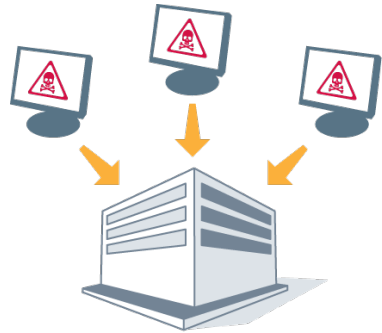


Webアプリケーションのための BIG-IP ADCファイアウォール

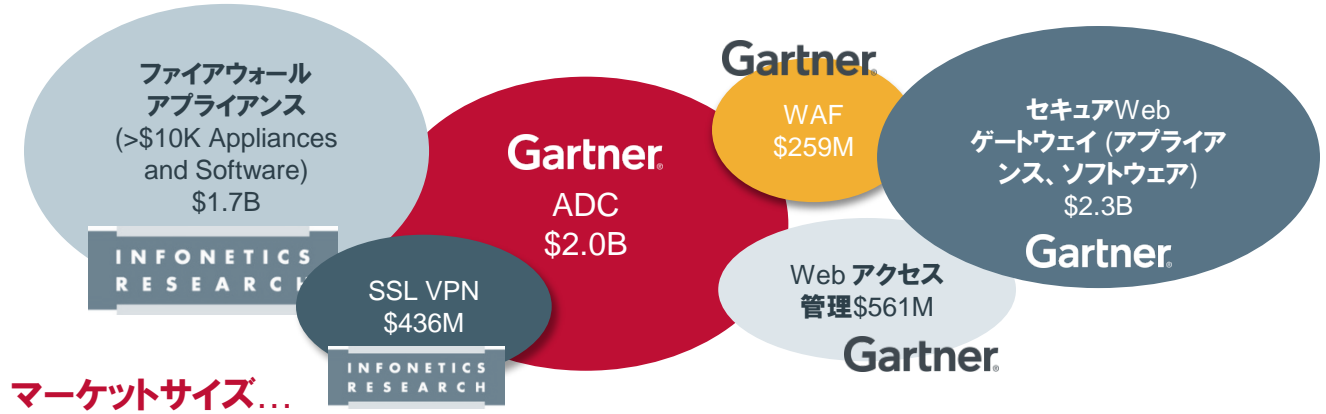


IT agility. Your way.®

セキュリティニーズの変化



90%以上のIT管理者が...
セキュリティのコンテキスト
を必要としている



マーケットサイズ...

セキュリティは以前として課題が山積み...
IT組織の9/10はパフォーマンスの為に
セキュリティを犠牲にしている



セキュリティデバイスの拡大は
最も困難な課題になりつつある...
セキュリティに関する最大の課題は
増大するデバイスへ柔軟に対応する
事である



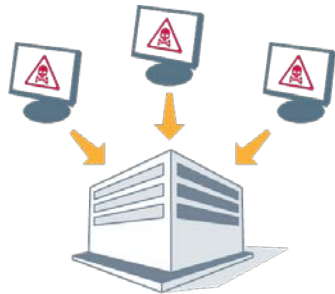
従来型のネットワークデバイスは高負荷時の問題がある
... メジャーなファイアウォールの3/6は安定性に問題がある、
5/6は一般的な攻撃に脆弱である

