



IoT/5G時代におけるセキュリティの新しい考え方

～既存技術でデジタルトランスフォーメーションをセキュアなものに

Infoblox 株式会社
システムエンジニアリング技術本部
本部長
高橋 徹

2019年11月7日（木）



脅威ランドスケープの進化



増え続けるセキュリティ運用上の課題

- SOAR (Security Orchestration, Automation and Response)の重要性

92%

1日500件以上のアラートを受信する企業の割合。
1人のサイバーアナリストは1日10件の対応が限界。

4%

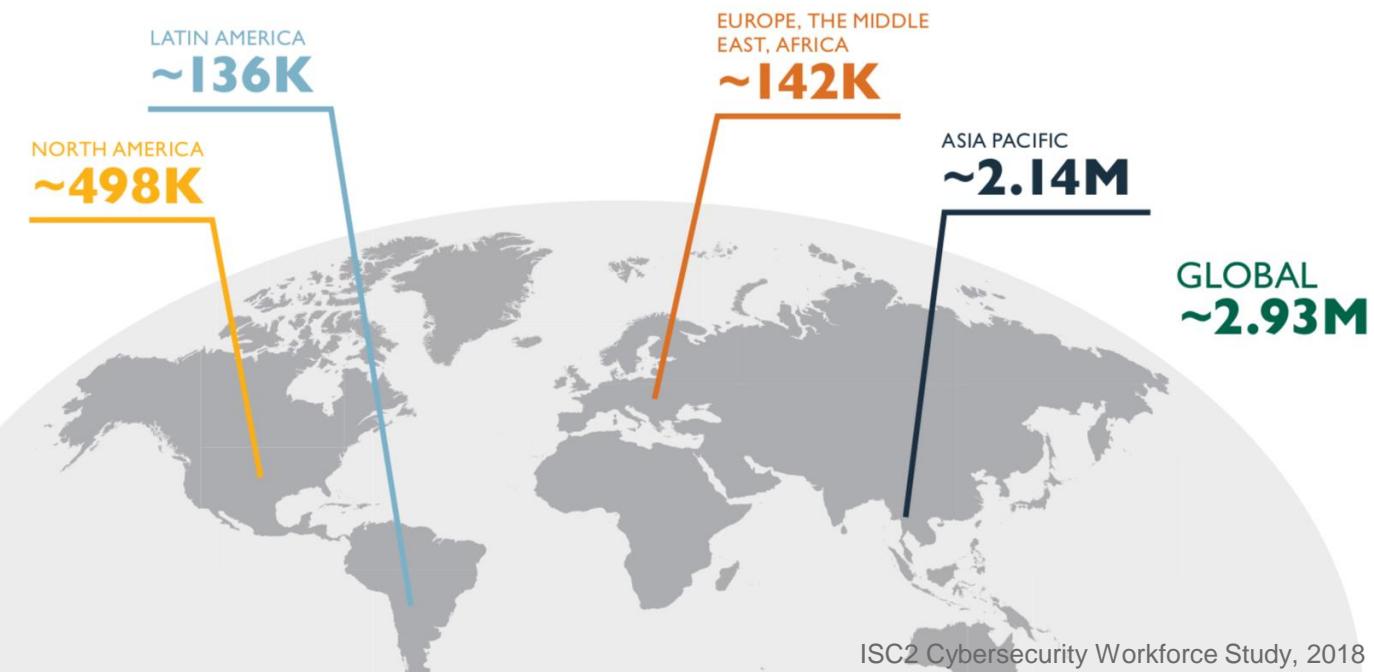
調査されているアラートの割合。組織の安全を守るには担当者数が不足。

30+

運用されているセキュリティツールの数。スタッフや専門家が管理できるのは12まで。

問題の解決にこれ以上の人材を投入するのは困難

地域ごとのサイバーセキュリティの専門家の数
Gap in Cybersecurity Professionals by Region



デジタルトランスフォーメーションには新たなパラダイムが必要

クラウドファースト エンタープライズ



場所を問わずクラウドアプリケーションに
ダイレクトにアクセス

ソフトウェアディファインド ネットワーク



ポリシードリブンのネットワーク
仮想化されたネットワーク機能

BYOD、モビリティ、IoT



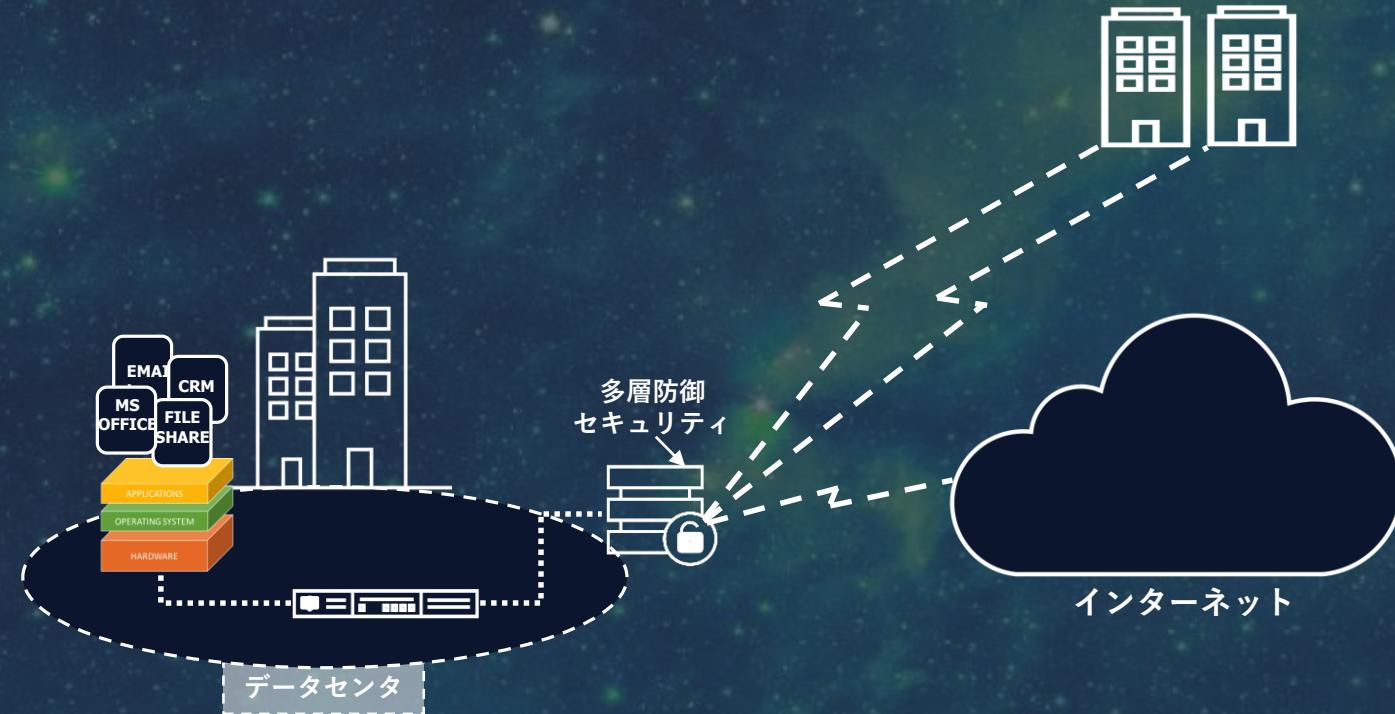
エンドポイントの爆発的な急増
スケーリングとセキュリティの課題

80% - 2030年までにクラウド上に
展開される新アプリケーションの割合

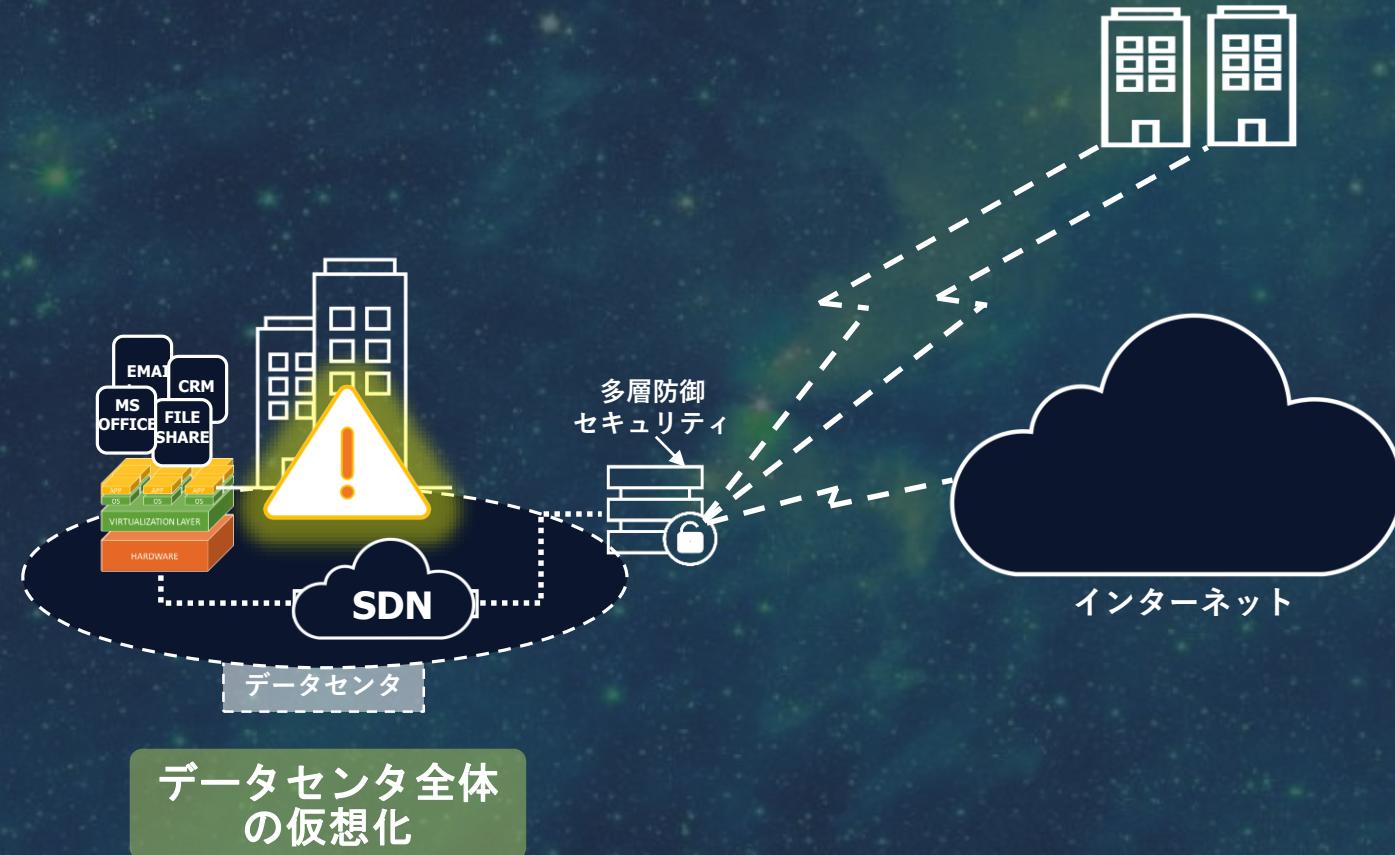
40% - 2019年末までにSD-WANを
採用予定の企業の割合

