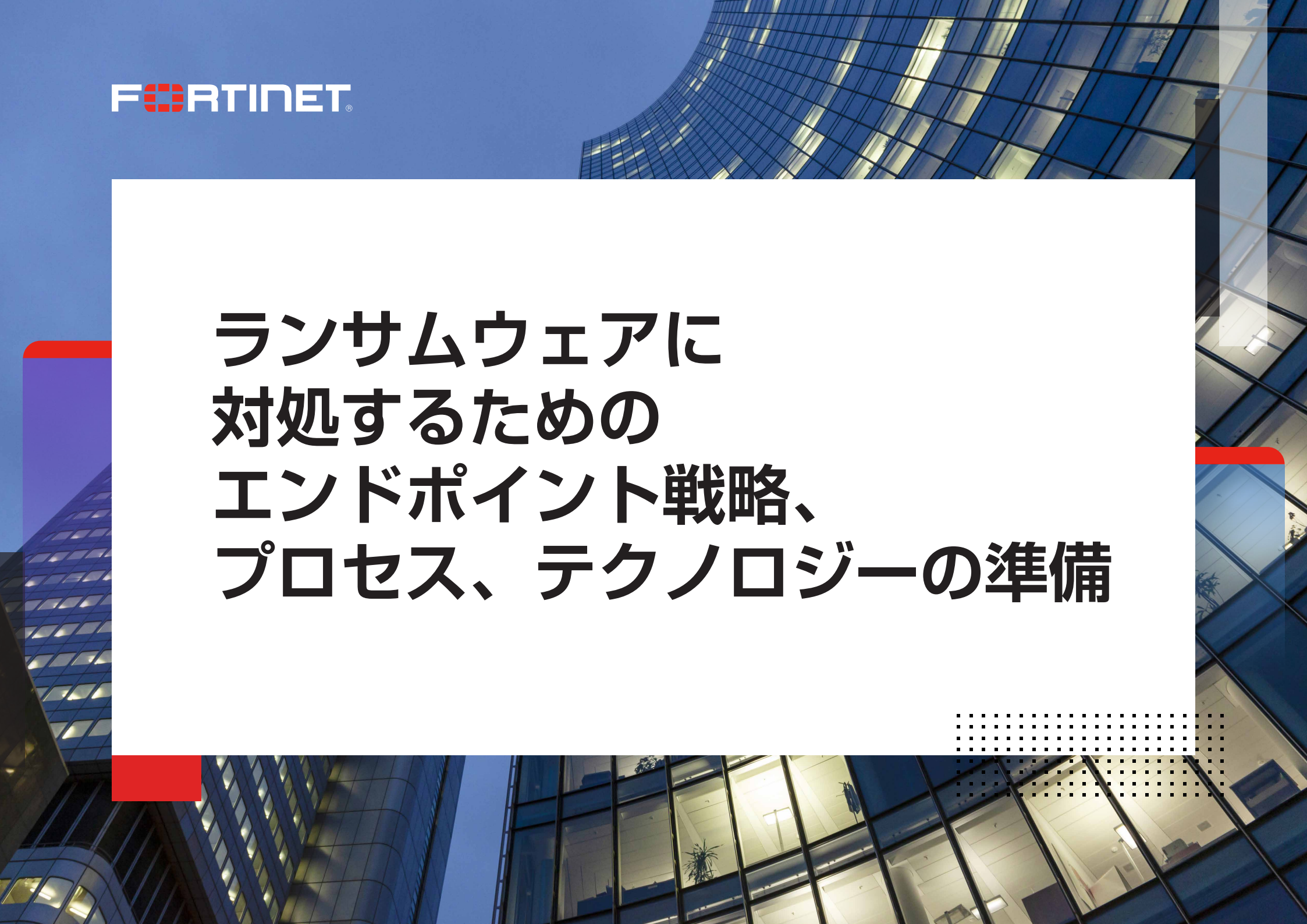


ランサムウェアに対処するためのエンドポイント戦略、プロセス、テクノロジーの準備

目次

概要

脅威動向は、攻撃技術や回避技術の巧妙化により進化し続けています。ランサムウェアは現在、企業が直面する最も厄介なサイバー犯罪の 1 つで、その勢いは衰える気配はありません。FortiGuard Labs のレポートによると、2020 年 12 月のランサムウェアの活動は、同年 7 月と比較して 7 倍に増加しました [1]。また、ランサムウェアのグローバル調査によると、企業の 67% がランサムウェアの標的になったことがあり、約半数が 2 回以上経験しています [2]。