3つ変化がセキュリティを複雑に

1. 攻撃の巧妙化



アプリ狙い



巧妙化する攻撃

2. ITインフラの変化



クラウドによる
アプリ展開の迅速/分散化



デバイス多様化
コンシューマライゼーション

3. ユーザの変化



マルチデバイス



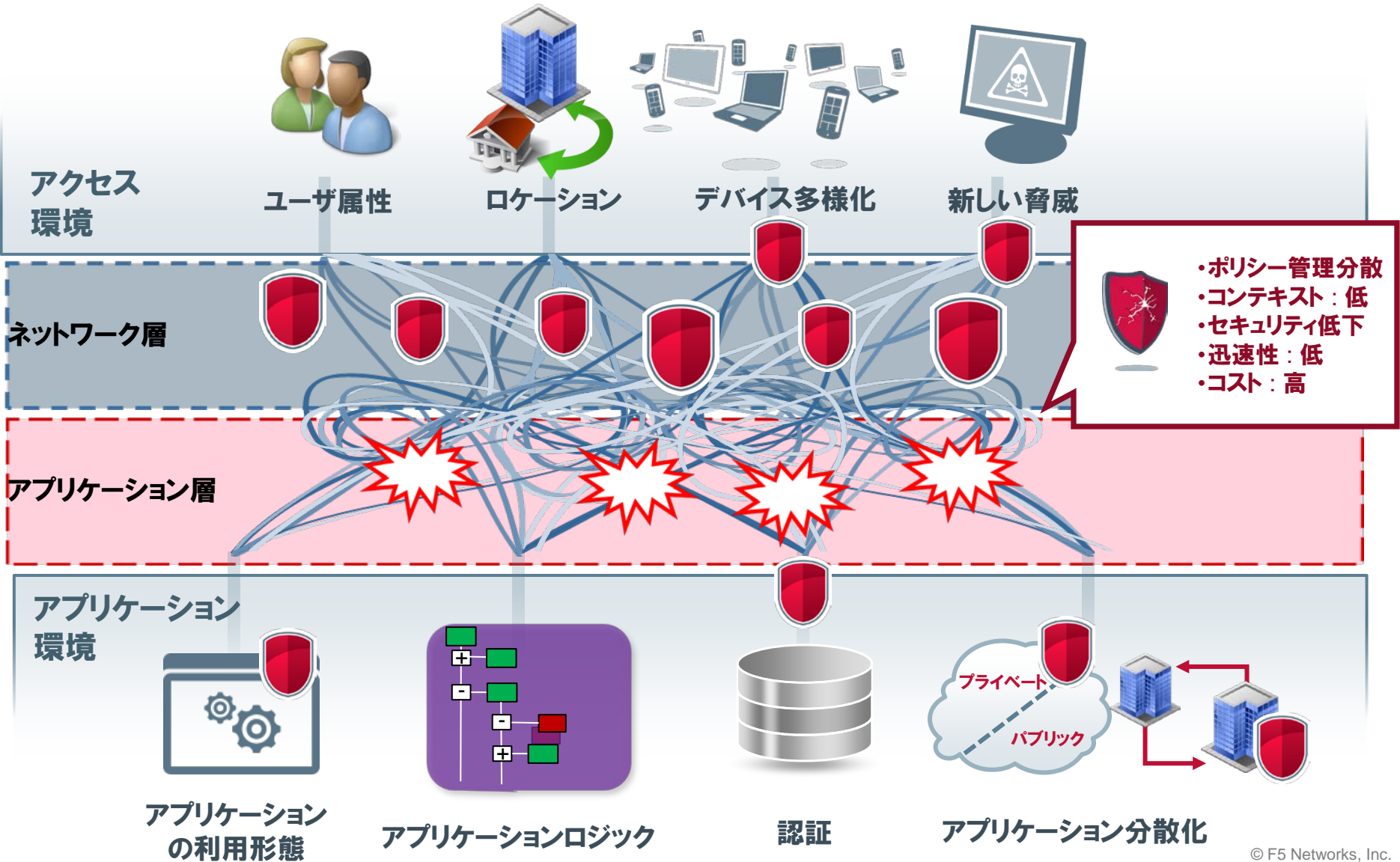
モバイル/テレワーク



ユーザの増減/多様化

セキュリティ
の複雑化

課題：アプリ視点の欠如、セキュリティ管理の分散化



アプリケーション視点のユニファイド・セキュリティ・コントロール

ネットワーク上に統合化セキュリティコントロールポイントを配置

アクセス環境



コンテキスト

- EPチェック
- アプリケーションロジック
- 認証連携

拡張/迅速/柔軟

- オンデマンド
- プログラマブル
- 認証基盤連携



統合化

- デバイス
- マルチレイ
- ワーク

コミュニティ

- DevCentral



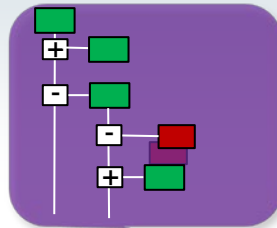
ユニファイドセキュリティ

- 再利用性が高い
- セキュリティ：高い
- 統合化
- コンテキストの理解
- 素早い対応
- コスト：低

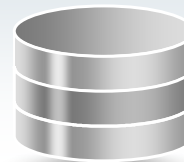
アプリケーション環境



アプリケーションの利用形態



アプリケーションロジック



認証



アプリケーション分散化

何故、アプリケーション・デリバリー・コントローラ (ADC) ファイアウォールなのか？

BIG-IPには、既に多数のセキュリティ機能がある:

