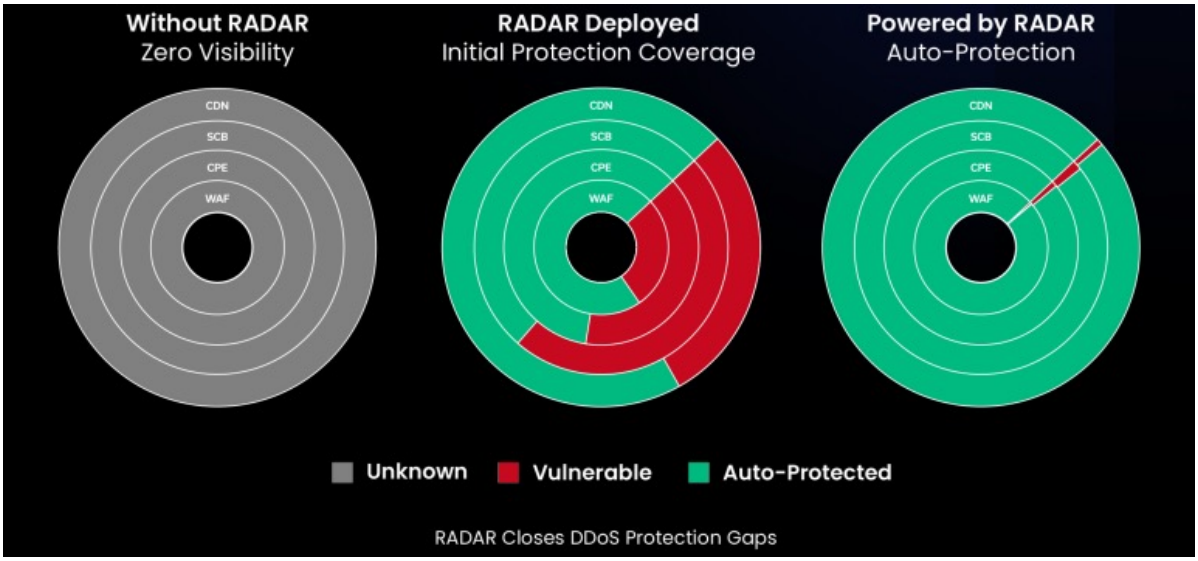
MAZEBOLT

MazeBolt RADAR™

動作中の実運用環境に対するDDoS脆弱性評価・管理製品

製品概要

Webページやデータベースの構築に用いられるサーバに対しては、インターネット上の悪意のあるユーザーから様々な攻撃が日夜行われています。サーバが攻撃されることで情報の不正窃取や動作停止等の被害に遭う危険性が高まり、生産活動への深刻な打撃や顧客からの信用失墜など、多くの不利益が発生します。
MazeBolt RADAR™は、サーバへの主要な攻撃手段として知られるDDoS攻撃対策に特化した脆弱性評価製品です。
運用中の本番環境を停止させることなく、DDoS攻撃に対する脆弱性を多様なDDoS攻撃ベクトルのエミュレーションにより検証し、持続的な脆弱性管理が行えます。



特長

■ 動作中の実運用環境への継続的なテスト
RADARでの検証にあたって、実運用環境の一時停止や検証用環境の準備等は不要です。本製品は、実運用環境の動作を停止することなく、DDoS対策の有効性に関するエミュレーション試験を実施できます。そのため、DDoS対策の継続的な検証と管理についても、組織に大きな損害を及ぼすダウンタイムを発生させることなく行えます。

■ 自動DDoS緩和の検証
RADARは、実運用環境に対して実施する擬似的なDDoS攻撃が自動的に緩和されるか否か、についても検証を行い、緩和されなかった場合には当該箇所を『DDoS攻撃による被害発生リスクが高い因子』として特定します。
その上で、自動的に攻撃緩和が行える状態へと修正を行うために必要な情報を提供し、DDoS攻撃がITサービスにダウンタイムや障害を引き起こしにくい環境の構築をサポートします。

■ 検証結果の集約
検証を通して判明した脆弱性は、レイヤーごと、および攻撃ベクトルごとにダッシュボードとレポートに集約され、全てのテストに占める防御が不十分だった箇所の割合も確認可能です。現状の対策がどの程度有効であるかも把握することが可能であると同時に、現在に至るまでの修正や保護の進捗推移を一目で確認することができるため、今後の対策指針策定にもお役立ていただけます。

ComWorth

検証手法

DDoSの攻撃手段は刻々と変化しています。そのため、ある時点で十分な対策を行えている状態であっても、その対策は時間経過とともに古いものになっていき、攻撃被害に遭うリスクが高まります。
しかしMazeBolt RADAR™は以下の検証サイクルを繰り返すことで、検証対象のDDoS対策にどの程度の有効性があるか、通常の運用を妨げることなく継続的にテストを行うため、気づかないうちに現在のDDoS攻撃に対して無力な状況に陥ってしまう事態を防ぐことが可能です。

