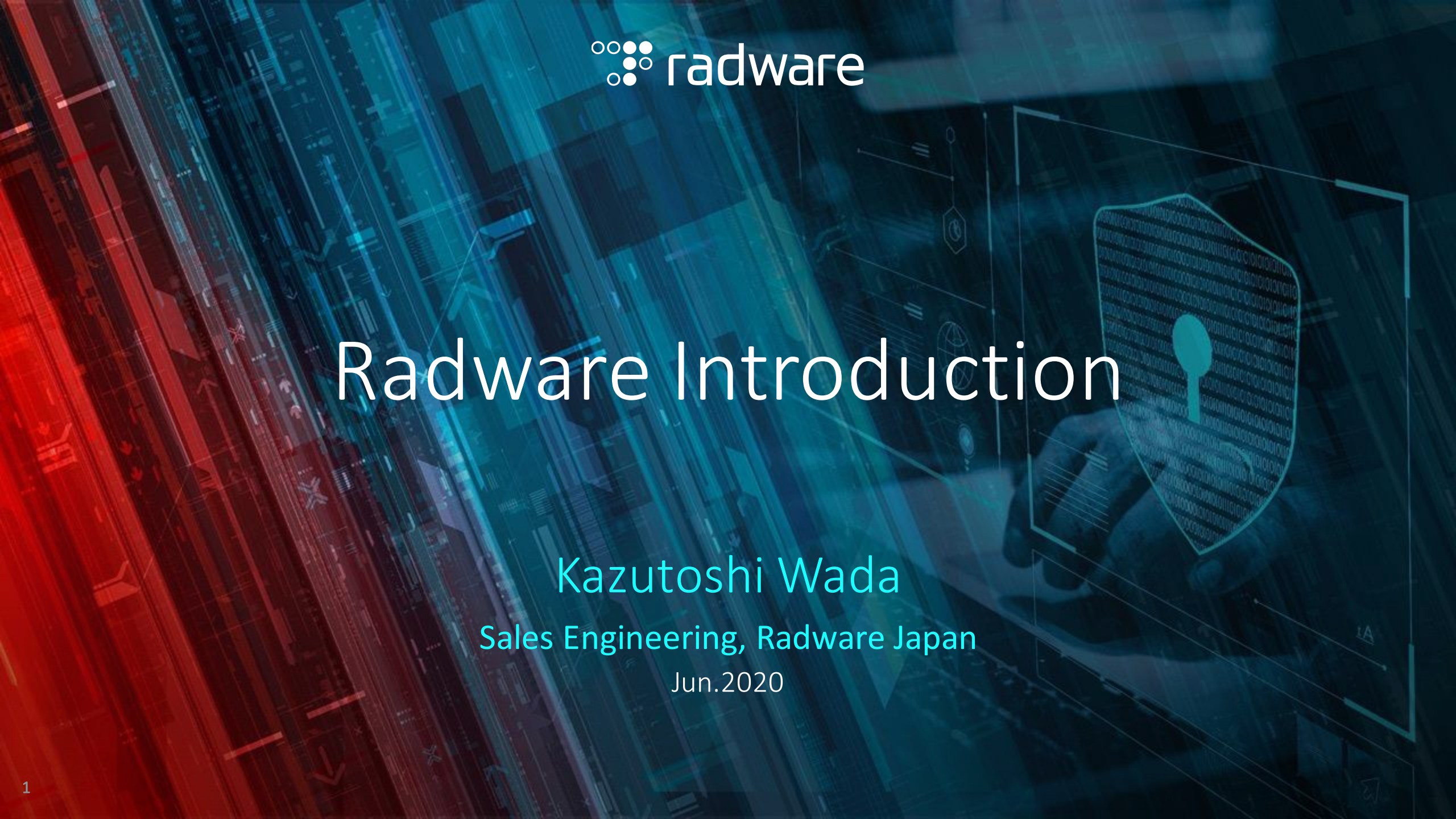


Radware Introduction

Kazutoshi Wada

Sales Engineering, Radware Japan

Jun.2020

Topics

- About Radware(Why Cisco - Radware?)
- Trend - Cyber Attacks
- Radware Solutions
- Summary

About Radware
(Why Cisco – Radware?)

About Radware

日本法人設立：2000年（HQ:1997年）

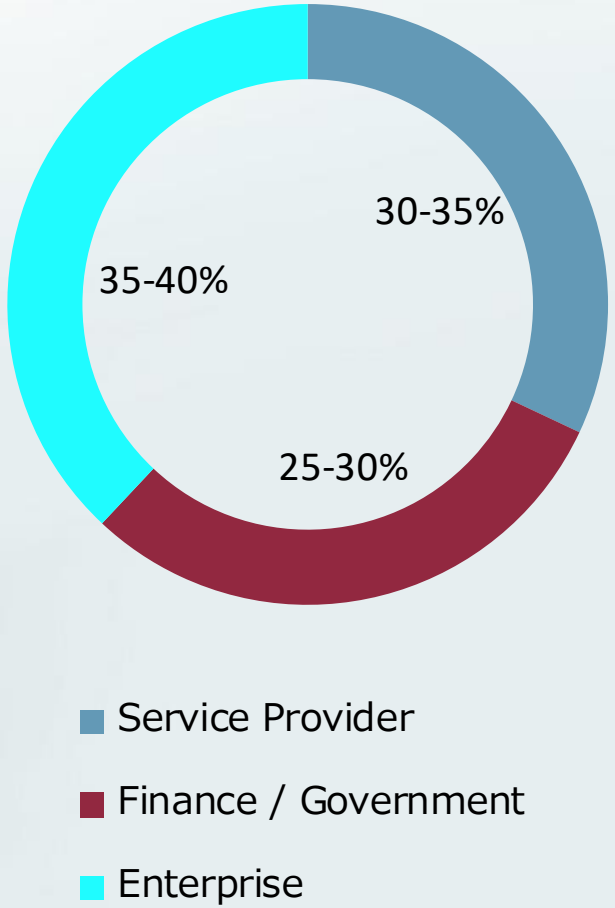
株式上場：1999年（NASDAQ）

売上 2億5200万ドル（2019年度）

従業員数 1,100名（2020年）

拠点数：世界35カ所
本社：テルアビブ（イスラエル）

顧客数 12,500社以上



About Radware

サイバーセキュリティ＆アプリケーションデリバリー
マーケットリーダー

12,500社以上の
エンタープライズと通信キャリアでの実績

マーケット評価

Gartner
ADC MQ Leader
WAF MQ Visionary

FORRESTER®
DDoS Wave Leader

パートナー

CISCO

Microsoft Azure

NOKIA

既存顧客実績

金融

世界Top 12為替取引所、8社

世界Top 20銀行、10社

Bank of America
Bloomberg
Capital One
HSBC
Deutsche Bank
ING
ADP
SBI

リテール、オンラインビジネス

世界Top 10リテール企業、5社

DELTA
ebay
GAP
Marriott VACATION CLUB
PayPal
SAMSUNG SDS
twitter
ups

通信キャリア、SaaSプロバイダー

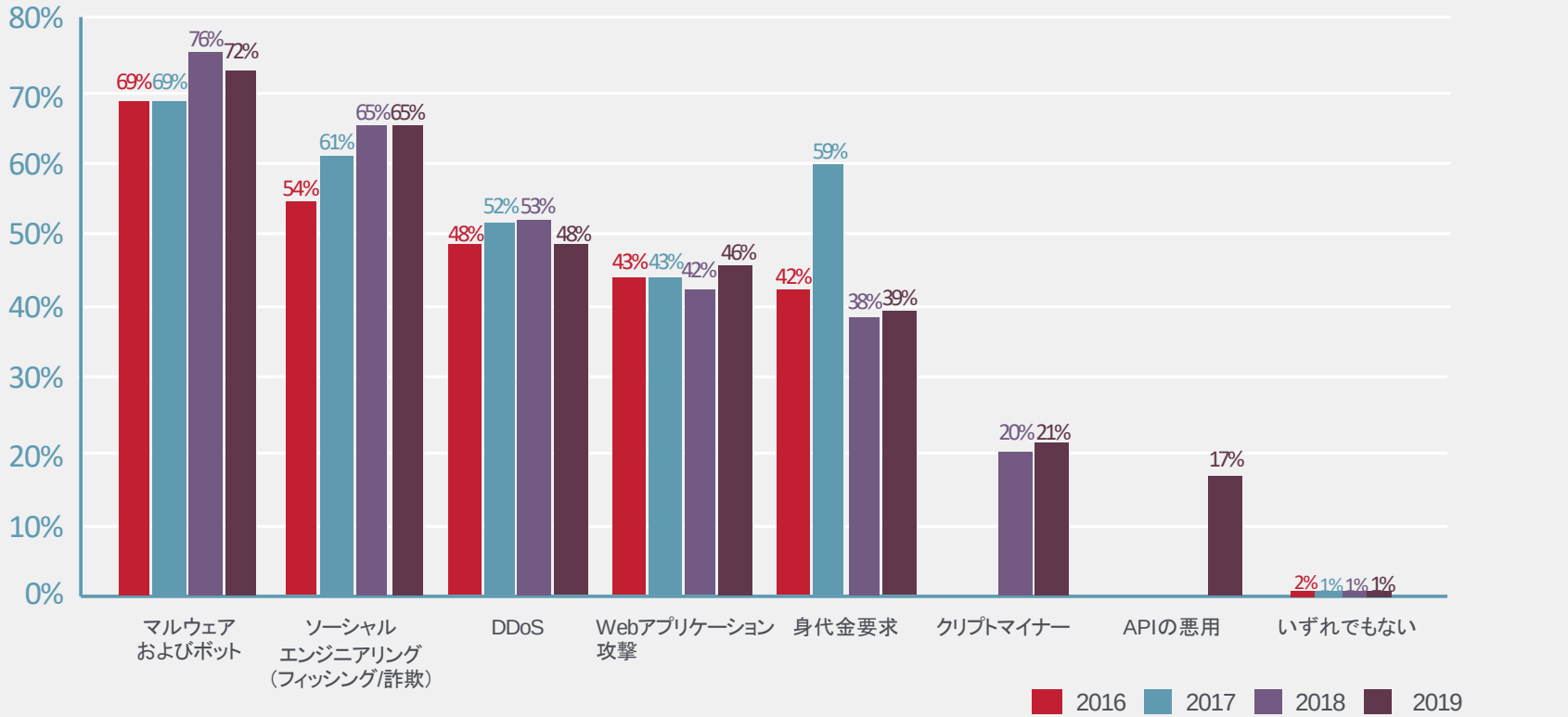
世界Top 10通信キャリア、10社

世界Top 10SaaSプロバイダー、5社

salesforce
AT&T
Cisco webex
workday
SAP
Tech Mahindra
verizon
Akamai

Why Radware needed for Cisco Customers?

