netAlly
simplicity • visibility • collaboration

CyberScope®

見えないものを
明らかに

エッジでの迅速かつ包括的な
セキュリティ評価

CyberScope®

包括的なエッジネットワーク脆弱性スキャナ

完全な可視性：それは必要なことですが、多彩なリソースがあるにもかかわらず、依然として重大なギャップが存在します。
今日のダイナミックでアクセス可能なエッジネットワークでは、エンドポイント (IT/OT/IoT) が急増しており、Wi-Fi 利用も拡大しているため、中央プラットフォームの監視からは見逃されがちです。
企業の境界のセキュリティを確保するためには、エッジにおけるサイバーセキュリティコントロールを発見、検証、評価するための定期的で徹底的な評価が不可欠です。

そこでNetAllyの CyberScopeの出番です。

CyberScope は、単一の強力なポータブルツールで、包括的なネットワークセキュリティの評価、解析、レポートを提供します。

- エッジでのコントロールを簡単に検証
- 有線/無線のIoT, OT, 管理外デバイスを含むすべての目録を作成
- ポリシー遵守を迅速にテスト/実証
- チーム間のコラボレーションと共有を可能に

CyberScope は、堅牢な専用オールインワンツールとして、壊れやすいラップトップやタブレットの使用を排除するネットワークセキュリティおよびテストソリューションです。
オンプレミスでエッジネットワークに迅速かつ実用的な洞察を提供し、他のサイバーセキュリティツールやテストツールでは対処できない重要な可視性のギャップを埋めます。

ネットワークの完全な可視化-オンサイトまたはリモート

セキュリティ担当者やネットワークエンジニアは、CyberScope を使用して、エッジネットワーク上のすべてのイーサネット、 Wi-Fi および BT/BLE デバイスを迅速に識別し、接続されている場所を正確に特定し、敵か味方かを即座に判断できます。

CyberScope ユーザはすべてのデバイスとポートを含むネットワークをいつも見て状況を把握しています。

セキュリティオペレーションチームが人手不足である場合、CyberScopeはその範囲を拡大し、サイバーセキュリティを向上させます。NetAllyのコラボレーション、レポート、解析プラットフォームであるLink-Live™で、簡単なリモートアクセスと安全なデータ収集、共有、解析ができます。

影響の大きいCVEを素早く見つける

Nmap テクノロジーは、簡素化されたユーザインターフェイスを備えた CyberScope に完全に統合されており、初心者にとってはスキャンの実行と CVE の検索が容易になり、熟練者には高度な機能を提供します。

トラックの横方向の動きを停止する

CyberScopeは、ネットワークセグメンテーションやプロビジョニングエラーなどの脆弱性をスキャンします。潜在的なデバイスと設定のリスクを特定し、悪意のある攻撃者がネットワーク内で横方向に移動するために使用できるエントリポイントを特定します。不正なAP、クライアント、または意図的に隠されたコンピューティングデバイスは、CyberScope から隠れることはできません。

サイバーセキュリティ評価のワークフロー

DISCOVER　VALIDATE　LOCATE　ANALYZE　REPORT　MONITOR

**CyberScope には 3 つの異なるモデルがあります。*
フル機能の CE モデルには、有線イーサネットと無線 (Wi-Fi および BT/BLE) 機能が含まれています。
XRF(有線専用) および AIR(無線専用) モデルも利用できます。
特定の機能はモデルによって異なります。

Discover

IoT、OT、管理対象外デバイス (有線および無線) を含むあらゆるものをインベントリする

有線または無線のネットワーク(すべてのデバイス) を把握します。

ネットワークディスカバリはサイバーセキュリティの重要なベストプラクティスであり、存在するネットワークインフラストラクチャ、レイアウト、デバイス、サービスに関する貴重な情報を提供します。

潜在的な攻撃対象領域をすべて特定できるため、セキュリティチームはネットワークを脅威や脆弱性からより適切に保護できます。

CyberScopeのディスカバリは、5つのネットワークインターフェースを介したスキャンとアクティブプロービングを組み合わせ、エンドポイントとネットワークインフラストラクチャ要素を検出します。

CyberScope および CyberScope Air はすべての Wi-Fi AP とクライアントを検出し、施設内外の電波到達範囲を把握します。AirMapper™ サーベイアプリは、1度のウォークスルーで AP だけでなくクライアントや BLE デバイスもサーベイし、同時にアクティブなディスカバリを実行します。