マッピング
公開状態のIPアドレスやFQDNをマッピングします。

検証
修正対応により、リスクが再発しない状態になっていることを検証します。

試験
各レイヤー毎に施されているDDoS対策へのテストを行います。

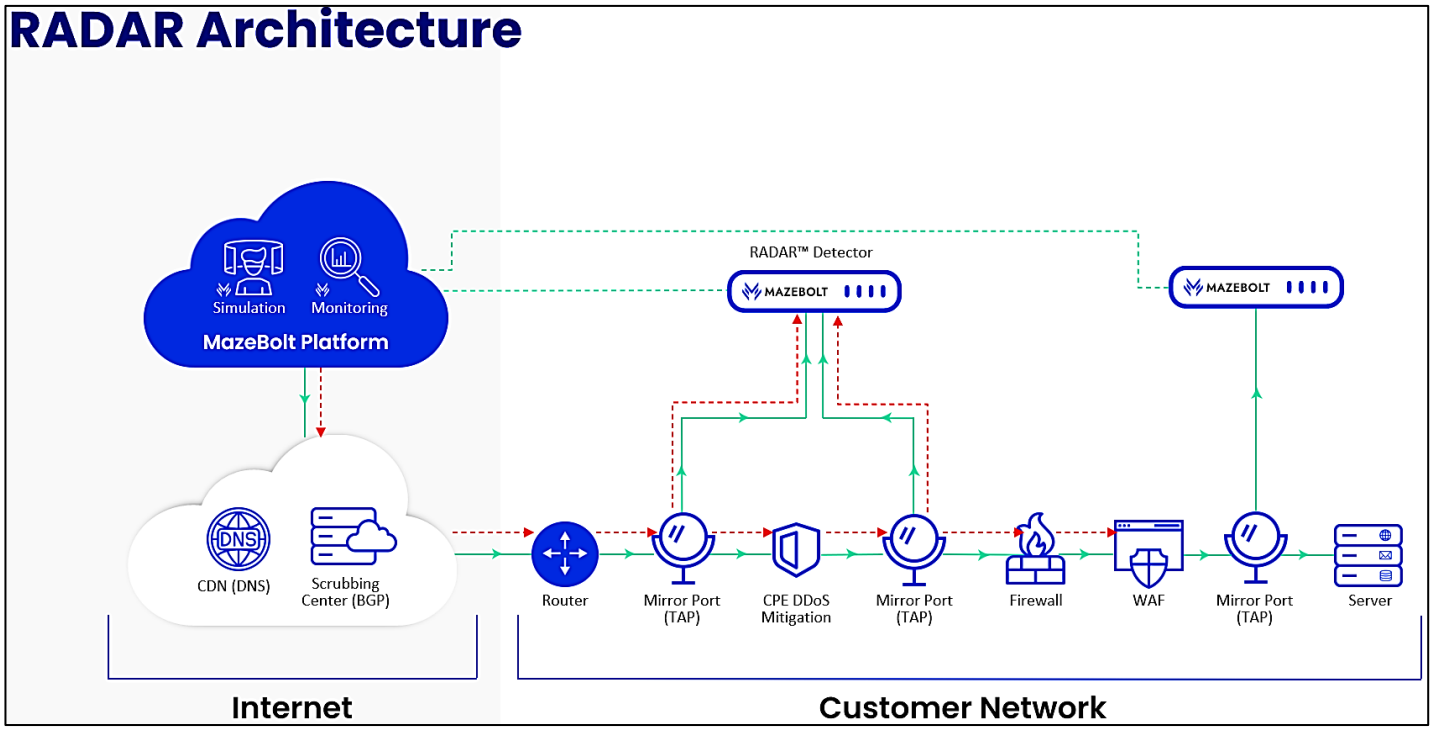
修復
優先順位情報を付した修復推奨事項をもとに、実際の修正対応を行います。

特定
テストを通して、DDoS対策が不十分である箇所を特定します。

優先順位付け
DDoS対策が不十分な箇所に関して、修復対応の優先順位付けを行います。

構成図

RADARは検証対象とするターゲットに対し、144種類以上にも及ぶDDoS攻撃ベクトルのエミュレーションを行います。
これらの攻撃エミュレーションに対し、ネットワーク内に導入されているCDNやWAFなどのDDoS対策コンポーネントがどのように機能しているか、すなわちこれらのコンポーネントのうちどの部分で当該の通信が遮断されているかを、各レイヤーにおける通信状況から判断します。
これにより、各攻撃ベクトルに対する対策の有効性や脆弱性がある箇所の特定といった評価が行えます。



1.0.0

お問い合わせ

株式会社コムワース 通信機器事業部
TEL: 03-3777-0888 FAX: 03-3772-8497
Web: https://www.comworth.co.jp
Mail: info2@comworth.co.jp