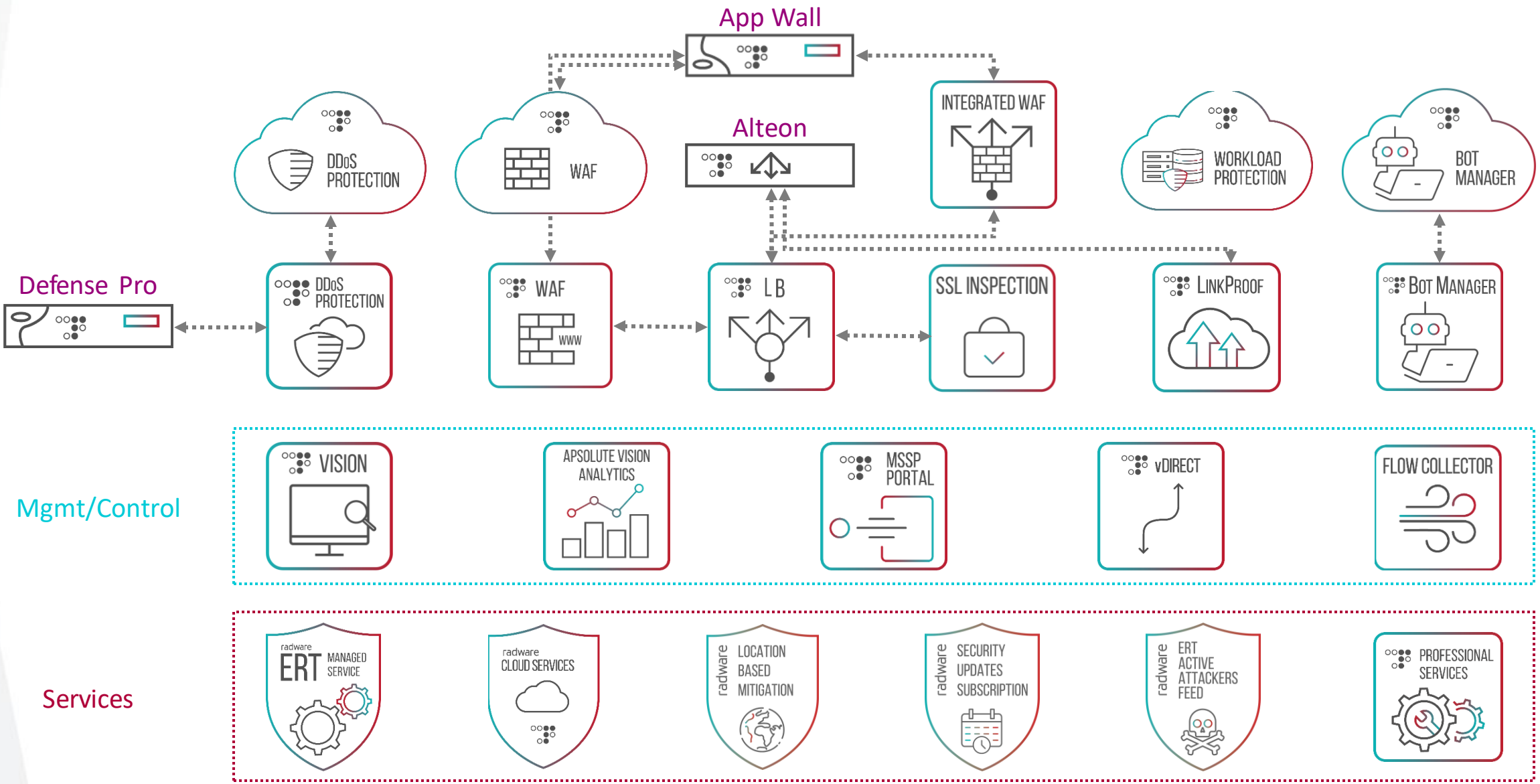
2016–2019年 企業が受けた攻撃の種類



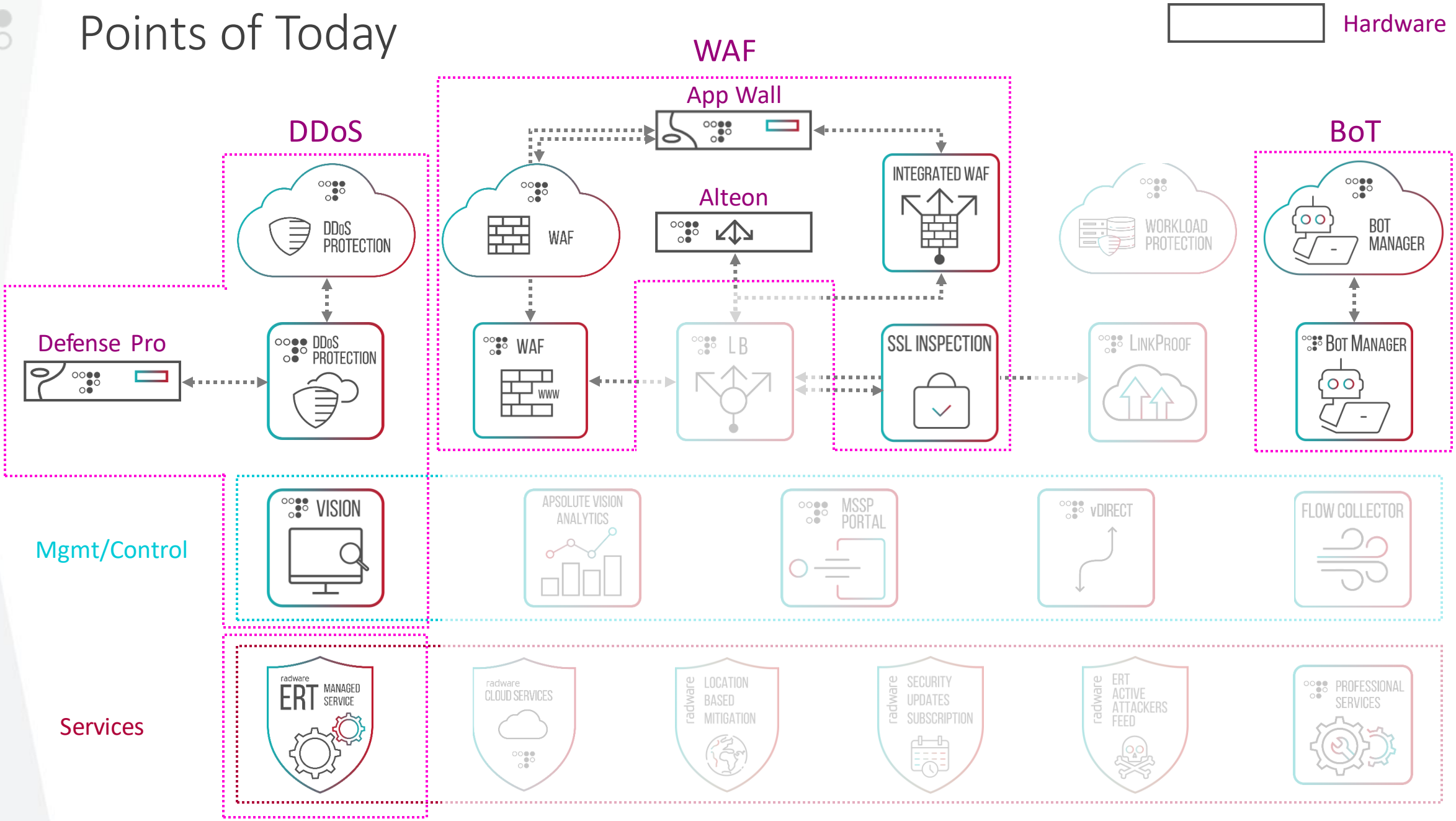
2019–2020年版　Radwareグローバルアプリケーション&ネットワークセキュリティレポート

Cisco + Radware = “Total” Security Solution

Radware feature-based portfolio



Points of Today



Recently Cyber Attacks

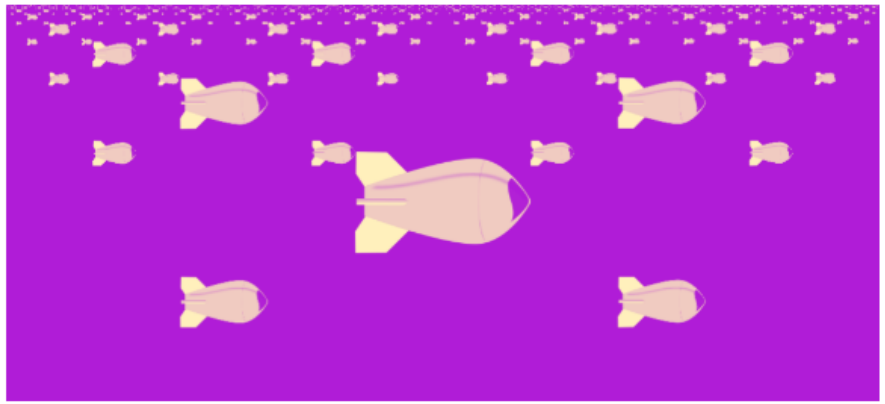
‘Carpet-Bombing’ DDoS Attack Campaign Sep/Oct 2019

'Carpet-bombing' DDoS attack takes down South African ISP for an entire day

Carpet bombing - the DDoS technique that's just perfect for attacking ISPs, cloud services, and data centers.

By Catalin Cimpanu for Zero Day | September 24, 2019 -- 19:30 GMT (20:30 BST) | Topic: Security

南アフリカのISPがDDoSにより丸一日ダウン



Mysterious attackers have taken down a South African internet service provider over the weekend using a DDoS technique called carpet bombing. *ZDNet* has learned.

The DDoS attacks took place on Saturday and Sunday, September 21 and 22, and have targeted Cool Ideas, one of South Africa's largest ISPs.

During the DDoS, attackers successfully managed to bring down Cool Ideas' external connections to other ISPs, as can be seen from open-source reporting tools.

SEE ALSO

10 dangerous app vulnerabilities to watch out for (free PDF)

Security
Chinese police arrest operators of 200,000-strong DDoS botnet

Security
Libarchive vulnerability can lead to code execution on Linux, FreeBSD, NetBSD

Security
Kamerka OSINT tool shows your country's internet-connected critical infrastructure

Security
Experts: Don't reboot your computer after you've been infected with ransomware

NEWSLETTERS

SEE ALL

RELATED STORIES

eurobet.it.DDos
@ItDdos

In risposta a @eurobetweet

we attacked your website eurobet.it. You have to pay $ 80,000 bitcoin. we won't stop until you pay.

Traduci il Tweet

8:18 PM · 13 ott 2019 · Twitter Web App

$80K 支払うまで攻撃を止めない

Seeweb @seeweblive · 31. Okt.

#halloween2019🎃, #rete in subbuglio per #attacchi di criminali informatici che hanno sfruttato #IP di #provider come #seeweb per presentarsi a grossi portali sotto falso nome.
Grazie ai nostri #hacker per il rapido lavoro di #mitigation 🎃

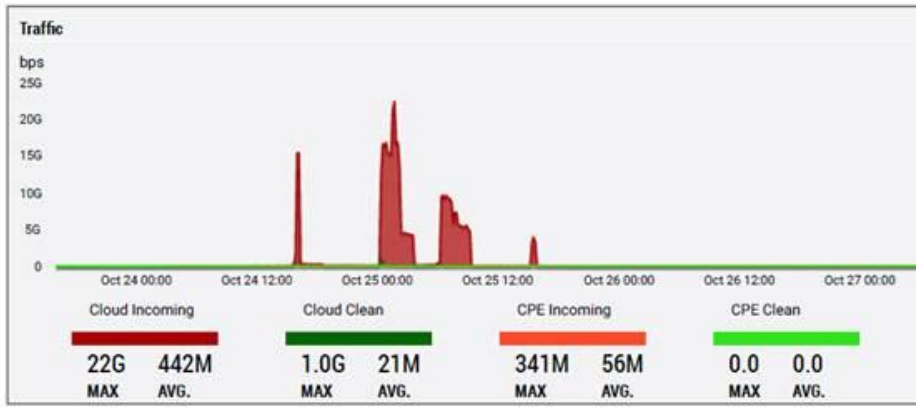
#DDoS #Attack #**lottomatica** #eurobet

Fancy Bear: Ransom DDoS Attacks

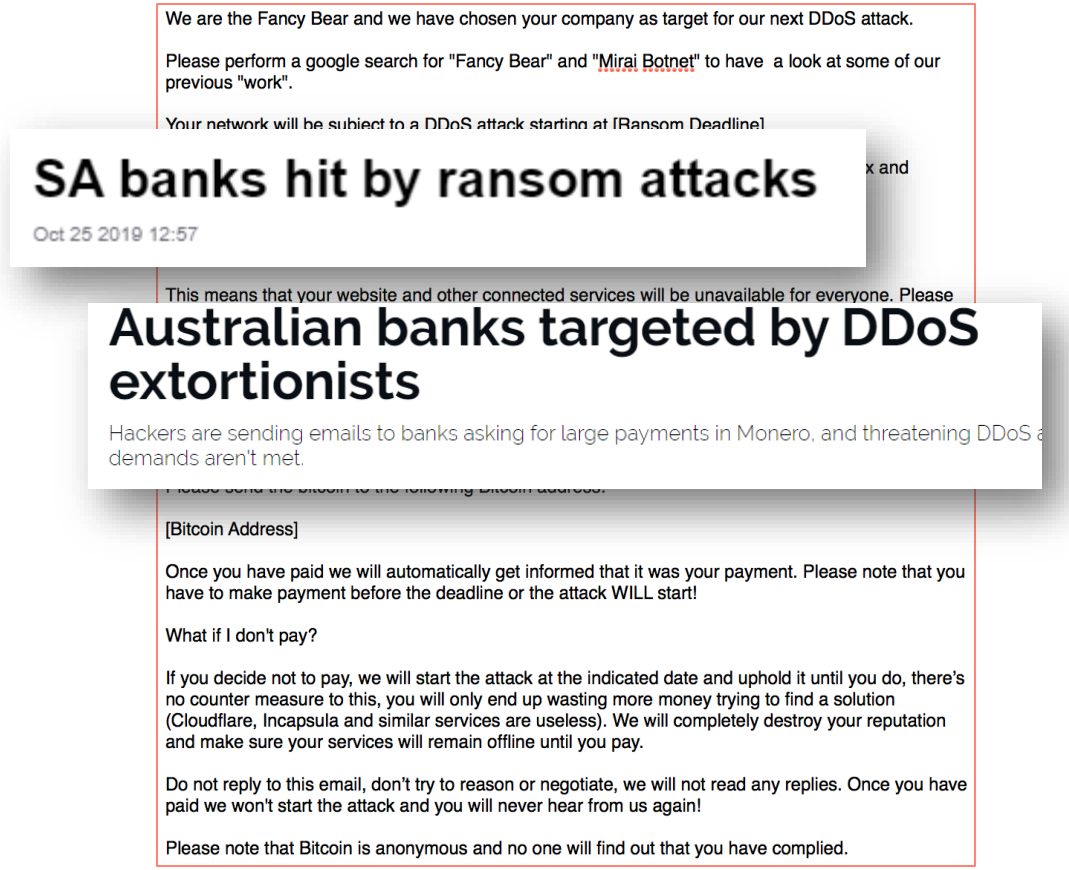
金融機関を狙った世界規模のランサムキャンペーン

“Fancy Bear” というサイバー犯罪グループが実施
1ビットコイン（当時 $8k）を要求
支払わなければ毎日1ビットコインずつ増える

Radwareは南アフリカ大手銀行 3行を保護し、
アラートとブログを公開



ある攻撃は22Gbpsを記録



“Fancy Bear”からの脅迫メール

Attacks on DNS Infrastructure – No One Is Safe

DNSはWebの大規模なサービスダウンを招く可能性のある、1つの重要な要素

October 2016: Dyn DNS US**東部リージョンが**Mirai botnet**により攻撃を受け、被害が**Twitter, Amazon, Tumblr, Reddit, Spotify, Netflix**等のサービスを数時間アクセス不可状態に**

October 2019: AWS Route 53(DNS Service)**にも同様の攻撃があり**AWS **全体サービスへの影響が数時間あった**

DNS Serverへの攻撃は**Web**サービスにとって非常に効果的な手法

COVID-19: Availability of Critical Services

Suspicious cyberactivity targeting HHS tied to coronavirus response, sources say

The activity happened Sunday night, sources said.