CyberScope®

DISCOVERの特徴

- 統合されたNmapによるディスカバリスキャン
- 拡張/除外ディスカバリレンジ
- ソート,フィルタ,検索
- AirMapper® Site Survey*

*Wi-Fi対応モデルのみ

Validate

エッジでのコントロールを簡単に検証

検出されたすべてのデバイスさらにはエンドポイントのメーカーも、認可済み、未承認、隣接、不明として分類できます。デバイス上でのソートとフィルタリングにより、異常値の特定が容易になります。

CyberScopeは、アクセスポイントで有線ネットワークと Wi-Fi ネットワークの両方が適切にセグメンテーションされていることを、明確な合否表示で検証できます。

また、スイッチポートが適切にプロビジョニングされているかどうかを調べ、VLAN に参加して正しいセグメンテーションを確認することもできます。

さらに詳細な解析のために特定のVLAN上のトラフィックをキャプチャします。

指定されたインフラストラクチャベンダーに対するAPIクエリにより、ポート構成とクライアント属性に関する入手可能なすべての情報が詳しく調べられます。

自動テストは、ネットワークのどの部分からでも包括的なセグメンテーションおよびプロビジョニング解析を実行できるよう、あらゆるスキルレベルの技術者に権限を与える標準化された方法を提供します。

参加する VLAN または SSID を指定するだけで、到達可能なものと到達不可能なものを数秒で検証できます。

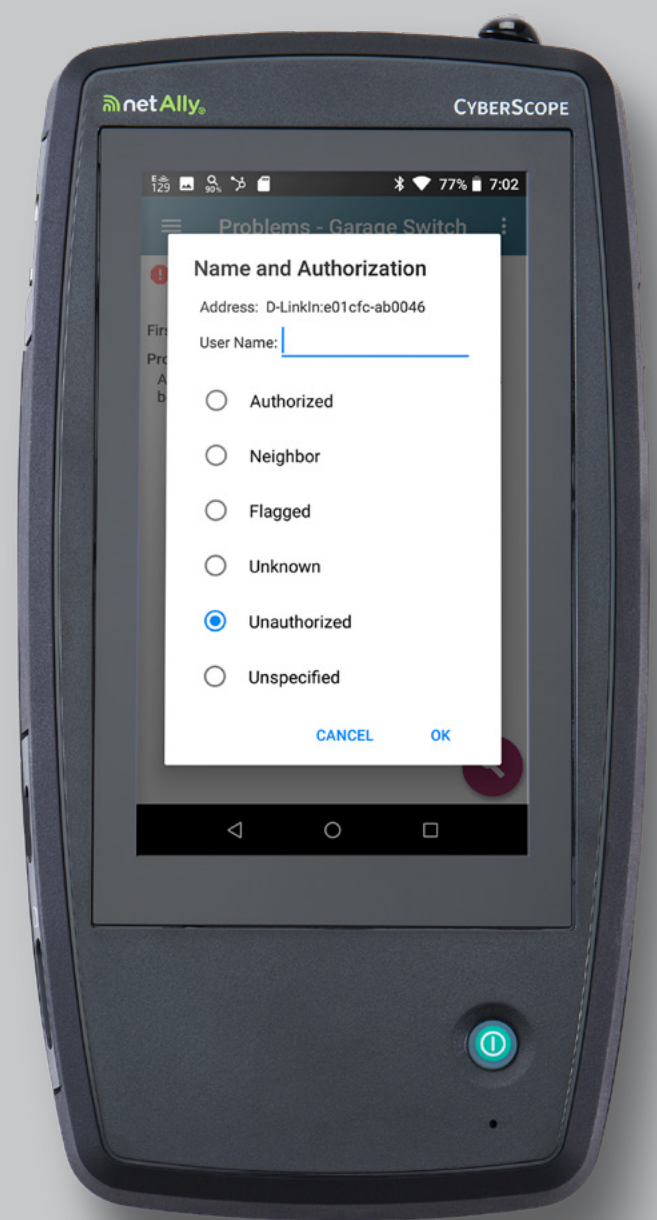
不正な DHCP または DNS サーバーを検出するインスツルメンテーションにより、すべての重要なサービスを検証できます。

Wi-Fi での自動テストは 3 つの帯域すべてにわたって最新の WPA3 セキュリティ設定をワンボタンで繰り返し検証します。

CyberScope®

VALIDATEの特徴

- 認可済みデバイスリスト
- ソート/フィルタ
- 自由文字列検索
- VLAN識別
- デバイスのタグ付け
- Ping,キャプチャ,ブラウズ
- 自動テスト