125 B – 2030年までにネットワーク
につながるIoTデバイスの数

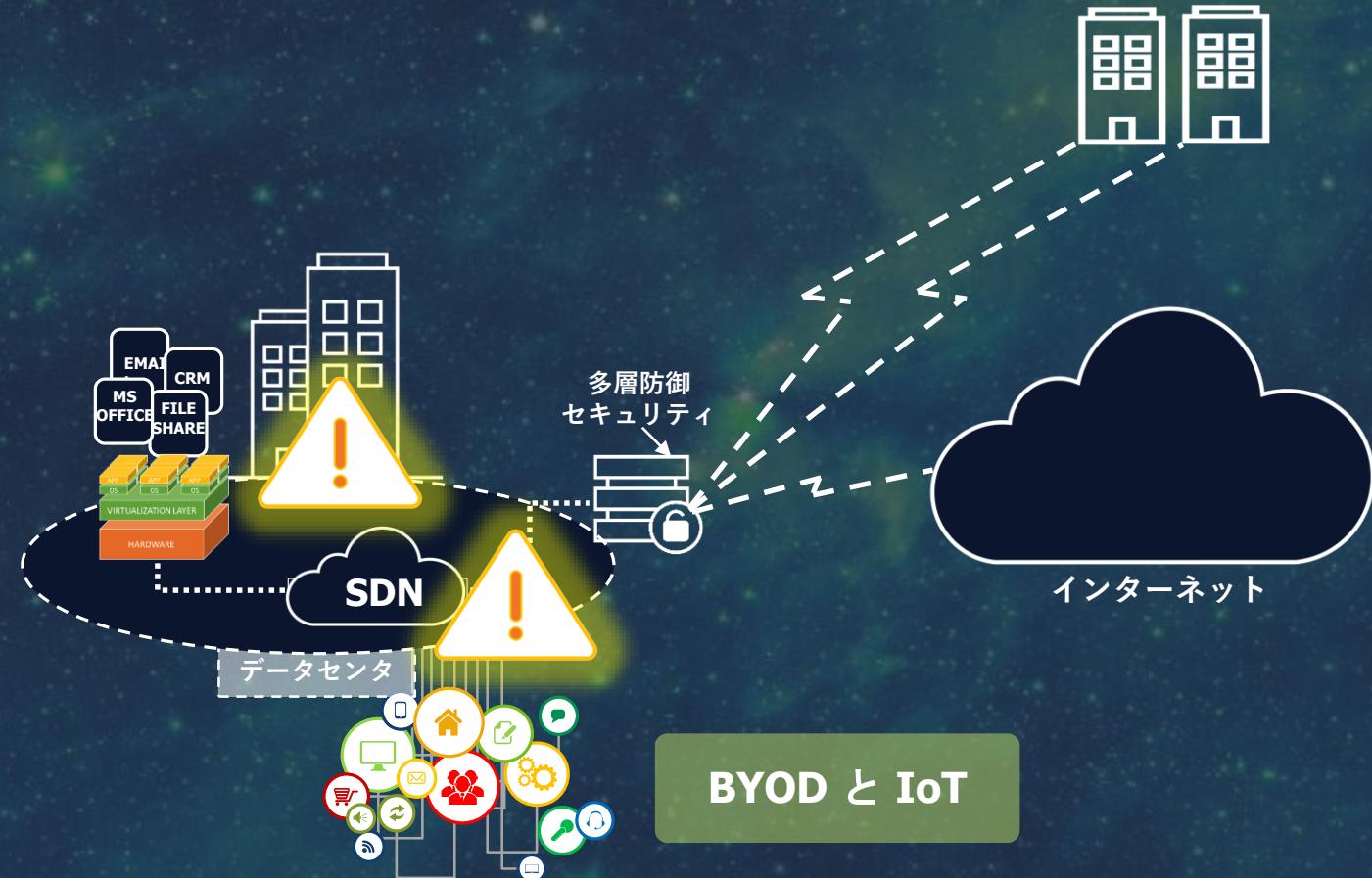
複雑さの増加～ネットワーキング



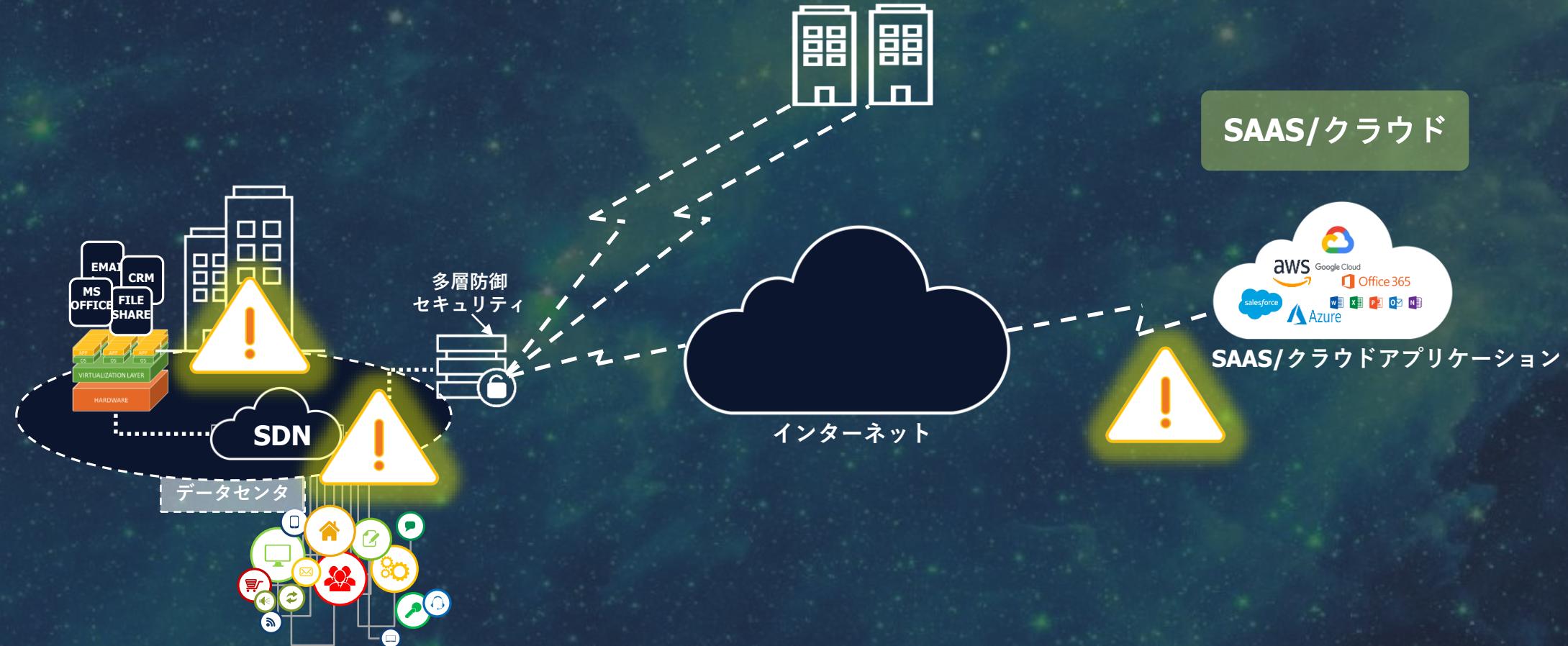
複雑さの増加～ネットワーキング



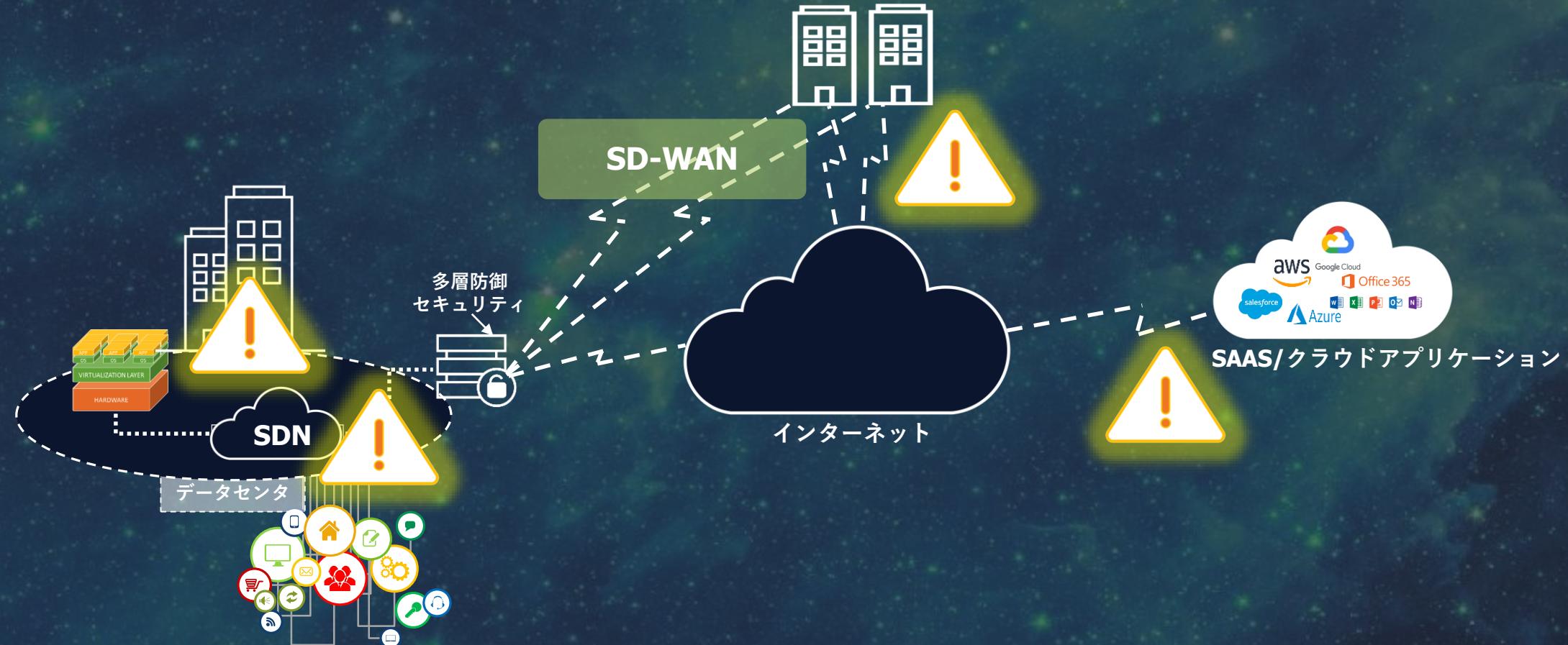
複雑さの増加～ネットワーキング



複雑さの増加～ネットワーキング

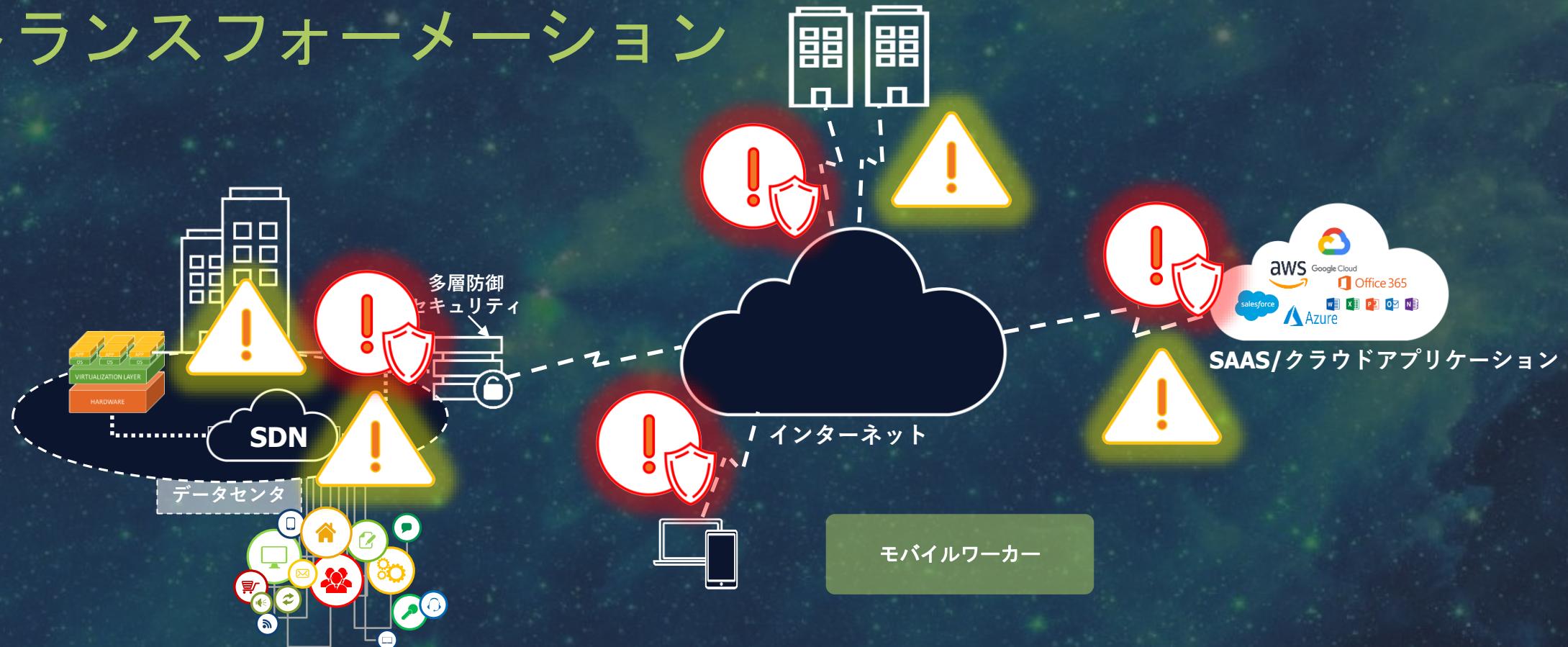


複雑さの増加～ネットワーキング



セキュリティへの影響

トランスマルチエーション



Addressing the challenges

ネットワークの課題

展開 - ハイブリッド＆マルチクラウドインフラ

可視化 - 全てのIT資産

管理 - 大規模化

自動化 - ITSM ワークフロー

セキュリティの課題

増加 - 攻撃対象ポイント

複雑化 - 脅威ランドスケープ

過負荷 - SOCチーム作業量の限界

脅威の検出 & 修復の大規模化



デジタルエコノミー: CIO/CTO/CISO の課題

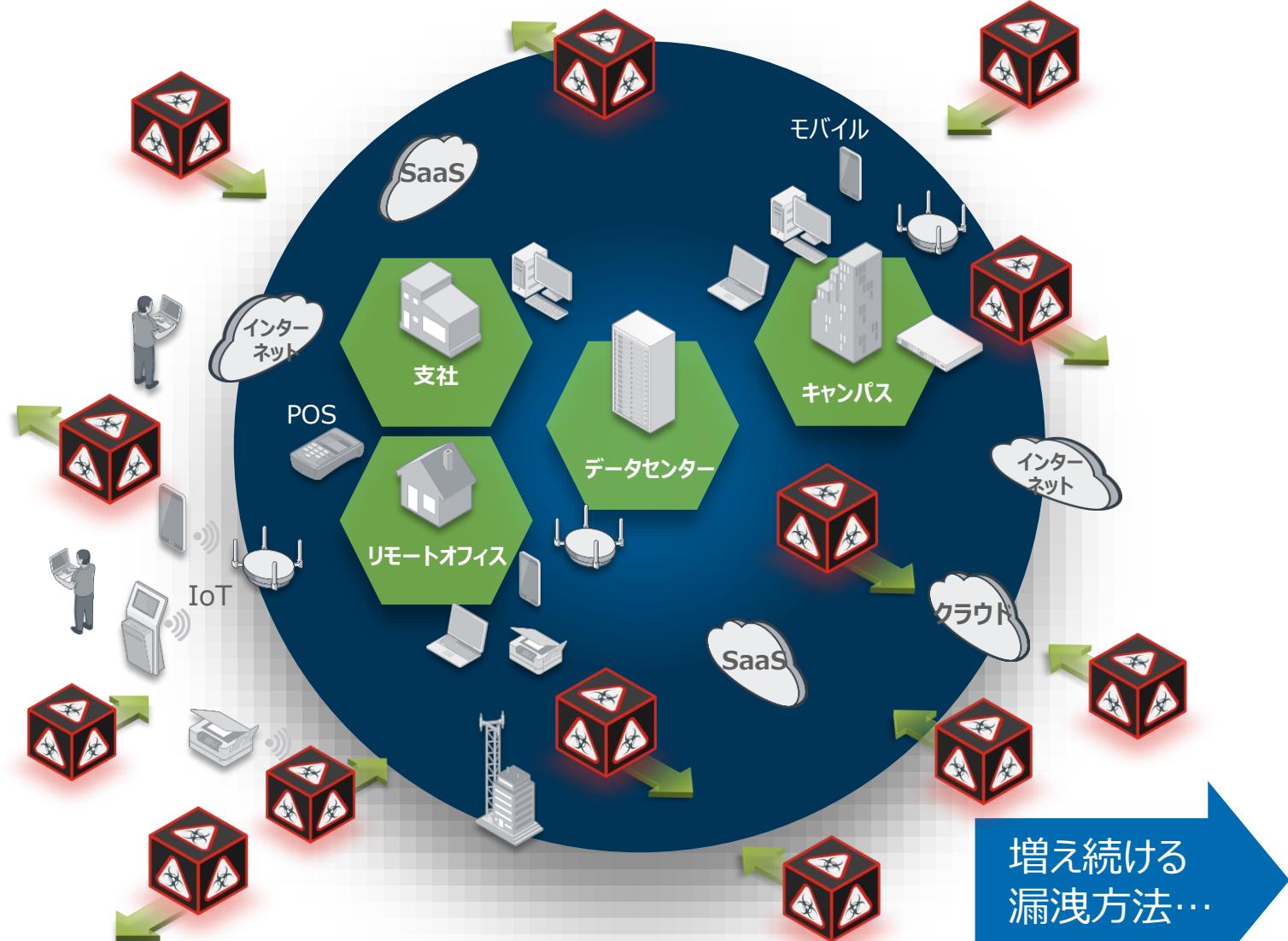


攻撃領域ポイントのボーダレス化 ~マルウェアはどこからでも企業内に

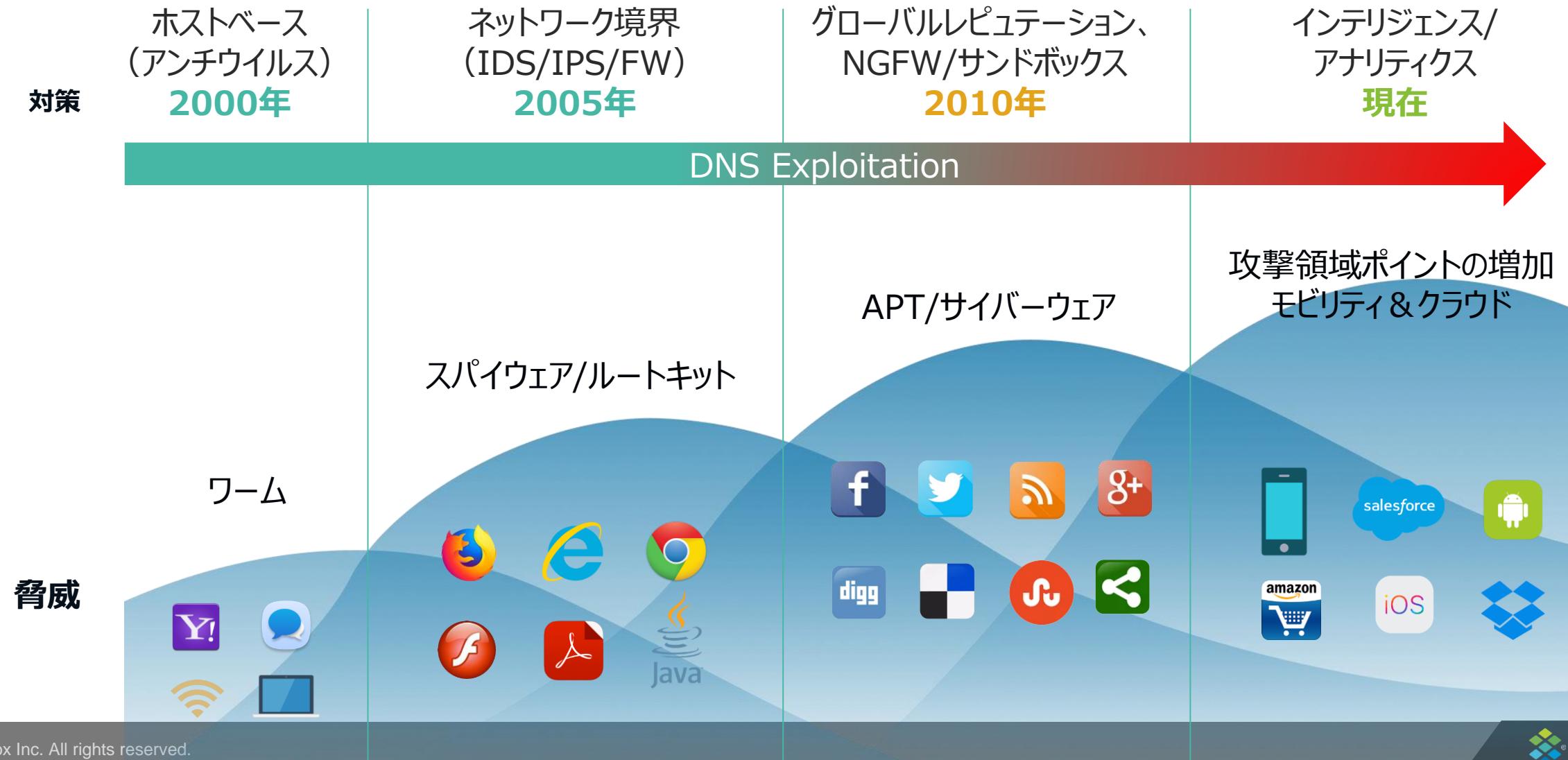
増え続ける
侵入方法…



全環境の唯一の共通項であるDNSは、
これら全てを一意に紐付け、
360度、全方位のビューを提供します。



脅威ランドスケープの進化



デジタルトランスフォーメーションには新たなパラダイムが必要

クラウドファースト エンタープライズ



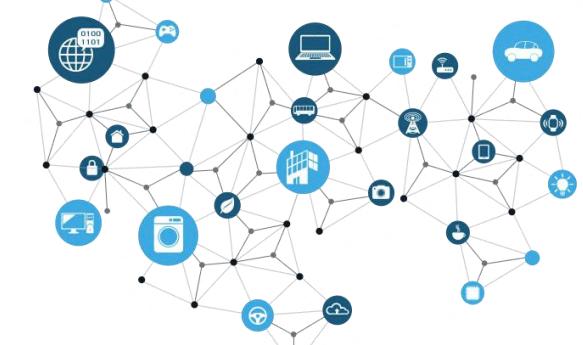