By John Santucci, Katherine Faulders, Josh Margolin, Luke Barr and Mike Levine
16 March 2020, 19:53 • 6 min read

US保健福祉省（Health and Human Services (HHS) ）へのDDoS

Coronavirus explained

Early cases of COVID-19 are believed to be linked to a live-animal market in Wuhan, China.

The Department of Health and Human Services experienced suspicio
cyberactivity Sunday night related to its coronavirus response,
administration sources confirmed to ABC News Monday.

The suspicious activity HHS was not a hack but it may have been a
distributed denial of service -- or DDOS -- attack, according to mult
sources.

DDoS Attack Targets German Food Delivery Service

**Liefrando delivers food from more than 15,000 restaurants in Germa
where people under COVID-19 restrictions depend on the service.**

ドイツのフードデリバリスタートアップ企業をDDoS攻撃

Cybercriminals have launched a distributed denial-of-service (DDoS) atta
against German food delivery service Takeaway.com (Liefrando.de),
demanding two bitcoins (about $11,000) to stop the flood of traffic. The at
has now stopped, according to a report from BleepingComputer.

The COVID-19 virus has caused Germany to implement severe restrictions on
the restaurant industry. As a result, Germans have grown more reliant on
delivery services, which includes Takeaway.com's Liefrando, which
delivers food from more than 15,000 restaurants.

Founder and CEO Jitse Groen shared an update of the incident via Twitter,
along with a note from the attackers indicating they planned to target other
websites. The company's German division then announced its systems had
entered maintenance mode to ensure data security in the attack. Food orders
were accepted but couldn't be processed; Liefrando had to issue customer
refunds.

Security experts anticipate these types of acts, intended to exploit essential services in times of crisis, will continue as restrictions due to COVID-19 remain in place. "Deplorably, we will likely see a further avalanche of cyberattacks targeting most susceptible online businesses," says ImmuniWeb founder and CEO Ilia Kolochenko. As a result, many organizations may be forced to pay cybercriminals or invest in DDoS protection services to defend against advanced attacks.

Parisian Hospitals hit by DDoS attack

Publication date: March 24, 2020 **Last edited:** March 24, 2020

f hospitals in Paris were hit by a DDoS attack. This temporarily
g the home work programs and their email.

フランス医療機関がDDoSを受ける

Paris. These hospitals are currently extremely busy taking care of a large
currently 665 corona patients in intensive care throughout Paris. With
ing the medical professionals, attacks like this one can do more damage

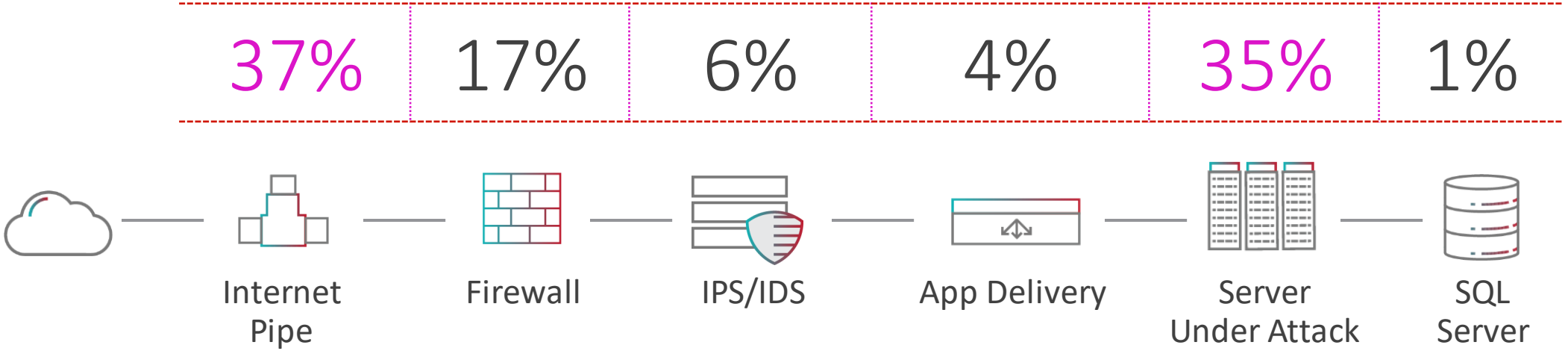
e Corona crisis

dvantage of the current crisis. On a small scale, people fall victim to
he fear the current crisis causes. But cyber criminals also target large
m home, which means that the consequences of shutting down systems
has even more consequences. Furthermore, you can imagine that in
cker when they fall victim to a ransomware attack.

bsite or system are overloaded with requests. Hackers do this by
ount of devices at the same time. Because the website is not built for

Failure points in the data center

- Internet でのインシデントは2016年から 50% 増
- Server が最も狙われるのは有用なデータを保持しているから
- 部分的な障害を超えた全体サービスダウンが 40% 増



情報漏えい被害

13億

流出レコード数, 2018

$150

1レコードあたり, 2019

$3.29 M

情報漏えいの
平均被害コスト,2019

31%

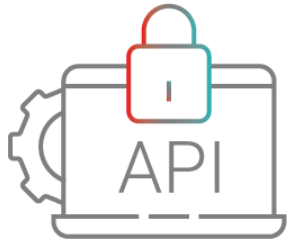
情報漏えいにより
誰かが職を失う確率

OWASP* Top 10に基づくアプリケーションの保護対策

- Injections
- Unauthorized access
- Data & credential theft
- Remote scripting
- Web-scraping
- Parameter Manipulation
- Protocol attacks
- Fraud
- Session hijacking
- Cookie poisoning