Locate

有線でも無線でも素早く エンドポイント見つける

パス解析は、デバイスがどのように相互接続されているかを理解するために重要です。

CyberScopeは、あらゆるデバイスへのネットワークパス（有線および無線の両方）のポートごとの詳細を提供します。

これは、未知のデバイスや悪意のあるデバイスを探し出す際に非常に重要です。

CyberScope CE および CyberScope Air は指向性アンテナを使用することによりWi-Fi上での不正なデバイスを迅速かつ容易に検出します。

Link-Liveを利用したコラボレーション、レポート作成、分析プラットフォームにより、正確なトポロジマップを作成し、接続を視覚化できます。
強力なフィルタリングとソートにより、Wi-Fi環境の異常値を簡単に検出できます。特にデバイスの急増が常態化しているWi-Fi環境に役立ちます。
時間がない場合や、データ解析に遠隔地の専門家が必要な場合、オンサイトで数分間でデータを収集し、いつでもどこでもLink-Liveで高度な解析とレポート作成を行うことができます。

指向性アンテナを使用した不正デバイス捜索

CyberScope®

LOCATEの特徴

- パス解析
- ポート/VLANの識別
- AP, クライアント, BT/BLEのサイトサーベイ
- 指向性アンテナ/信号強度追跡
- トポロジマッピング
- 接続テクノロジの識別

  (リンクタイプ/速度, 周波数/帯域/チャネル)

Analyze

テストと実証
ポリシーの遵守

CyberScope は、Nmap を組み込み開かれたバックドア、CVE、設定不十分なファイアウォールや侵入検知システムなどの潜在的な脆弱性を特定します。しかし、Nmapのコマンドラインインターフェースの不可解な性質と過剰なテキスト出力は、多くのセキュリティエンジニアやネットワーク技術者がNmapを最大限に活用することを妨げています。

CyberScopeの直感的なユーザインターフェースは、コマンド/スクリプトの実行と出力の解析の両方において、Nmapの強力な機能を迅速かつ繰り返し利用できます。熟練したユーザであっても、攻撃の成功リスクを低減するのに役立つ使いやすさを高く評価することでしょう。

ネットワークに接続されたすべてのエンドポイントデバイスの脆弱性を自動的にスキャンします。Nmapは、内蔵スクリプトまたはカスタムスクリプトを実行することにより、各デバイスから収集した情報を詳細な解析によって強化し、警告やエラーの通知を自動的に生成します。これらにより、潜在的なセキュリティ上の弱点を特定し、リスク低減のための修正作業の優先順位付けを行うことができます。

CyberScopeおよびCyberScope Airモデルでは、Wi-FiおよびBT/BLE分析により、チャネル、AP、SSID、BSSID、クライアントなど、関心のある領域に基づいてネットワークエッジを評価できます。付属のスペクトラムアナライザーは、妨害デバイスの影響を表示し、機密ネットワーク信号の漏洩がないことを確認できます。

ヒートマップやトポロジマップなどの視覚化により、ネットワークを理解する際に「なるほど」と感じる瞬間が得られます。 Link-Live のディスカバリモニタリングは、新しいデバイス、見失ったデバイス、または一時的なデバイス、または最後のスナップショット以降の変更を示します。

CyberScope®

ANALYZEの特徴

- Nmapエンドポイントの脆弱性診断
- リアルタイムWi-Fi解析*
- AirMapper site survey デバイスと信号ヒートマップ*
- 自動テスト,接続性確認、セグメンテーション,エンドポイントの解析
- UDP/TCPポートスキャン, OSとサービスの識別
- トポロジマッピング
- デバイスディスカバリモニリングと差異解析
- パケットキャプチャ

*Wi-Fi対応モデルのみ

Report

チーム間のコラボレーションと共有を可能に

コンプライアンスおよび監査証拠のレポート作成

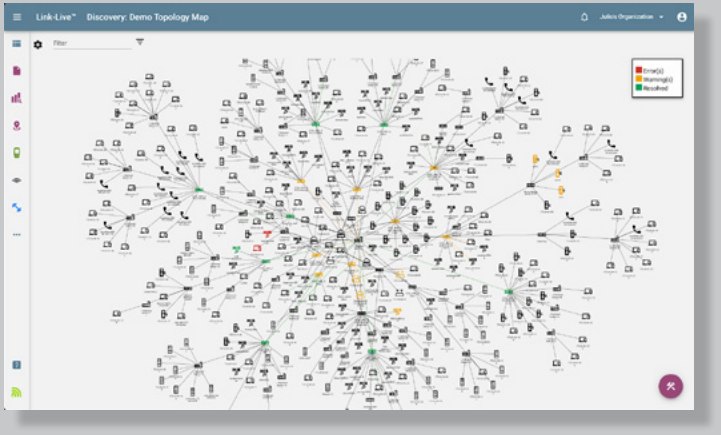
結果の比較、ディスカバリモニタリング、ヒートマップ、トポロジマップなどの機能を備えたLink-Live を使用すると、レポート作成が簡単になります。Link-Live は安全なクラウド経由ですべての NetAlly アナライザと結果を組織全体で管理します。

