netAlly

simplicity • visibility • collaboration

CyberScope®

Reveals
what you cannot see

Fast and comprehensive security
assessments **at the edge.**

CyberScope®
Comprehensive Edge Network Vulnerability Scanner

Complete visibility. It's what you need but despite all the resources you have, there are still critical gaps. Today's dynamic and accessible edge networks, with their proliferation of endpoints (IT/OT/IoT) and increasing Wi-Fi use cases are often beyond the sight of central platforms.

To ensure the security of your enterprise perimeter, regular thorough assessments to discover, validate, and assess cybersecurity controls at the edge are essential.

That's where NetAlly's CyberScope comes in

CyberScope offers unique and comprehensive network security assessment, analysis and reporting from a single, powerful, portable tool:

- Easily validates controls at the edge.
- Inventories everything including IoT, OT, unmanaged devices, wired and wireless.
- Quickly tests and demonstrates policy compliance.
- Enables collaboration and sharing between teams.

As a ruggedized, purpose-built all-in-one tool, CyberScope is a network security solution that eliminates the use of fragile laptops and tablets. With multiple functions, it provides fast, actionable insights on-prem into your edge networks, filling the critical visibility gaps that other cybersecurity tools may not address.

Complete network visibility – On-site or remote

Security practitioners and network engineers can use CyberScope to quickly identify every Ethernet, Wi-Fi, and BT/BLE device on your edge network, pinpoint exactly where it is connected, and instantly determine if it is friend or foe.

CyberScope users see their network, and KNOW their network – every device, every port, every time

When SecOps teams are short-staffed, CyberScope expands their reach and improves cybersecurity. You get easy remote access and secure data collection, sharing and analysis in Link-Live™, NetAlly's collaboration, reporting and analysis platform.

Quickly find high impact CVE's

Nmap technology is fully integrated in CyberScope with a simplified user interface making scan execution and finding CVE's easy for beginners while providing advanced features for experienced users.

Stop lateral movement in its tracks

CyberScope scans for vulnerabilities such as network segmentation and provisioning errors. It locates potential device and configuration risks, and identifies entry points bad actors could use to move laterally inside your network. Rogue APs, clients, or purposely hidden computing devices cannot hide from CyberScope.

Cybersecurity Assessment Workflow

CyberScope is available in three different versions. The full function CE version includes wired Ethernet and wireless (Wi-Fi and BT/BLE) capabilities. Wired only (XRF) and wireless only (AIR) models are also available - specific capabilities depend on the version.

Discover

INVENTORY EVERYTHING INCLUDING IOT, OT, AND UNMANAGED DEVICES, WIRED AND WIRELESS

First, know your network – every device – on the wire or in the air. Network discovery is a critical cybersecurity best practice, providing valuable information about the network infrastructure, layout, devices, and services that are present. You will **identify all potential internal attack surfaces** so your security teams can better protect your network from threats and vulnerabilities.

Based on model, the CyberScope Discovery app combines scanning and active probing from up to five different network interfaces using multiple technologies to find endpoints and network infrastructure elements.

CyberScope and CyberScope Air models detect all Wi-Fi APs and clients to fully understand the scope of RF reach inside and outside your facility. The AirMapper™ survey app surveys not just APs but also clients and BLE devices in a single walkthrough, while simultaneously performing active discovery.

DISCOVER Features

- **Discovery scanning with integrated Nmap**
- **Extended/Excluded Discovery ranges**
- **Sort, Filter, Search**
- **AirMapper® Site Survey**