場所を問わずクラウドアプリケーションに
ダイレクトにアクセス

ソフトウェアディファインド ネットワーク



ポリシードリブンのネットワーク
仮想化されたネットワーク機能

BYOD、モビリティ、IoT

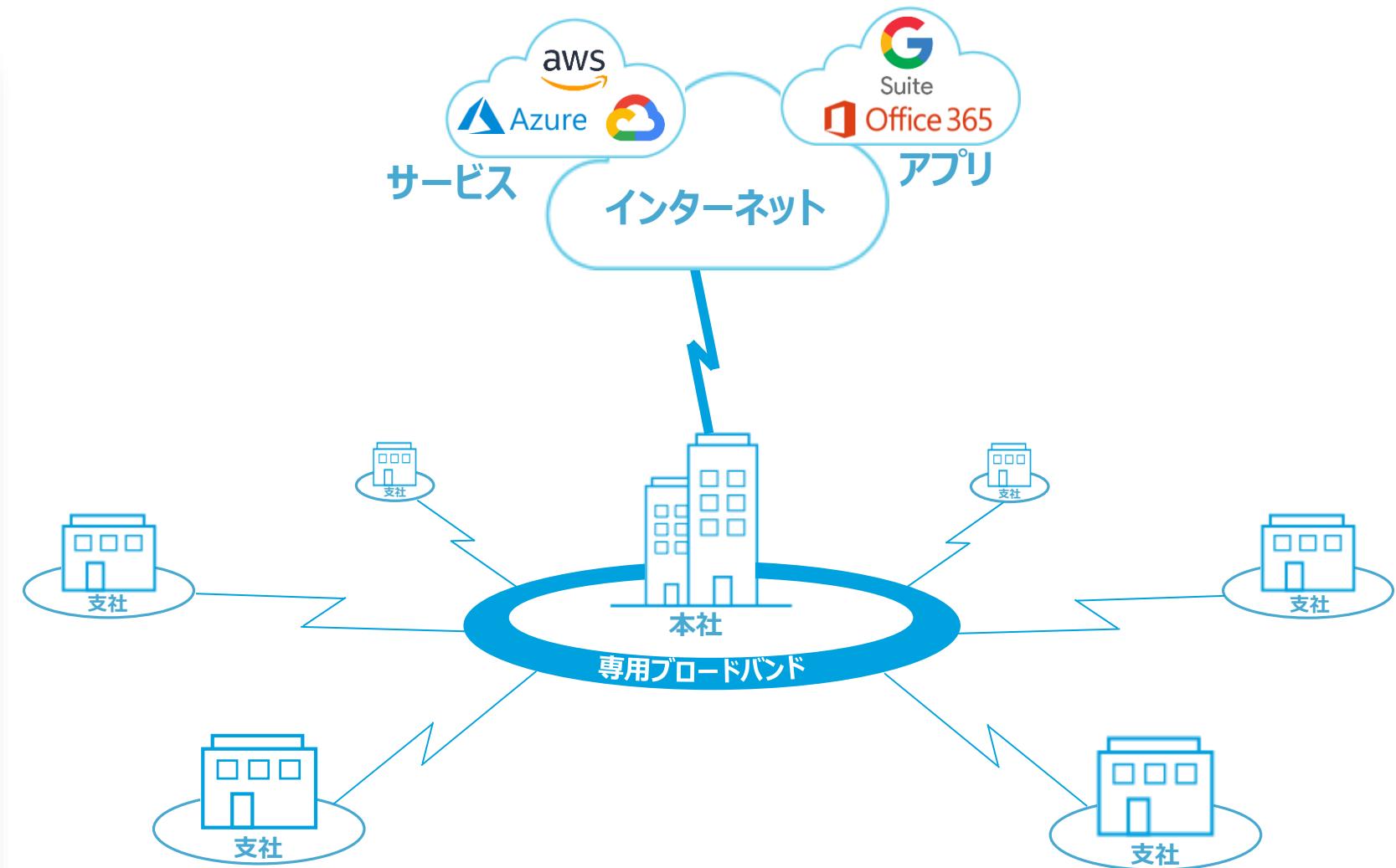


エンドポイントの爆発的な急増
スケーリングとセキュリティの課題

DNS、DHCP、IPAMは、パブリック/ハイブリッドクラウド環境、SD-WANブランチ、IoTのデプロイメントをセキュアなものにし、全資産の正確な可視性とともに、セキュリティ部門に対してフォレンジックデータを提供することができます。

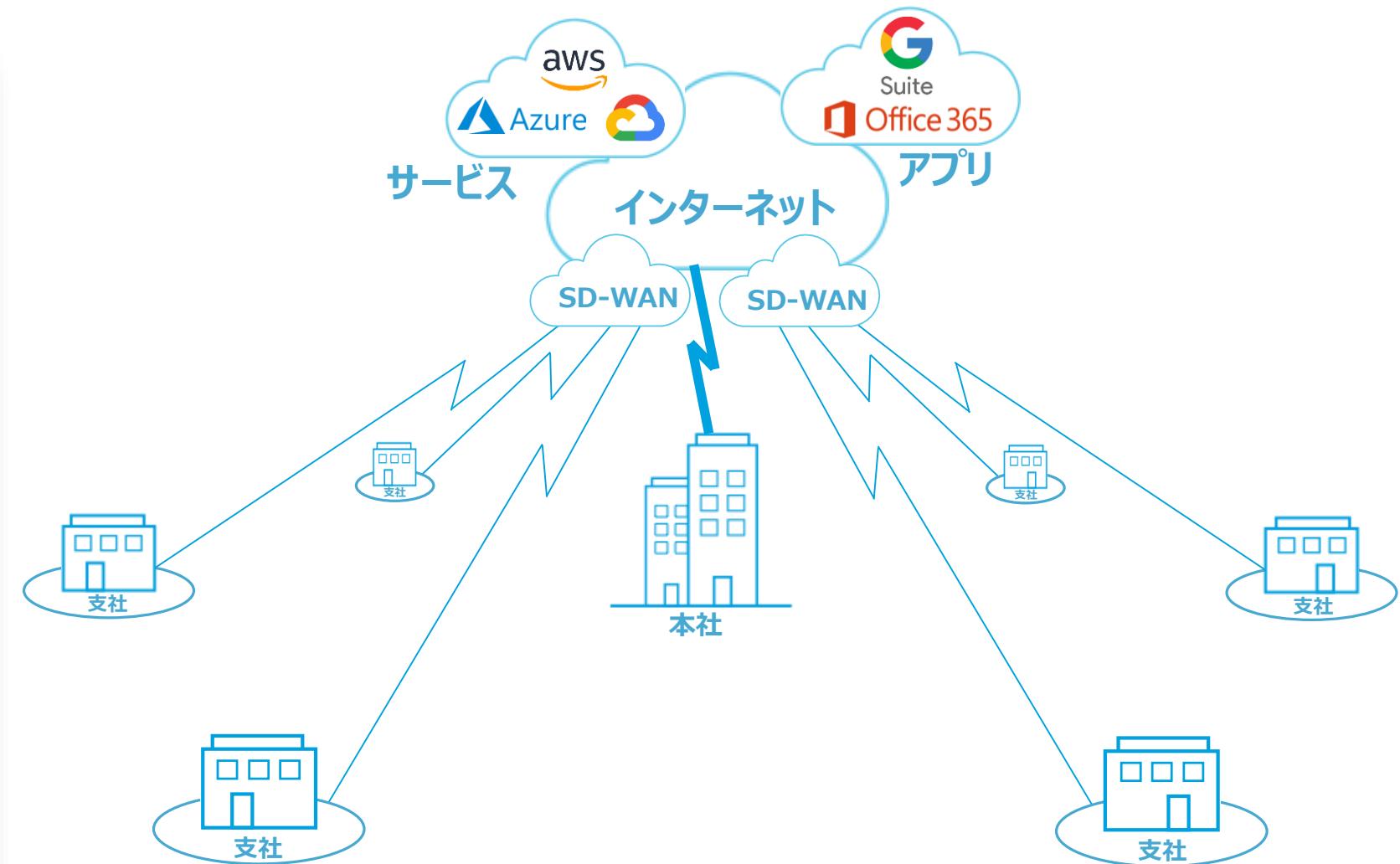
従来のアーキテクチャ

- 専用のWAN回線
- 手動による静的な構成
(DNS、DHCP)
- 自動化の欠落
- センター管理された境界ベース
のセキュリティ



新たなアーキテクチャ：クラウド、SaaS、SD-WAN

- ・リモート接続に SD-WANを活用
- ・分散化されたインフラ
- ・ユーザー エクスペリエンスを向上
- ・セキュリティ、可視性、管理を制御





ビジネスの基盤となる必須のサービス

DNS

DHCP

IPアドレス管理 (IPAM)

DDI



あらゆるアーキテクチャに対応したコア基盤要素

IPアドレス管理

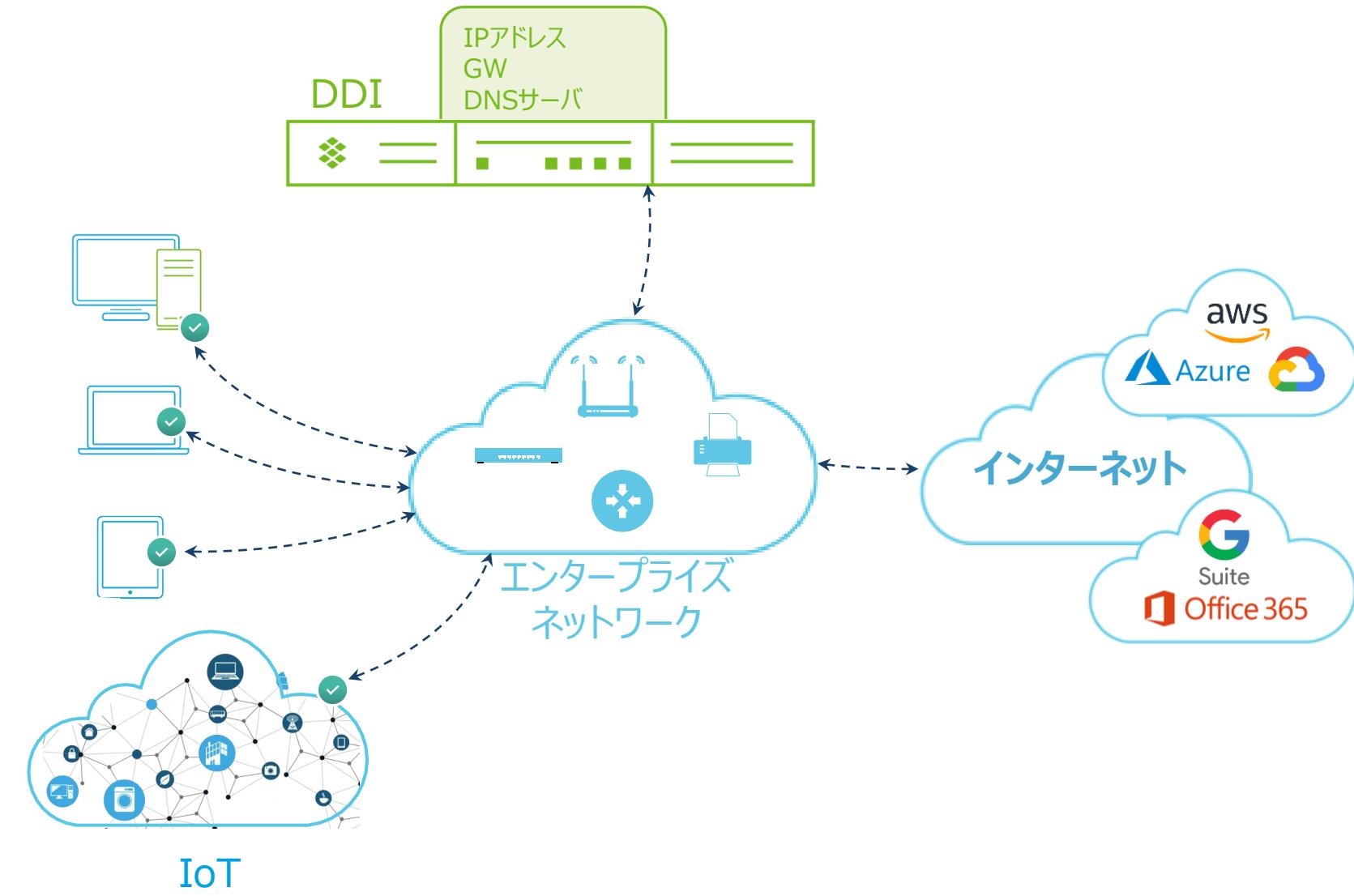
- ・デバイスのIPアドレス
- ・ネットワーク&デバイス情報
- ・一元管理
- ・ネットワークコンフリクトを解消

インターネット接続を提供

- ・DHCPにてネットワークにつながる環境の提供
- ・ネクストホップゲートウェイ
- ・DNSサーバロケーション
- ・サービス/宛先の検索にDNSを使用
- ・内部/外部システムをサポート