- L3セキュリティ - パケット・フィルタリング、IPプロトコル検証、フラグメンテーション、チェックサム、長さなど
- L4セキュリティ - TCPプロトコル検証、長さ、チェックサム、TCP DoS攻撃など
- L5セキュリティ - HTTP、SMTP、SIPなどのプロトコルレベルのセキュリティ
- L7セキュリティ - Webアプリケーションのセキュリティ
- リモート・アクセス・セキュリティ - L4 ACL、L7 ACL、クライアント側セキュリティ

| TMOS持つ強み | ユーザーメリット |
|---------------|------------------------------|
| 高パフォーマンス | TMOSはパフォーマンス最適化を追求して設計 |
| バーチャル・サーバ | 一致しないパケットは破棄などの使い方が可能 |
| フルプロキシアーキテクチャ | トラフィックを理解し管理する |
| iRules | ゼロデイ攻撃などに対して迅速に対応可能 |
| ASM | 豊富な実績を誇るWebアプリケーション・ファイアウォール |

ADC Firewall機能により何が変わるか

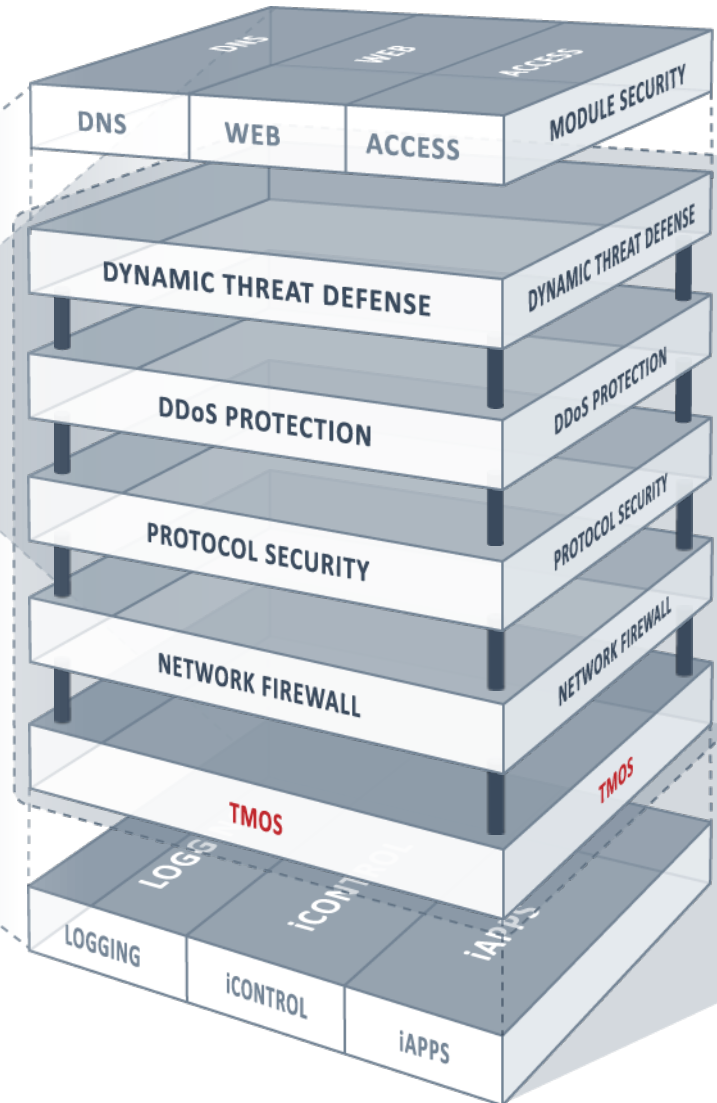
▼ 新しいBIG-IPの価値

- アプリケーション層を最も理解するファイアウォールソリューション
- 今までにないセキュリティに特化したビジネスへ参入
- Firewall機能を統合した「strategic point of control」
- ICASA認証取得による信頼性