3
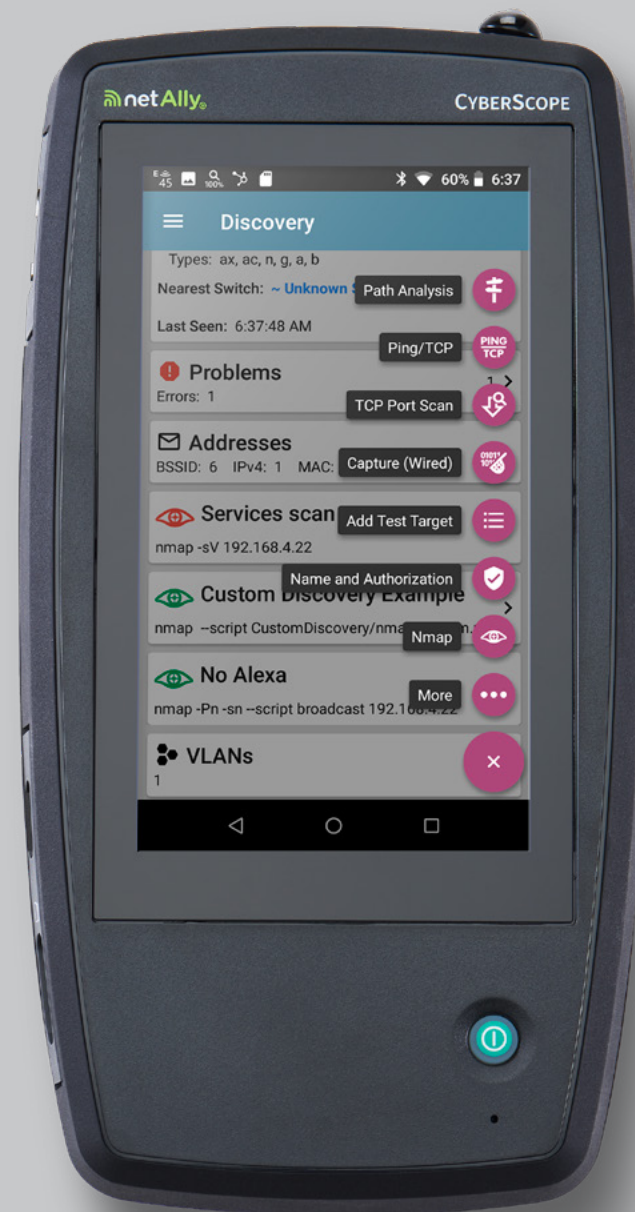
Validate

EASILY VERIFY CONTROLS AT THE EDGE

All discovered devices and even endpoint manufacturers can be classified as Authorized, Unauthorized, Neighbor or Unknown. On-device sorting and filtering makes it easy to identify outliers.

Network segmentation and provisioning can be complicated and prone to error. CyberScope can verify proper segmentation of both wired and Wi-Fi networks at the point of access with clear pass/fail indication. CyberScope can also examine switch ports for proper provisioning, join a VLAN to ensure correct segmentation, and capture traffic on a specific VLAN for deeper analysis. CyberScope's high-performance hardware ensures 100% packet capture at line rate speeds.

API queries for specified infrastructure vendors provide a deep dive into all available information about port configurations and client attributes.

AutoTest provides a standardized way to empower technicians of any skill level to perform comprehensive segmentation and provisioning analysis from any part of your network. Simply specify the VLAN or SSID to join and validate what can and cannot be reached in seconds. You'll validate all critical services with instrumentation to **detect rogue DHCP or DNS servers.** On Wi-Fi, AutoTest validates the latest WPA3 security configurations across all three bands, in a one button, repeatable manner.