DEFENSE

アプリケーションレイヤ



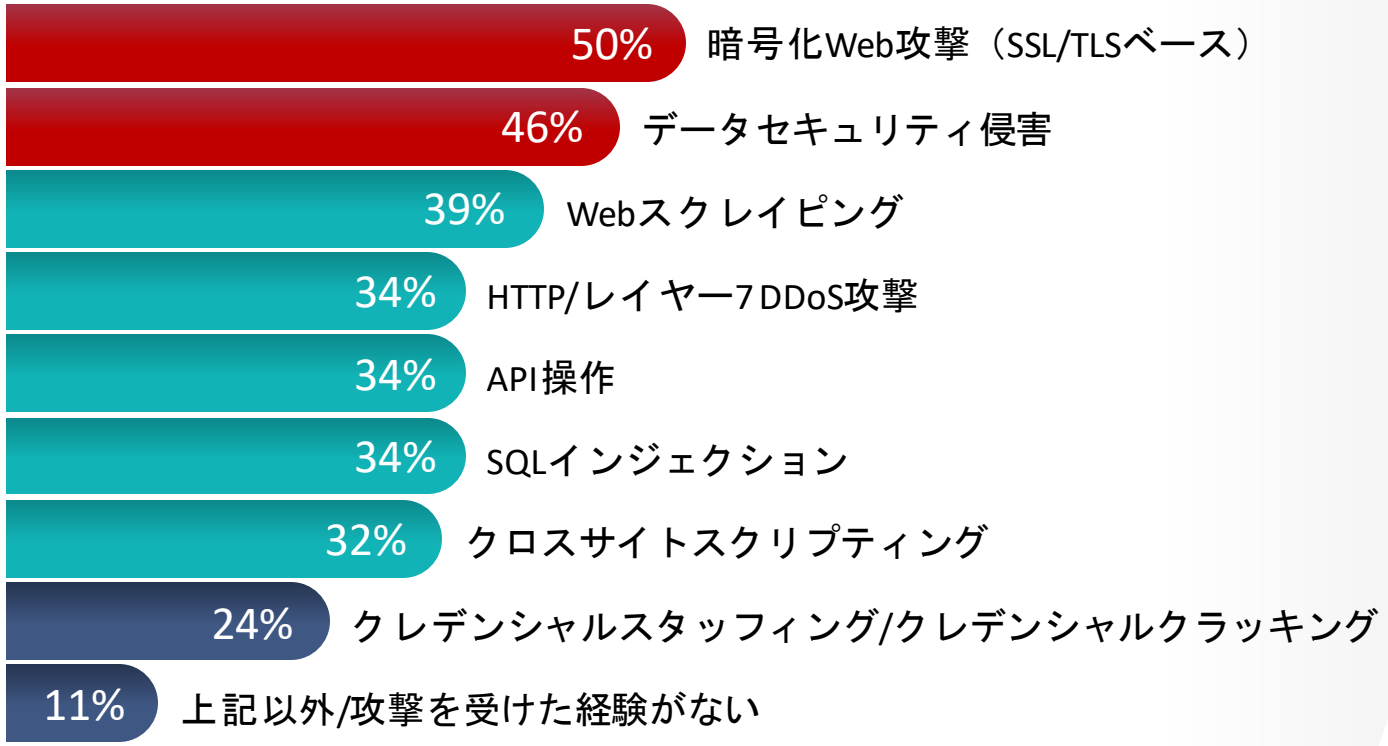
API

BoT

*Open Web Application Security Project

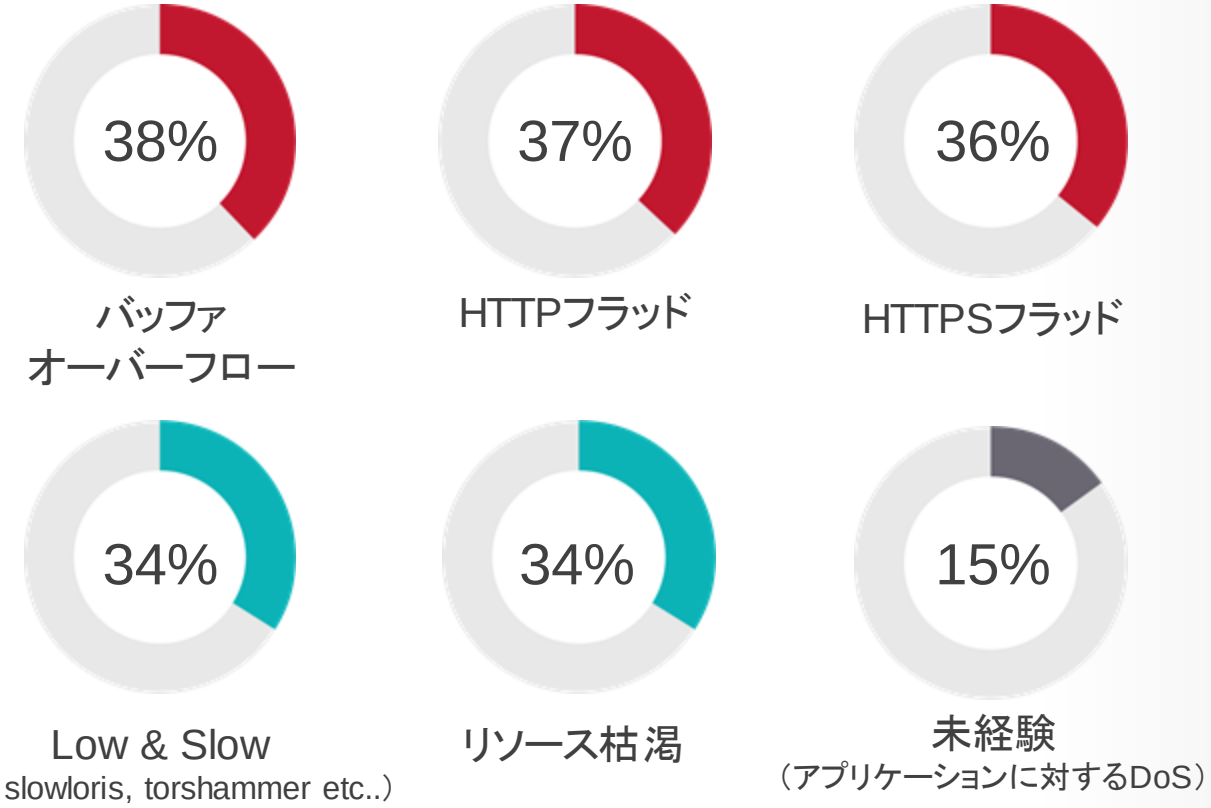
Application Layer Attacks

2018年 発生頻度が高かったアプリケーション攻撃



アプリケーション層でのDoS攻撃

2018年で発生頻度が高かったDoS攻撃

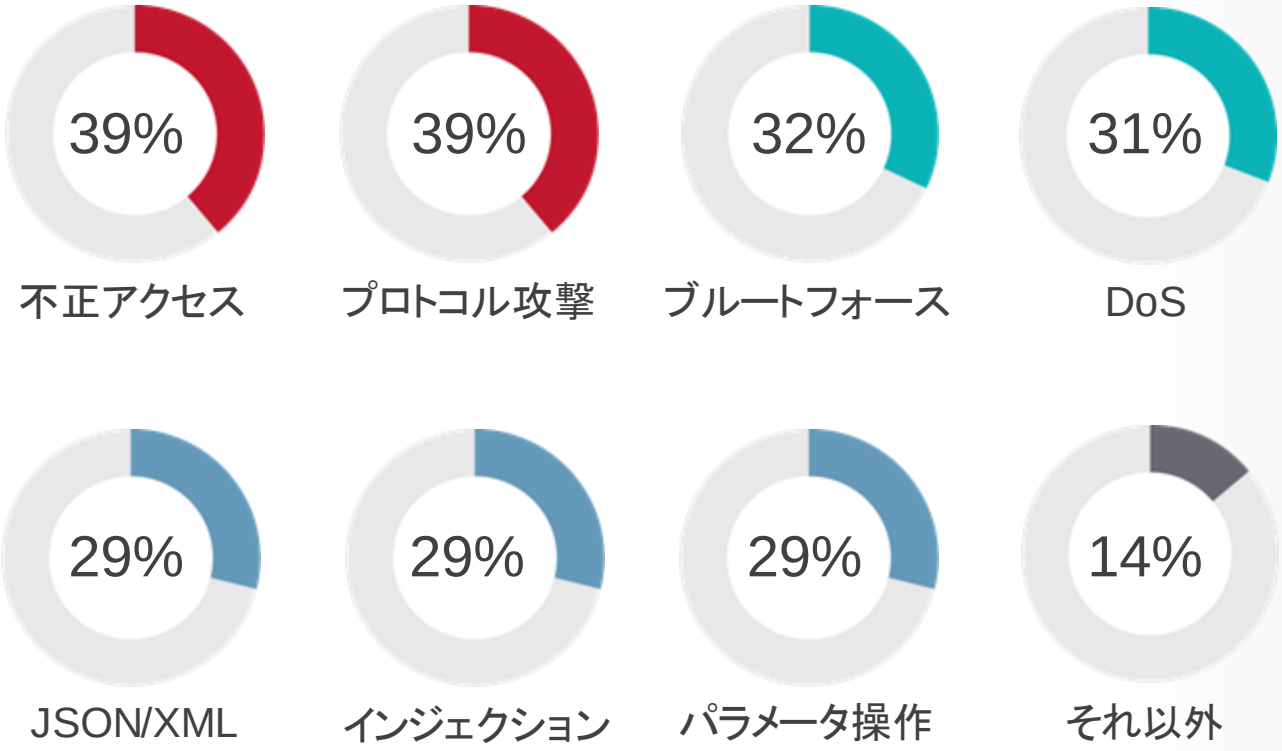


- IoTは大量にHTTP/Sトラフィックを生成
- アプリケーション層DoS攻撃は検知と軽減が困難
- アプリケーションに対する大容量型および非大容量型サービス拒否攻撃の拡大規模は同程度

Source: Radware NETWORK AND APPLICATION SECURITY THREAT LANDSCAPE 2018-9

見落としがちなAPIセキュリティ

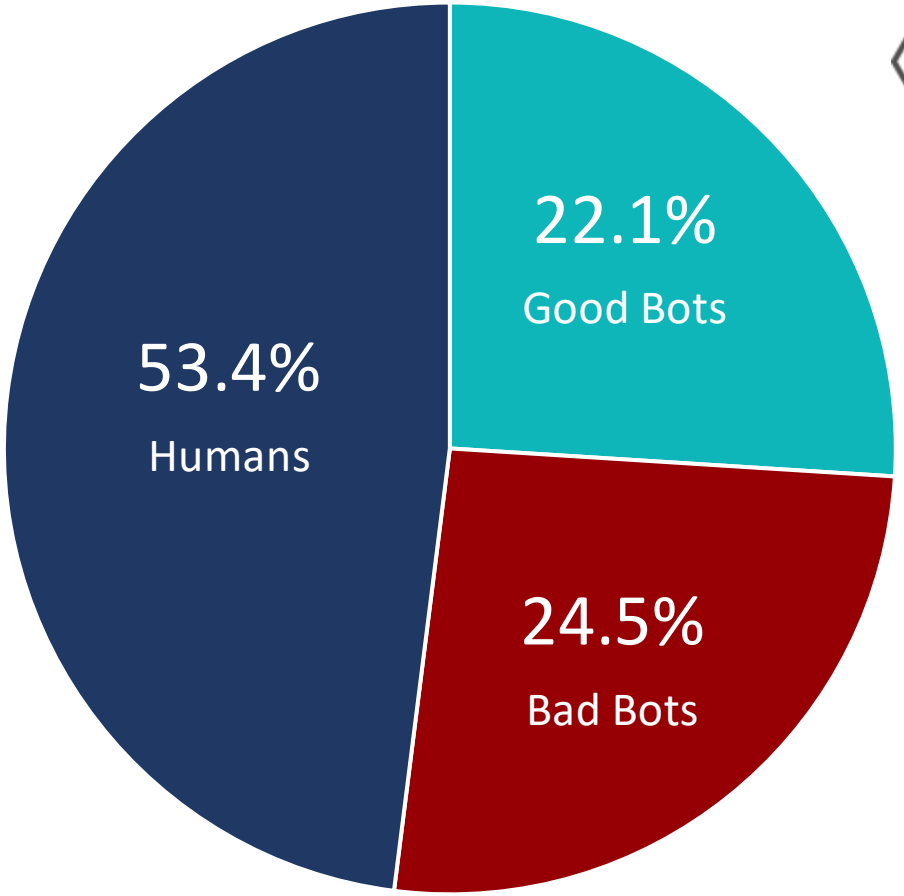
APIに対する7つの一般的な攻撃

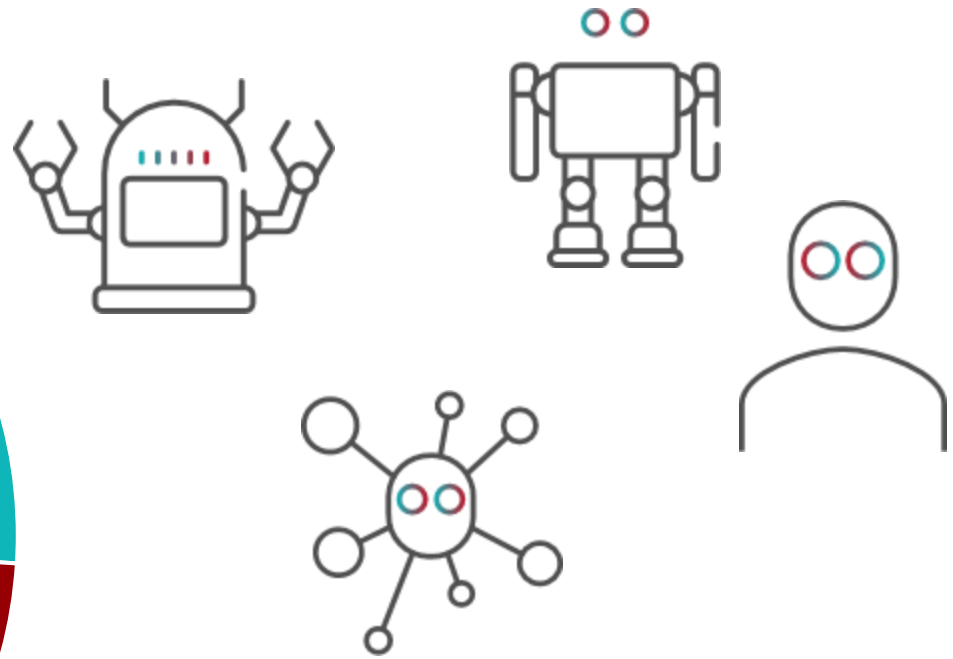


- 転送されたデータは検査や検証の対象ではない
- APIにはアプリケーションと同様の脆弱性がある
- 最も頻発している攻撃はプロトコル攻撃と違反アクセス

Source: Radware NETWORK AND APPLICATION SECURITY THREAT LANDSCAPE 2018-9

Bots in The Internet





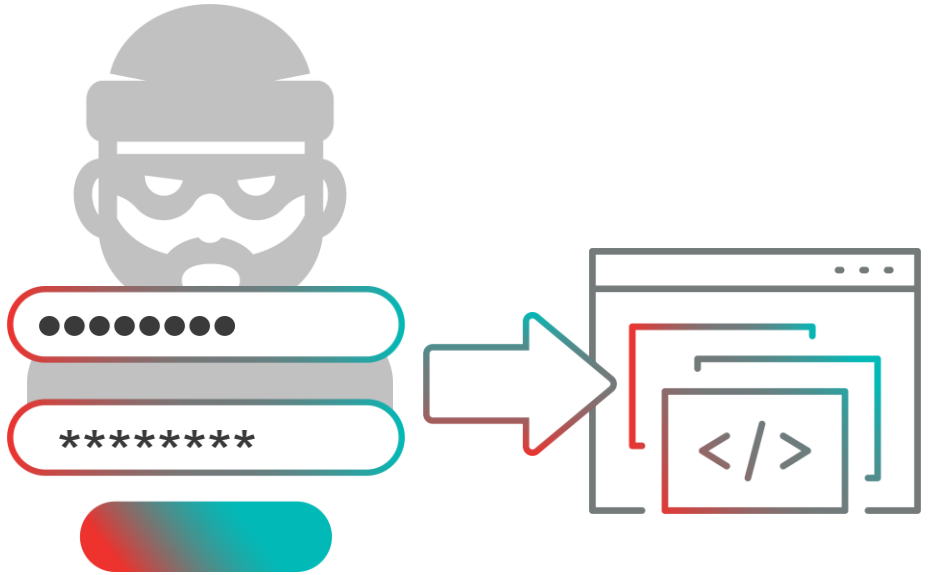
24%がBad Bots

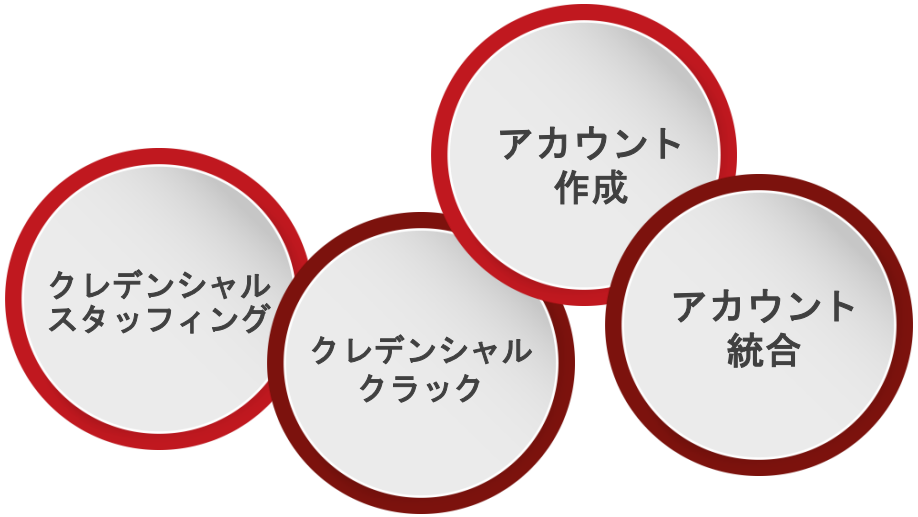
Source: Radware The Big Bad Bot Problem 2020

75%の組織が***Good or Bad***を判別できていない

Bad bot example: Account Takeover

アカウント盗用から、製品やサービス情報を抜き出す





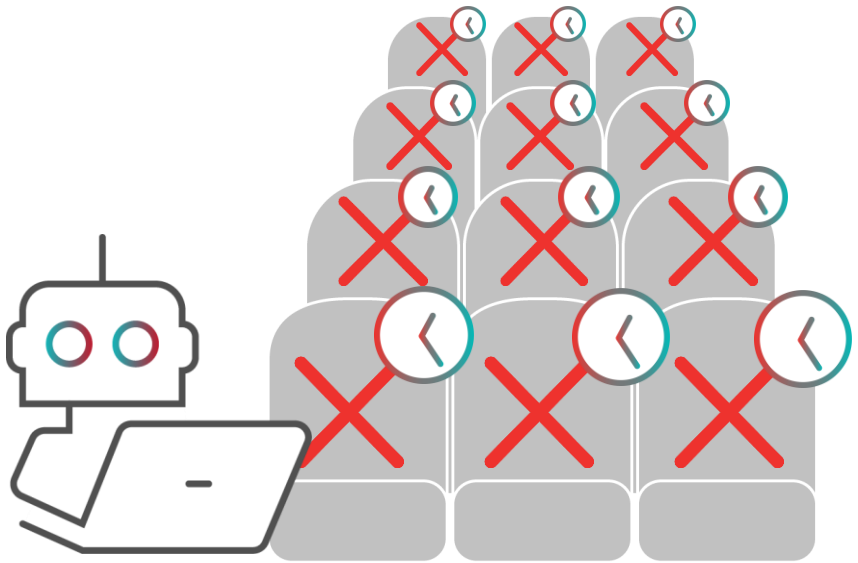
データ流出

企業評価下落

経済損失

Bad bot example: Denial of Inventory

実際に購入することなく、買い物かごや予約枠を埋め尽くす



45% 品薄を経験*

32% 実際に枯渇を経験*

顧客損失

企業評価下落

経済損失

*Source: Radware Research: Web Application Security in a Digitally Connected World, Nov 2017

