A10 DDoS対策
ソリューションのご紹介

ハイパフォーマンスでフルオートのDDOS対策

増大するセキュリティの脅威

4x

2年間で拡大した
平均DDoS攻撃規模

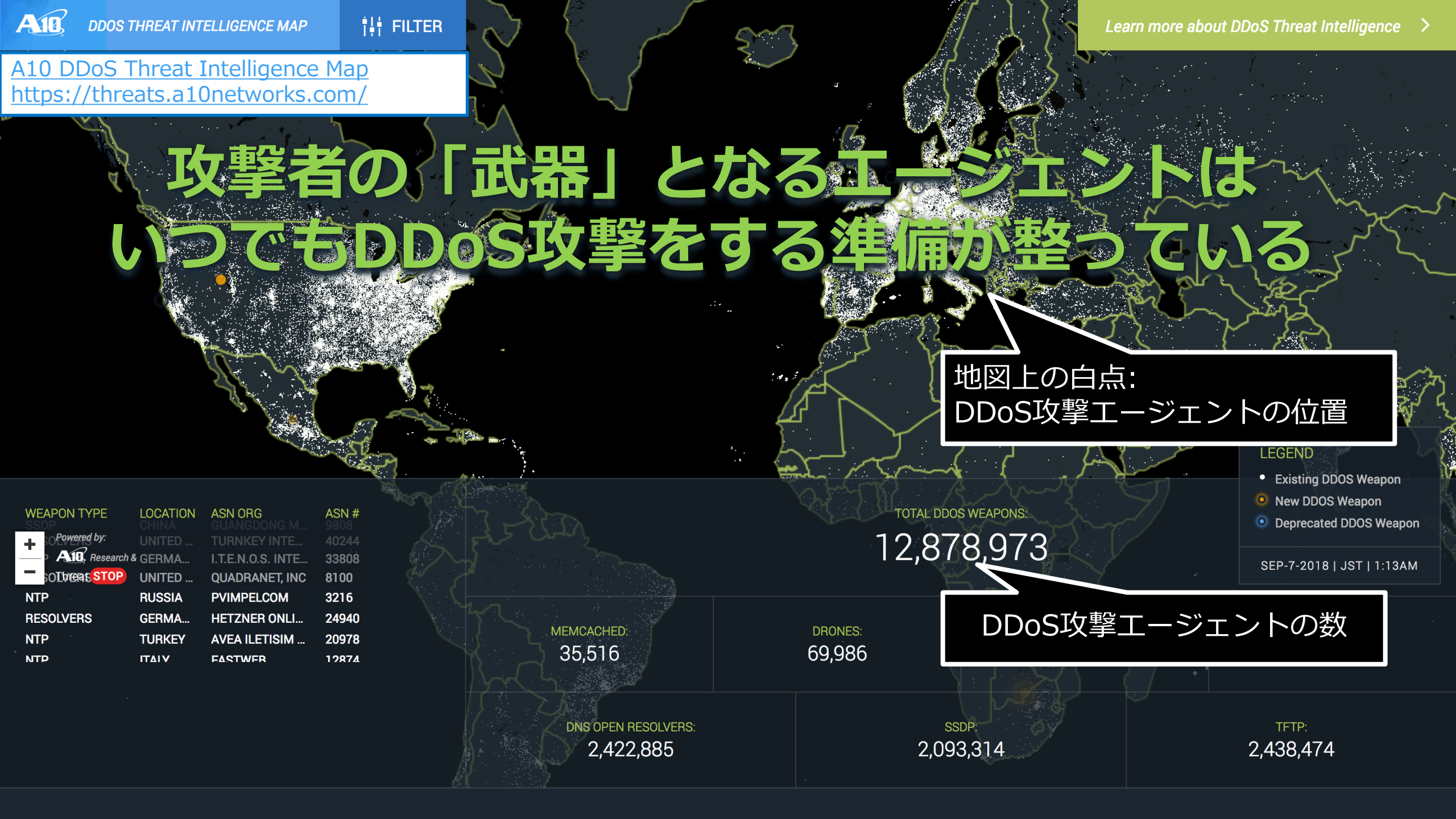
125B

2030年までに”武器化”される
可能性があるIoTデバイス

29%

ボットネットによる
インターネット
トラフィック

1. SecurityIntelligence.com ; 2. IHS Markit ; 3. SC Magazine


DDOS THREAT INTELLIGENCE MAP
FILTER
Learn more about DDoS Threat Intelligence
A10 DDoS Threat Intelligence Map
https://threats.a10networks.com/
攻撃者の「武器」となるエージェントは
いつでもDDoS攻撃をする準備が整っている
地図上の白点:
DDoS攻撃エージェントの位置
LEGEND
Existing DDOS Weapon
New DDOS Weapon
Deprecated DDOS Weapon
SEP-7-2018 | JST | 1:13AM
WEAPON TYPE
LOCATION
ASN ORG
ASN #
NTP
RUSSIA
PVIMPELCOM
3216
RESOLVERS
GERMA...
HETZNER ONLI...