IDENTIFY Features

- **Authorized device list**
- **Sort/Filter**
- **Free-string search**
- **VLAN Identification**
- **Device Tagging**
- **Ping, Capture, Browse**
- **AutoTest**
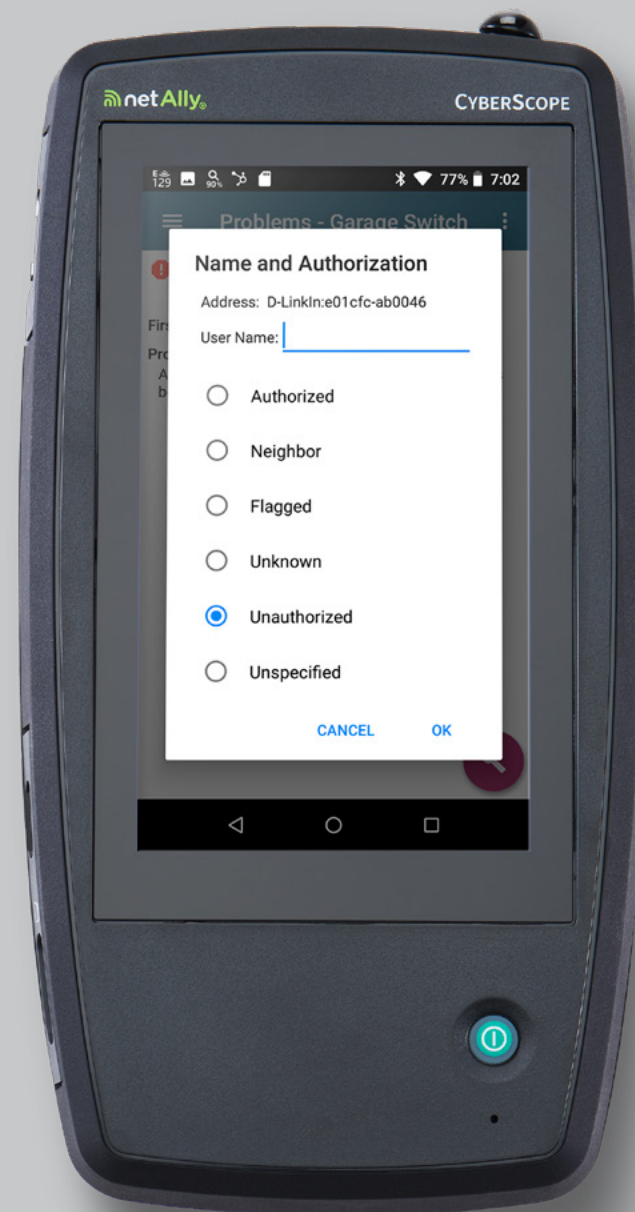
Locate

CYBERSCOPE®

FIND ENDPOINTS FAST – ON THE WIRE OR IN THE AIR

Path analysis is critical to understand how devices are interconnected. CyberScope provides complete port by port details of the network path to the device (Ethernet, wireless, or both) under investigation. This is crucial when hunting down unknown or rogue devices. CyberScope CE and CyberScope Air make hunting rogue wireless devices fast and easy with the tuned directional antenna.

The companion Link-Live collaboration, reporting and analysis platform lets you generate up-to-the-minute accurate topology maps to visualize connections.

Powerful filtering and sorting make it easy to spot device outliers, useful in particular for your Wi-Fi environment where device proliferation is the norm. Pressed for time or need remote experts to analyze the data? Collect the data in minutes on-site and do the heavy analysis and reporting in Link-Live, anytime from anywhere.
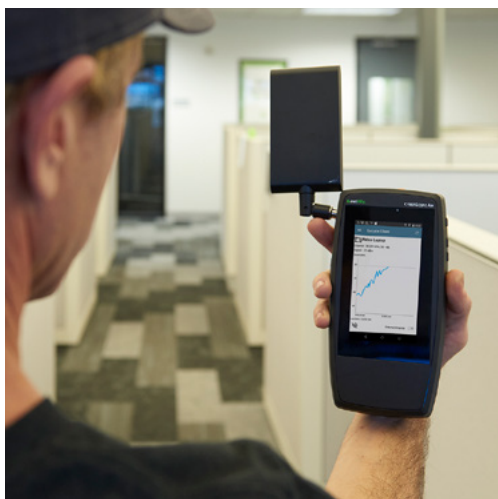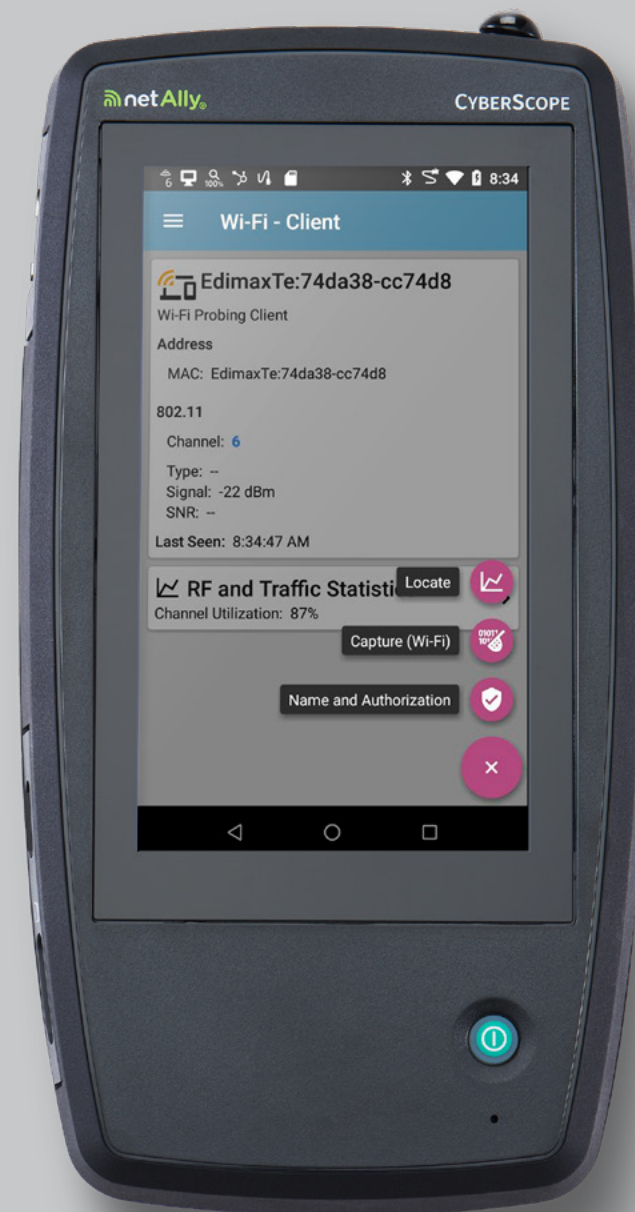
Rogue hunting with CyberScope's directional antenna