アセット管理とディスカバリ

- ・自動化されたデバイスディスカバリ
- ・物理/仮想ネットワークアセットの権威インベントリ



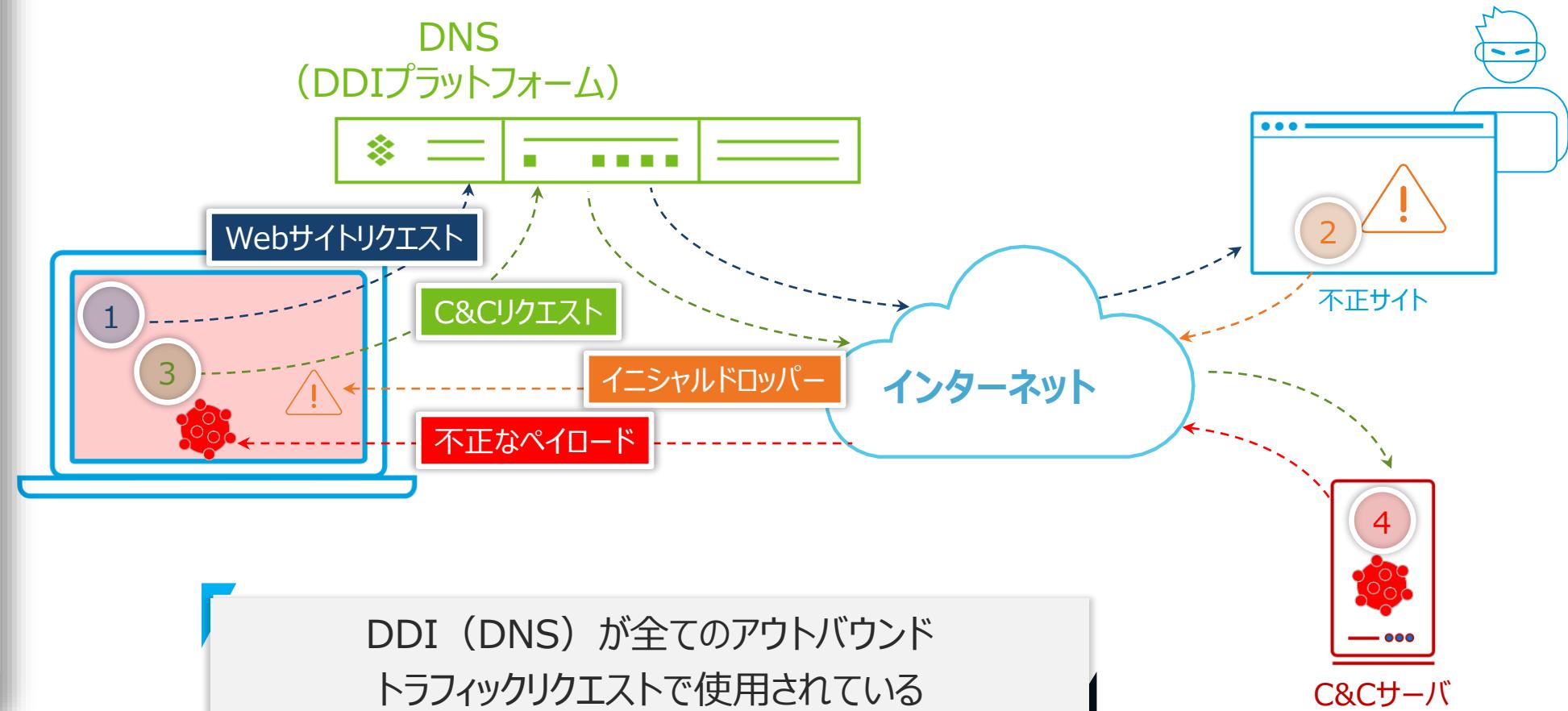


1. エンタープライズセキュリティにDDIを活用



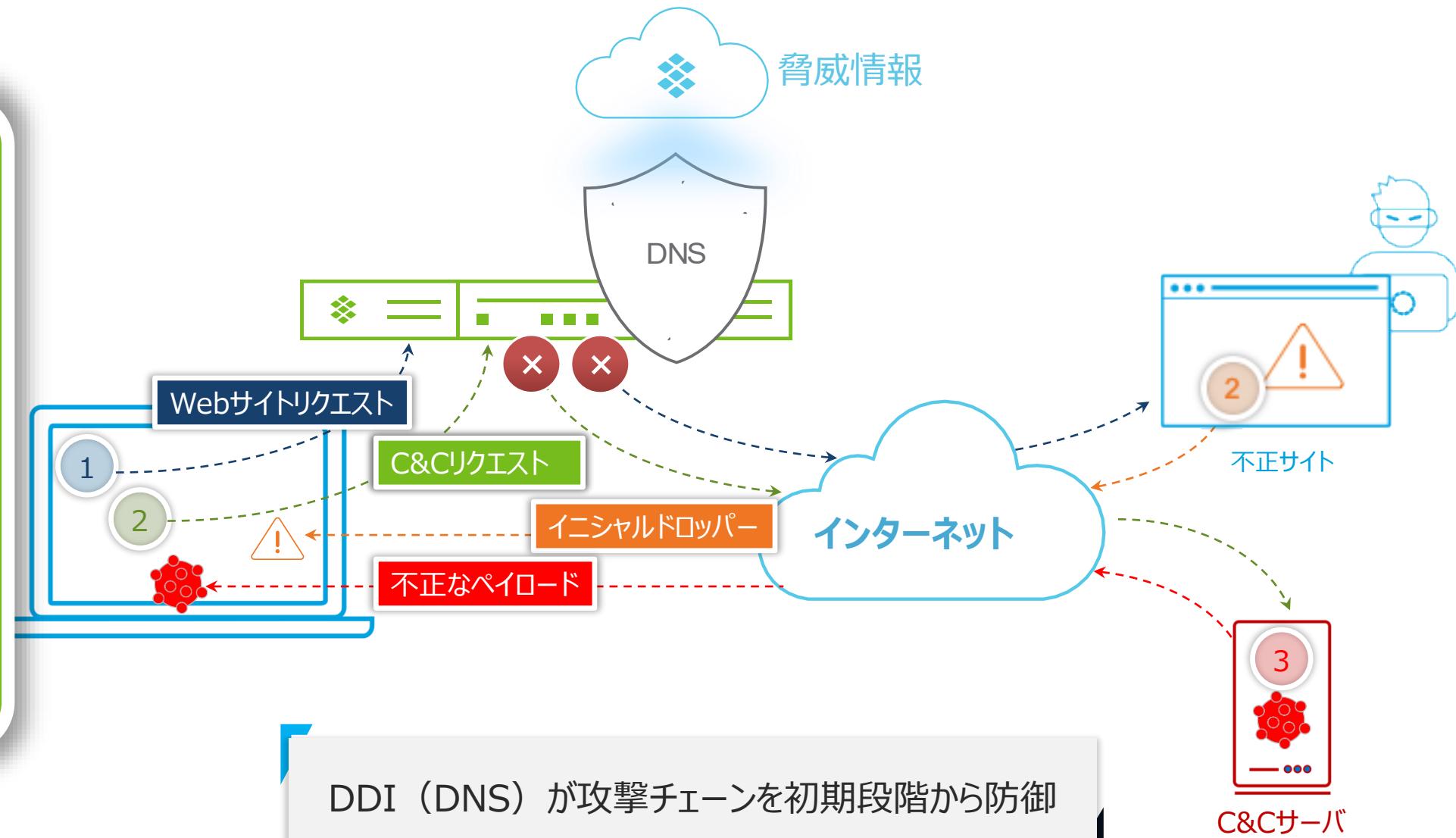
一般的な攻撃のステップ

1. ユーザーを不正サイトに誘導
2. Webサイトからイニシャルエクスプロイトを送信
3. エクスプロイトがC&Cサーバと通信
4. 不正なペイロードをダウンロード



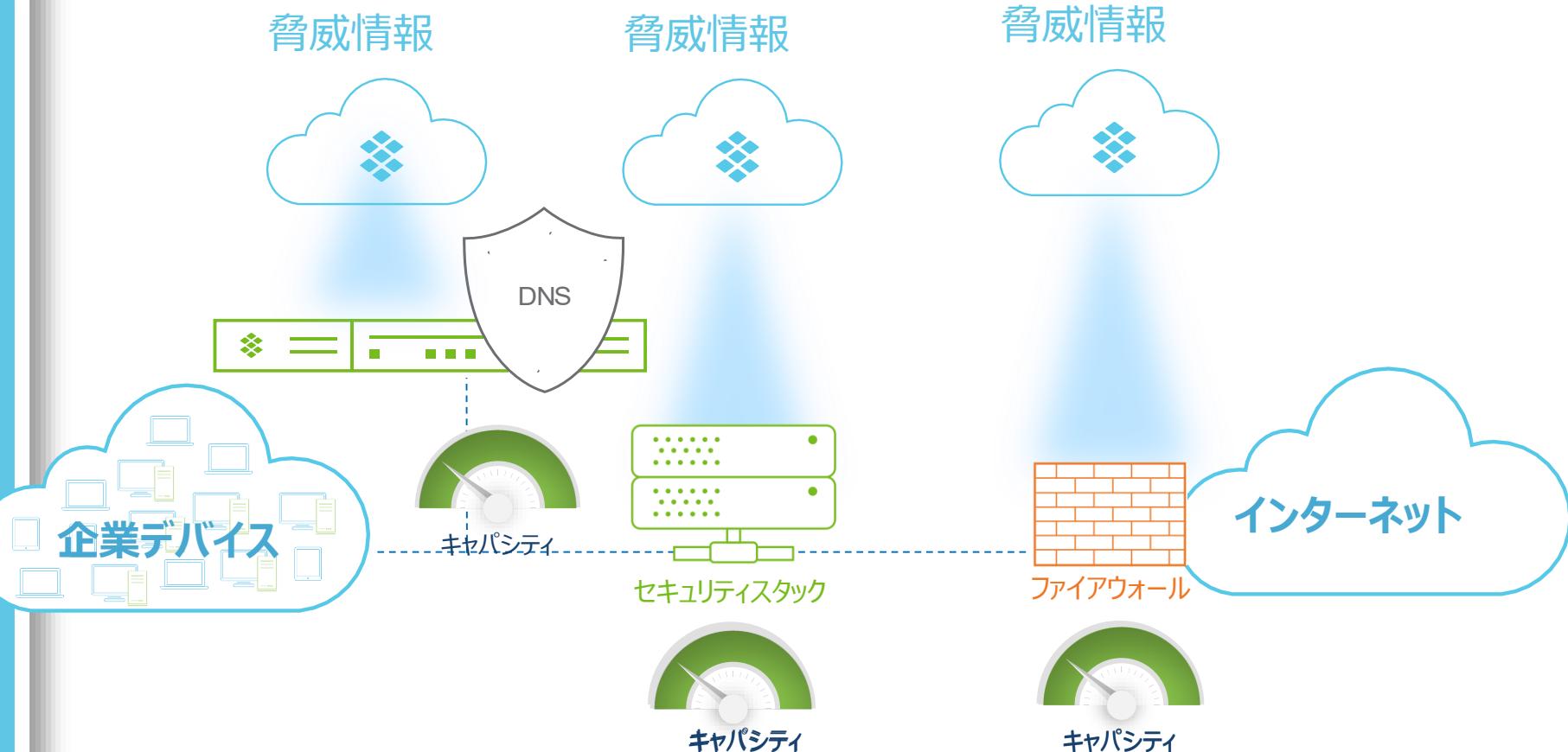
セキュリティ基盤にDDIを活用

1. DNS向けに精選された脅威情報
2. 不正サイトへの接続をDNSで防御
3. 感染した場合、C&Cサーバへの接続をDNSで防御



DNSを活用したセキュリティアプローチのメリット

1. ファイアウォールのフィルタリングは貴重な処理能力を消費している
2. セキュリティスタックのフィルタリングは不要なリソースを消費している
3. DNSは膨大なデステイネーションを参照するように設計されている



実行能力の拡張でインフラを最適化

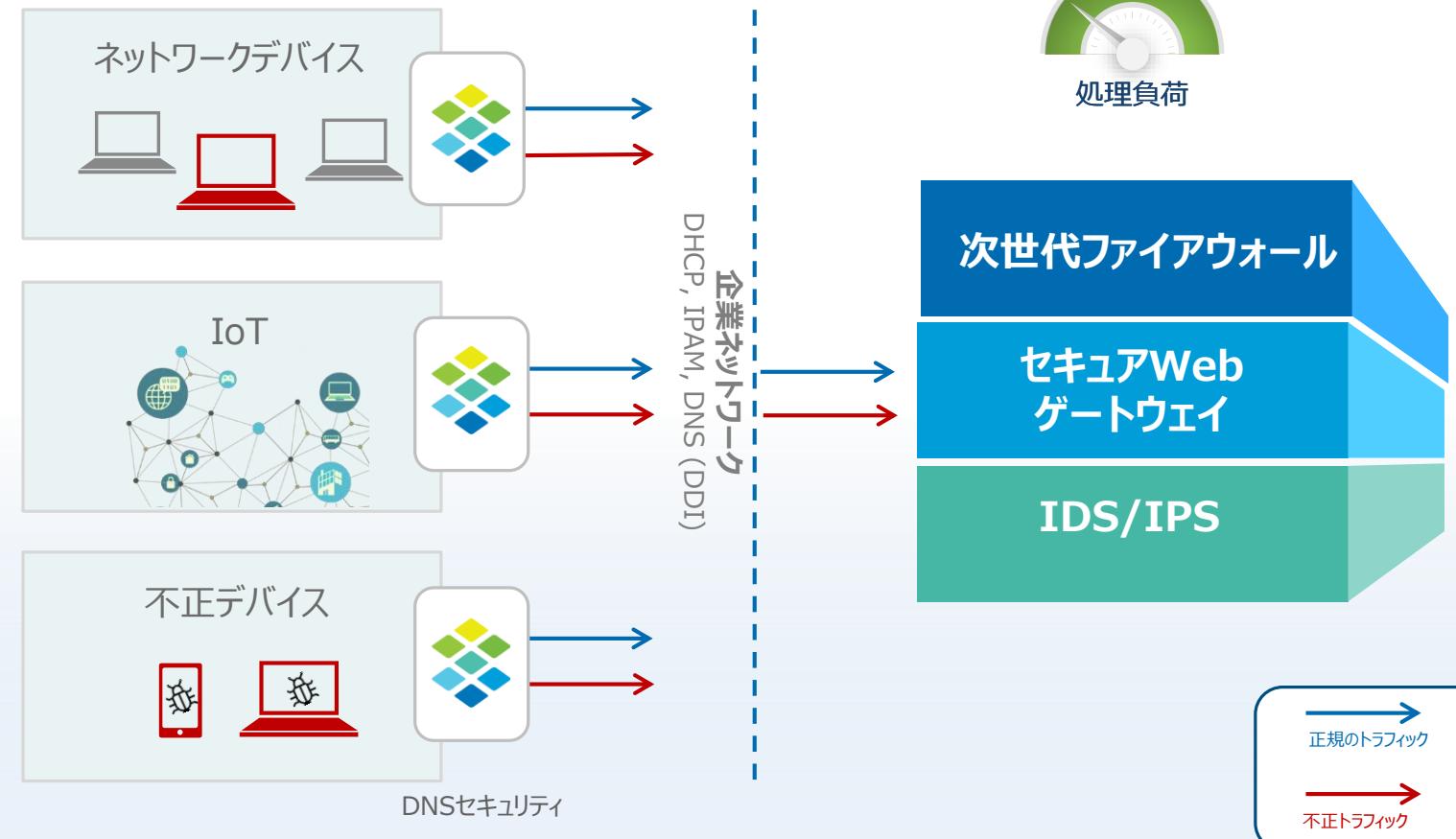
全方位のセキュリティを保全

スケーラビリティを確保

- 既知の攻撃・脅威に対するブロッキングのオフロード
- NGFW、SWG、IDS/IPSへの「ジャンク」トラフィックの削減
- セキュリティ境界の処理能力を保全
- ロギング容量をも軽減させ、セキュリティオペレーション業務改善への貢献