Use Case

Challenge

BotによるDeniel of Inventoryを受ける
IPが動的に変わる攻撃だった

Radware Solution

22 xWAF

Why Radware

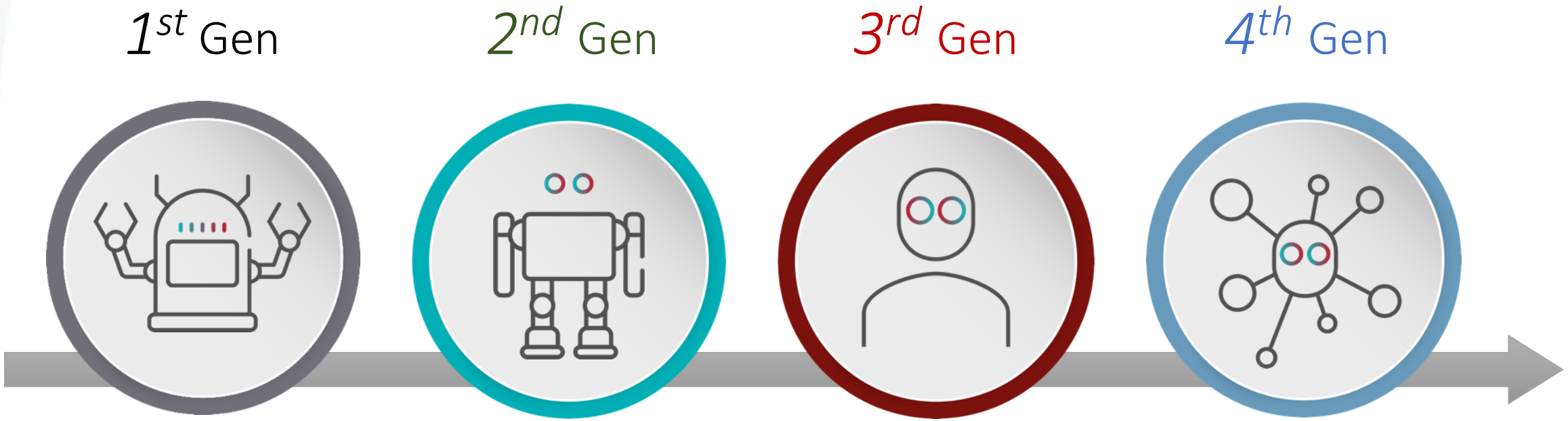
WAFのアンチBotプロテクト
（Fingerprintingによる動的IP攻撃からの防御）
自動ポリシー作成
SSL攻撃防御の優位性

Competition

F社　　パフォーマンスで脱落
A社　　検知率で脱落

Delta Airlines Project Architect – 予約サイトは一番の収益源であり、ダウンタイムがあってはならない。Radware WAFのFingerprinting技術と自動ポリシー作成は何か問題が起きたときにすぐルールを作成し実装できるので、Radwareに決めました。

Bot Generations



1st Gen

SCRIPT BOT

単純なスクリプト
反復動作

2nd Gen

HEADLESS BROWSER BOT

ブラウザを模擬して活動

3rd Gen

HUMAN-LIKE BOT

ブラウザを利用
「人っぽく」振る舞う

4th Gen

DISTRIBUTED BOT

より「人に近い」
直線ではなくランダム
何万ものIPに分散

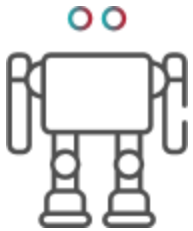
Radware Bot Manager

Radware Bot Manger

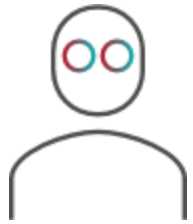
他社

Bot

Script Bots



Headless Browser Bots



Human-like Bots

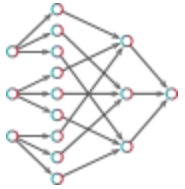
Distributed Bots

Technology

IP, User Agent

デバイス＋ブラウザ
フィンガープリント

ふるまい検知



ビッグデータ
相関解析、機械学習

Bad Bot Analyzer

ボットトラフィックやボット攻撃検査用の無料評価ツール

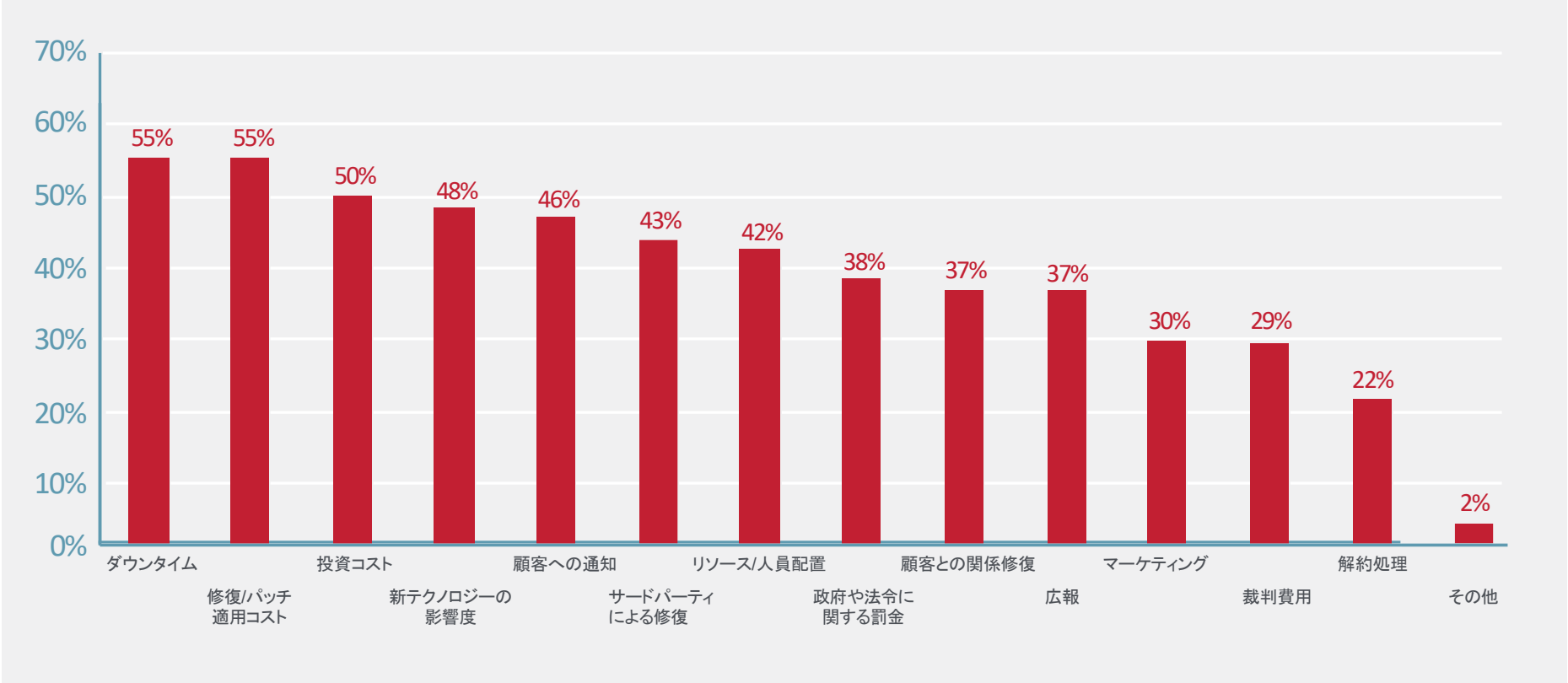
- 有害なボットトラフィックのボリュームを評価します。
- アカウントの乗っ取り試行、インベントリの偽装確保、架空請求、Webスクレイピングに対する可視性が得られます。
- あらゆるチャネルのテスト：Webサイト、モバイルアプリ、API
- 有害なボットのトラフィックを分析して巧妙度をレベル分けし、人に似た振る舞いを追跡します。
- ヒントとアドバイスが得られます。

*顧客は、サーバー、CDN、またはWAFのアクセスログを共有する必要があります。

サイバー攻撃で発生する損害

$1,700,000/売上高 $10億以上企業

（2017: $720,000, 2018: $1,090,000）

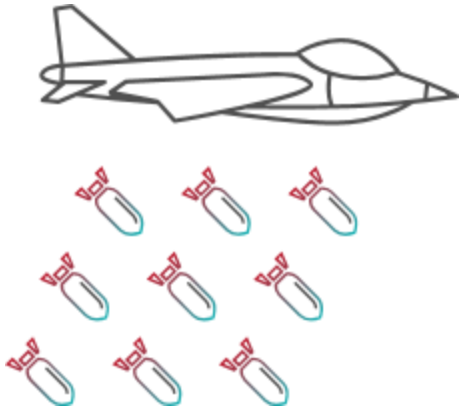


サイバー攻撃による被害コストの要素

Source: 2019-2020 Radware Annual Security Report

Radware Solutions

Radware Solutions against 3 threats

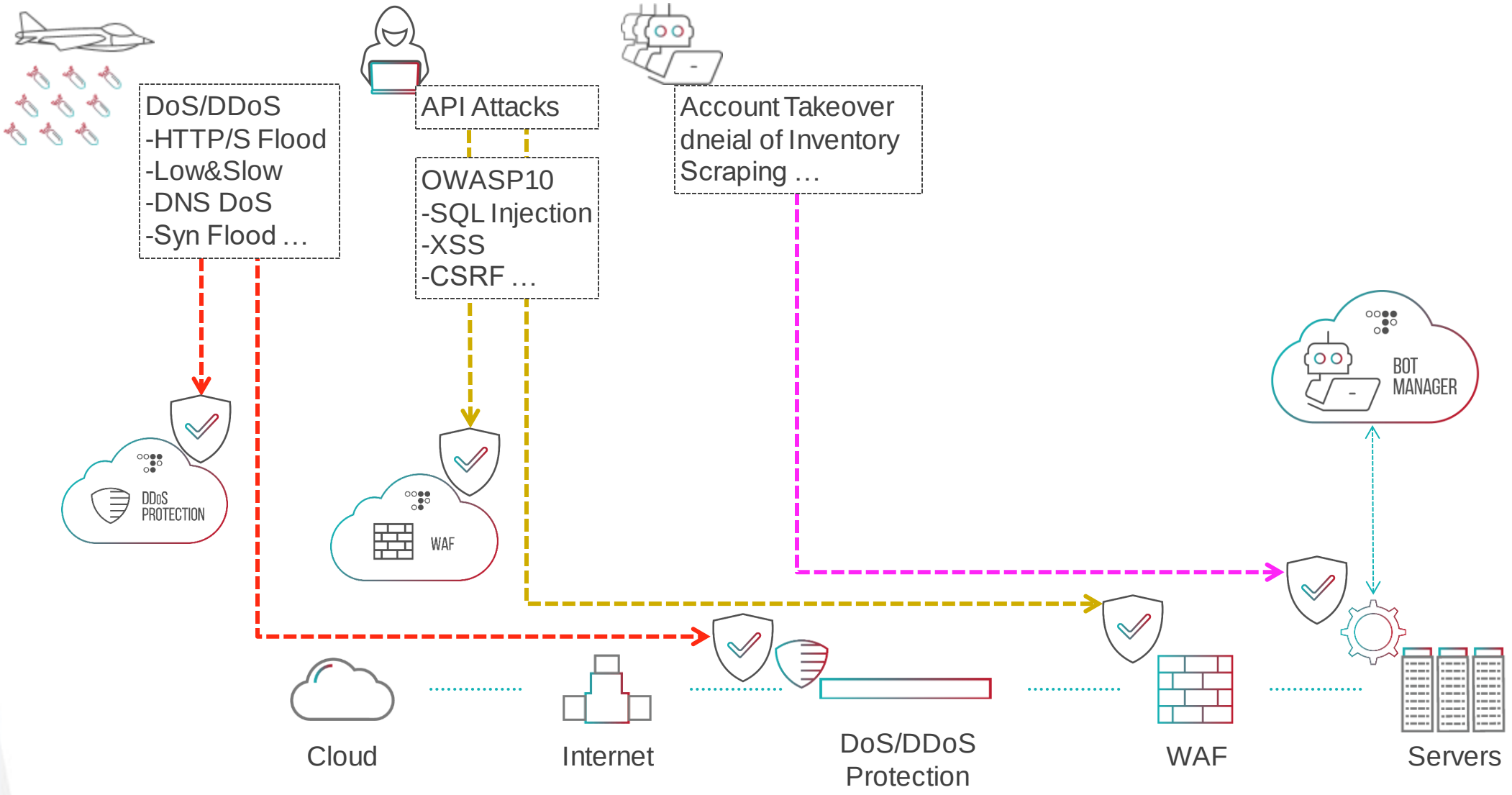


DoS/DDoS

WebApp(OWASP10) / API

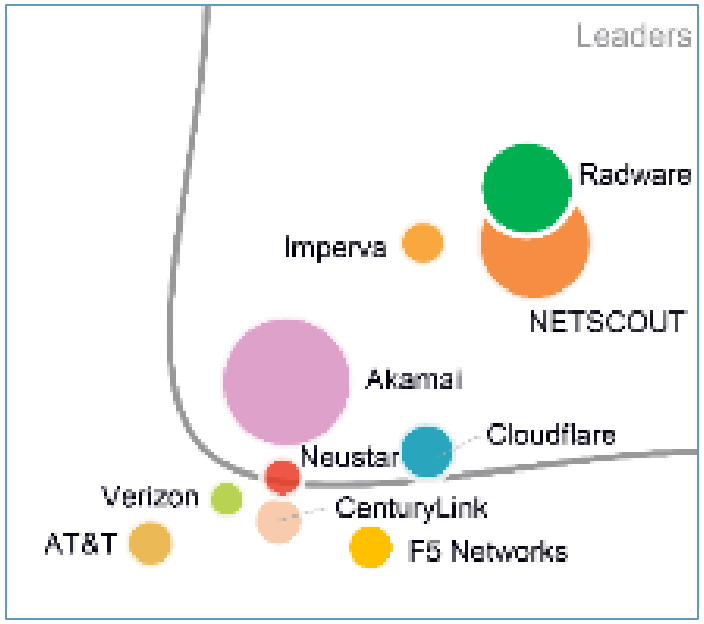
Bot

Radware Solution Map (abstraction)