ランサムウェアはさまざまな方法でシステムにアクセスすることが可能で、大概数回のクリック、あるいは一度もクリックせずにアクセスすることもできます。ランサムウェアは非常に一般的になっており、対策が求められています。企業や組織は、戦略を策定し、ランサムウェアの攻撃時、およびその前後にレスポンスできるようにしておく必要があります。成熟した企業の多くはすでにインシデントレスポンス計画を持っています。ただし、潜在的なインシデントのリスクや範囲を軽減するには、事前に多くのことを実施して、インシデントのリスクを減らし、攻撃時にすべきことを把握しておく必要があります。

RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）の継続的な進化、「ビッグゲームハンティング」（大きな標的に対する巨額の身代金）に対する注目、要求に従わない場合に漏洩データが公開される脅威が重なり、サイバー犯罪から大きな利益に転換する巨大な成長市場が誕生しました[3]。

はじめに

ランサムウェア攻撃は増加しており、攻撃は非常に徹底しています。攻撃者は時間をかけて偵察し、特定の被害者を標的にしており、一度に数週間、環境の中に身を潜めて計画を策定し、セキュリティ制御を回避します。攻撃者が身を潜める時間が長いほど実行による被害は大きくなります。攻撃者にとってこの期間は、ランサムウェアのペイロードをドロップしたり、データを流出させたりして、その情報を人質にとる方法を発見する絶好の機会となっています。企業や組織は、基幹システムをできるだけ早急に復旧できるように、包括的な予防、レスポンス、修復の戦略が必要になります。

インシデント前の戦略

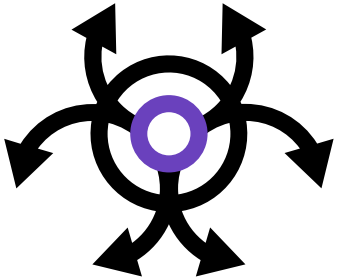
データバックアップの頻度、場所、セキュリティは、場合により根本的に変更する必要があります。デジタルサプライチェーンのセキュリティ侵害に加え、ネットワークに接続する従業員の在宅勤務が重なり、場所を問わず攻撃されるリスクが現実化しています。リスクを最小限に抑え、ランサムウェア攻撃の感染の影響を低減するには、クラウドベースの各種ソリューションをすべて検討する必要があります。これにはネットワーク外のデバイスを保護する SASE（Secure Access Service Edge：セキュアアクセスサービスエッジ）、マルウェア攻撃を途中で中断できる EDR（Endpoint Detection and Response：エンドポイントの脅威検知とレスポンス）などの高度なエンドポイントセキュリティ、ポリシーやコンテキストに基づいてアプリケーションやネットワークへのアクセスを制限するゼロトラストアクセス戦略、およびネットワークセグメンテーション戦略が含まれます。最後に、人的な要素は、テクノロジーと同様に重要であることに変わりありません。ソーシャルエンジニアリングの新たな攻撃手法を従業員に対して継続的に共有し、必要事項と禁止事項を把握できるようにすることが重要です。

とはいえ、ランサムウェアの最終目的地はエンドポイントであるため、エンドポイントセキュリティの強化に取り組む必要があります。このプロセスは、まず、各エンドポイントの攻撃対象領域を軽減するために、不要なポートを閉じて周辺機器を終了し、システムにインストールされているアプリケーションを制御し、エクスプロイトに対する脆弱性を防御することで、セキュアな構成を維持する必要があります。次に、脅威インテリジェンスと機械学習を組み合わせた強力な静的解析を利用することが重要です。脅威を検知するには、デバイスに追加されるすべてのコードに対して解析を実施し、補完として、すべてのランタイムのアクティビティに対して振る舞いベースの動的検証を行う必要があります。手動によるアラートの分類やレスポンスを待たずに、リアルタイムに実施し、進行中の攻撃を阻止できることが非常に重要です。