LOCATE Features

- **Path Analysis**
- **Port/VLAN identification**
- **AP, client, BT/BLE device surveys, directional antenna / signal strength tracking (select models)**
- **Topology Mapping**
- **Connection technology identification (link type/ speed, frequency/ band/channel)**

5

Analyze

TEST AND DEMONSTRATE POLICY COMPLIANCE

CyberScope identifies potential vulnerabilities like open backdoors, CVEs, and poorly configured firewalls and intrusion detection systems with embedded Nmap technology. However, the cryptic nature of Nmap's command line interface and excessive textual output prevents many security and network engineers and technicians from using it to its fullest extent.

The CyberScope **intuitive user interface harnesses Nmap's robust capabilities quickly and repeatably,** both on command/script execution as well as on the analysis of output. Even seasoned users will appreciate the ease of use that helps reduce the risk of successful attacks.

CyberScope can automatically scan for vulnerabilities on all endpoint devices connected to the network. Nmap enhances the information gathered from each device with deep analysis by running built-in or custom scripts and automatically generates warning and error notifications. All this can help identify potential security weaknesses and prioritize remediation efforts to reduce risk.

On CyberScope and CyberScope Air models, Wi-Fi and BT/BLE Analysis allow you to evaluate the network edge based on your area of concern be it channels, APs, SSIDs, BSSIDs, or clients. The included spectrum analyzer can show the affects of jamming devices and ensure no leakage of confidential network signals.

Visualizations such as heat maps (select models) and topology maps provide "aha moments" in understanding your network. Discovery Monitoring in Link-Live indicates the presence of new, missing, or transitory devices or changes since the last snapshot.

ANALYZE Features

- **Nmap Endpoint Vulnerability Assessment**
- **Real-time Wi-Fi analytics***
- **AirMapper Site Survey device and signal heatmaps***
- **AutoTest connection, segmentation, and endpoint analysis**
- **UDP/TCP port scans, OS, and services identification**
- **Topology Mapping**
- **Device Discovery Monitoring and Difference Analysis**
- **Packet Capture**

Available on select models

Report

ENABLE COLLABORATION AND SHARING BETWEEN TEAMS

Create reports for compliance and audit evidence

Reporting and compliance documentation is easy using the Link-Live collaboration platform. Features include interactive dashboard-based analysis in two versions: Discovery and Wi-Fi*. Each provides flexible workflows, with easy navigation between distinct data visualizations that begin with high-level summary consoles, flexible drill-down, persistent sorting, and free string searching for efficient investigations into anomalies and rapid problem troubleshooting. Also available is results comparisons, discovery monitoring, wireless heatmaps, and topology maps.

