



INFOBLOX DDI WEEK

東京エレクトロン デバイス株式会社

2025/5/29

- 東京エレクトロンデバイスのご紹介
- Infoblox社BloxOne Threat Defenseご紹介
- Infoblox社BloxOne Dossierご紹介とデモ
- 東京エレクトロンデバイスのアセスメントサービスのご紹介
- まとめ



東京エレクトロンデバイスのご紹介

「商社機能」と「メーカー機能」を融合して
技術・製品・情報・サービスを提案しています。



半導体製品

ボード製品・
一般電子部品

製品販売

システム
構築

保守
サポート

プライベート
ブランド製品

設計・量産
受託サービス

商社機能

メーカー機能

東京エレクトロンデバイスは、「**商社機能**」と「**メーカー機能**」を融合して**技術・製品・情報・サービス**をご提案しています。



Semiconductor



IT Solution



Private Brand

設立

1986年

本社：東京都渋谷区
東京証券取引所プライム市場

資本金・売上高

資本金：24億円
売上高：2,428億円
(2024年3月期)



海外
ITセンター

東京エレクトロンデバイス

製品調達

構築サービス

保守サービス



お客様

データセンタネットワーク

ロードバランサ



スイッチ



DNS/DHCP



仮想化基盤ソリューション

All Flash Storage



HCI



サーバー



ゼロトラストソリューション

EPP・EDR



CASB/SASE



DNS FW

DNS FW
NW可視化



バックアップソリューション

重複排除
ストレージ



ランサム対策
ストレージ



バックアップソフト



セキュリティ態勢管理

CNAPP



SSPM



自動ペンテスト



AIインフラソリューション

超高集積GPU



AIアクセラレータ



AIインフラ
エンジニアリング
サービス



弊社サービス

マネージド
セキュリティ



セキュリティ管理

SIEM



暗号鍵保護

HSM



AI関連サービス

自社開発
LLM



AOAI構築
サービス



AI人材
育成トレーニング



継続・安定した長期の取扱実績により、豊富なナレッジを有しています

実績

年数
19年



現契約台数

1500+



業種

通信・政府機関・
官公庁...



体制

体制

Infoblox製品専任
エンジニアで構築・サポート



Infoblox製品群

セキュリティ	コアネットワークサービス	IPアドレス管理	ネットワーク自動化
アドバンスド DNS プロテクション (ADP)	Infoblox DDI: (DNS, DHCP, IPAM)	IPAM (IPアドレス管理)	ネットエムアルアイ (NetMRI)
BloxOne Threat Defense (B1TD)	DNS トラフィックコントロール (DTC)	ネットワークインサイト (スイッチのポート情報などIPAM強化)	
サイバーセキュリティ・エコシステム	クラウドネットワークオートメーション	Microsoft マネジメント (Windows の DNS・DHCP サーバを Infoblox で一元管理)	
レポートینگ アプライアンス			
Infoblox Grid™ リアルタイムネットワークデータベース			
物理 & 仮想アプライアンス (サブスクリプション)			