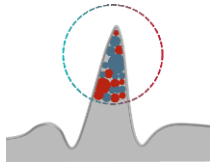
Radware DDoS Protection

テクノロジ ポジション



Source: IDC MarketScape WW DDoS Prevention Solutions 2019

高いプロテクション能力



振る舞い検知
機械学習による適切な保護

ゼロデイ検知
自動リアルタイム
シグネチャ生成

SSLキーレス検知
低遅延、独自の緩和手法

業界唯一の”6”SLA
検知時間や緩和への時間
etc…

柔軟な展開方式

Cloud Service
Always-on/On-demand

Hybrid
Cloud & Appliance

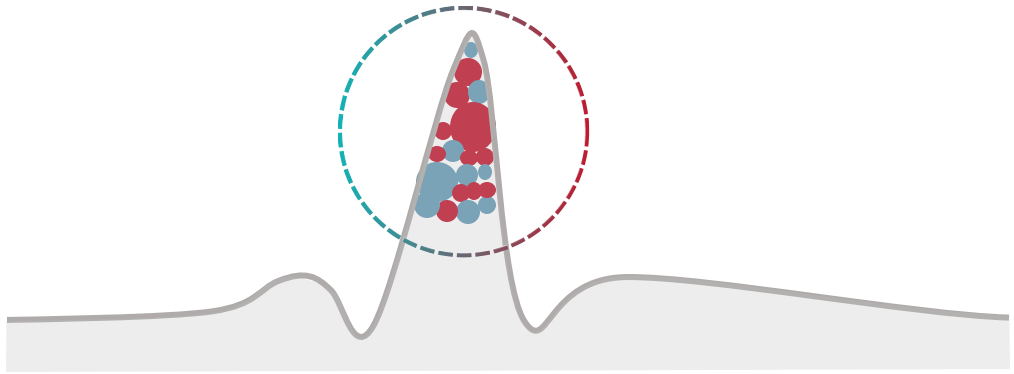
Appliance
Physical/Virtual

Managed Service
Emergency Response Team

Behavioral-Based Detection

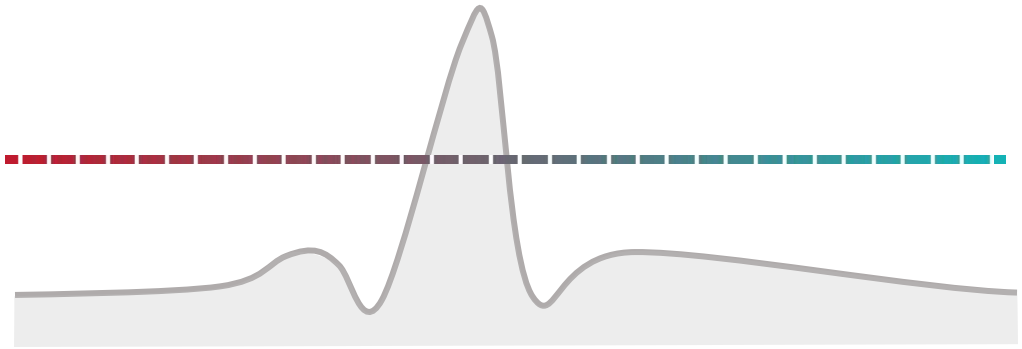
Radware

振る舞い検知



Non-Radware

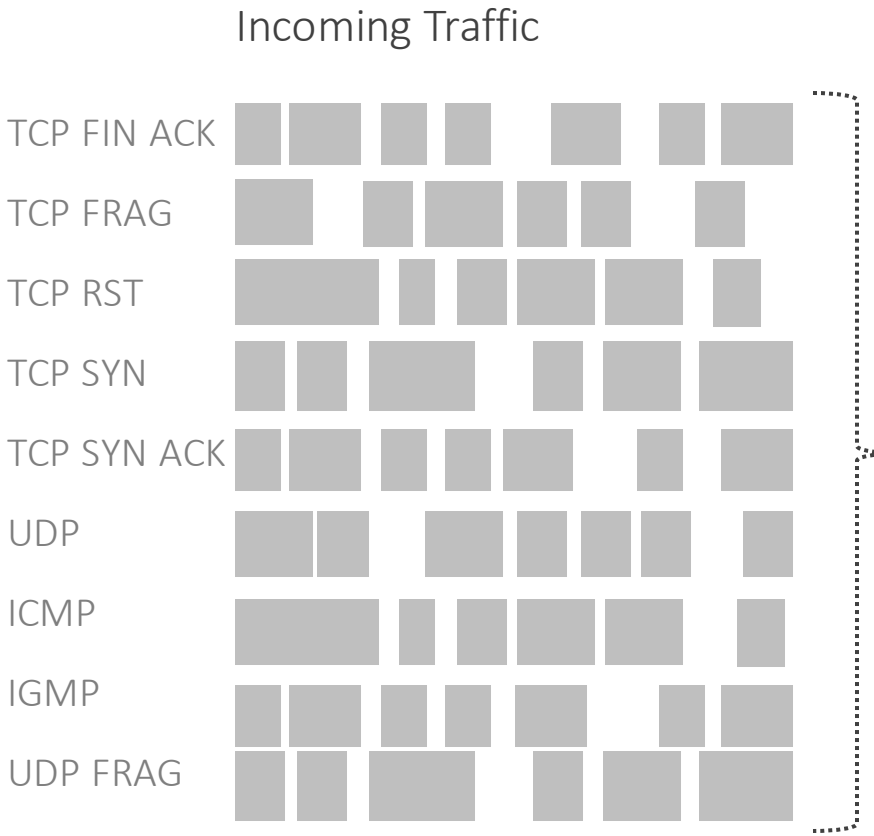
単純なレートリミット



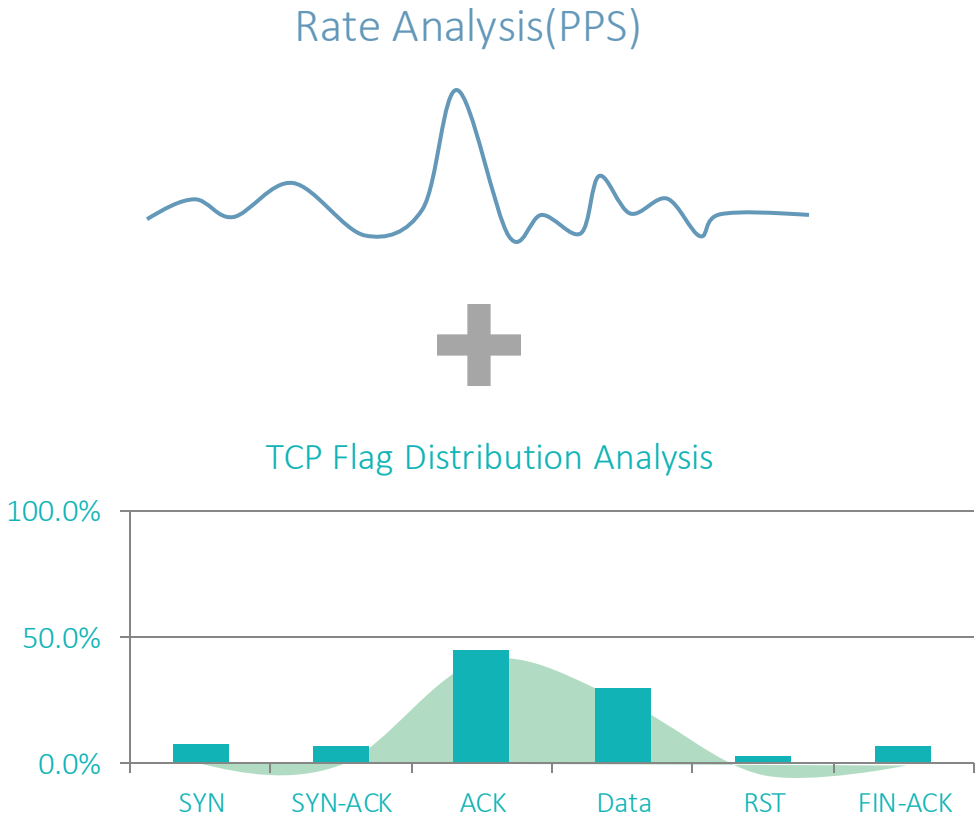
Radware独自の機械学習アルゴリズムで攻撃トラフィックと通常トラフィックを分別

