの脅威を一早く検知し、その脅威が Web アプリケーションサーバやデータベースサーバなどのアプリケーション層へ到達する前に未然にブロックすることが可能な、世界初のセキュリティ連携ソリューションです。当社が 20 年のノウハウを有する Web/デ

ータベースセキュリティ製品「Imperva (SecureSphere)」と、当社が国内総代理店を担うフルパケットキャプチャの先進 NDR 製品「Network Blackbox」を、当社独自ノウハウで技術連携させることで、レイヤー横断型の脅威に対する可視化・検知・防御を実現します。

既存のセキュリティ市場において、これまでも複数のセキュリティ製品が連携するケースはよく見られてきました。
しかしながら、本来、アプリケーション層に対する監視・脅威検知・防御の機能を提供する Imperva (SecureSphere) のポーリング監視技術を使い、別レイヤーのネットワーク層を監視する Network Blackbox による脅威検知情報をトリガーとして Web アプリケーション・データベースを保護する「L3to7 Auto-response」は、API に依存することなく「既存市場に初めて提供する自動連携ソリューション」と言えます。

近年、日本国内の企業や、公共団体を狙ったランサムウェアの猛威は留まることを知らず、コロナ禍以降におけるテレワーク環境の普及と相まって、VPN やリモートデスクトップ経由によるランサムウェアのネットワークへの侵入が後を絶ちません。情報処理推進機構(IPA)が年次で発表している「情報セキュリティ 10 大脅威」においても、「ランサムウェアによる被害」が組織向けの脅威の順位として、2021 年から本年 2025 年まで 5 年連続 1 位にランキングされています。
出典: 独立行政法人 情報処理推進機構「情報セキュリティ 10 大脅威」
https://www.ipa.go.jp/security/10threats/index.html

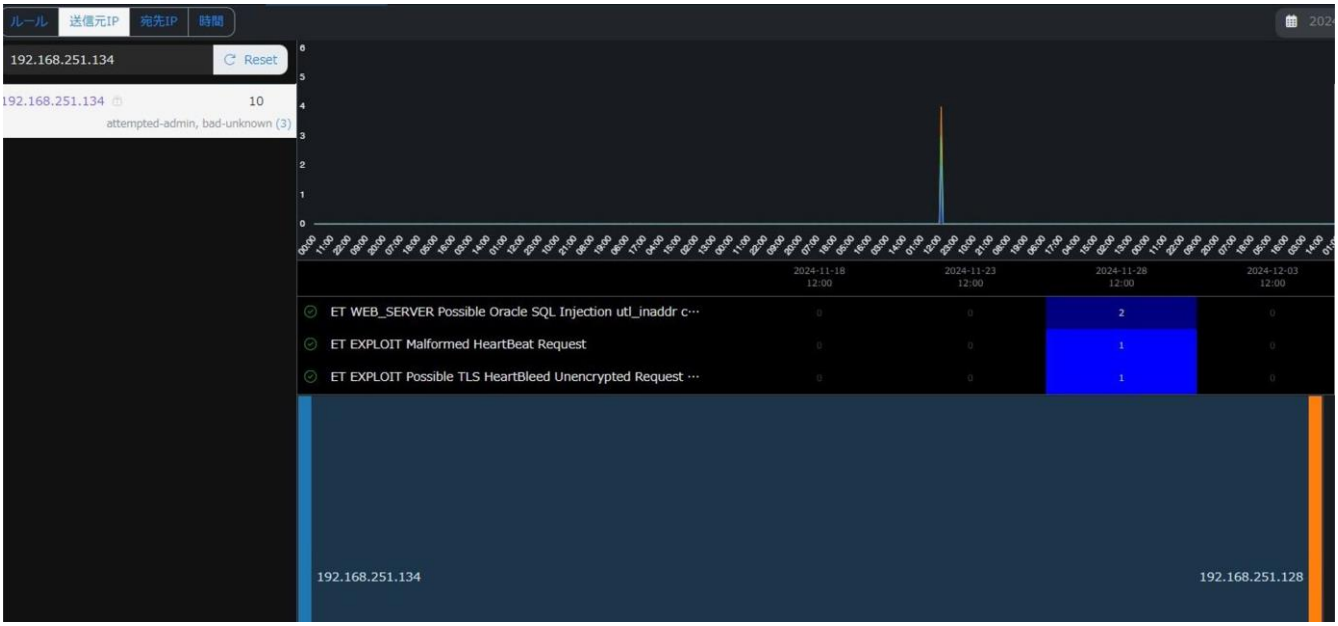
このランサムウェアによる攻撃ターゲットは、ネットワーク上に格納されている非構造データ(ファイル)だけでなく、よりミッションクリティカルな情報に該当する構造データ(データベース)にも及んでいます。近年は、データベースソフトウェアの開発メーカ各社においても、ランサムウェアからのデータベース保護の重要性を訴える内容を、ブログなどを通じて情報発信する機会がよく見られます。
一方で、日本ネットワークセキュリティ協会(JNSA)が 2024 年 2 月 29 日に公開した、企業のデータベース管理者(DBA)に対するアンケートによれば、「ランサムウェア対策としてデータベースのセキュリティ対策ソリューションの強化を行っていますか？」という問いに「はい」と回答した比率は 26.0%に留まっており、対策があまり普及していない状況にあります。また、同アンケートでは、「ランサムウェア対策としてのデータベース保護の強化策」として「暗号化」と回答した比率が最も多く 52.1%を占めています。しかし、実際には、データベース向けのランサムウェア攻撃は、データベースソフトウェアに標準実装されている透過的データベース暗号化(TDE)というセキュリティ機能を悪用し、クエリ実行による自動復号データを窃取後に別の暗号アルゴリズムを使って不正暗号化してしまいます。
出典: 特定非営利活動法人 日本ネットワークセキュリティ協会 データベースセキュリティ WG 「「DBA 1,000 人に聞きました」アンケート調査報告書(2023)」
https://www.jnsa.org/result/dbs/2024.html