エキスパートによる安全な共有とアナライザのリモート制御により、場所に関係なくチーム全体のコラボレーションを円滑に行うことが可能です。

CyberScope®

REPORTの特徴

- ディスカバリモニタリングレポート
- ネットワークトポロジマップ
- Wi-Fi & BT/BLE ヒートマップ*



*Wi-Fi対応モデルのみ

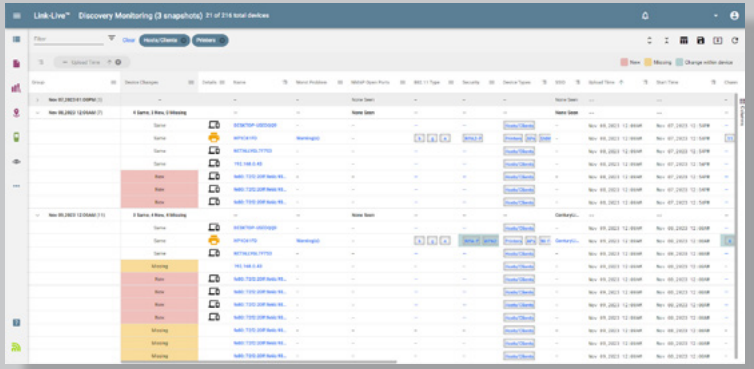
Discovery Monitoring

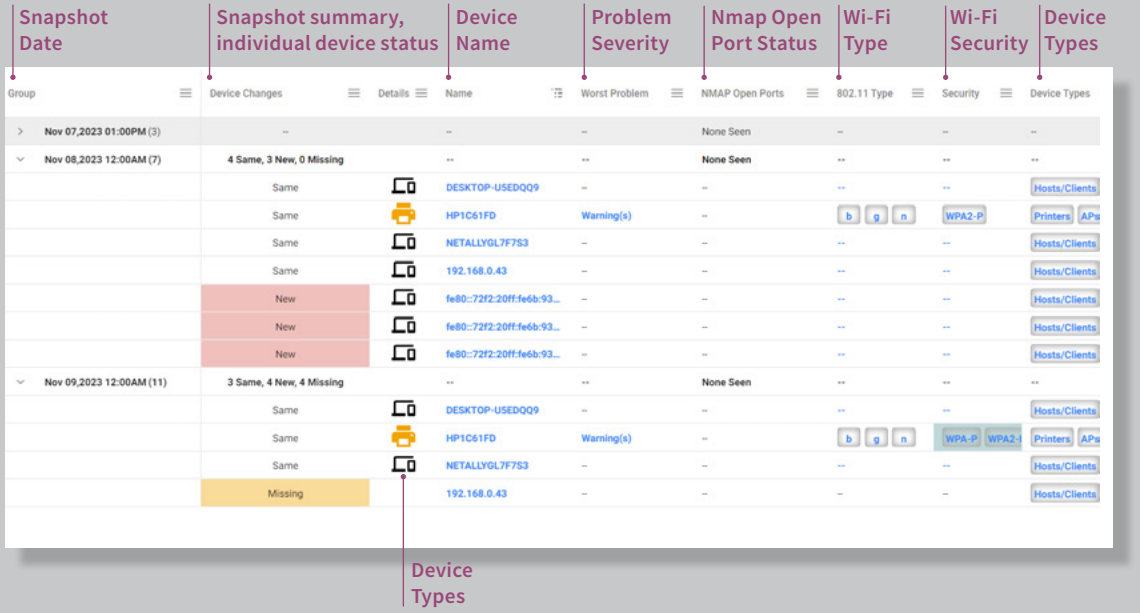
新しいエンドポイントと変更を迅速に検出

ネットワークとエッジデバイスの絶え間ない変化により、これまで状況認識が困難になっていました。 CyberScope と Link-Live の機能を組み合わせることで、セキュリティ運用チームは、ネットワークやデバイスの変更とともに、新しいデバイス、見失ったデバイス、または一時的なデバイスを迅速に検出できるようになりました。
検出プロセスが自動化され、エッジネットワーク評価の有効性が大幅に向上し、継続的な状況認識が簡単になりました。
一度設定すると、ディスカバリは設定した時間に定期的に実行され、自動的に Link-Live にアップロードされるネットワークインベントリスナップショットを生成できます。
ベースライン (最初の検出) から始まり、新しい各スナップショットが以前に実行されたスナップショットと比較されます。デバイスとネットワークの違いが検出され、結果は Link-Live 内で表形式またはグラフ形式でレポートされ、新しいデバイス、見失ったデバイス、または一時的なデバイスが、見やすい色分けで表示されます。 デバイスの問題を等級分けすることは、調査の優先順位をさらに高めるのに役立ちます。
Discovery、BSSID、 Clients の 3 つの異なるテーブル形式が使用可能です。後の2つは無線対応モデルでのみ使用できます。
ネットワークエッジに多数のエンドポイントが存在する可能性があるため、強力なフィルタリングやソートを利用できます。
CyberScopeのモデルに応じて、フィルタの選択にはデバイスの変更、デバイスタイプ、その他多くのカテゴリが含まれます。 自由文字列検索は、単独でまたは組み合わせて使用して、特定の懸念事項をターゲットにしたり、問題を正確に特定したりすることもできます。 どのデバイスが「安定」しているか、新しいデバイス、見失ったデバイス、または一時的なデバイスかを確認するのは迅速かつ簡単です。

DISCOVER MONITORINGの特徴

- 新しいデバイス、見失ったデバイスまたは一時的なデバイスを迅速に発見
- 強力なフィルタリング、並べ替え、および自由文字列検索により、疑わしいデバイスの調査が迅速かつ簡単に





Features

パワフルなツールを手のひらに

可搬性に優れたポータブルタイプ