24940
NTP
TURKEY
AVEA ILETISIM ...
20978
TOTAL DDOS WEAPONS:
12,878,973
DDoS攻撃エージェントの数
MEMCACHED:
35,516
DRONES:
69,986
DNS OPEN RESOLVERS:
2,422,885
SSDP:
2,093,314
TFTP:
2,438,474

マルチベクトル型攻撃時代へ

マルチベクトル攻撃に対応できる防御・検知機能が重要

出典：VERISIGN DISTRIBUTED DENIAL OF SERVICE TRENDS REPORT
https://www.a10networks.com/resources/ddos-trends-report

DDoS攻撃の現状

クラウドスクライビング

ボリューム型攻撃

オンプレミス側の防御

アクセス回線帯域内のボリューム型攻撃

マイクロバースト攻撃

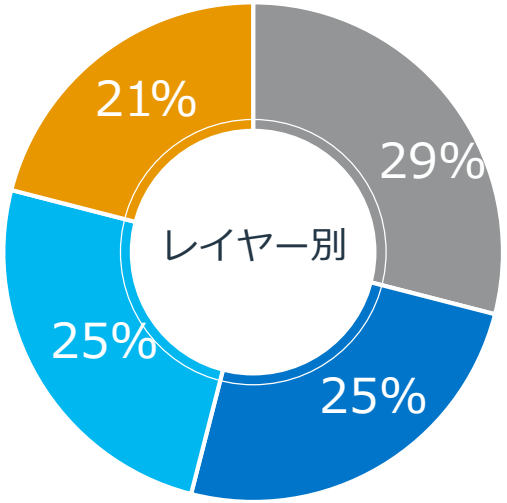
ネットワークプロトコル攻撃

アプリケーションレイヤー攻撃

スロー攻撃

巧妙な攻撃

DDoS攻撃のターゲット



インフラサービス
(DNS, CGNATなど)

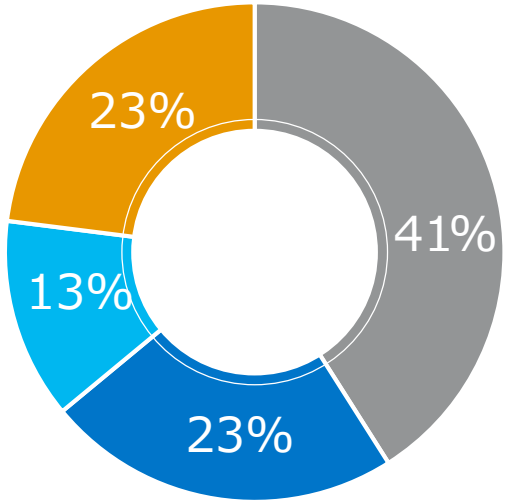
ネットワークレイヤー
(ファイアウォール、ルーターなど)

ボリューム型
(回線帯域)

アプリケーションレイヤー
(アプリケーション・サーバ)