ハイレベルセキュリティと誤検知率低下を両立

Behavioral-Based Detection



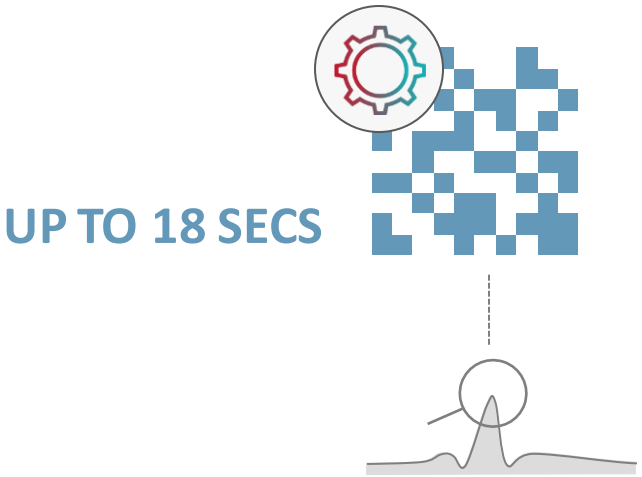
Statistics and Comparing



Zero-Day Detection and Quick Mitigation

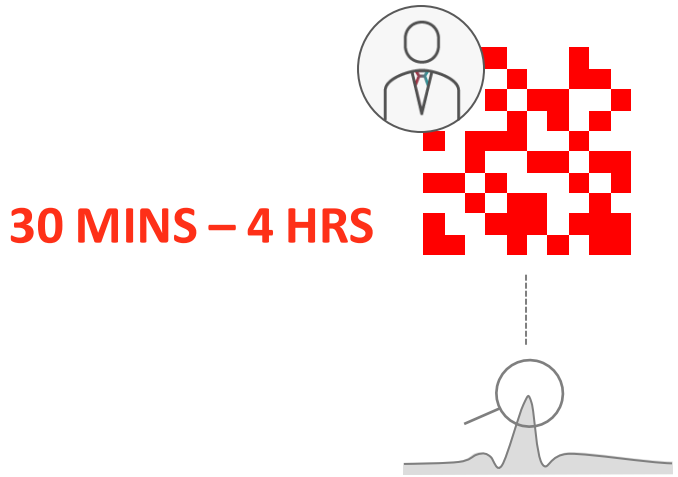
Radware

リアルタイムSignature自動生成



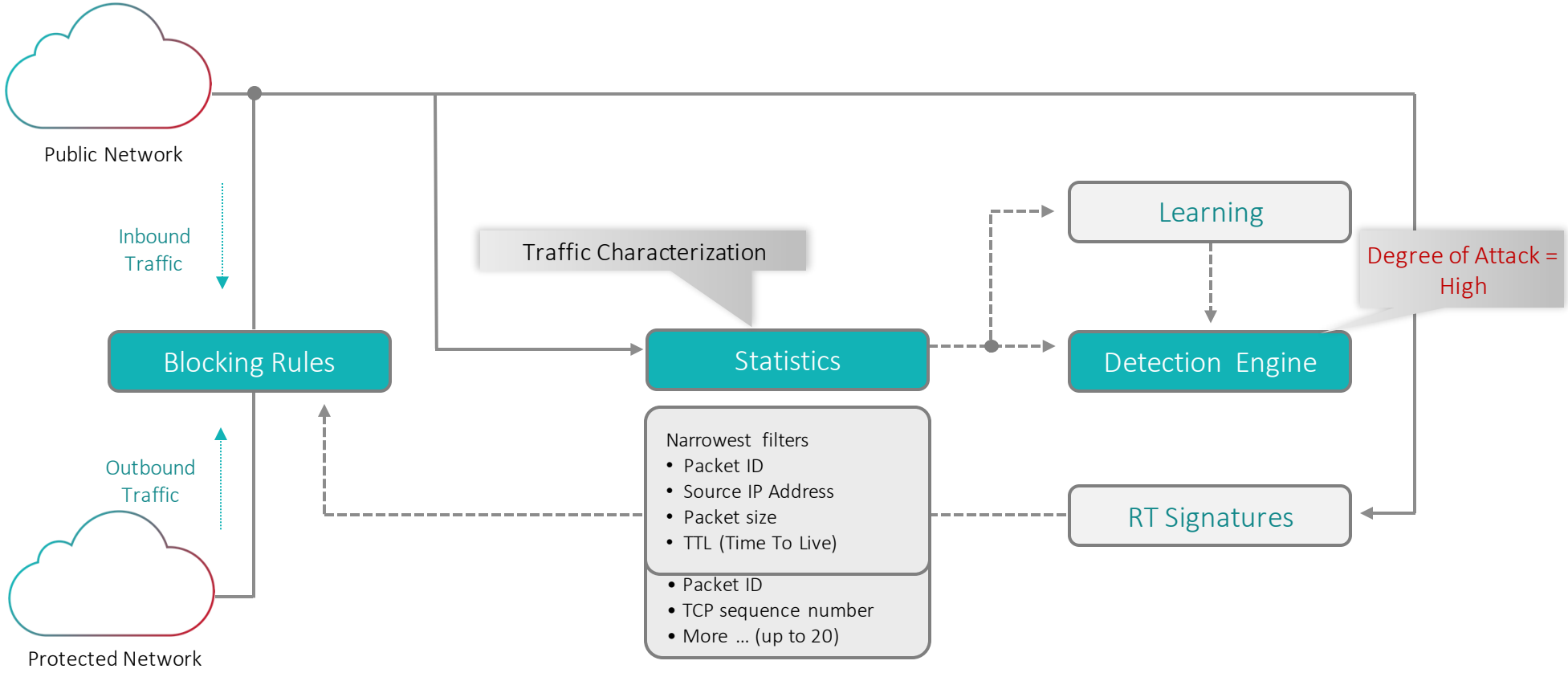
Non-Radware

マニュアルSignature作成



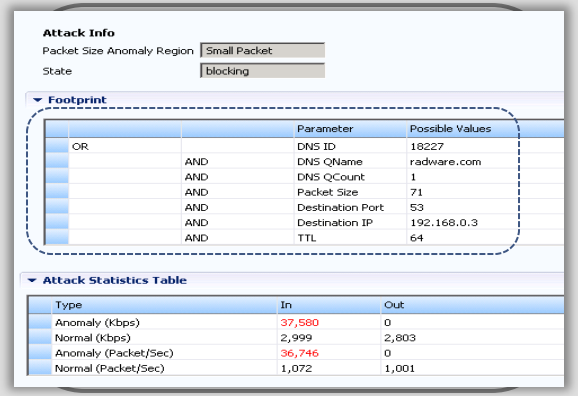
リアルタイムにSignatureを自動生成し適用、調整（SourceIP以外にも複数のパラメータを利用）
ゼロデイ攻撃に秒単位で対応可能

Behavior Analysis + Real Time Signature technology



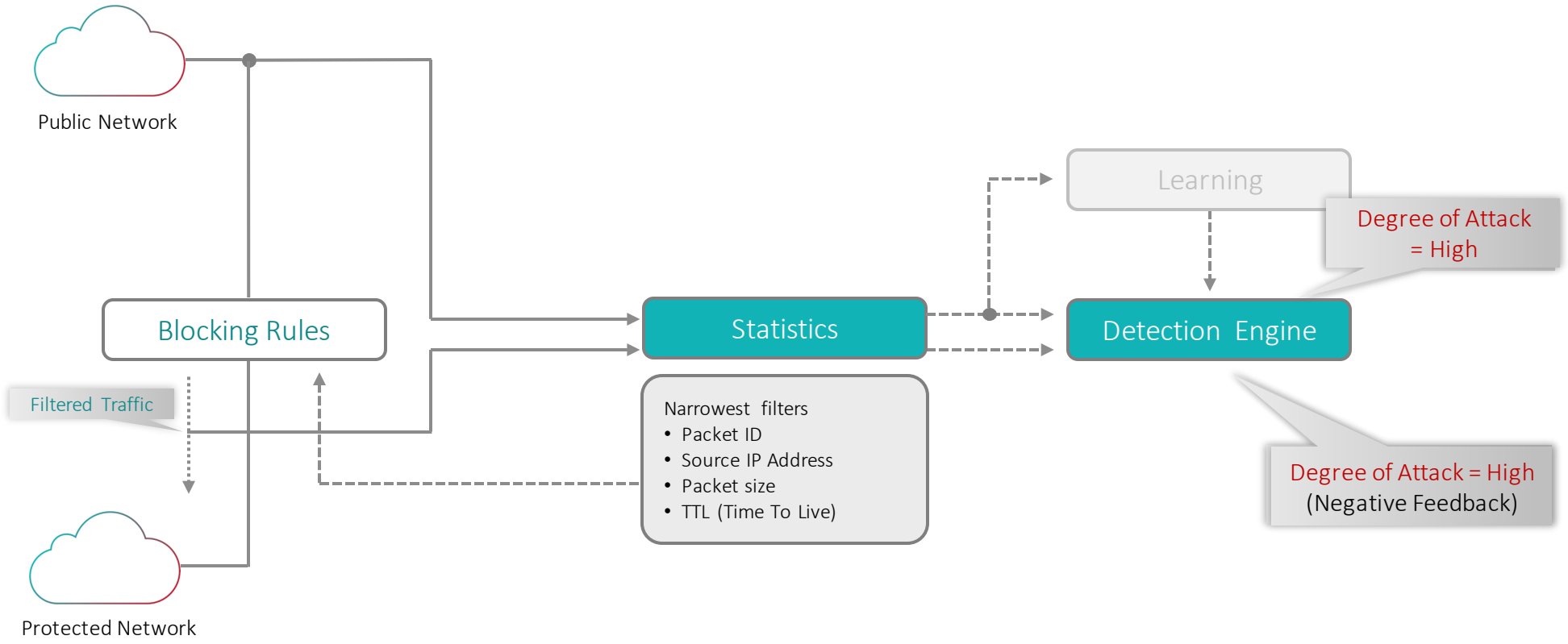
Behavior Analysis + Real Time Signature technology

Mitigation Optimization Process



- Initial filter is generated: Packet ID
- Filter Optimization:
  - Packet ID AND Source IP
  - Packet ID AND Source IP AND Packet size
  - Packet ID AND Source IP AND Packet size AND TTL

Real-Time Signature



Global Cloud Security Network

11 Scrubbing Center **5TB/s** Backbone

業界最大規模のバックボーン（DDoS/WAF）

“6” Service Level Agreement(SLA)

Time to Detect
検知までの時間

Time to Alert
アラートまでの時間

Time to Diversion
切替までの時間
（on-demandの場合）

Time to Mitigate
緩和までの時間

Consistency of Mitigation
緩和の一貫性

Service Availability
サービス可用性

Time to Detect SLAはRadwareだけ

Radware WAF Positive Security Model

Negative Security Model

大半のクラウドWAFサービスとWAFテクノロジーで標準的に採用

既知シグネチャ/ルールを用いて既知攻撃をブロックする

OWASP TOP-10に対して完全な防御は不可能

未知の脆弱性（ゼロデイ攻撃）は防御不可能

Positive Security Model

どのアクションが正規トラフィックであるか学習し定義

権限のないアクセスや未許可のアクションをブロックする

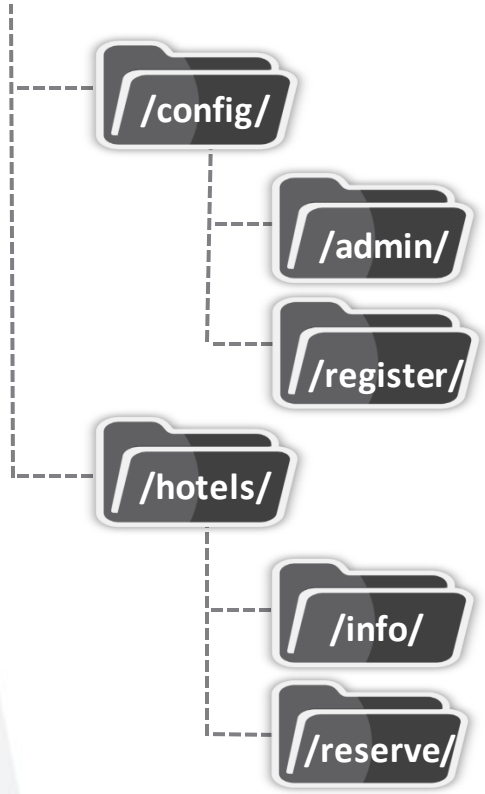
ゼロデイ攻撃や未知の脆弱性を独自の方法で防御

ハイレベル防御：OWASP TOP-10を完全に防御、最小限の誤検知

Radware WAF Auto Policy Generation

App Mapping

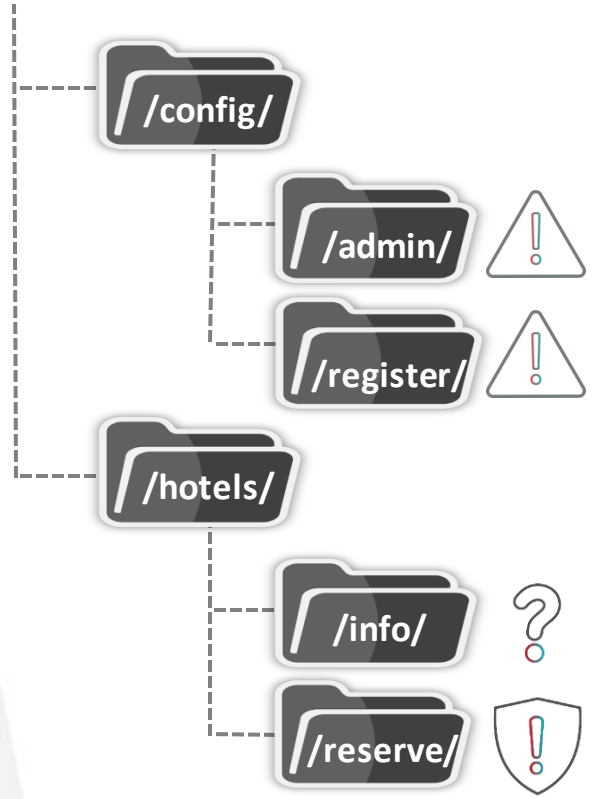
www.reservations.com



Radware WAF Auto Policy Generation

App Mapping | Threat Analysis

www.reservations.com

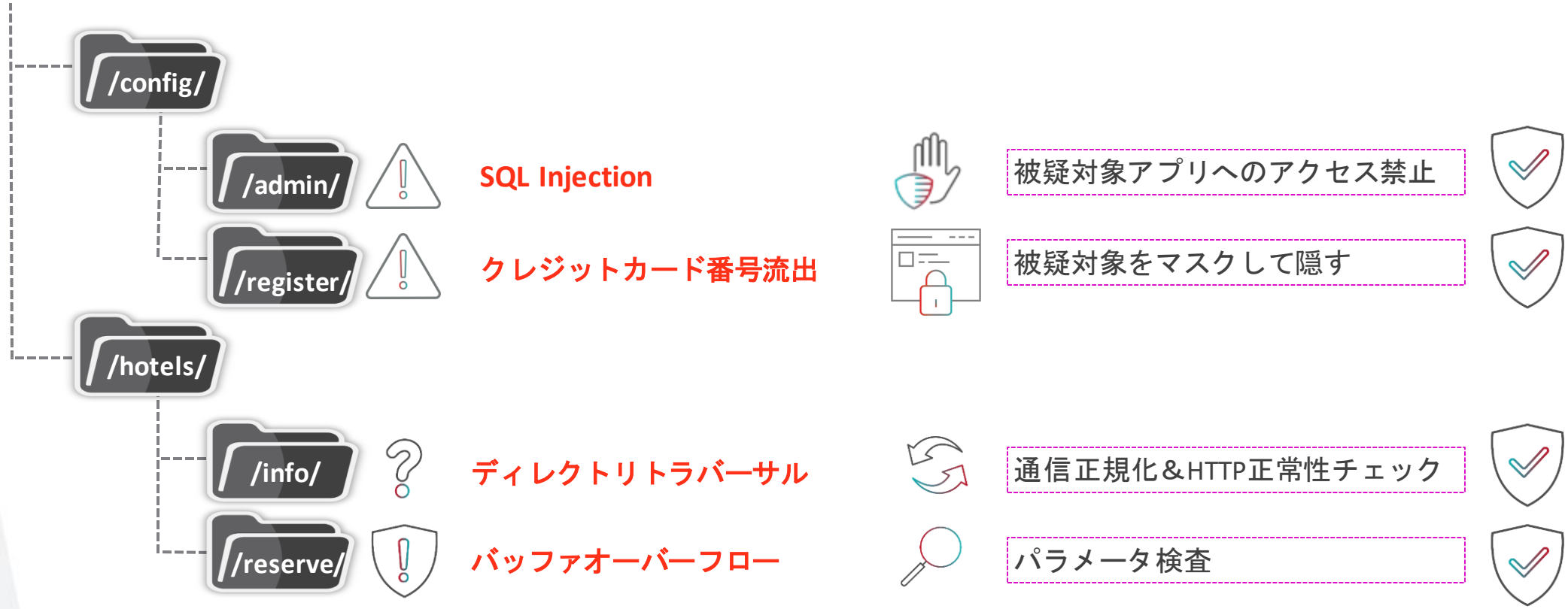


SQL Injection	なりすまし、情報漏えい、 データ改ざん
クレジットカード番号流出	情報漏えい
ディレクトリトラバーサル	ルートアクセス権奪取
バッファオーバーフロー	システムクラッシュ、 性能の著しい低下