F5のアプリケーション・デリバリー・コントローラは ファイアウォール・セキュリティ・ゲートウェイ

TMOS

- 全く新しい次元のパフォーマンスを提供
 - 従来のファイアウォールの5~8倍のパフォーマンス
- 設備投資や運用コストを削
 - ITインフラの運用、セキュリティの共通コントロールプレーンを作成
- フルプロキシ・アーキテクチャ
- サービス管理を効率化
 - TMOSは、高速ロギング、監査、ポリシー管理、SIEM(Security Information and Event Management)と呼ばれるセキュリティ情報およびイベント管理に関する概念に準拠

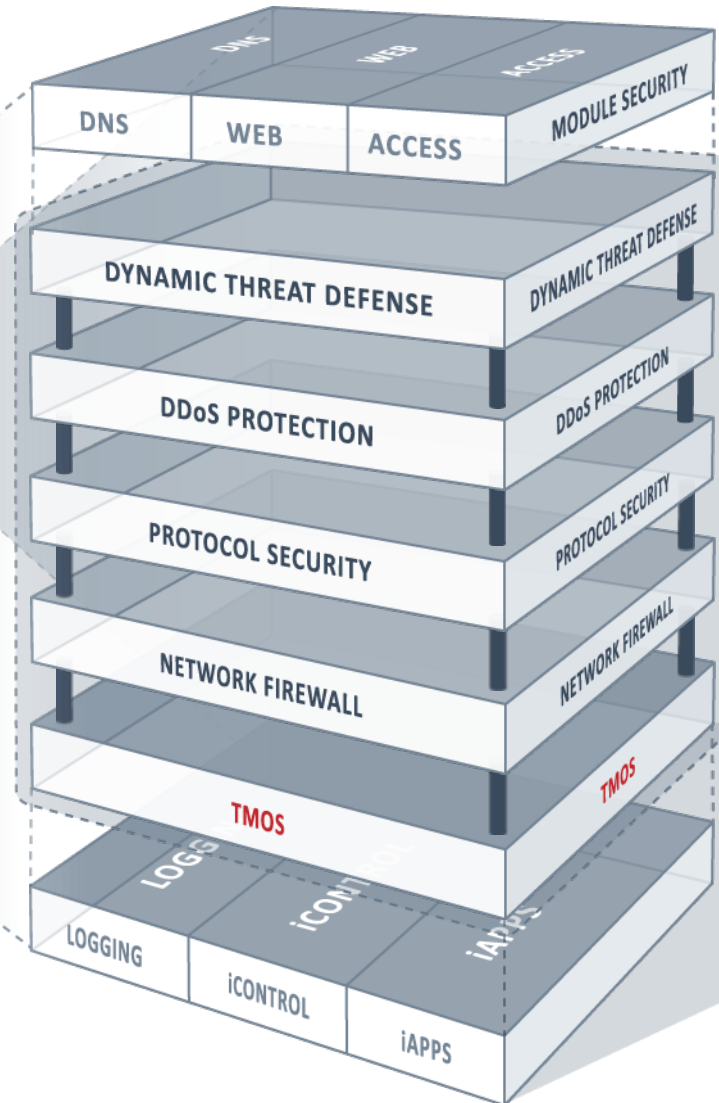


F5のアプリケーション・デリバリー・コントローラは ファイアウォール・セキュリティ・ゲートウェイ



ネットワーク・ファイアウォール