全てのデバイスを保護

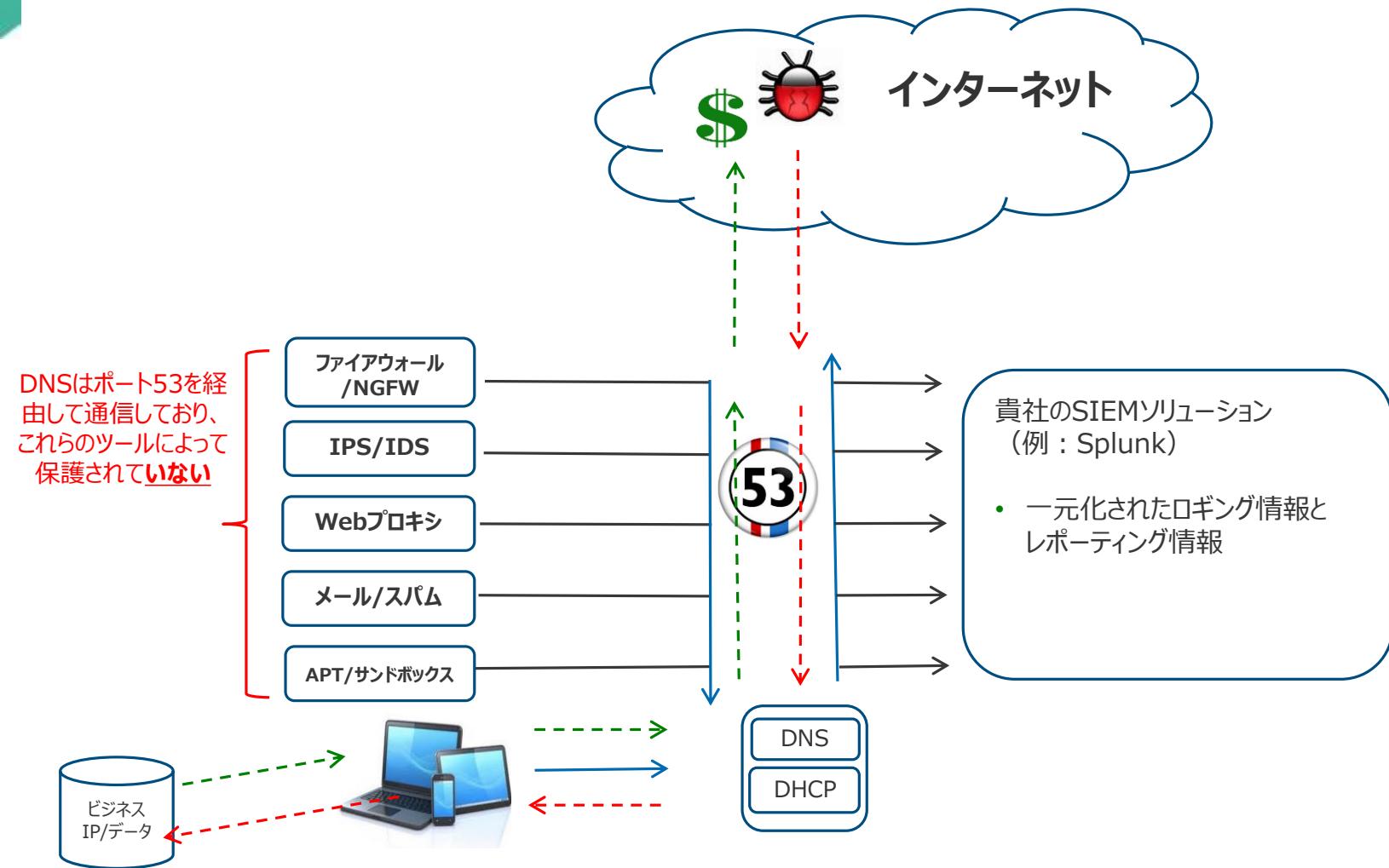
- DHCP、IPAM、DNSの基盤
- 広範に保護
 - 全ての企業デバイス
 - 全てのIoTデバイス
 - 不正デバイス





2. DNSセキュリティでプロテクションのギャップを解消

DNSの脅威とは何か？



AN AVERAGE DAY IN AN ENTERPRISE ORGANIZATION

Every **1 min** a host accesses a malicious website

Every **3 mins** a bot is communicating with its command and control center

Every **9 mins** a High Risk application is being used

Every **10 mins** a known malware is being downloaded

Every **27 mins** an unknown malware is being downloaded

Every **49 mins** sensitive data is sent outside the organization

Every **24h** a host is infected with a bot



DNSベースの脅威を防ぐとは？



レピュテーション (ブラックリスト)

マルウェア、C&Cサーバ、ランサム
ウェアの通信を検知し防御

米英両国政府はじめ、主要政府機
関で利用されている自前脅威情報

エコシステム、複数他社脅威情報
の統合



シグネチャ (DPIルール)

ビジネスに重要なコアインフラ
サービスのインフラ保護

キャリアレベルの詳細なDPI
(ディープパケットインスペクション)

典型的な既知トンネリングツールの
即時識別、プロトコル攻撃から保護

01100
10110

リアルタイムAI (AI機械学習)

特許取得済みの
リアルタイムデータ分析

情報漏洩の検知と阻止

DGA, Fast Flux, ホワイトリスト,
ファイルレス・マルウェア,
未知0-Day攻撃の検知



脅威情報（DNS専用）+ アナリティクス=高度な脅威検知

✓ 振舞いモデル – リアルタイム機械学習ベースの統合解析により以下を検知 :

- DNSを利用した情報漏洩
- DGA、Fast Flux、ホワイトリスク
- ファイルレスマルウェア、ゼロデイ

✓ 高精度のIOC

- 広範なIOC収集ネットワーク
- リバースエンジニアリング、ハンティング
- 高精度のスコアリングアルゴリズム
- 最新のマルウェアに対する保護 – ランサムウェア、マルウェアC&C、フィッシング、エクスプロイトキット、APT

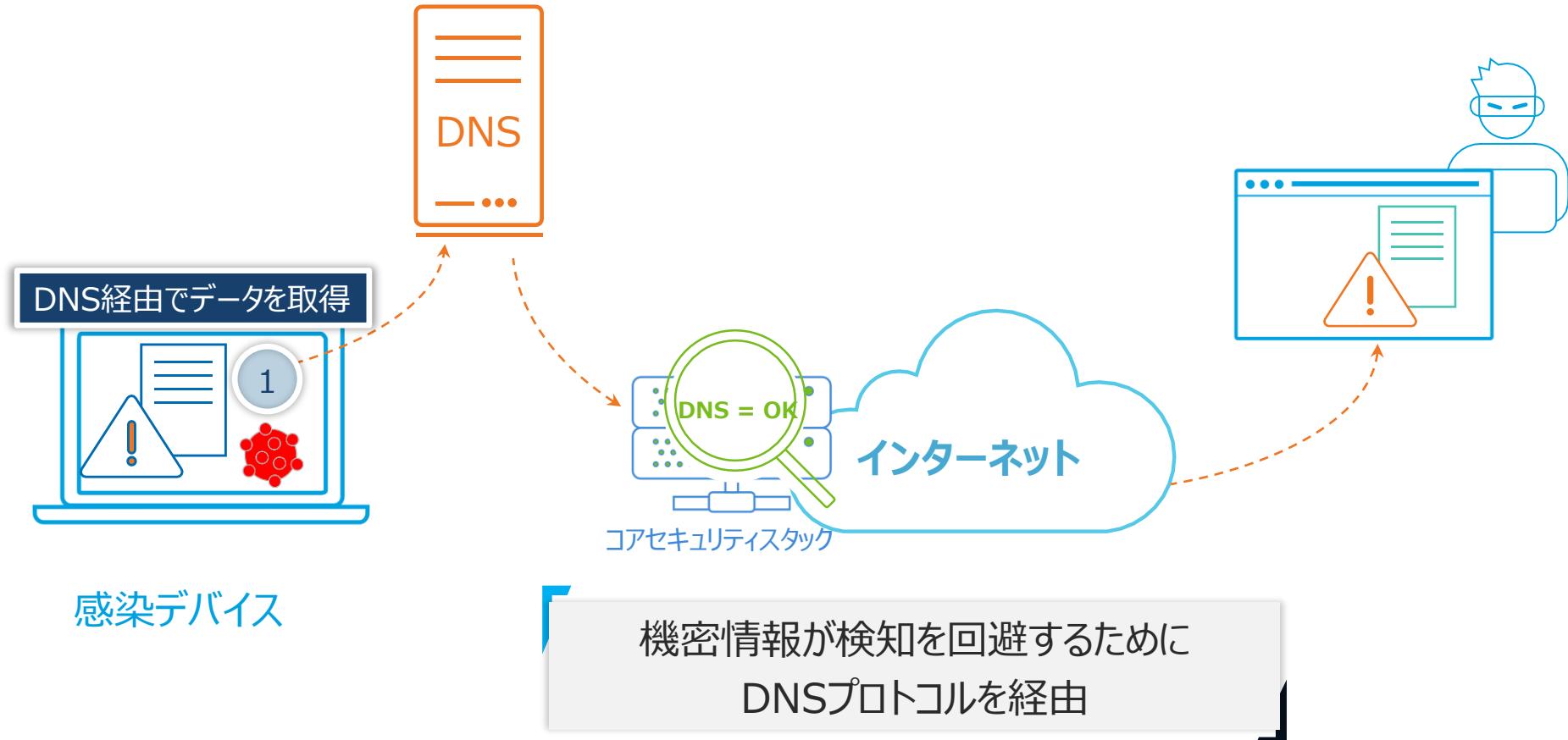
✓ DNS攻撃シグニチャ

- プロトコル攻撃からネームサービスを保護
- プロトコルのミス構成を保護



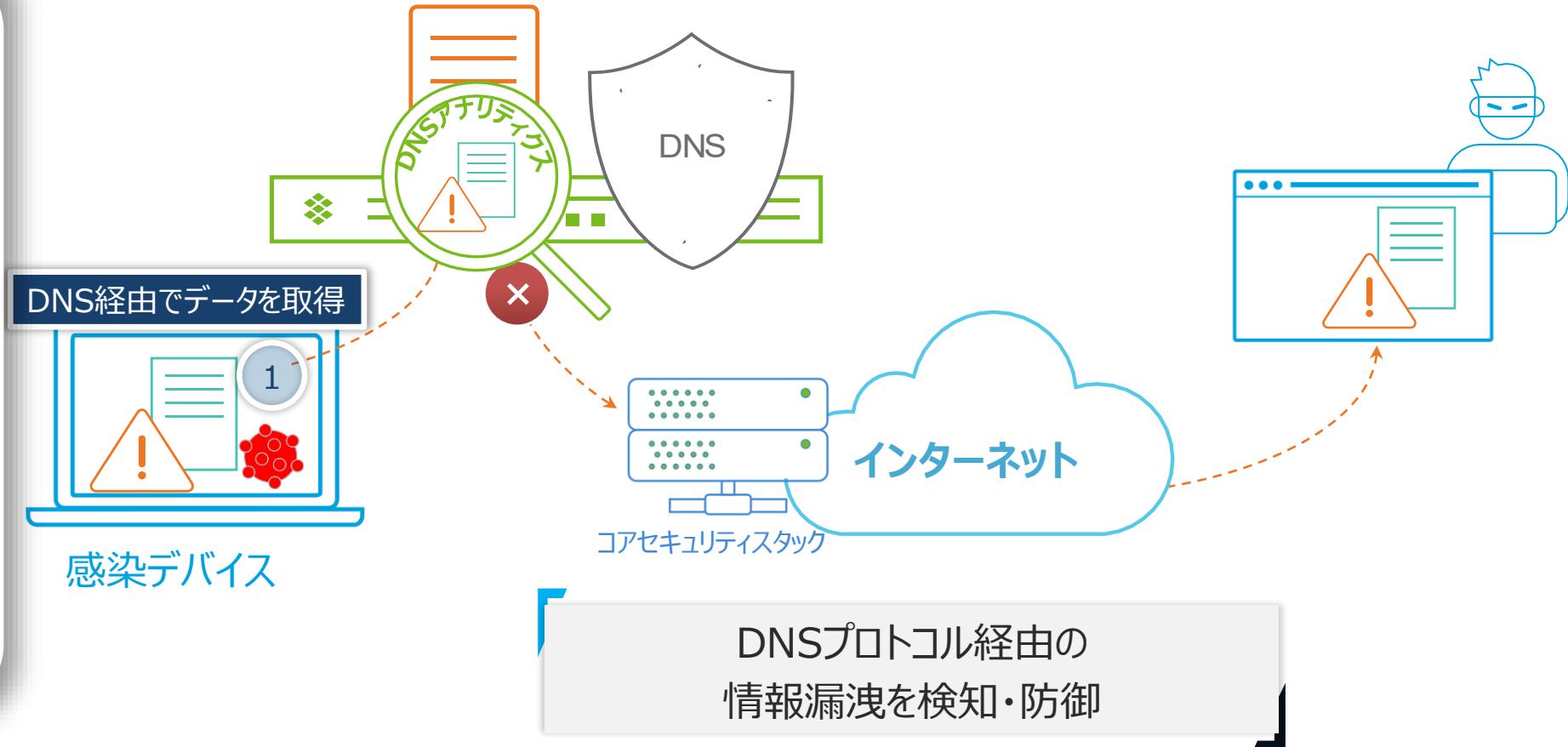
DNSを利用した情報漏洩

1. デバイス上のマルウェアが機密データを検索
2. マルウェアがDNS経由でデータを送信
3. 従来のセキュリティはDNSトラフィックを“検査しない”