Radware WAF Auto Policy Generation

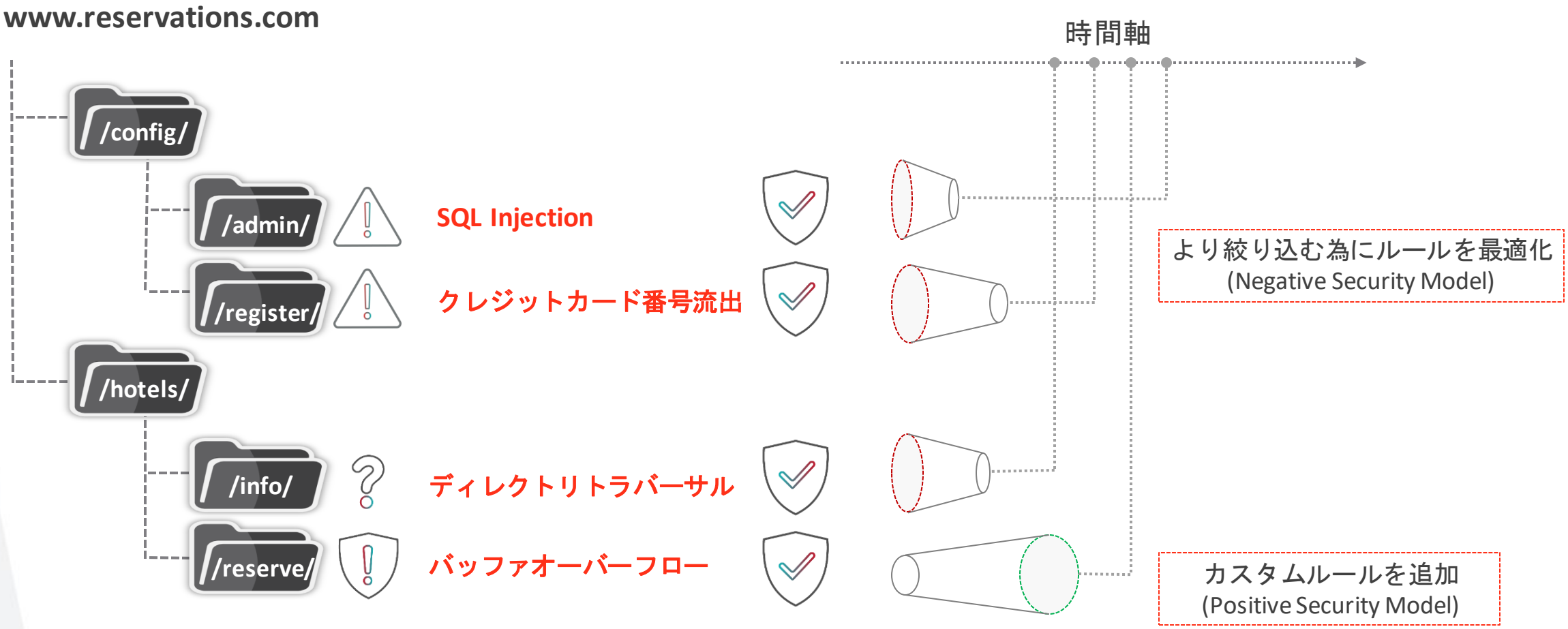
App Mapping | Threat Analysis | Policy Generation

www.reservations.com



Radware WAF Auto Policy Generation

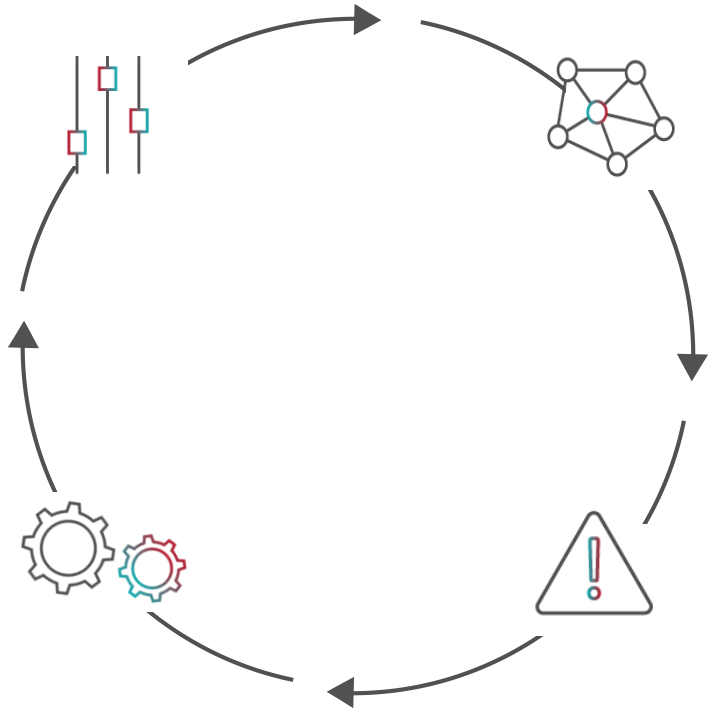
App Mapping | Threat Analysis | Policy Generation | Policy Activation



Radware WAF Auto Policy Generation

自動ポリシーアクティベーション
カスタマイズしたアプリルールを
最適化し精度向上

自動最適化によるポリシー生成
誤検知を最小化する
独創的なルール



アプリマッピング
Webアプリの新規/変更を検知

自動脅威分析
OWASP Top-10すべてと
150以上の攻撃ベクトルに対応

アプリの変化とユーザの振る舞いを継続的に監視しつつ、最適な保護環境を調整

Use Case: Cisco Webex

Challenge

30x DatacenterのWebSecurityとDDoS対策

Radware Solution

DCあたり、
1x DefensePro(DDoS)
4x AppWalls(WAF)
2x Alteon(ADC)

Why Radware

DDoS
- 攻撃手法に対するカバー範囲の広さ
- 検知率の高さ、誤検知無
- 緩和までの時間

WAF
- Auto Learning
- 導入と運用がEasy
- UIがEasy

Competition

A社:
- いくつかの攻撃が通った
- 誤検知（正規ユーザがブロック）
- 誤検知率が高かった

Points of Presence(PoP) for Cloud WAF Service

グローバルに張り巡らされたアプリケーションセキュリティネットワーク（5TB/s）

30のPoPにより対象を低遅延で保護, DDoS 1GB/s Default付与, Bot Manager Option選択可

Radware PoPとAzure DCを活用してCloud WAFを実装

AzureネイティブのクラウドWAFサービス

独自のクラウドセキュリティネットワークに加え、ラドウェアのクラウドWAFサービスは、Microsoft Azureのネットワーク内でネイティブに動作する

Azureのデータセンター内からネイティブに実行できる
唯一のクラウドWAFサービス

ラドウェアのWAFテクノロジーに基づく
エンタープライズレベルの防御

マイクロソフトの光ファイバーバックボーンに基づく**最小遅延時間**

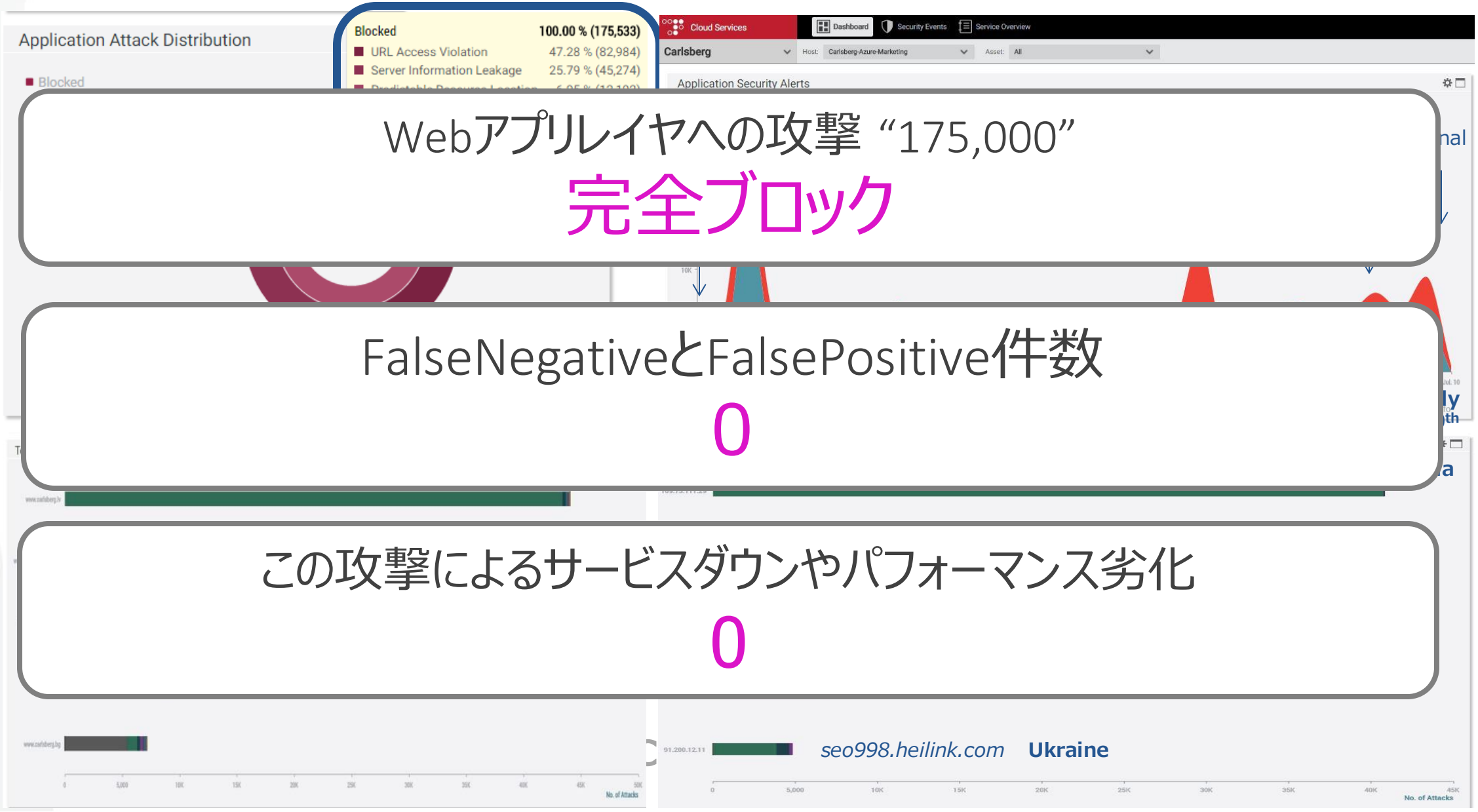
Use Case: Carlsverg

Carlsberg Probably the best beer in the world

インフラ保護	アプリケーション保護
Cloud DDoS Protection 4 つのデータセンター 1 Gbps の正規トラフィック フルマネージド	**Cloud WAF** Azure上の150 のアプリケーション 500 Mbps の正規トラフィック フルマネージド

UEFA EURO2016 FRANCE

UseCase: Carlsverg



Webアプリレイヤへの攻撃 “175,000”

完全ブロック

FalseNegativeとFalsePositive件数

0

この攻撃によるサービスダウンやパフォーマンス劣化

0

Emergency Response Team(ERT)

Attack時の対処等、迅速に対応可能
24時間365日稼働
セキュリティ専門家専任チーム

Security Managed Service w/Experts

- テクニカルアカウントマネージャ
- アナリストおよび専門家
- 脅威のリサーチ
- SOCおよびクラウドの運営

Emergency Response Team(ERT)

ERT攻撃時対応サービス

サイバー攻撃発生時
セキュリティ専門家に即時コンタクト可能

10分 SLA

24時間365日稼働

分析サービス
（Forensic & Advice）

ERTマネージドサービス

Radware Expertsが監視/管理

サクセスマネジャー

24/365 DDoS Protection

On-premise も対応

Emergency Response Team(ERT)

サービスコンポーネント	攻撃時対応サービス	マネージドサービス
24時間365日対応直通回線	✓	✓
攻撃時対応セキュリティ専門家	✓	✓
SLA	10分	10分
攻撃後のフォレンジック分析およびアドバイス	✓	✓
Customer Success Manager（CSM）		✓
プロアクティブ自動脅威アラート		✓
サービスチケット優先処理		✓
セキュリティ構成の最適化		✓
脅威インテリジェンス		✓

Summary

- Cisco – Radware Alliance
- Trend – Cyber Attacks
- Radware Solutions
  - DDoS Protection
  - Web Application Firewall(WAF)
  - BotManager
  - ERT(Emergency Response Team)


radware
THANK YOU!

セキュリティ機能	Bot Manager	従来からあるWAF	両方の併用
シンプルなボットの防御	あり	あり	あり
悪意のあるデバイスのフィンガープリンティング	あり	あり	あり
動的IPおよびヘッドレスブラウザ攻撃の防御	あり	限定的	あり
巧妙なボット攻撃の検知	あり	なし	あり
正規ユーザーをブロックするリスク（誤検知）	なし	高度	なし
ボットインテリジェンスの収集（IP、フィンガープリント、振る舞いパターンなど）	あり	なし	あり
不審なボットタイプに対するアクションのカスタマイズ	あり	なし	あり
OWASP Top 10の脆弱性の防御	なし	あり	あり
APIの脆弱性の防御	限定的	あり	あり
レイヤ7サービス拒否（DoS）攻撃の防御	限定的	あり	あり
HTTPトラフィックインスペクション	なし	あり	あり
機密データのマスキング	なし	あり	あり
HIPAA、PCIへの準拠	限定的	あり	あり
DevOpsとの統合	なし	あり	あり
ネットワークレベルでの悪意のあるソースのブロック - アクセス制御リスト（ACL）	なし	あり	あり