

マルウェア感染拡大防止ソリューション

～サイバー攻撃を受けた端末を自動で切断、悪意ある通信をあぶりだす～

シグネチャベースだけのアンチウイルス対策でなく多層防御が必要

激増する未知のマルウェアへのシグネチャベース以外での対応

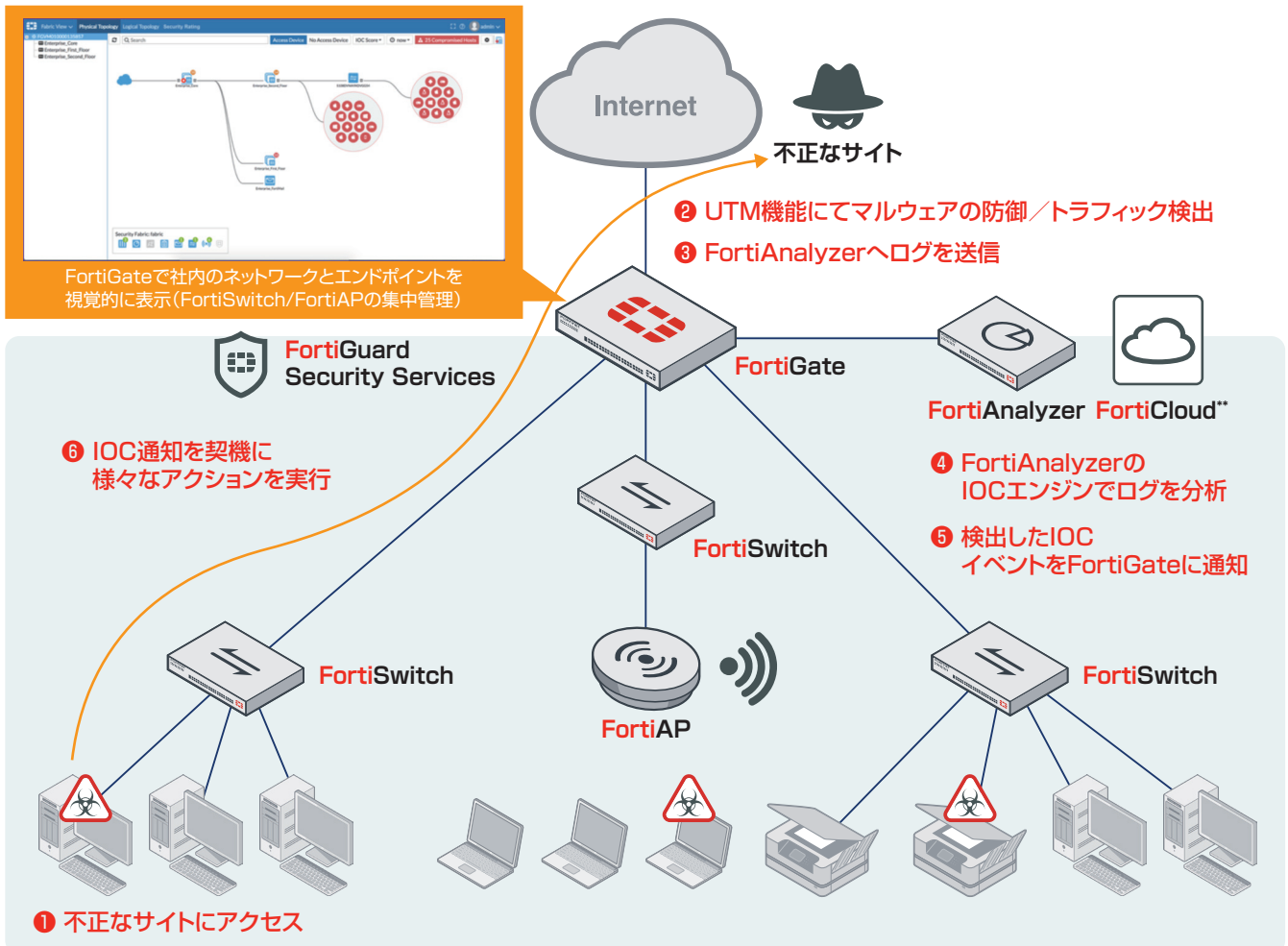
疑わしいWebサイトにアクセスした端末の洗い出し

感染の疑われる端末への早期対応

社内感染速度の速いマルウェアへの対策が必要

これからは、サイバー攻撃に対して防御だけでなく「検知」と「対応」が必要
脅威を高い精度で検出するIOC*が様々なマルウェアの検知を支援

自動化された防御で
脅威に即応



*:IOCは"Indicator of Compromise"の略で、感染端末の挙動、通信先のURL、IP、ドメイン名等を追跡しマルウェア定義を元に比較分析します。検体を必要とせず、マルウェアによりアクセスされたURLが評価対象です。累積されたアクセスログが相関分析を行い、マルウェア感染の挙動が疑われるデバイスを検出します。

**：FortiCloudでのIOC対応はロードマップ

フォーティネットソリューションによる優位性

複数のトリガー*と
多様なアクション**に対応

有線PCから
スマートデバイスまで
自動及び手動で隔離可能



フォーティネットの
優位性

FortiGateで
社内LANを集中管理
(FortiSwitch/FortiAP)

社内LAN接続端末を
自動／視覚的に表示

*:感染端末やシステムの再起動 **:自動隔離や自動通知メール

設定例：感染端末のネットワークからの自動隔離

<FortiGateの管理画面>

トリガー
侵害されたホスト

アクション
Eメール FortiExplorer通知 アクセスメッセージ

[アラートEメール]+[アクセスレイヤー隔離]で自動で隔離を実施

感染端末は赤く表示され隔離された端末は黄と黒の破線で囲み表示

設定例：管理者による手動隔離

<FortiAnalyzerの管理画面>

#	エンドユーザー	最後の検知	ホスト名	OS	判定	脅威数	確認
1	10.130.155.30	07/25/2018	10.130.155.30	Windows 10	ウイルス感染	1	ok
2	Kodaka (172.16.10.2)	07/30/2018	DESKTOP-2070A93	Windows 10	ウイルス感染	1	Ask

FortiAnalyzerで侵害されたホストを検知し、アラートEメールを送信

アラートEメールの情報(IPアドレス、MACアドレス)をもとにセキュリティファブリックのトポロジで検索し、デバイスを特定

特定したデバイス上で右クリックし[ホストを隔離]で隔離実施

送信元アドレス(172.16.0.2)でドリルダウンして詳細表示
Quarantine Host on FortiSwitch

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