継続的モニタリング戦略

Aberdeen 社の最新レポートによると、従来のシグネチャベースのエンドポイント保護の場合、セキュリティの有効性の基準値は 91.5% となっています（感染リスクは 7.5%）。また、当レポートの記載によると、攻撃対象領域が減ると、感染リスクの値は 4.7% になり、有効性は 96% になります。振る舞いベースのエンドポイントセキュリティの場合、計算によると実質的に有効性が 99.6% に上昇します（つまり、感染リスクはわずか 0.4%）[4]。

すべての予防措置について、セキュリティオペレーションセンター（SOC）を持つ 1 日 8 時間×週 5 日または 1 日 24 時間×週 7 日で対応している企業は、営業時間後の対応やエスカレーションサポートのため、エンドポイントセキュリティベンダーやマネージドセキュリティサービスパートナーとサービス契約を締結することをお勧めします。これらのサービスでは、アラートや疑わしい脅威を集中的に監視し、インシデントレスポンス担当者に対してガイダンスや次のステップを提供します。これらの内容には、IOC（Indicators of Compromise：侵害指標）の検索、潜在的に脆弱なプログラムや未承認プログラムの特定、フォレンジックアーティファクト（フォレンジック分析の対象オブジェクト）の収集や分析などのプロアクティブな脅威ハンティングが含まれます。イベントの分析が終わると、インシデント通知を通じて、脅威内容の確認や改善ステップのための推奨事項が説明されます。



ランサムウェアはマルウェアの
セキュリティインシデントの
27% を占めています [5]。

レスポンス戦略

セキュリティインシデントが見つかった場合、封じ込めの実施を含め直ちにレスポンスし、潜在的な損害を最小限に抑える必要があります。脅威を効果的に軽減するには、特別なスキルやツール、繰り返し可能なプロセスが必要になります。レスポンス戦略は、状況を評価したり、脅威の封じ込め方法やオペレーションの復旧方法を決定したりするために使用されます。

人、ツール、プロセスが整備されている場合でも、新たなサイバーインシデント中にレスポンスアクションを円滑に行うには、詳細な準備や実習が欠かせません。これらのアクティビティには以下の項目が含まれます。

- インシデントレスポンス準備の評価：組織の現在のセキュリティ体制を、ネットワークアーキテクチャ、セキュリティ制御、スタッフの職務分掌のレビューを通じて評価します。目的は、テクノロジー、人、プロセスを特定することです。
- インシデントレスポンスプレイブックのレビュー：ランサムウェア攻撃などの大きなセキュリティインシデント時における詳細手順について、充足度や改善エリアを判断します。
- インシデントレスポンスの机上練習：レスポンスプロセスの実習と改善を目標にインシデントタイプをシミュレーションし、組織の実際のインシデントレスポンス計画や実行をテストします。

まとめ

企業がランサムウェア攻撃に遭遇したタイミングで、戦略やプロセス、テクノロジーを整備して損害を阻止するのでは遅すぎます。攻撃が発生する前に計画と準備を行うことが鍵になります。セキュリティチームが脅威による被害を軽減し、レスポンスにかかる時間を最小限に抑えるには、攻撃対象領域の削減、脅威の防止や検知、封じ込め、レスポンスのすべての段階をカバーするソリューションに投資する必要があります。

[1]「フォーティネットグローバル脅威レポート」、FortiGuard Labs、2021 年 2 月：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-20H2.pdf

[2]「2021 年ランサムウェア調査レポート」、Fortinet、2021 年 11 月 3 日：https://www.fortinet.com/jp/demand/gated/ransom-survey-2021

[3]「フォーティネットグローバル脅威レポート」、FortiGuard Labs、2021 年 2 月：https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-20H2.pdf

[4]「Quantifying the Risk Reduction of Evolving Endpoint Security Technologies」、Aberdeen Strategy and Research、2021 年 7 月（英語）：https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-aberdeen-quantifying-risk-reduction.pdf

[5]「2020 Data Breach Investigations Report」、Verizon、2020 年（英語）：https://www.verizon.com/business/resources/reports/dbir/2020/summary-of-findings/

フォーティネットジャパン合同会社

〒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

EB-Endpoint-Ransomware-202203-R1