

2019年の脅威予測

McAfee Labs

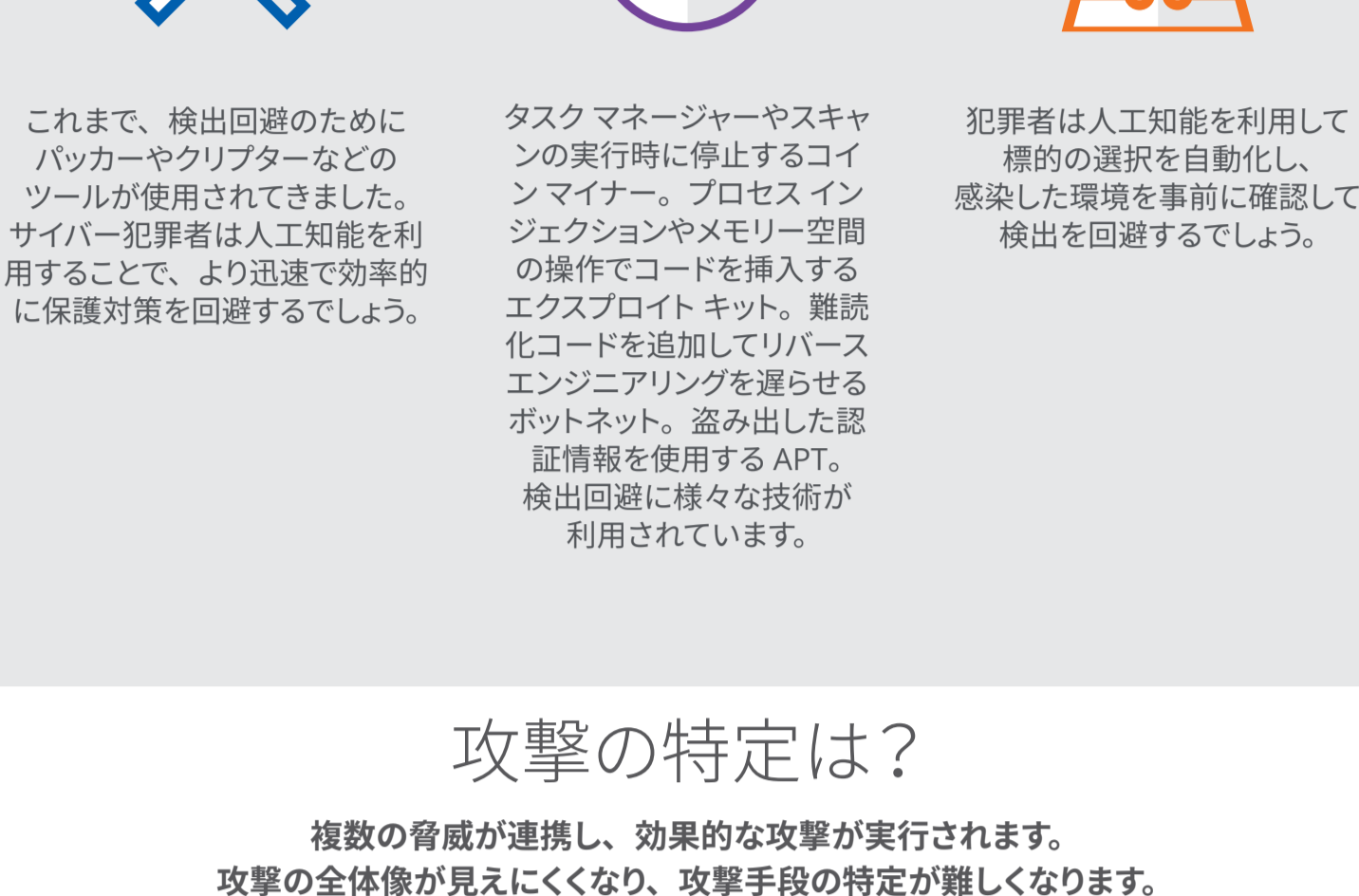
サイバー犯罪者の連携

サイバー犯罪者の連携が進み、サービスとしてのマルウェアが増加します。



回避技術

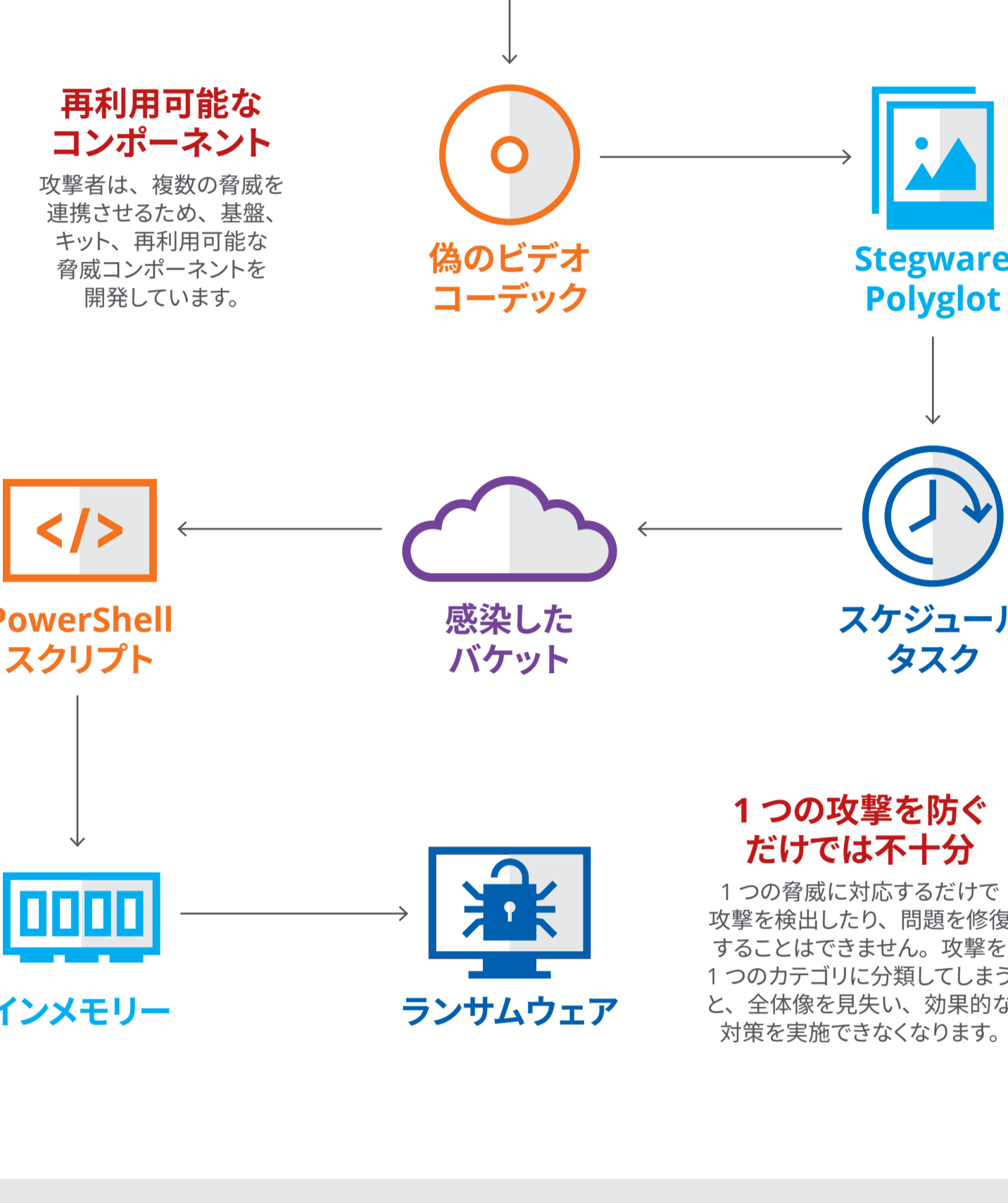