Link-Live provides organization wide management of all NetAlly analyzers and scan results via secure cloud access. Or there's a licensed, containerized version for on-prem or private cloud use.

Every test result is captured and can be easily compared to previous results. Secure sharing and even analyzer remote control by centralized experts fully enables collaboration across your team regardless of their location.

REPORT Features

- **Discovery Monitoring Reports**
- **Wi-Fi and BT/BLE Heatmaps***
- **Discovery and Wi-Fi*** **Analysis Dashboards**
- **Network Topology Maps**

Available on select models

7
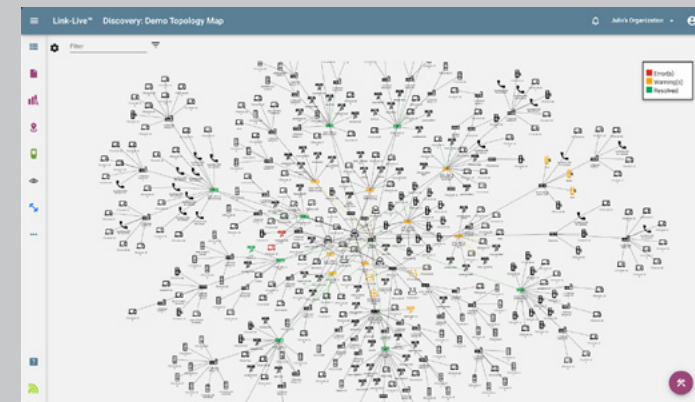
Discovery Monitoring

QUICKLY DETECT NEW ENDPOINTS AND CHANGES

Relentless flux in your network and edge devices makes situational awareness difficult—until now. Combining the power of CyberScope and Link-Live, SecOps teams can now quickly detect new, missing, or transitory devices along with network and device changes.

The Discovery process has now been automated, greatly increasing the effectiveness of edge network assessment, and making on-going situational awareness simple.

Once configured, Discovery can run periodically the same time every day, week, or month generating a network inventory snapshot which is automatically pushed to Link-Live.

Beginning with a baseline (initial discovery), each new snapshot is compared to the previous ones performed. Device and network differences are detected, and results reported within Link-Live in tabular or graphical format with new, missing, or transitory devices called out in easy-to-see color coding. Grading of device problems helps to further prioritize investigations. Three different table formats are available, Discovery, BSSID, and Clients—the latter two on select models only.

Given the potential for large numbers of endpoints at the network edge, powerful filtering and/or sorting is available (individually and in combination). Depending on CyberScope model, filter selections include device changes, device type, and many other categories. Free string searches can also be used alone or in conjunction to further target specific concerns or pinpoint issues. Seeing which devices are "stable" versus new, missing, or transitory is fast and simple.

DISCOVERY MONITORING Features

- Quickly find new, missing, or transitory devices
- Powerful filtering, sorting and free-string search make investigations into questionable devices fast and easy.
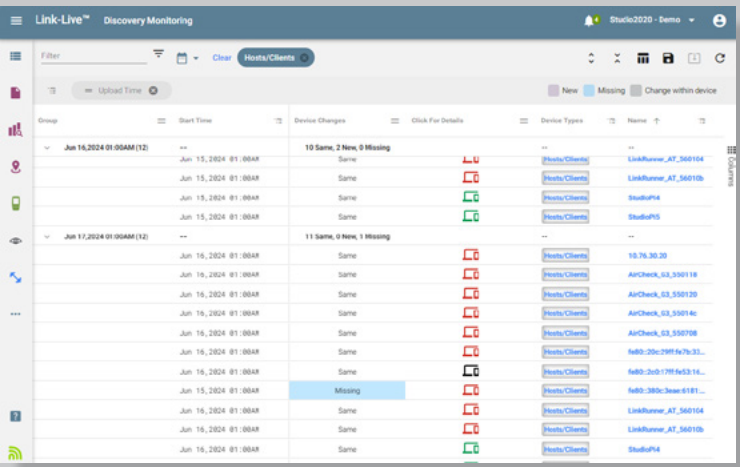
| Snapshot Date | Snapshot summary, individual device status | Device Name | Problem Severity | Nmap Open Port Status | Wi-Fi Type | Wi-Fi Security | Device Types |