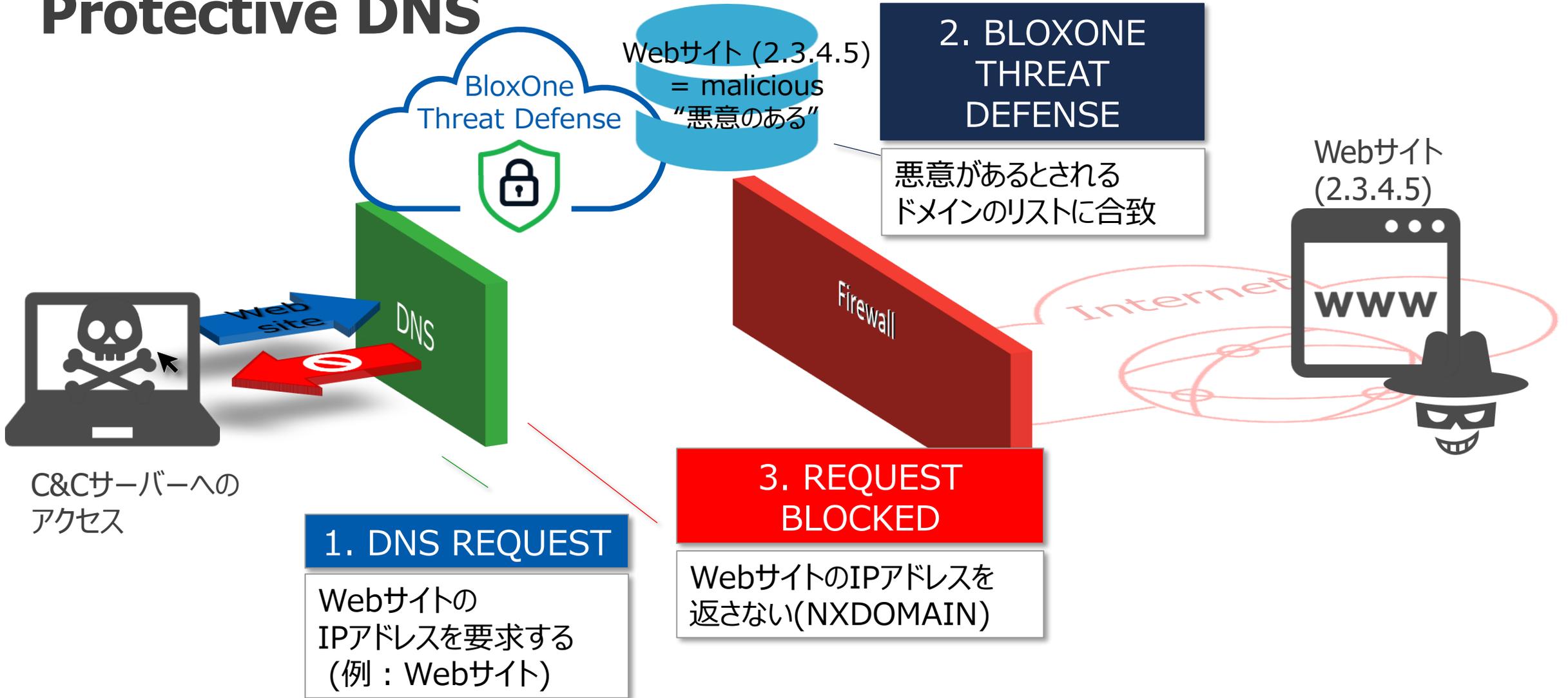
全てのオプション製品群をカバー
様々な基盤での構築実績有



Infoblox社BloxOne Threat Defense ご紹介

DNSベースのマルウェア/ランサムウェアの検出方法

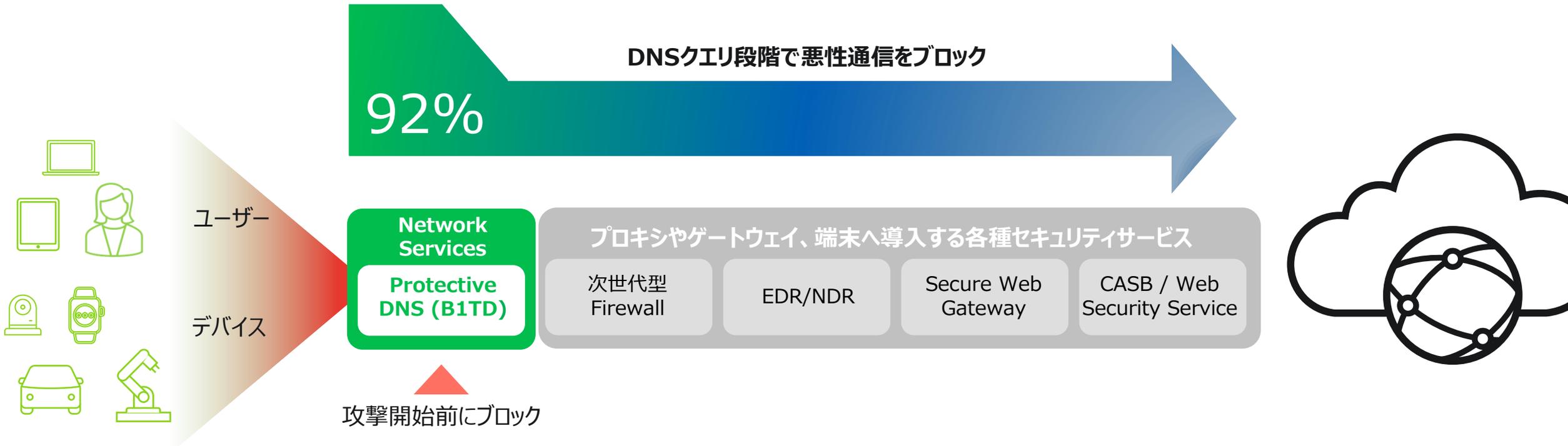
Protective DNS