出典: IDG

2017 第一四半期の攻撃規模



< 1Gbps

1-5 Gbps

5-10 Gbps

> 10 Gbps

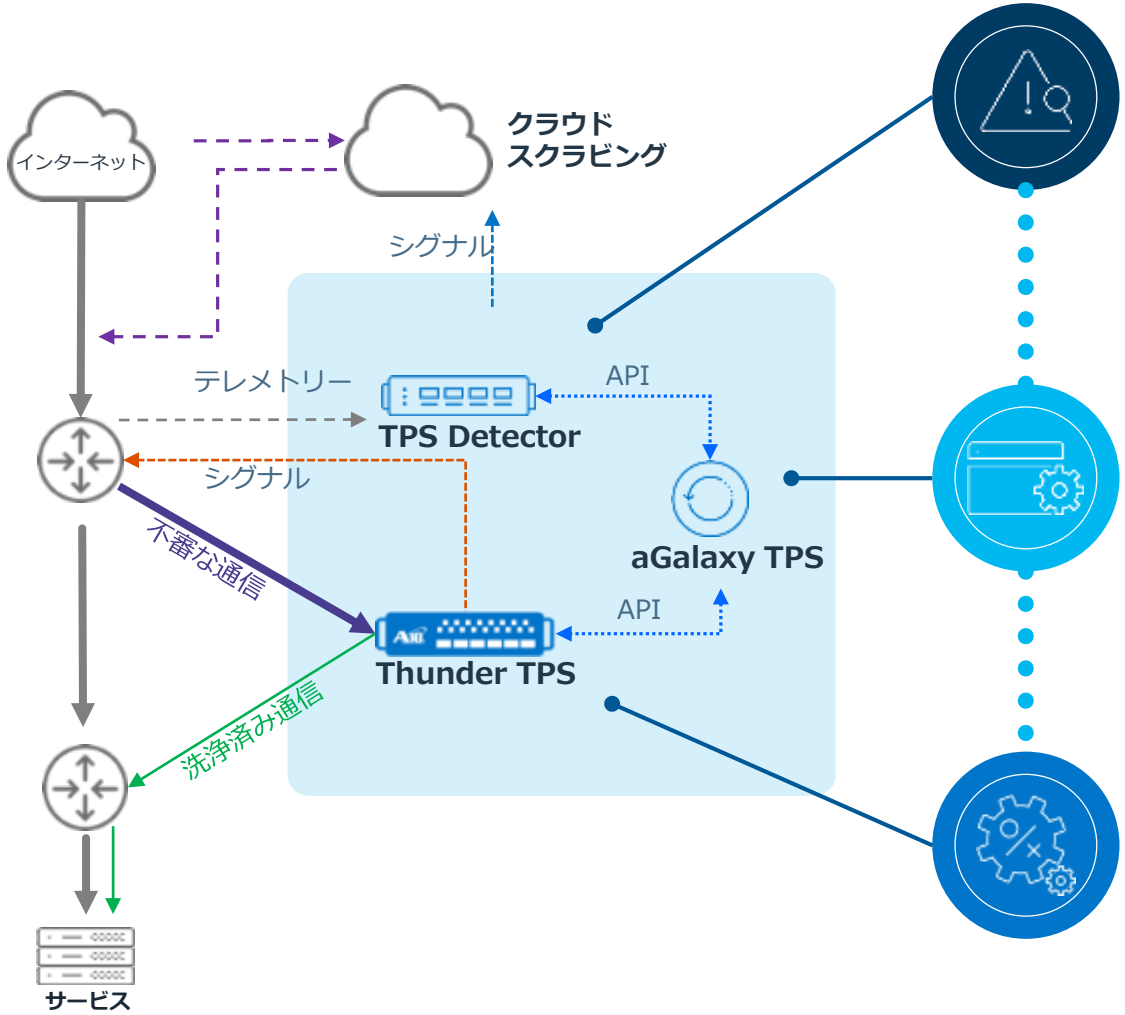
出典: Verisign

- クラウドによる対策はボリューム攻撃に有効だが万能ではない
- ハイブリッドのアプローチで広範囲な保護が必要

- 25%の攻撃がボリューム型攻撃
- 75%の攻撃がオンプレミス側の対策で有効

- 77%が10 Gbps未満の攻撃
- 41%が1 Gbps以上の攻撃
- 多くのトラフィックがオンプレミス側で防御可能

ハイブリッドDDoSソリューションの必要性



クラウド

DDoSクラウドスクラビング

ボリューム型攻撃

オンプレミス

- アクセス回線内のボリューム攻撃
- マイクロバースト攻撃
- ネットワークプロトコル攻撃
- アプリケーションレイヤー攻撃
- スロー、小量攻撃
- 巧妙な攻撃

オンプレミスによる対策