■L3to7 Auto-response の概要(詳細 URL:https://www.fuva-brain.co.jp/products_services/l3to7autoresponse/)

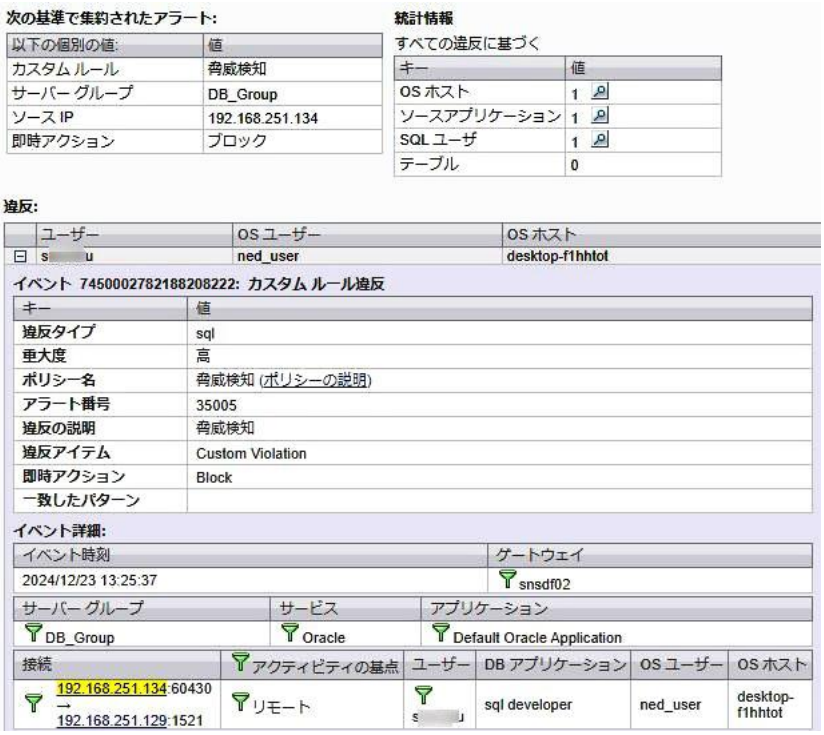
1. Imperva DSF (SecureSphere Database Firewall[*2]) が、Network Blackbox を一定間隔で自動的にポーリングし、Network Blackbox が検知した危険度の高いネットワーク脅威パケット情報を自動取得します。
2. Imperva DSF (SecureSphere Database Firewall[*2]) のカスタムポリシー機能を使い、ネットワーク脅威パケットによるデータベースサーバへのアクセスをブロックするセキュリティルールを事前定義します。
3. この技術連携によって、Network Blackbox が検知した脅威パケットに該当するユーザは、正規のクエリを実行してもデータベースへアクセスできなくなります。ただし、ユーザのネットワークセキュリティが改善されることにより自動的にブロックが解除され、ユーザは通常通りデータベースへアクセスできるようになります。

*2: データベース保護を目的とする場合は、Imperva DSF (SecureSphere Database Firewall) を導入し Network Blackbox と技術連携させます。Webアプリケーション保護のために、Imperva Web Application Firewall を導入し連携させることも可能です。

画像 1: 危険度の高いネットワーク脅威の送信元 IP アドレスによる、データベースへのアクセスを禁止するセキュリティルール



画像 2: ランサムウェア(IP アドレス: 192.168.251.134)が、正規ユーザになりすましてWebアプリケーション(IP アドレス: 192.168.251.128)の管理者権限を不正取得する挙動を検知



次の基準で集約されたアラート:

以下の個別の値:	値
カスタム ルール	脅威検知
サーバー グループ	DB_Group
ソース IP	192.168.251.134
即時アクション	ブロック

統計情報

すべての違反に基づく

キー	値
OS ホスト	1
ソースアプリケーション	1
SQL ユーザ	1
テーブル	0

違反:

	ユーザー	OS ユーザー	OS ホスト
⊟	s[redacted]u	ned_user	desktop-f1hhtot

イベント 7450002782188208222: カスタム ルール違反

キー	値
違反タイプ	sql
重大度	高
ポリシー名	脅威検知 (ポリシーの説明)
アラート番号	35005
違反の説明	脅威検知
違反アイテム	Custom Violation
即時アクション	Block
一致したパターン	