攻撃のアウトソーシング化が進み、回避技術で人工知能が活用されます。



攻撃の特定は？

複数の脅威が連携し、効果的な攻撃が行われます。

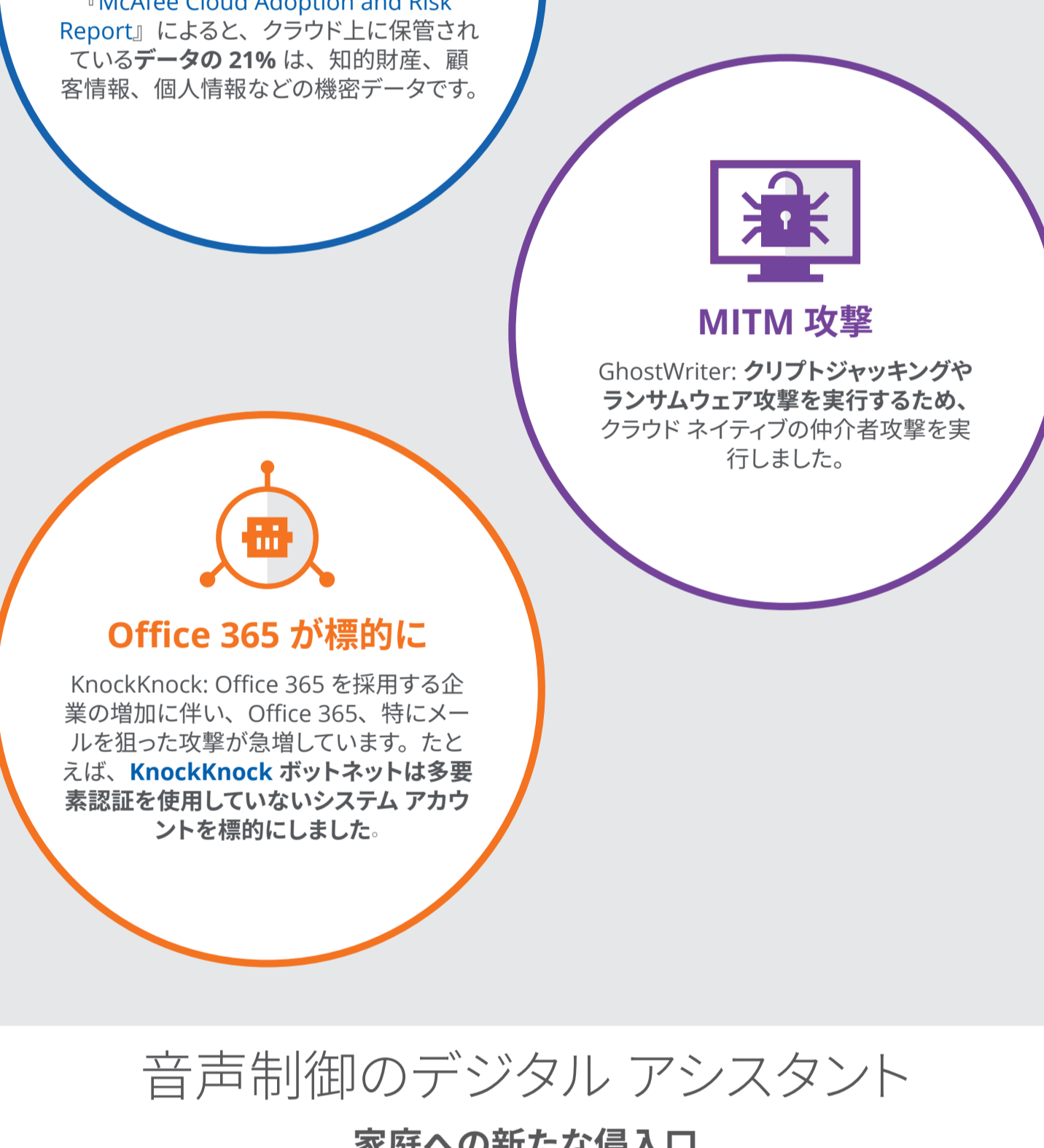
攻撃の全体像が見えにくくなり、攻撃手段の特定が難しくなります。



クラウドを狙うデータ侵害攻撃

より多くのデータが盗まれる

複数のクラウドモデル (SaaS、PaaS、IaaS) を採用する企業が増え、クラウド上に存在するデータも増大しています。攻撃者もこのような動向を見逃しません。クラウドサービスを狙った攻撃が増加するでしょう。