Device Types

Features

POWERFUL TOOLS IN THE PALM OF YOUR HAND

Portable, for complete mobility

CyberScope is a rugged, hand-held instrument that is truly portable, so you can spot all your network vulnerabilities with a single walk through. It has all-day battery life (in Wi-Fi only operation, depending on model) giving you complete mobility; you can even send the analyzer to another location and securely control it remotely. Smart hands collaboration allows on-site field engineering services for proactive or reactive activities.

• **A handy, portable, yet powerful tool**
• **Remote Analysis capability**
• **Smart hands collaboration**

Purpose-built with everything you need

A dedicated, purpose-built tool, the CyberScope integrates all the capabilities you need for complete network edge assessment and analysis. Depending on the model, this includes RJ45 and fiber optic Ethernet ports for 10 Mbps to 10 Gbps and high-power PoE – capabilities you won't find on a laptop or tablet. USB ports provide connectivity for accessories, like the NXT-2000 Spectrum Analyzer, headset for voice communications, label printer, and more. Plus, you can run third-party apps, such as manufacturer's apps used to configure or control other assets like security cameras and building controls.

• **Purpose-built hardware**
• **Ensures repeatable, consistent test patterns**
• **USB port for accessories**
• **Expandable storage**
• **Leverage third-party apps**

Easy to use

You get a consistent user interface for all the different tools integrated into the CyberScope, including Nmap. AutoTest gives you a single-button pass/fail grading for fast, repeatable and fool-proof results. It's the easy way to have complete visibility of your edge network.

• **AutoTest for single button operation**
• **Visibility through layers 1 to 7**

Remote access empowers smart hands

Most times the expert is not where the problems are. CyberScope provides secure remote access using Link-Live or 3rd party apps. Within moments of the instrument's arrival on-site an unskilled admin can connect the instrument to allow complete remote operation.

Need to train new personnel? The bi-lateral remote operation allows you to drive the unit while training staff or looking over their shoulder to ensure understanding.

USB ports

RJ45 and fiber optic Ethernet ports*

*Available on select models

9
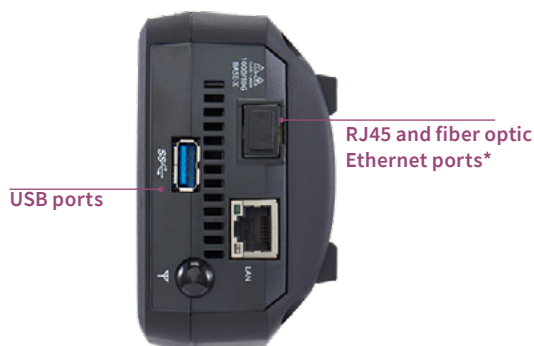
Models

Wi-Fi regulatory compliance implementation of the 6 GHz spectrum varies by country. CyberScope models are available in three versions: Full Tri-Band (capability across the entire 6 GHz band), Partial Tri-Band (capability for only certain channels in the 6 GHz band as determined by 802.11d regulatory domain information), and Dual Band Only (for countries where operation in the 6 GHz band is not allowed.)