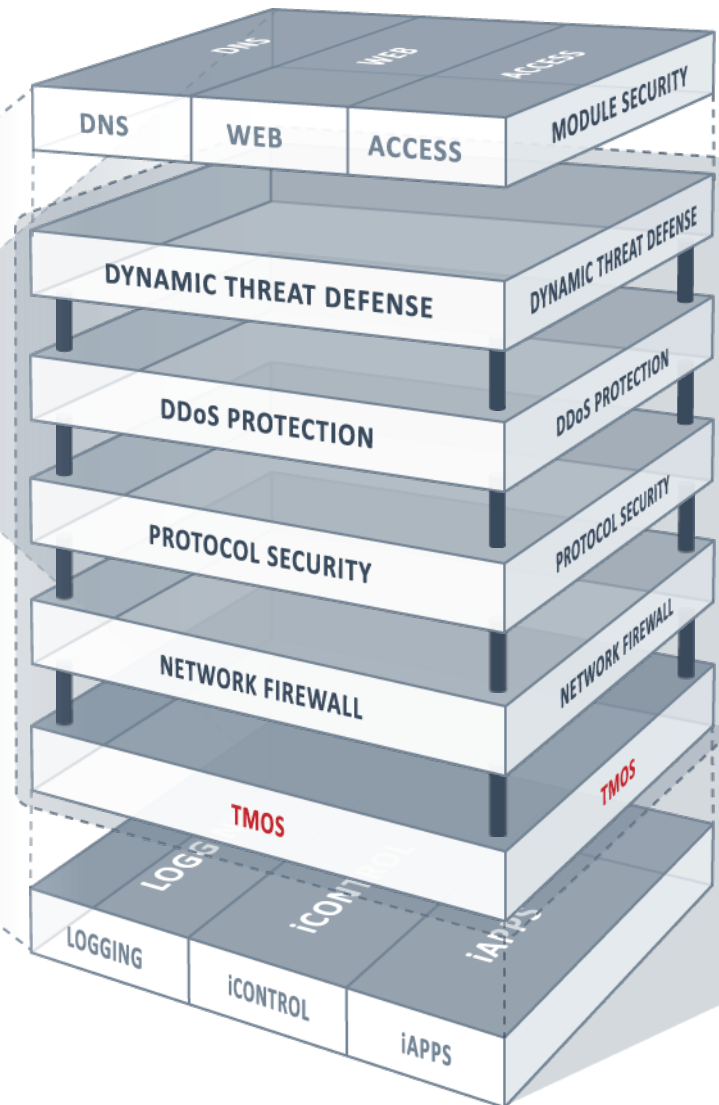
- ステートフル・ファイアウォール
 - ICSAネットワーク・ファイアウォール認証取得
- 堅固なセキュリティ設計
 - デフォルト拒否、パケットフィルタACL機能等
- 包括的な検査
 - SSL終端機能、検査、再暗号化と証明書保管



F5のアプリケーション・デリバリー・コントローラは ファイアウォール・セキュリティ・ゲートウェイ

プロトコル・セキュリティ

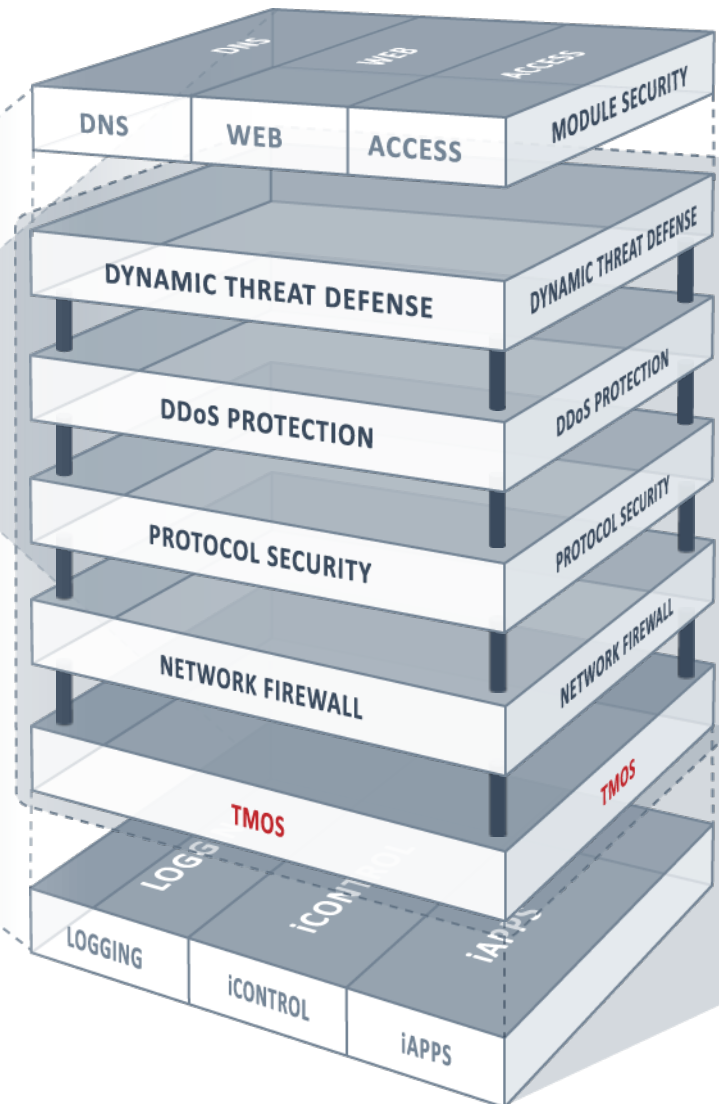
- プロトコル準拠
 - 標準的に下記のプロトコルのデコードをサポート
 - IPv4、IPv6、TCP、HTTP、SIP、DNS、SMTP、FTP、Diameter、RADIUS
- 迅速な実装が可能
 - 新しいプロトコルなどに対する管理、コントロールを素早く適用