音声制御のデジタル アシスタント

家庭への新たな侵入口

家庭内の IoT 機器を管理する音声制御のデジタル アシスタントが増えています。ここがホーム ネットワークへの新たな侵入口として狙われる可能性があります。



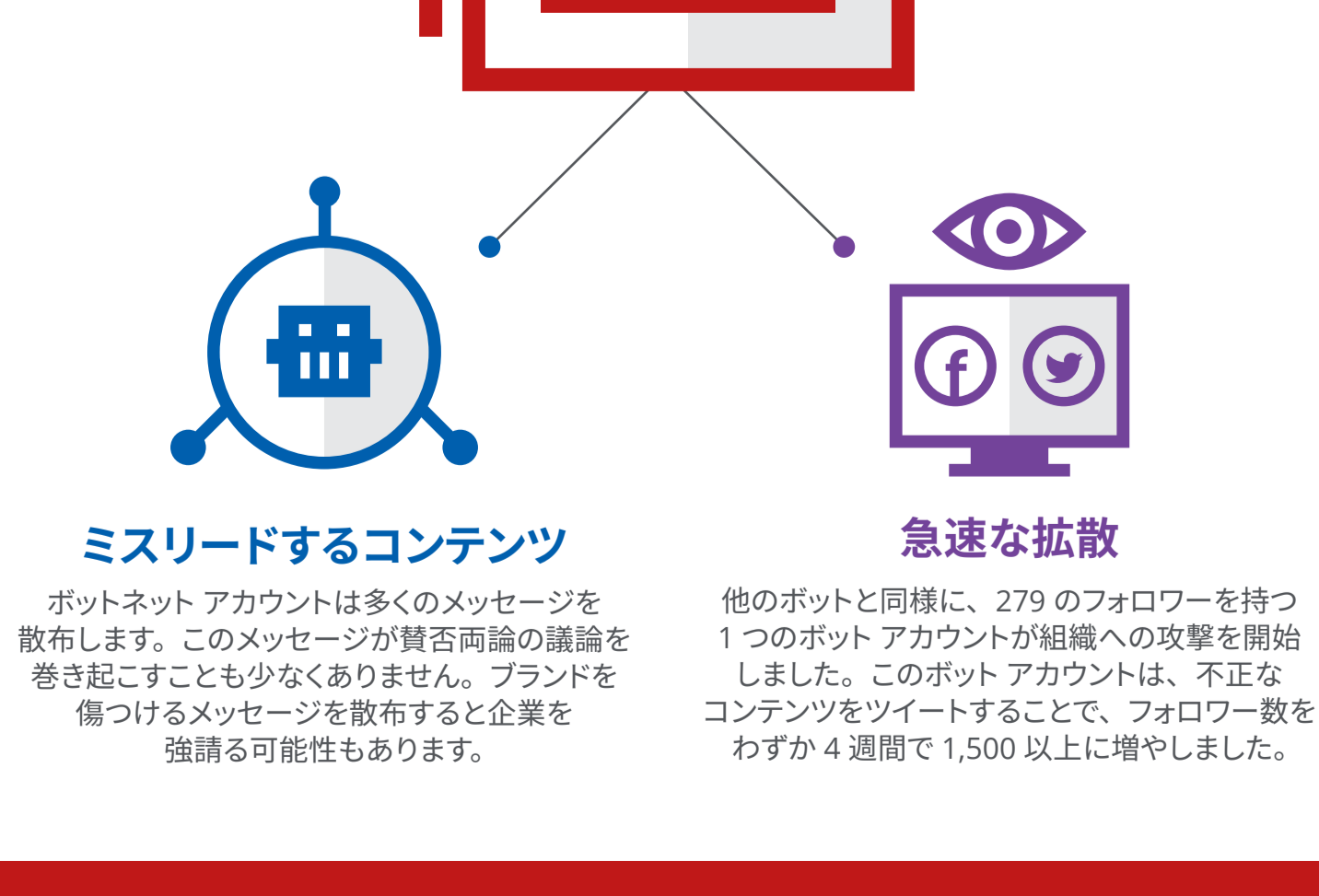
ID プラットフォームとエッジ デバイスへの攻撃

大規模な ID プラットフォームでは、IT 環境のユーザー、デバイス、サービスの認証と承認が一元管理されています。このようなプラットフォームを犯罪者は見逃しません。



企業に関する偽情報の増加

ソーシャル メディアを利用して企業にフェイクニュースを配信したり、強請りを行う国家組織や犯罪グループが増えるでしょう。



詳細については、『McAfee Labs 脅威予測レポート』をご覧ください。
レポートの完全版は www.mcafee.com/2019Predictions をご覧ください。