イベント詳細:

イベント時刻	ゲートウェイ
2024/12/23 13:25:37	snsdf02

サーバー グループ	サービス	アプリケーション
DB_Group	Oracle	Default Oracle Application

接続	アクティビティの基点	ユーザー	DB アプリケーション	OS ユーザー	OS ホスト
192.168.251.134:60430 → 192.168.251.129:1521	リモート	s[redacted]u	sql developer	ned_user	desktop-f1hhtot

画像 3: ランサムウェア(IP アドレス: 192.168.251.134)が、データベース(IP アドレス: 192.168.251.129)へアクセスする挙動をブロック

データベースを狙ったランサムウェア攻撃は、一般的にデータベースソフトウェアの標準暗号化機能を悪用することから、ネットワークへ侵入を許した場合の対策が困難であり、被害を受けた後のデータ復旧にもデータベースの高度な専門知識が必要と言われています。「L3to7 Auto-response」は、このような対策が困難なサイバー攻撃の分野に一石を投じるセキュリティソリューションであり、法人組織の情報セキュリティ担当者や DBA は、脅威に対する不安が一掃され、本来の業務に効率的に集中することができます。

■Imperva (SecureSphere) 開発元: タレス　サイバーセキュリティプロダクト事業本部 本部長　兼子 晃氏のコメント

「この度、Quad Miners 様の Network Blackbox との技術連携を実現できたことを大変嬉しく思います。Imperva は長年にわたり WAF やデータベースセキュリティのソリューションを提供し、脅威の検知とデータの保護に貢献してきました。

今回、Quad Miners の NDR ソリューションが可視化するネットワークレベルの脅威情報をトリガーとして、Imperva の WAF/DBF ソリューションによってカスタマイズされたセキュリティルールを追加することで、Web アプリケーションやデータベースの保護を効率化するための自動連携が実現しました。この連携が、捉えにくかった盲点を補完する革新的なソリューションとして、お客様の重要なデータの保護強化に寄与すると確信しております。」

■Network Blackbox 開発元: Quad Miners クワッドマイナージャパン 代表取締役社長　蘇 明燮氏のコメント

「このたび、Imperva (SecureSphere) との技術連携を実現できたことを大変嬉しく思います。本連携により、高度化・巧妙化するサイバー脅威に対して、より迅速かつ精度の高い防御が可能となりました。

特に、ランサムウェアなどの脅威がネットワーク層に侵入した段階でいち早く検知し、アプリケーション層へ到達する前にブロックできる点は、企業のセキュリティレジリエンス向上に大きく貢献します。本技術連携は、両社にとってイノベーションの加速と市場価値の向上につながる重要なステップであり、今後も密接に協力しながら、お客様の重要なデータとシステムを守るための最先端セキュリティソリューションの提供を推進してまいります。」

【タレスDISジャパン株式会社 会社概要】

会社名: タレスDISジャパン株式会社
代表: 代表取締役 アラン・コレイア
本社: 〒107-0052 東京都港区赤坂2丁目17−7 赤坂溜池タワー 8 階
URL: https://cpl.thalesgroup.com/ja
設立: 2003 年 9 月
資本金: 非公表
事業内容: サイバーセキュリティソリューションの提供・導入（データセキュリティ/アプリケーションセキュリティ/IDとアクセス管理/ソフトウェア収益化ソリューション）

【株式会社クワッドマイナージャパン 会社概要】

会社名: 株式会社クワッドマイナージャパン
代表: 代表取締役社長 蘇 明燮
本社: 〒100-6090 東京都千代田区霞が関 3-2-5 霞ヶ関ビル 5 階
TEL 03-3500-3221
URL: https://www.quadminers.co.jp/
設立: 2021 年 7 月 7 日
資本金: 100 百万円
事業内容: ●システムソフトウェアの企画、研究、開発、制作及び販売
●ソフトウェア及びハードウェアの開発、制作及び販売
●その他これらに関する一切の事業

【株式会社フーバーブレイン 会社概要】

会社名: 株式会社フーバーブレイン
代表: 代表取締役社長 奥水 英行
本社: 〒102-0094 東京都千代田区紀尾井町 4-1 ニューオータニガーデンコート 22F
TEL 03-5210-3061（代表）
URL: https://www.fuva-brain.co.jp/
設立: 2001 年 5 月 8 日
資本金: 796 百万円（2025 年 3 月 31 日現在）（東京証券取引所グロース市場：証券コード 3927）
事業内容: ●サイバーセキュリティソリューションの提供
●テレワーク環境の構築
●生産性およびクオリティオブライフ向上支援
●受託開発・SES（子会社）
●採用支援・人材紹介（子会社）
●投資事業・投資助言（子会社）

＜本件に関するお問い合わせ先＞

株式会社フーバーブレイン 管理部 齋藤

TEL： 03-5210-3061 MAIL：pr@fuva-brain.co.jp