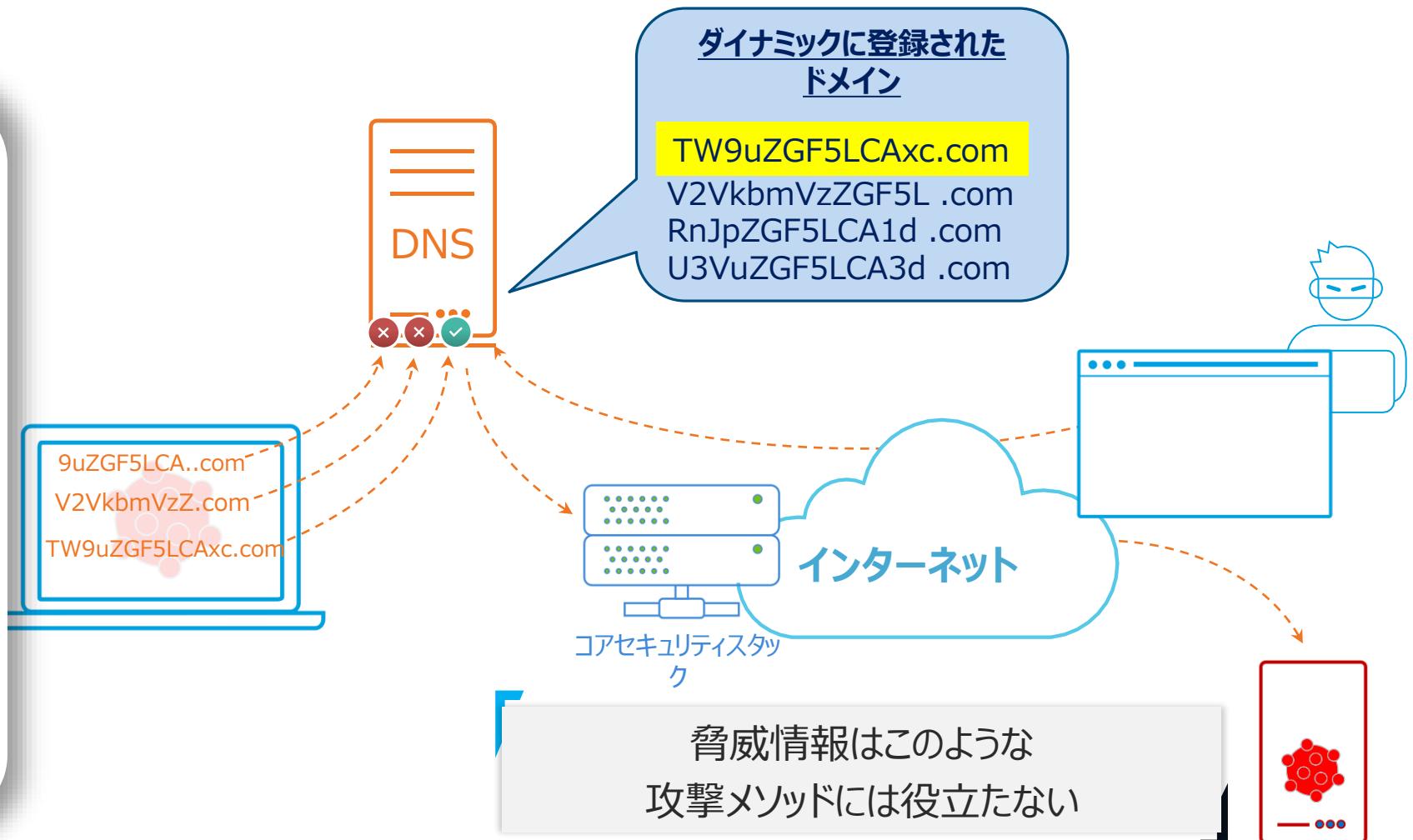
DNSを利用した情報漏洩を防止

- 脅威情報とアナリティクスを備えたDNS
- 機械学習のアナリティクスでDNSトラフィックをリアルタイムに検査し、情報漏洩を検知
- デスティネーションへのDNSリクエストを防御することでデータの流出を防止



ダイナミックにドメインを生成

1. 攻撃者がダイナミックなドメイン作成のアルゴリズムを使用
2. マルウェアも同様のアルゴリズムでC&Cサーバを「検索」
3. 生成されたドメインによりマルウェアとデスティネーションが接続

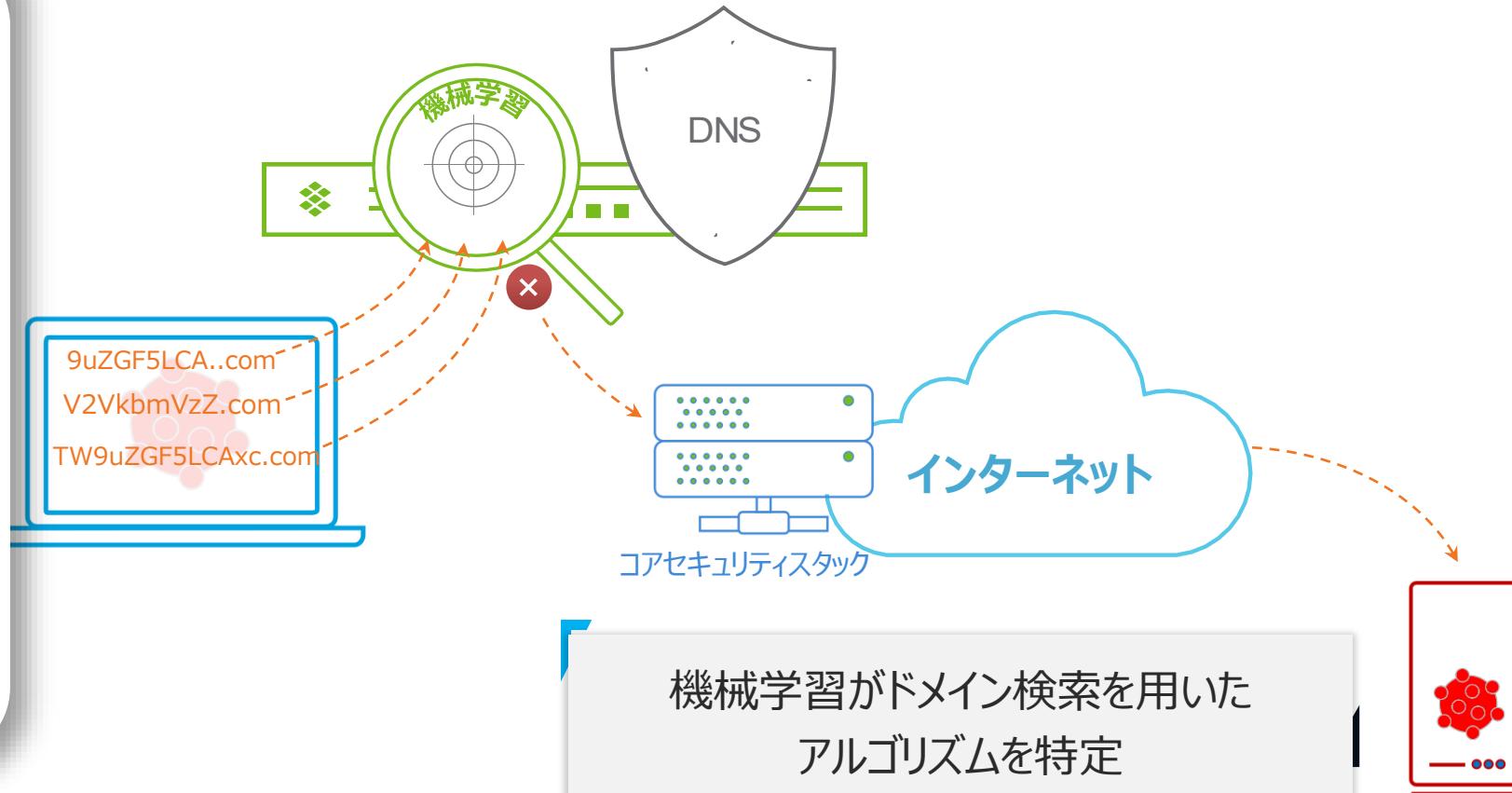


TW9uZGF5LCAxc.com



ダイナミックにドメインを生成

1. 機械学習のアナリティクスでDNSクエリをリアルタイムにて検査
2. DGAメソッドを用いたパターンを特定
3. 同様のパターンを用いた一連の接続を防御

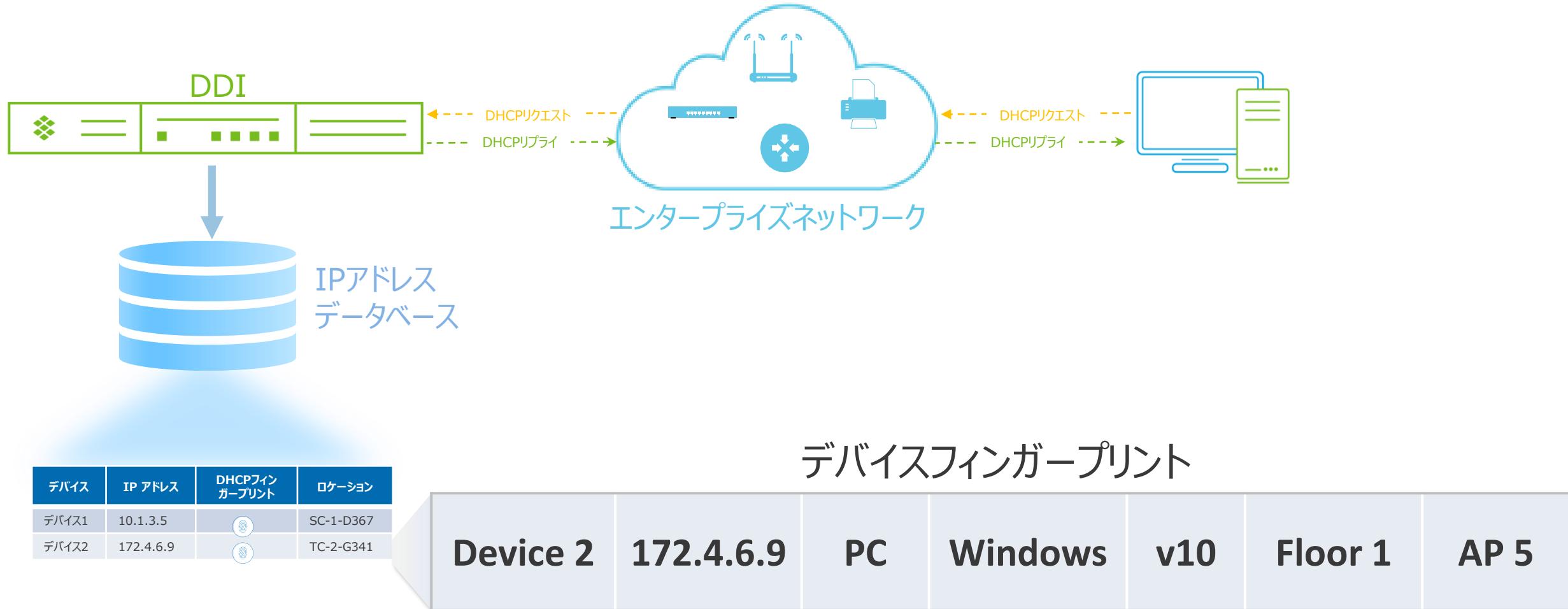


TW9uZGF5LCAxc.com



3. インシデントレスポンスにDDIを活用

DDIでデバイスデータを収集



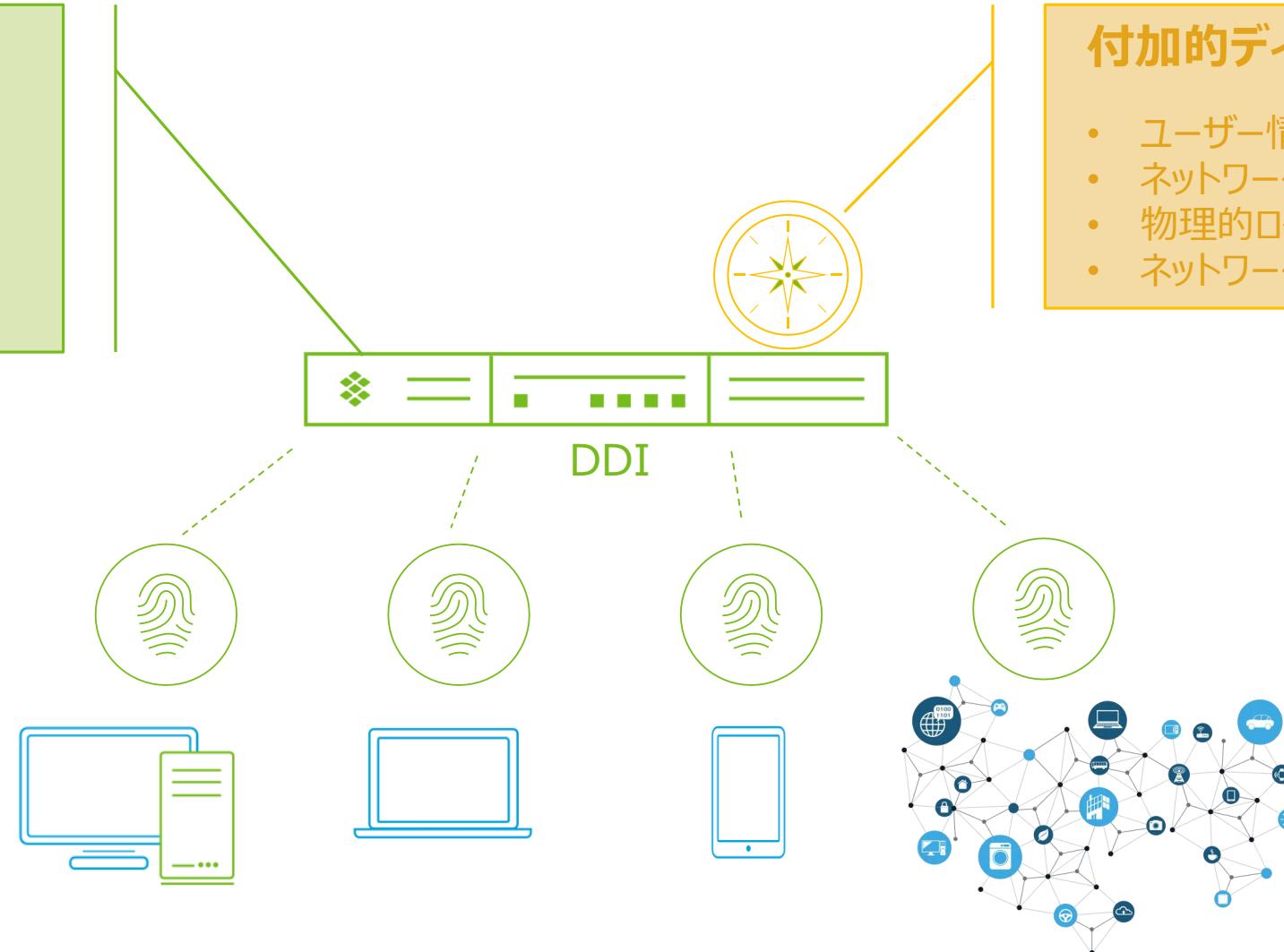
インフラストラクチャ全体のDDIフィンガープリント

DHCPディスカバリ

- MACアドレス
- デバイスタイプ
- OS情報
- 既存IP
- 以前のIPとロケーション

付加的ディスカバリ

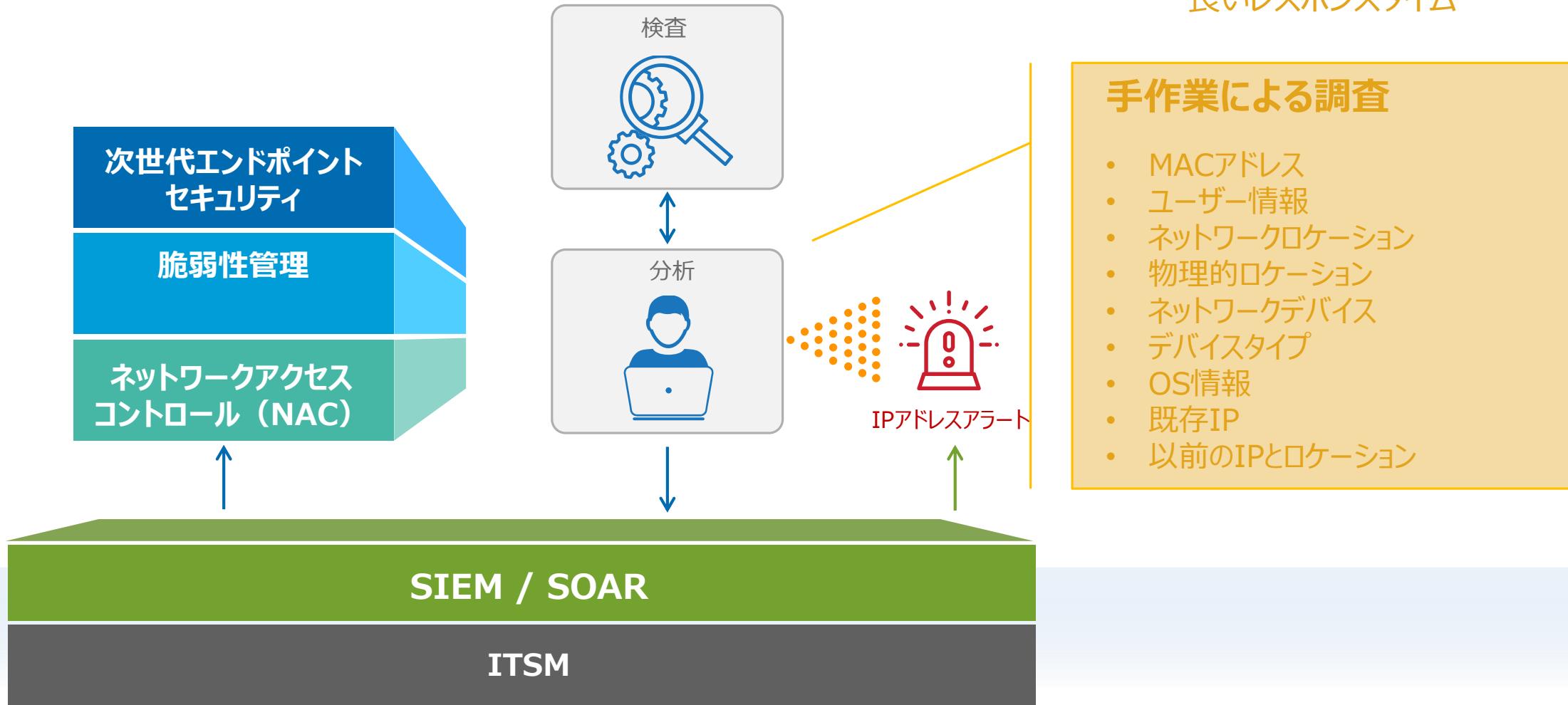
- ユーザー情報
- ネットワーククロケーション
- 物理的ロケーション
- ネットワークデバイス