DNSセキュリティ(=Protective DNS)が Firewall に到達する前に検出/ブロック

プロテクトティブDNSソリューション BloxOne Threat Defense

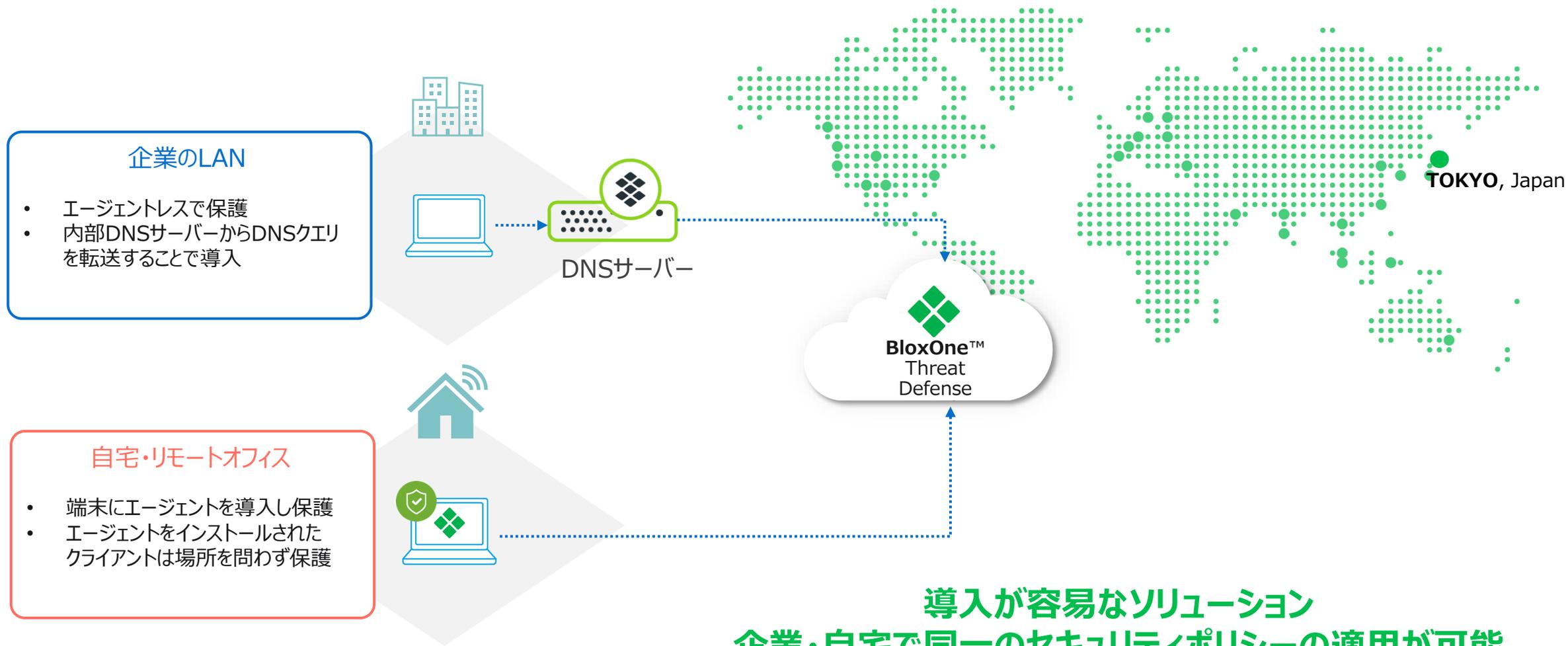
多層防御の1層目として **Protective DNS = “BloxOne Threat Defense”** の活用を