CyberScope は、堅牢なハンドヘルド機器であり、非常に持ち運びやすいため、1回のウォークスルーですべてのネットワークの脆弱性を見つけることができます。アナライザを別の場所に送り、リモートで安全に制御することもできます。 スマートハンズのコラボレーションにより、事前対応型または事後対応型の活動のためのオンサイトフィールドエンジニアリングサービスが可能になります。

- **手のひらサイズでありながら強力なツール**
- **リモート解析機能**
- **スマートハンズコラボレーション**

必要なものがすべて揃った専用設計

CyberScope は、専用ツールでありネットワークエッジの評価と解析の機能を備えています。
有線対応モデルには、10Mbps ～ 10GbpsのRJ45ポートと光ファイバーポートおよび高出力PoEが含まれており、これはノートPCやタブレットでは見られない機能です。
USB ポートは、NXT-1000 スペクトラムアナライザ、音声通信用のヘッドセット、ラベルプリンタなどのアクセサリへの接続を提供します。
また、サードパーティ製の Android アプリを実行することもできます。

- **専用ハードウェア**
- **一貫性のあるテストパターンを提供**
- **アクセサリ用USBポート**
- **拡張可能なストレージ**
- **サードパーティ製アプリが利用可能**

使いさすさ

Nmap を含め、CyberScope に統合されたすべてのさまざまなツールに対して一貫したユーザインターフェースが得られます。 自動テストでは、ボタン1つで合格/不合格を評価し、迅速かつ再現可能で確実な結果を得ることができます。 これは、エッジネットワークを可視化する簡単な方法です。

- **シングルボタンの操作の自動テスト**
- **レイヤ1～7の可視性**

リモートアクセスがスマートハンドを強化

ほとんどの場合、サイバーセキュリティの専門家は問題の場所にいません。
CyberScope はLink-Live またはサードパーティアプリを使用して安全なリモートアクセスを提供します。機器が到着したらすぐに、熟練していない管理者でも機器を接続して完全なリモート操作を行うことができます。新人をトレーニングする必要がありますか？
双方向の遠隔操作により、スタッフをトレーニングしたり、肩越しに見ながら理解を深めたりすることができます。

*有線対応モデルのみ

Models

CyberScope®

Wi-Fi 6/6E の 6GHz スペクトルの法規制への準拠の実装は国によって異なります。
CyberScopeのモデルは、フルトライバンド (6 GHz 帯域全体にわたる機能)、部分的トライバンド (802.11d 規制ドメイン情報によって決定される 6 GHz 帯域の特定のチャネルのみの機能)、およびデュアルバンドのみ (6GHz 帯域での動作が許可されていない国)