典型的なインシデントレスポンス



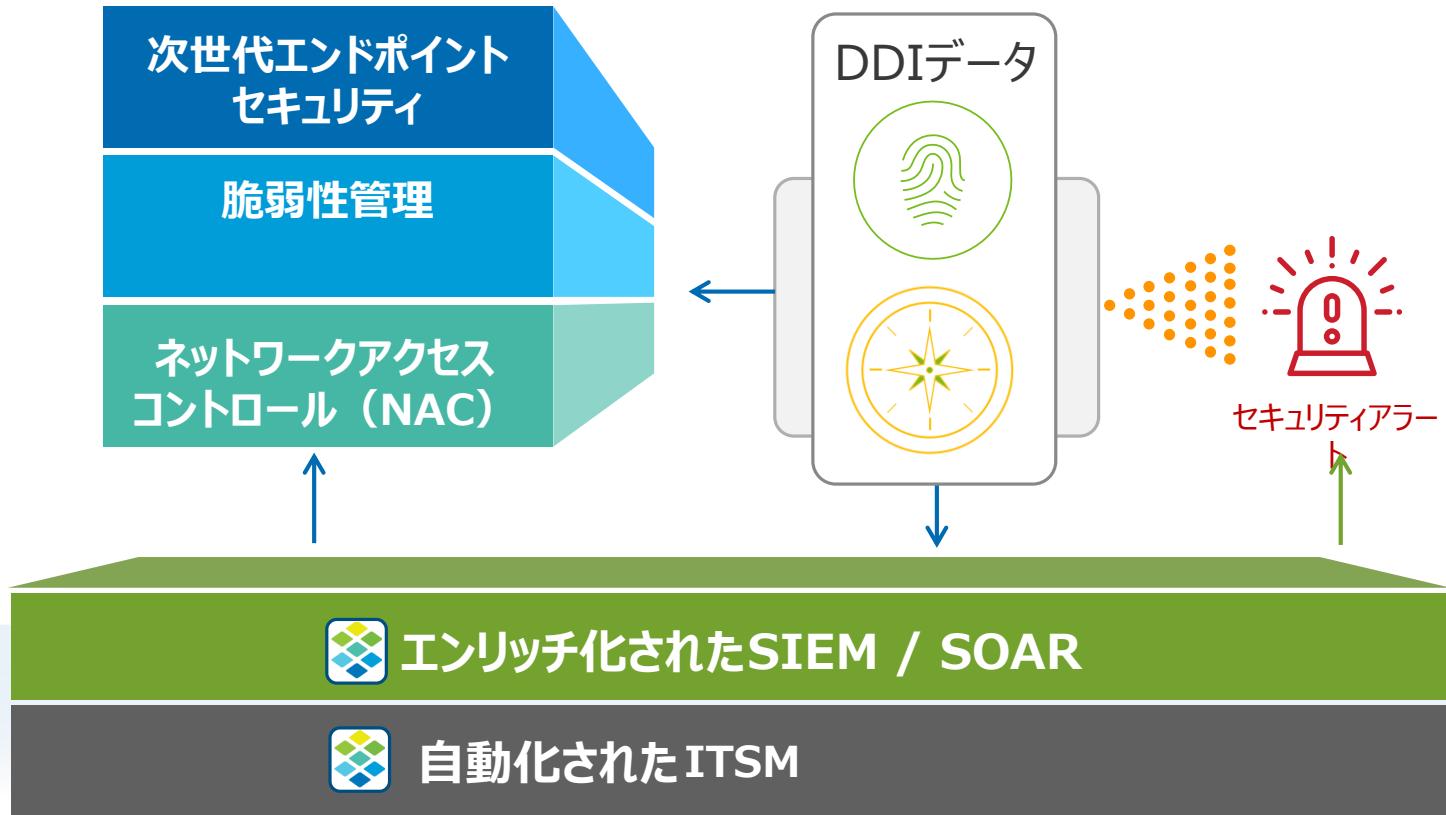
長いレスポンスタイム



DDIデータによりインシデントレスポンスタイムを短縮



レスポンスタイムを短縮



DHCP

- デバイスの監査ログとフィンガープリント
- デバイス情報、MAC、リース履歴

IPAM

- プリケーションとビジネスコンテキスト
- 拡張された属性による「メタデータ」：オーナー、アプリ、セキュリティレベル、ロケーション、チケットナンバー
 - 正確なリスクアセスメントとイベントの優先順位付けに役立つコンテキスト

DNS

- セキュリティ境界内の不正な活動
- BYODとIoTデバイスにも対応
- デバイスとユーザー活動をプロファイリング



BloxOne™ Threat Defense のご紹介

～ ディジタルトランスフォーメーションのためのセキュリティーアーキテクチャ



BloxOne™ Threat Defense

脅威情報データ共有 プラットフォーム (TIDE : タイド)

- 脅威情報
 - Infoblox
 - ビジネスパートナー
 - オープンソース
 - カスタム
- 情報内容：
 - C&C IP
 - フィッシングURL
 - マルウェアURL
 - C&C/マルウェアホスト/ドメイン
 - Webサイトカテゴリ



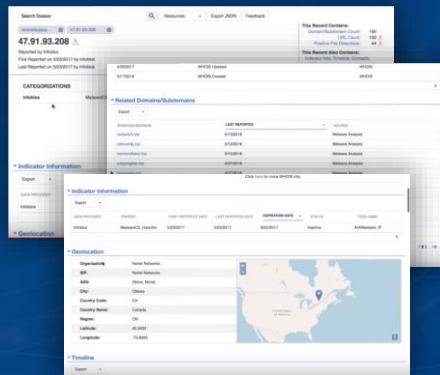
レスポンスピリシーゾーン/DNSファイアウォール

- アクティブDNSプロテクション
- 通信防御
- DNSシンクホール
- ランディングページ/
ウォールドガーデンにリダイレクト



Dossier (ドシエ)

- 脅威検索ツール
- コンテキスト情報
- **Dossierに含まれるもの：**
 - 履歴
 - 登録
 - レピュテーション
 - インフラストラクチャリレーション