下流のセキュリティデバイスでの大量のアラートを削減

BloxOne Threat Defense導入方法

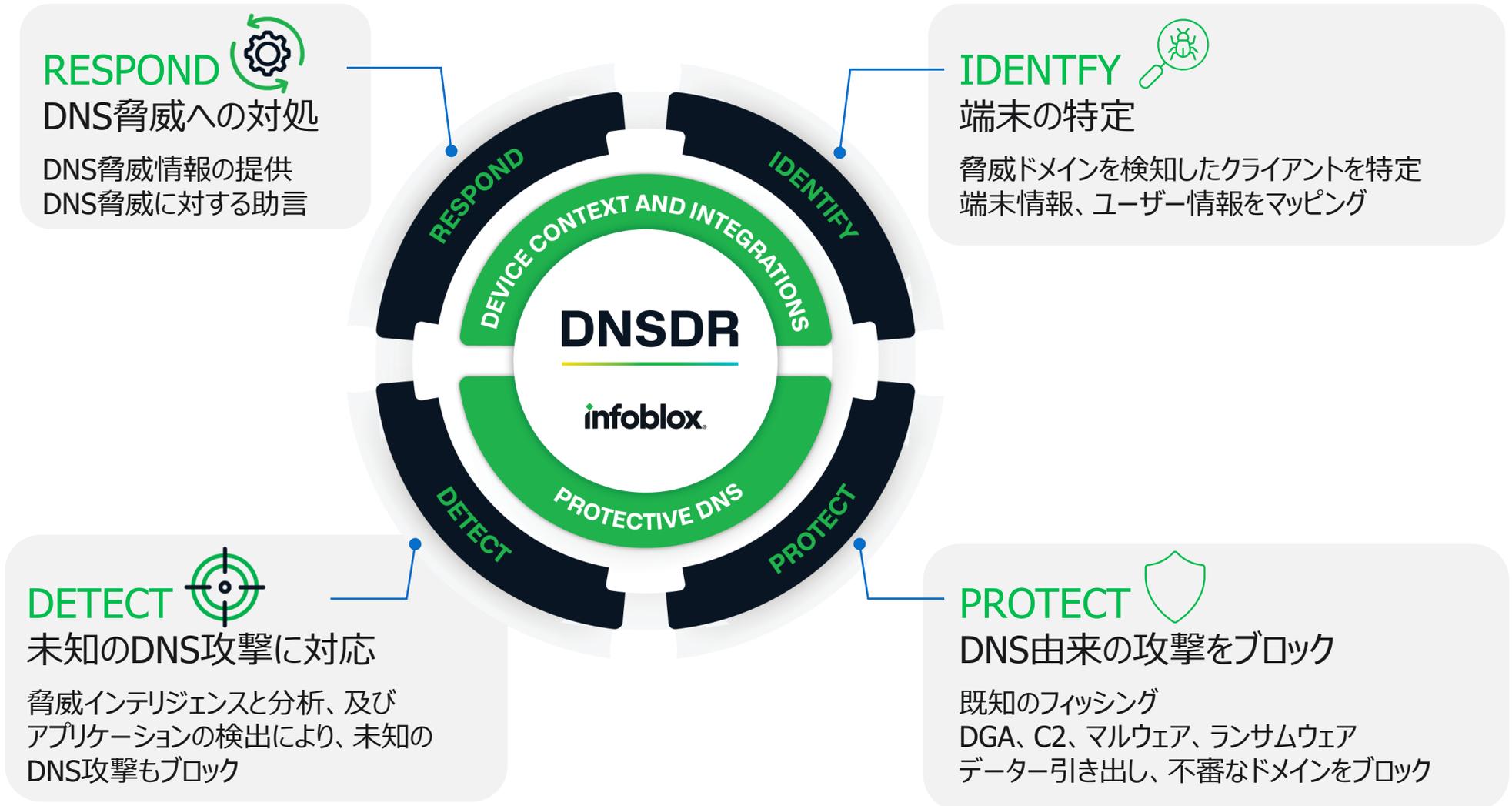
クラウドから提供されるDNSを利用したセキュリティサービス



導入が容易なソリューション
企業・自宅で同一のセキュリティポリシーの適用が可能

DNS Detection and Response ソリューション

PROTECTIVE DNSとして通信の最初の防衛



DNS分析に特化したチーム Infoblox threat intel

- 8つのタイムゾーンにまたがる5カ国のDNS脅威分析集団
- DNSデータから見える脅威に特化
- DNS、データサイエンス、ML/AI、インテリジェンス分析、S/Wリバーズエンジニアリング、悪質なスパム検出に関する深い専門知識
- BloxOne Threat Defenseの脅威インテリジェンスを作成
- これらの専門家は、世界で最初で唯一のチーム！