F5のアプリケーション・デリバリー・コントローラは ファイアウォール・セキュリティ・ゲートウェイ

DDoS攻撃からの保護

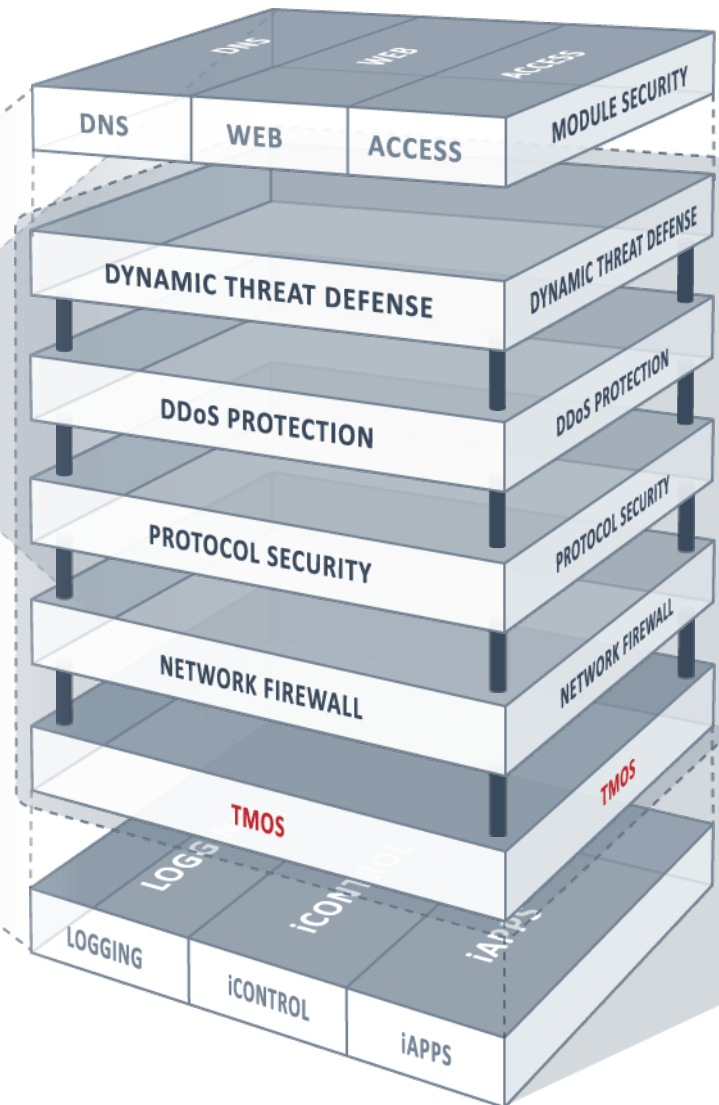
- 高パフォーマンス
 - 従来のソリューションに比べて5~8倍の数のコネクションをサポート
- 多様なDDoS攻撃に対する防御
 - 30種以上の攻撃に対応可能
- 様々なレイヤーの攻撃を防御
 - HTTP、DNS、SIPを狙ったネットワークレイヤーからアプリケーションレイヤーへの攻撃まで幅広く阻止



