Press Release
2022 年 8 月 16 日（火）
Gigamon Inc.

エンドポイント保護への過度な依存により、企業・組織がランサムウェアにさらされるリスクが高まる可能性を示す調査結果

Gigamon の調査により、グローバルの IT リーダーのうちネットワークの盲点を全て把握しているのは僅か 6 パーセントであることが明らかに

2022 年 8 月 16 日（火）– Deep Observability（高度な可観測性）のリーディング・カンパニーである Gigamon Inc.（本社：米国カリフォルニア州サンタクララ、日本代表：大久保 淳仁）は、Gartner Peer Insights に委託して実施したランサムウェア向け防御に関する調査から得られた新たな知見を発表致しました。北米、APAC（アジア・太平洋地域）および EMEA（欧州・中東・アフリカ地域）のグローバル IT および情報セキュリティのリーダーを対象とした調査では、情報セキュリティのプロフェッショナルの 96 パーセントがエンドポイント検知レスポンス（EDR）を、ランサムウェア向け保護対策として、最も重要であると考えていることが明らかになりました。しかし、回答者のうち、攻撃に対する保護の備えができていると自信を持つ回答者はわずか 4 パーセントにとどまり、大半の回答者は、その結果として、ビジネスに大きな支障をきたす可能性があると予測しています。

昨年、3 分の 2 以上（69 パーセント）の組織がランサムウェアの被害を受け、大半の IT およびセキュリティプロフェッショナルは、この種のサイバー犯罪が自身の職業キャリアにどのような影響を及ぼすかについて懸念を持っています。ランサムウェアの脅威に対抗するため、本調査では、回答者の大半が EDR（エンドポイント検知レスポンス）を不可欠なものと考えている一方で、ネットワーク上の管理外のデバイスが持つリスクに注意を払っている回答者は僅か 3 パーセントであることを確認しています。この為、IT プロフェッショナルは、今後 12 カ月以内に自社がランサムウェアによる攻撃を受けることを予測しており、EMEA の回答者の 75 パーセントが、攻撃を受ける可能性が高いまたは非常に高いと予測しており、強く懸念しています。

また本調査では、ネットワークの可視化が、ランサムウェアの全体的な防御戦略の基礎として考えられていることも明らかになりました。グローバルのサイバーセキュリティ専門家の 83 パーセントが、ランサムウェアの迅速な検知と対応には、ラテラルムーブメント（侵入拡大）の脅威を可視化することが重要であることに同意しています。しかし、ネットワークの盲点の大半または全てを把握していると回答したのは、わずか 60 パーセントにすぎません。EMEA（欧州・中東・アフリカ地域）の企業・組織は、自社のセキュリティ態勢における盲点の全てまたは大半を認識しているのは僅か 50 パーセントで、その一方で APAC（アジア太平洋地域）は 61 パーセント、北米は 64 パーセントとなっています。フィールド CTO 兼ワールドワイドセキュリティアーキテクチャチーム ディレクターのイアン・ファーカー氏は、本調査結果について、「企業・組織がエンドポイント保護対策に対して過渡に依存する場合、ランサムウェアのリスクにさらされる可能性があります。BYOD 戦略や IoT は日々拡大しており、企業・組織が EDR（エンドポイント検知レスポンス）を優先した場合、ネットワークは充分に保護されません。その代わりに、セキュリティ運用チームには、Deep

Observability（高度な可観測性）すなわちリモート監視の能力を向上させる実用的なネットワークレベルのインテリジェンスを活用することで、深いネットワークレベルの防御を実現することが必要です。60%の回答者が主張するように、大半の盲点を認識できたとしても、それだけでは十分ではありません。攻撃者にとってセキュリティを脅かす盲点やネットワークに対する侵入脅威は 1 つだけで充分なのです。

その他の主要な調査結果は以下の通りです。

- **ビジネスに重大な支障をきたす事を予測しています。**
  53 パーセントの回答者が、1 日あるいはそれ以上、業務に支障をきたすと予測しています。
- **大半の IT リーダーがランサムウェアにより自身の職業キャリアに影響を及ぼす事を懸念しています。**
  85 パーセントの回答者が、ランサムウェアによってビジネスが中断された場合、自身の職業上の不利益を被ることを懸念していることに対して、同意または強く同意しています。
- **APAC 地域の回答者は、脅威ハンティングを全てアウトソースする傾向があります。**
  APAC 地域の回答者の 3 分の 1 以上（36 パーセント）は、脅威ハンティングをアウトソースする事が唯一の施策であると回答しているのに対し、北米および EMEA（欧州・中東・アフリカ地域）の回答者の約 3 分の 2（65 パーセント）が社内リソースとアウトソースを連携して活用していると回答しています。

調査結果の詳細については、以下をご覧下さい。（英文資料）
https://www.gigamon.com/content/dam/resource-library/english/analyst-industry-report/ar-gartner-peer-insights-network-visibility-and-ransomware.pdf

【Gigamon について】

Gigamon Inc. は、実用的なネットワークレベルのインテリジェンスを活用し、Observability（可観測性）ツールの機能を強化した Deep Observability（高度な可観測性）を提供しています。この高度な連携により、IT 組織はセキュリティとコンプライアンスのガバナンスを保証し、パフォーマンスのボトルネックの根本原因の分析を迅速化し、ハイブリッドおよびマルチクラウド IT インフラの管理に関連する運用負荷を大幅に削減することができます。全世界で販売パートナーおよびサービスプロバイダを通じて、4,200 社以上の企業へ、物理、仮想、クラウドネットワーク向けに可視化基盤ソリューションを提供しています。米国連邦政府機関のトップ 10 すべて、グローバル銀行トップ 10 の 7 行、Fortune100 企業の 83 社、モバイルネットワーク通信事業者トップ 10 の 9 社、テクノロジー企業トップ 10 の 8 社、医療関連プロバイダートップ 10 の 8 社に導入されています。Gigamon のミッションは、中堅・中小企業や分散拠点を持つ大企業や組織で、効率的運用かつ高 ROI のセキュリティ、監視システム環境を実現することです。本社を米国カリフォルニア州サンタクララに置き、世界 20 か国にオフィスを展開しています。
さらなる詳細情報、プロモーション活動、最新動向は https://www.gigamon.com/jp/をご覧下さい。

【本プレスリリースに関するお問合せ】
Gigamon Inc.
〒105-0022
東京都港区海岸 1-2-20
汐留ビルディング 3F
Sales 担当
Tel:03-6721-8349
Email： sales-japan@gigamon.com
URL： https://www.gigamon.com/jp/