NSA(米国国家安全保証局)で22年のキャリアを持つレニー・バートン博士がチームを率いる

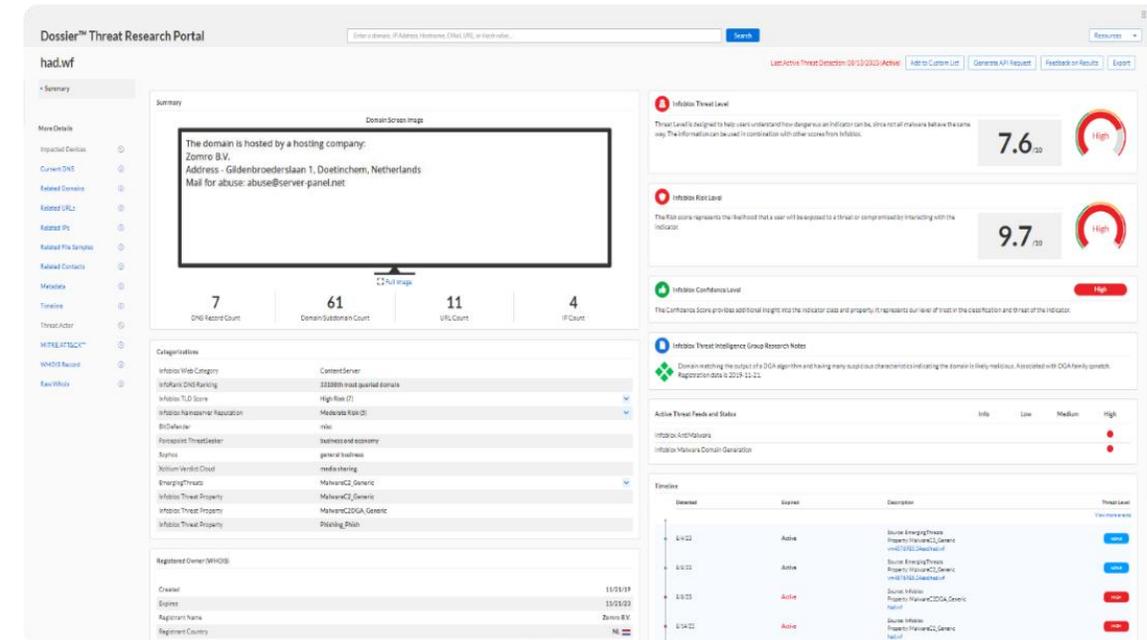
Infoblox Threat Intel team は世界唯一のDNSエキスパート集団



Infoblox社BloXOne Dossier ご紹介とデモ

Infoblox社Dossierとは？

- 複数のデータソースからの脅威情報の一元的な表示
- オープンソース、独自仕様、商用データソースを活用
- ドメインの利用履歴、リスクレベル、MITRE情報など



Dossier™ Threat Research Portal

had.wf

Summary

Domain Screenings

The domain is hosted by a hosting company:
Zomro B.V.
Address - Gildenbroederlaan 1, Doetinchem, Netherlands
Mail for abuse: abuse@server-panel.net

7 DNS Record Count 61 Domain Subdomain Count 11 URL Count 4 IP Count

Chaperon Intelligence

Infolux VAD Category	Content Server
Infolux DNS Ranking	1108th most queried domain
Infolux TLD Score	High Risk (7)
Infolux Namespace Reputation	Medium Risk (2)
BitCrawler	none
Footprint ThreatFeeder	business and economy
Scans	general business
Xenomik Verdict Cloud	media sharing
EmergingThreats	Malware/C2, Generic
Infolux Threat Property	Malware/C2, Generic
Infolux Threat Property	Malware/C2/DGA, Generic
Infolux Threat Property	Phishing, Email

Registered Owner (WHOIS)

Created	11/21/19
Expires	11/21/23
Registrant Name	Zomro B.V.
Registrant Country	NL

Infolux Threat Level: 7.6 (High)

Infolux Risk Level: 9.7 (High)

Infolux Confidence Level: High

Infolux Threat Intelligence Group Research Notes

Domain matching the output of a DGA algorithm and having many suspicious characteristics indicating the domain is likely malicious. Associated with DGA family speech. Registration data is 2019-11-21.