注: すべての新しい CyberScope 本体は、初年度 (1 年間) の AllyCareサポートが含まれて販売されます。
最初に電源を入れてから 30 日以内に製品登録とアクティベーションを行う必要があります。

	型名	内容
無線 / 有線	CYBERSCOPE-CE-E	CYBERSCOPE-CE-E メインフレーム (部分トライバンド)、初年度の Ally Care サポート付き (CYBERSCOPE-1YS)、NXT-1000 スペクトラムアナライザ、G3-PWRADAPTER、SFP+MR-10G850、RJ-45 カプラ、EXT-ANT-TRIBAND指向性アンテナ、WIREVIEW 1、クイックスタートガイド、ハードキャリーケース
無線のみ	CYBERSCOPE-AIR-E	CYBERSCOPE-AIR-E メインフレーム (部分トライバンド)、初年度のAlly Care サポート付き (CYBERSCOPE AIR-1YS)、NXT-1000 スペクトラムアナライザ、G3-PWRADAPTER、EXT-ANT-TRIBAND 指向性アンテナ、 クイックスタートガイド、ハードキャリーケース
有線のみ	CYBERSCOPE-XRF	CYBERSCOPE-XRF メインフレーム、初年度の AllyCare サポート付き (CYBERSCOPE-XRF-1YS)、WIREVIEW1、 G3-PWRADAPTER、SFP+MR-10G850、RJ-45 カプラ、クイックスタートガイド、ハードキャリーケース

CyberScope®
Edge Network Vulnerability Scanner

CyberScope® Air
WiFi Vulnerability Scanner & Tester

netAlly
simplicity • visibility • collaboration

NetAllyとは?

NetAllyの革新的なネットワークテストソリューションファミリーは、ネットワークエンジニアや技術者が、今日の複雑な有線/無線ネットワークの導入、管理、保守をより良く行えるよう、長きにわたり支援しています。

NetAllyは25年以上にわたり、世界中のネットワーク専門家の一番の味方であり続けています。世界初のハンドヘルドネットワークアナライザであるLANMeter®の製造から始まり、業界の先頭に立ち、ポータブルネットワークテストのスタンダードを確立してきました。

仕事を迅速に遂行するために必要な可視性を提供するNetAllyの最高クラスのツールは、世界中のネットワーク専門家からの信頼があります。

NetAlly 日本総代理店東洋計測器株式会社
〒101-0021 東京都千代田区外神田1-3-12 計測器ランドビル
TEL: 03-3255-8026
E-mail: netally@keisokuki-land.co.jp

Literature number: CS-BR-24-V1-JP

More information:cyberscope.netally.com/all-vulnerability-scanners

SIMPLICITY

- 簡単で高速な自動テストにより無駄な時間を省き、初心者はより生産的に、熟練者はより効率的に
- 直感的なUIでより多くの人が高度な技術（Nmap）を効果的に使用できるようになる
- 標準化された手順により、一貫して正しい作業

VISIBILITY

- 他の人には見えない問題が見える
- より多くの人が、より多くの問題を自力で解決できる
- 可視化により解決までの平均時間の短縮

COLLABORATION

- コラボレーションを促進することで、問題解決を迅速化し、チームのリソースを解放
- 自動文書化により時間を節約
- 簡単なレポート作成と共有により、円滑な連携を可能に

AllyCare Support

AllyCare は、NetAlly のネットワークツールおよび AirMagnet® ソフトウェアの包括的なサポートおよびメンテナンスサービスであり、標準の保証よりも大きな価値を提供します。AllyCare のメンバーシップは1年間または3年間の付加価値のあるメンバーシップとして購入することができます。

AllyCareと標準保証の比較

内容	AllyCare	標準保証
最新ソフトウェア&ファームウェア	Yes	製造上の欠陥のみ（90日間）
製品拡張機能	Yes	No
本体修理対応*	Yes	製造上の欠陥のみ（1年間）
本体修理対応中の代替機貸出**	Yes	No
アクセサリ修理対応***	Yes	製造上の欠陥のみ（90日間）
動作点検****	Yes	No

*事前の診断が必要となります。通常利用での損傷に限ります。故意または不慮の事故による損傷は対象外です。
**AllyCareご契約中に修理対応をする場合に限ります。
***製品に同梱されているアクセサリの一部が対象となります。事前の診断が必要となります。
****1年ごとに1回の動作点検が可能です。