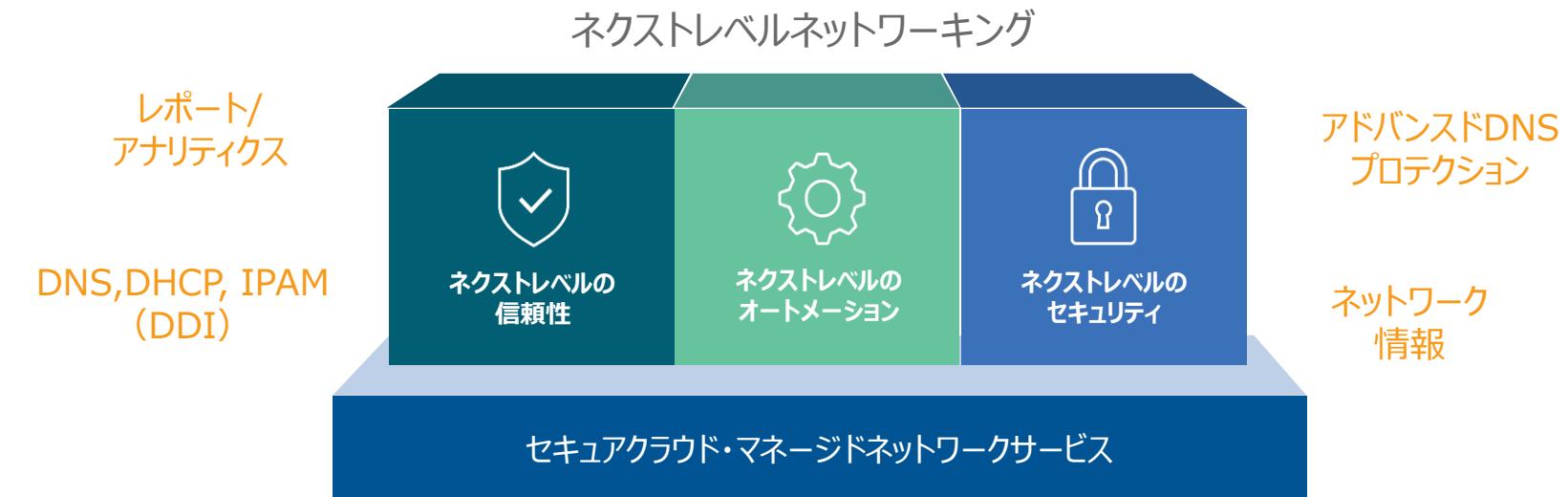


Ecosystem

- パートナーソリューションとの連携（脅威情報、検知情報、DDI情報）
- データ共有の自動化



BloxOne™ Threat Defense



デプロイオプション – オンプレミス

Infoblox DDIプラットフォーム

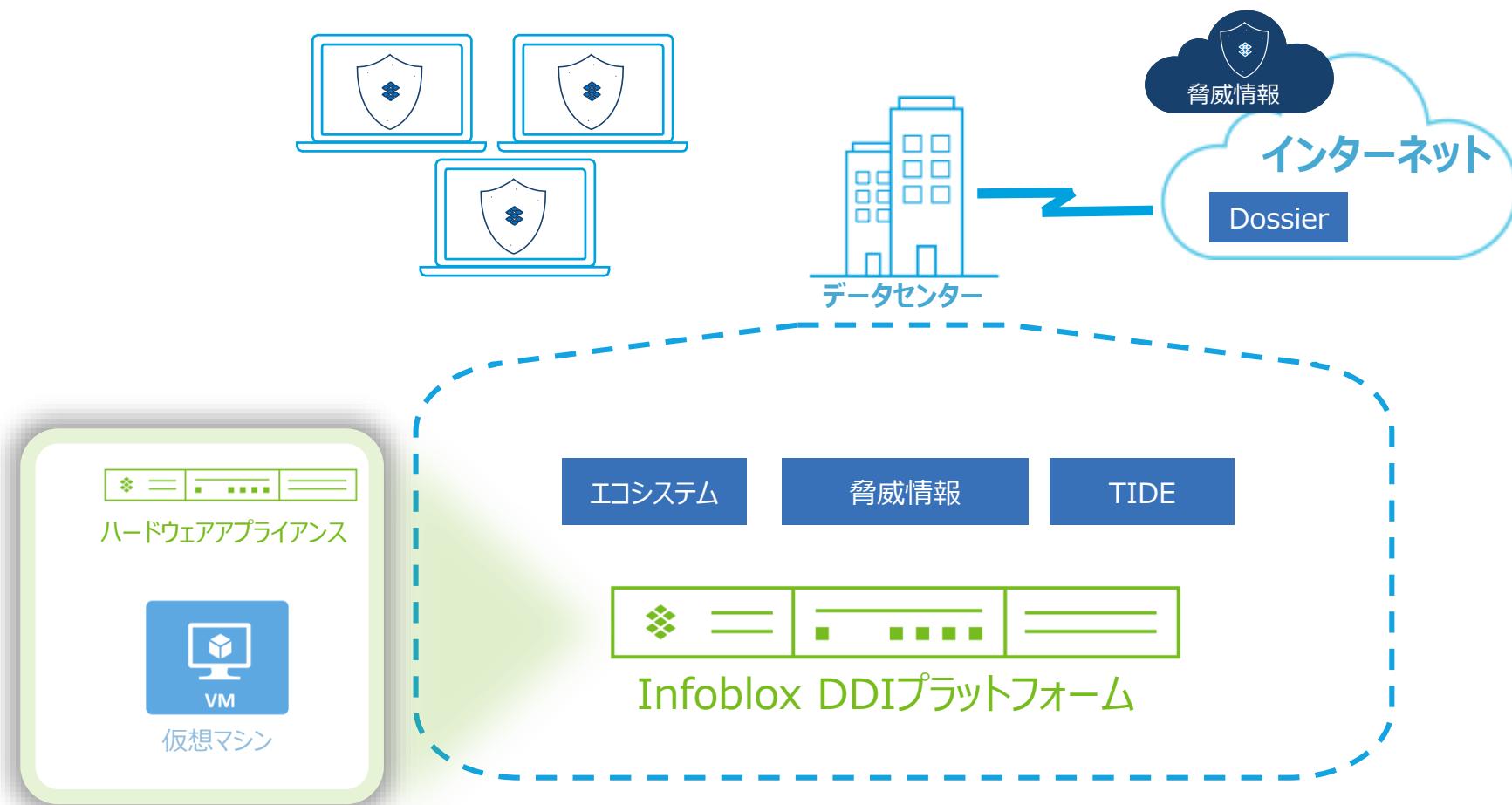
- オンプレミスによるデプロイ
• 物理アプライアンス
• 仮想アプライアンス

BloxOne Threat Defense – モジュール

- DNS専用の脅威情報
- Dossier
- エコシステム連携API
- オンプレミスおよび/またはコンテナベースのプラットフォーム上で提供されるクラウド

BloxOne Threat Defense – クライアント

- リモートデバイス情報をThreat Defense Cloudに転送



デプロイオプション – ハイブリッド

Infoblox DDIプラットフォーム

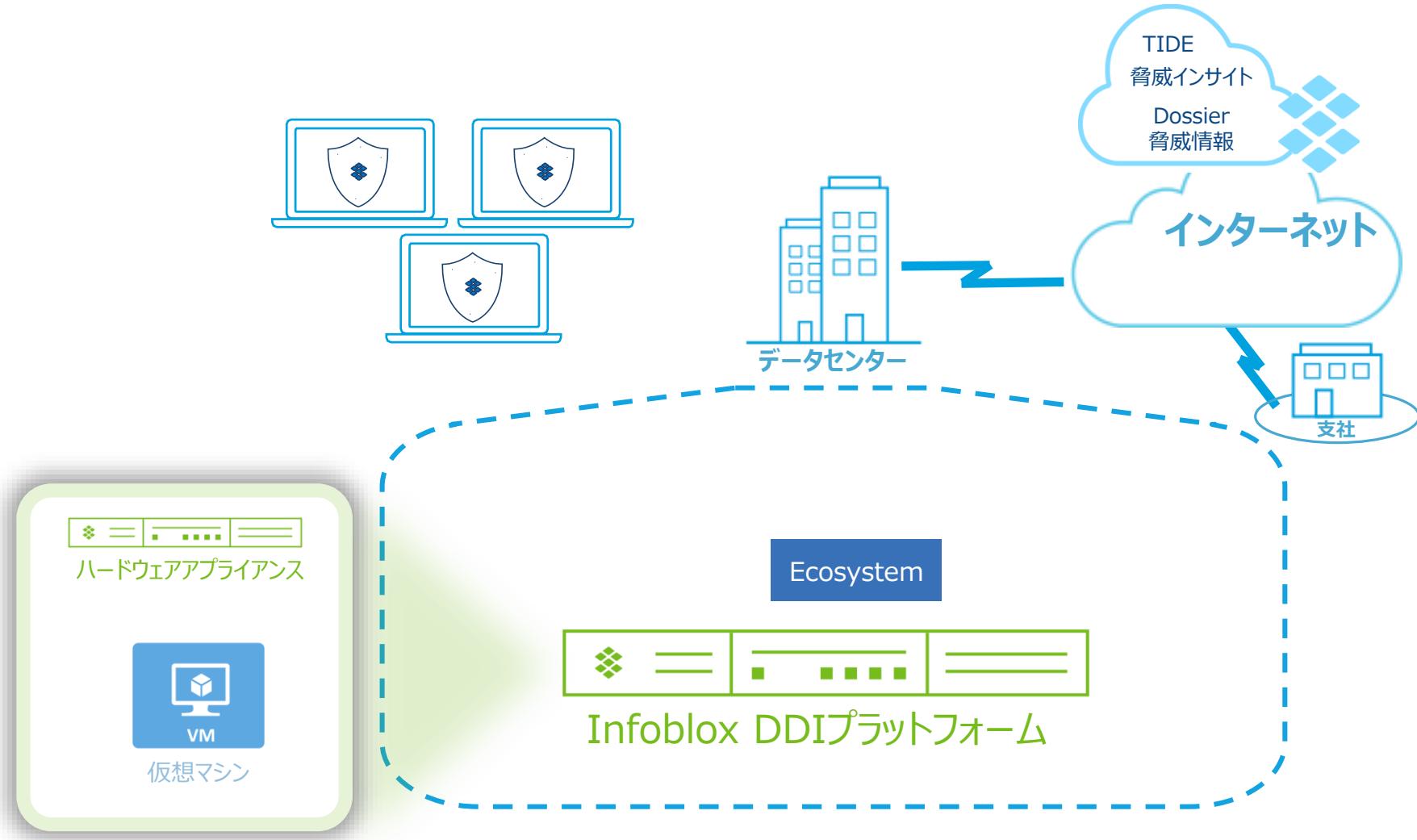
- オンプレミスによるデプロイ
 - 物理アプライアンス
 - 仮想アプライアンス

BloxOne Threat Defense – クラウド

- DNS専用の脅威情報/脅威インサイト
- Dossier
- エコシステム連携API
- オンプレミスおよび/またはコンテナベースのプラットフォーム上で提供されるクラウド

BloxOne Threat Defense – クライアント

- リモートデバイス情報をThreat Defense Cloudに転送



デプロイオプション – クラウド (Infoblox DDI以外)

3rd パーティー DNS/DDI プラットフォーム

オンプレミスによるデプロイ

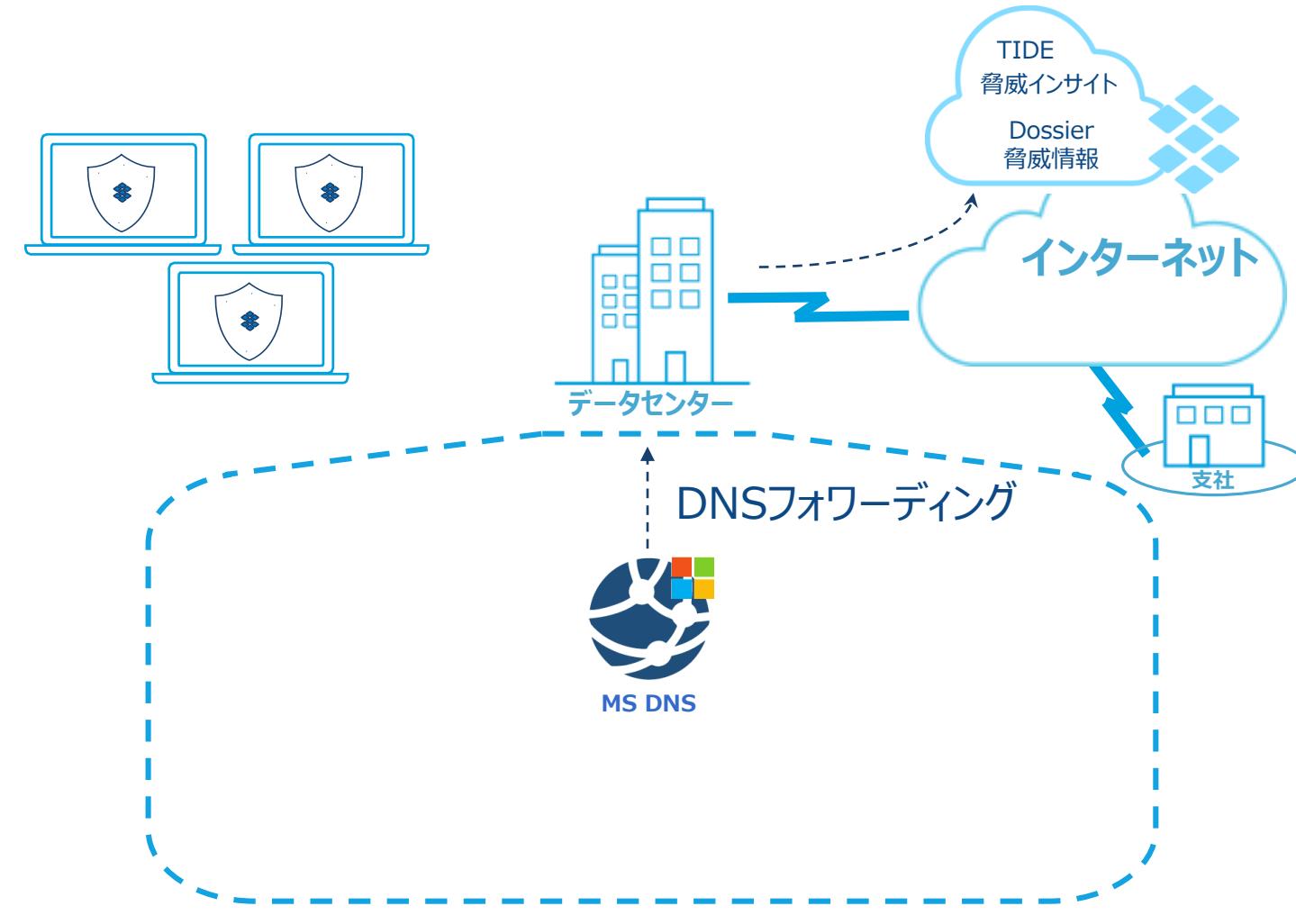
- Microsoft AD
- BIND

BloxOne Threat Defense – クラウド

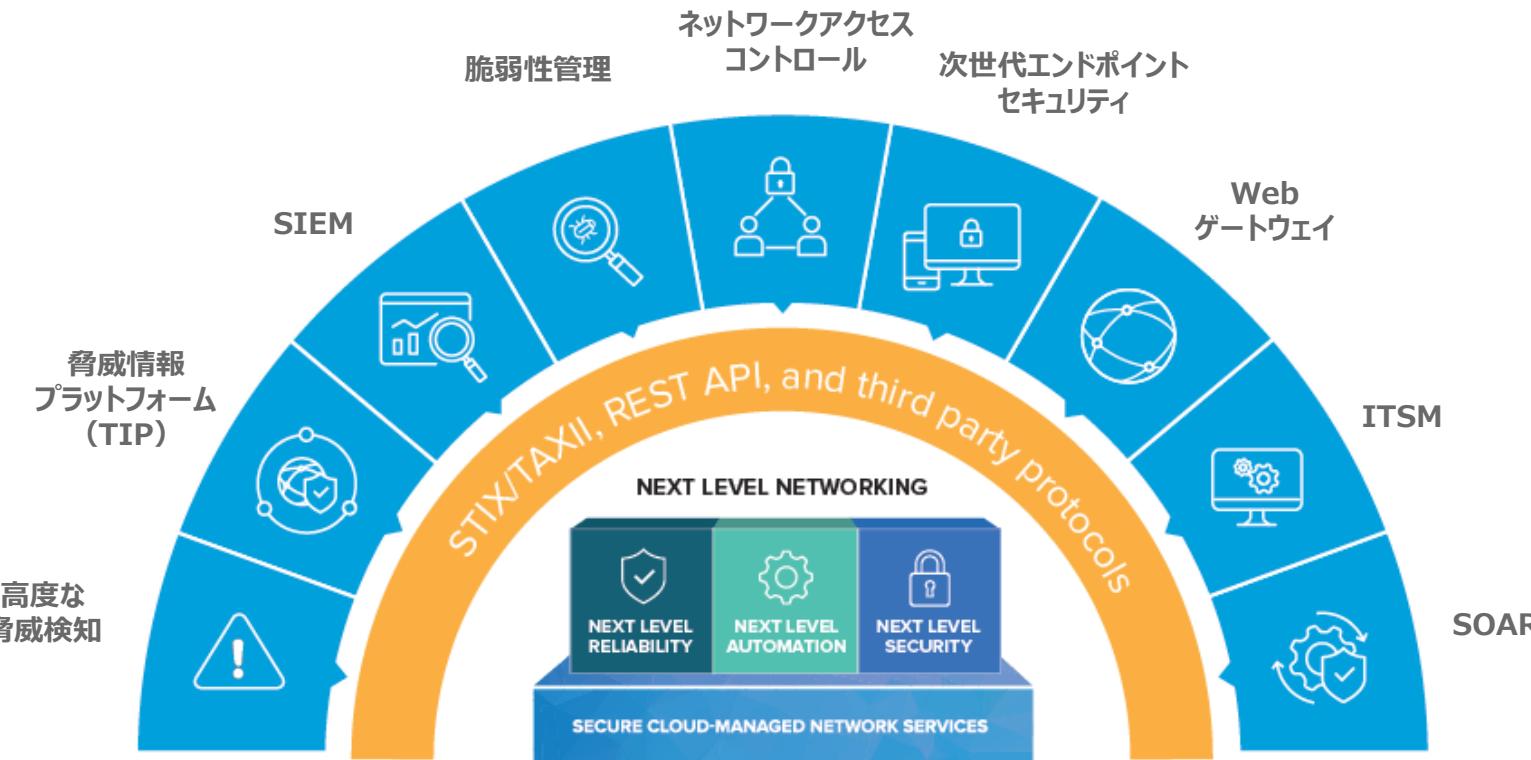
- MD DNSをInfobloxクラウドにフォワーディング
- 外部IPに基づくポリシー
- クラウドオンリーのThreat Defenseソリューション

BloxOne Threat Defense – クライアント

- リモートデバイス情報をThreat Defense Cloudに転送



検知情報、脅威情報、ネットワークコンテキスト（DDI）情報の自動連携により、エコシステム全体を強化 ~SOARソリューション基盤への貢献



膨大なアラートを優先順位付け | インシデントレスポンスを自動化 | 人為的ミスによるコストを削減

(SOAR: Security Orchestration, Automation and Response)





McAfeeとの連携

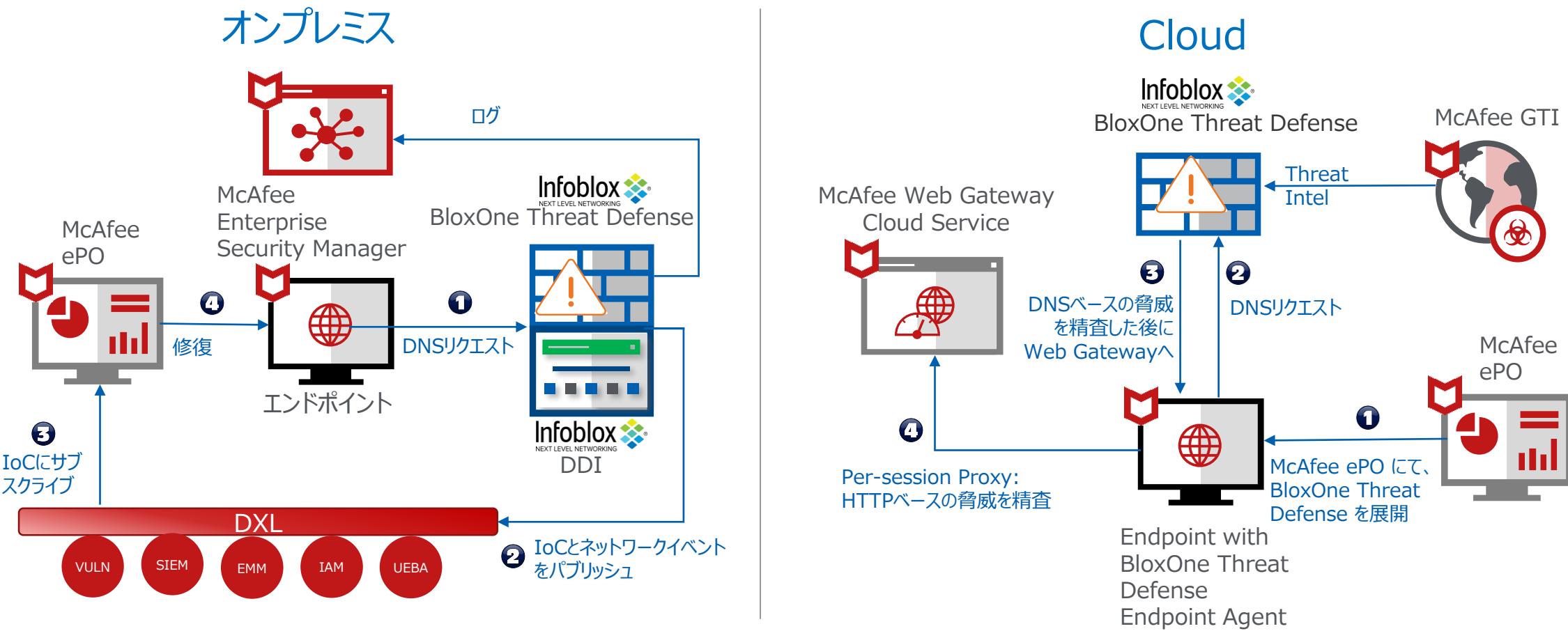
～「HTTPレイヤ」と「DNSレイヤ」の脅威を同時に深く精査。より広範な保護を自動連携で。

DDIを活用したエンタープライズセキュリティ



InfobloxとMcAfeeの連携

より広範な保護（HTTP + DNS）、より迅速な修復（自動化 + 検知情報 + 脅威情報 + DDI情報）を実現



総体的な可視性

オン/オフプレミスでWebおよびDNSセキュリティを統合

脅威レスポンスタイムの短縮



重要ポイント

IoT/5G/SaaSが先導する
デジタルトランスフォーメーション
のための
セキュリティアーキテクチャ

DNSを活用したセキュリティ基盤により効率性の
向上を図る

- ✓ キルチェーンの開始時点で攻撃を防止する
 - サイバー攻撃プロテクションのオフロード
- ✓ DNSを利用した攻撃を防ぐ
 - セキュリティギヤップへのアプローチ
- ✓ インシデントレスポンスの効率性を高める
 - 最新ネットワークコンテキスト情報の保持
- ✓ 既存の投資対効果を向上させる
 - 他社との自動連携でSOARへの貢献

既にお持ちのDDIデータは、より迅速なトリアージ
(行動優先順位の決定) を可能にするための
貴重なネットワークコンテキスト情報を提供します。





ご清聴ありがとうございました！