Active Threat Feeds and Status

Feed	Status	Description	Threat Level
6/4/22	Active	Source: EmergingThreats, Research: Malware/C2, Generic, Infolux: DNS, Searcher of	High
6/6/22	Active	Source: EmergingThreats, Research: Malware/C2, Generic, Infolux: DNS, Searcher of	High
6/8/22	Active	Source: Malware, Research: Malware/C2/DGA, Generic, Infolux: IP	High
6/14/22	Active	Source: Malware, Research: Malware/C2, Generic, Infolux: IP	High

Timeline

Event	Date	Threat Level
Infolux: DNS/Whois	6/4/22	High
Infolux: Malware/Domain Generation	6/14/22	High

脅威インテリジェンスデータを提供するツール

The screenshot shows the Infoblox Dossier Threat Research Portal. The browser address bar displays `csp.infoblox.com/#/security_research/dashboard`. The page header includes the Infoblox logo, a location dropdown set to 'TOKYO ELE...', a search icon, a calendar icon showing '13', and a user profile icon for 'TED Kenta Iga...'. The main navigation sidebar on the left contains 'Monitor' and 'Configure' options. The main content area features a search bar with the placeholder text 'Enter a domain, IP Address, Hostname, EMail, URL, or Hash value...' and a 'Search' button. Below the search bar, there is a brief description of Dossier™ as a threat research tool. The dashboard is divided into several sections: 'Insight' with a 'Threat Feed with greatest activity in your environment' (listing 'blacklist') and a 'Top Malicious Host in your environment' (listing 'c.pki.goog'); 'Threat feeds with the most activity in your environment' with a table showing 'blacklist' (1378) and 'Infoblox_Base' (214); and 'Latest Reports from Infoblox Threat Research' with two articles: 'Uncovering Actor TTP Patterns and the Role of DNS in Investment Scams' (dated May 2, 2021) and 'A Phishing Tale of DoH and DNS MX Abuse' (dated March 28, 2021). The bottom left sidebar includes 'Guidance' and 'Help' icons.

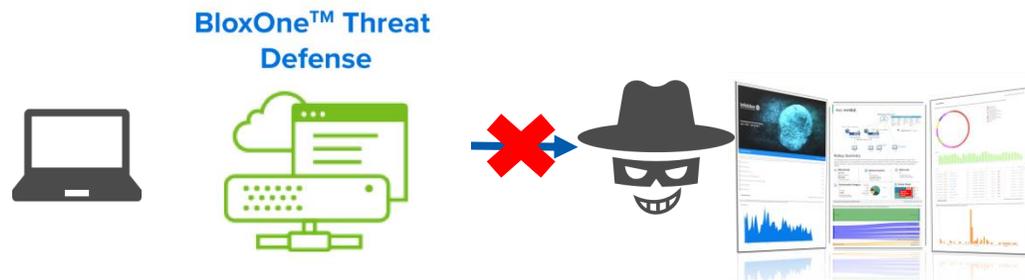


東京エレクトロンデバイスの アセスメントサービスのご紹介

infoblox Infoblox 事前アセスメントサービス

プロテクトティブDNSを納入前に効果をレポート

Infoblox BloxOne Threat Defenseを利用したアセスメントサービス



プロテクトティブDNSを利用した診断サービス

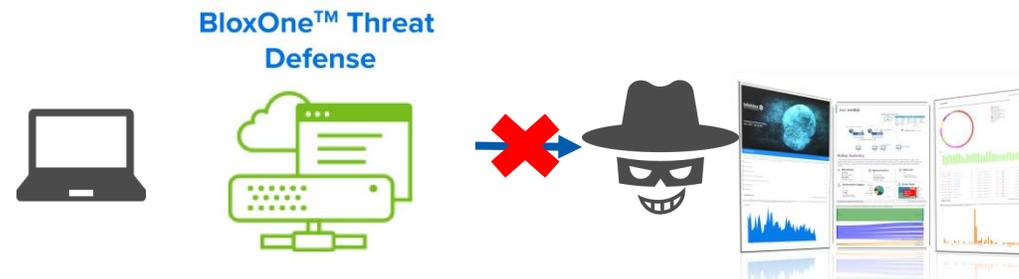
- 外部DNSの参照先をInfobloxのクラウドDNSに切り替えるのみで利用可能
- セキュリティエンジニアがアセスメントサービスを全面支援
- B1TDでの脅威検知状況や利用状況の統計をまとめ、分析レポートご提供しWEB会議にて説明会を実施
- 納入前にプロテクトティブDNSの効果を確認可能

**DDI week御覧の皆様へ
今回限り無償ご提供**

infoblox Infoblox 運用アセスメントサービス

プロテクトティブDNSの効果を運用後もレポート

納入後Infoblox BloxOne Threat Defenseの利用状況をレポート



Infoblox B1TDを利用の運用レポート

- B1TDでの脅威検知状況や利用状況の統計をまとめ、分析レポートご提供しWEB会議にて説明会を実施
- 納入後もプロテクトティブDNSの効果を確認可能



まとめ