F5のアプリケーション・デリバリー・コントローラは ファイアウォール・セキュリティ・ゲートウェイ

多様な外部脅威に対して有効

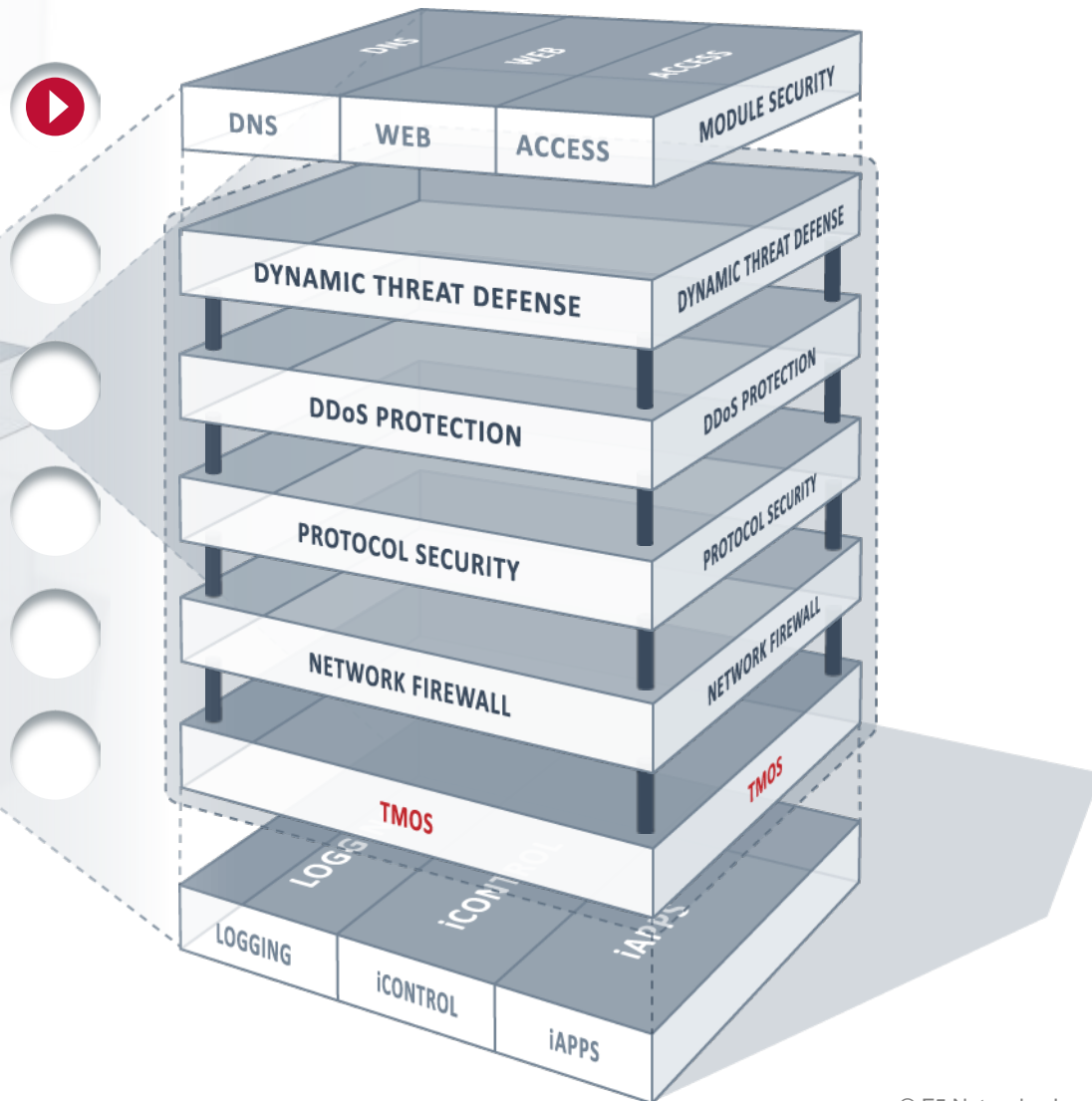
- 新たな脅威からの保護
 - ASP.NETのパディング・オラクル攻撃
 - TLS中間者攻撃【man-in-the-middle attack】(マン・イン・ザ・ミドル攻撃)攻撃
 - FTPブルートフォース攻撃
 - HTTP “Accept” ヘッダ攻撃
 - PushDoポット攻撃の緩和
- コンテキストを理解し適切な対応
 - Traffic Steering
 - ジオロケーション
 - 接続数の制限
- 活発なユーザーコミュニティの活用
 - ツール、テクニック、コラボレーション



F5のアプリケーション・デリバリー・コントローラは ファイアウォール・セキュリティ・ゲートウェイ

モジュール構造のセキュリティ

- DNS関連のセキュリティ機能
 - DNS Express
 - DNSSEC
 - IP Anycast
- Webセキュリティ
 - Webアプリケーション・ファイアウォールおよびWebサービスセキュリティ
- アクセスのセキュリティ
 - 認証、承認、シングルサインオン (SSO)





IT agility. Your way.®