	Model #/Name	Description
WIRED & WIRELESS	**CYBERSCOPE-CE-X2**	CYBERSCOPE-CE mainframe (FULL TRI-BAND) with one-year of AllyCare support (CYBERSCOPE-1YS), NXT-2000 Spectrum Analyzer, G3-PWRADAPTER, SFP+MR-10G850, RJ-45 inline coupler, EXT-ANT-TRIBAND directional antenna, WIREVIEW 1, Quick Start Guide, and hardened carry case.
	CYBERSCOPE-CE-E-X2	CYBERSCOPE-CE-E-X2 mainframe (PARTIAL TRI-BAND) with one-year of AllyCare support (CYBERSCOPE-1YS), NXT-2000 Spectrum Analyzer, G3-PWRADAPTER, SFP+MR-10G850, RJ-45 inline coupler, EXT-ANT-TRIBAND directional antenna, WIREVIEW 1, Quick Start Guide, and hardened carry case.
	CYBERSCOPE-CE-C-X2	CYBERSCOPE-CE-C-X2 mainframe (DUAL BAND) with one-year of AllyCare support (CYBERSCOPE-1YS), NXT-2000 Spectrum Analyzer, G3-PWRADAPTER, SFP+MR-10G850, RJ-45 inline coupler, EXT-ANT-TRIBAND directional antenna, WIREVIEW 1, Quick Start Guide, and hardened carry case.
WIRELESS ONLY	**CYBERSCOPE-AIR-X2**	CYBERSCOPE-AIR-X2 mainframe (FULL TRI-BAND) with one-year of AllyCare support (CYBERSCOPE AIR-1YS), NXT-2000 Spectrum Analyzer, G3-PWRADAPTER, EXT-ANT-TRIBAND directional antenna, Quick Start Guide, and hardened carry case.
	CYBERSCOPE-AIR-E-X2	CYBERSCOPE-AIR-E-X2 mainframe (PARTIAL TRI-BAND) with one-year of AllyCare support (CYBERSCOPE AIR-1YS), NXT-2000 Spectrum Analyzer, G3-PWRADAPTER, EXT-ANT-TRIBAND directional antenna, Quick Start Guide, and hardened carry case.
	CYBERSCOPE-AIR-C-X2	CYBERSCOPE-AIR-C-X2 mainframe (DUAL BAND) with one-year of AllyCare support (CYBERSCOPE AIR-1YS), NXT-2000 Spectrum Analyzer, G3-PWRADAPTER, EXT-ANT-TRIBAND directional antenna, Quick Start Guide, and hardened carry case.
WIRED ONLY	**CYBERSCOPE-XRF**	CYBERSCOPE-XRF mainframe (WIRED ONLY) with one-year of AllyCare support (CYBERSCOPE-XRF-1YS), G3-PWRADAPTER, SFP+MR-10G850, RJ-45 inline coupler, WIREVIEW 1, Quick Start Guide, and hardened carry case.

NOTE: All new CyberScope mainframes are sold with the first year (one-year) of AllyCare support included. Additional year(s) of support may be added. Product registration and <u>activation is required within 30 days of first power-on.</u>

CYBERSCOPE®
Edge Network Vulnerability Scanner

CYBERSCOPE® AIR
WiFi Vulnerability Scanner & Tester

Who is NetAlly?

For decades, our family of innovative network test solutions have been helping engineers and technicians better deploy, manage, maintain, and secure today's complex wired and wireless networks.

For more than 25 years, we have been the #1 ally of network and security professionals worldwide. We began by making the world's first handheld network analyzer – the LANMeter® – and have continued as industry pacesetters ever since, setting the standard for portable network testing and assessment. Our best-in-class tools deliver the visibility needed to get the job done, fast.

SIMPLICITY

- Simple, fast AutoTest makes novices more productive and experts more efficient
- Intuitive user interface allows more people to effectively use advanced technologies(Nmap)
- Standardized procedures ensure consistency

VISIBILITY

- See issues others cannot
- Visualization speeds time to understanding
- Multi-functional for faster answers and fewer tools

COLLABORATION

- Facilitating collaboration speeds time to incident resolution and frees up team resources
- Automated documentation saves time
- Easy report generation and sharing stops finger-pointing among teams

AllyCare Premium Support Services

AllyCare is a comprehensive support and maintenance service for NetAlly's network tools and AirMagnet® software that offers significant value over standard warranty. AllyCare can be purchased as either a one-year, two-year, or three-year membership.

KEY FEATURES*

Feature	With AllyCare	Standard Warranty
Latest Software & Firmware Versions	Yes	90-day manufacturing defects only
Repair Service Covered*	Yes	One-year manufacturing defects only
Accessory Replacements*	Yes	90-day manufacturing defects only
AllyCare-Enabled Product Features	Yes	No
Exclusive Online Product Tutorials	Yes	No
Priority access to Customer Experience & Solutions expert	Warranty support, plus priority product functionality and issue troubleshooting	License, installation, registration, application launch and warranty repairs only

*AllyCare Restrictions *(See Support Services Terms & Conditions for complete coverage and limitations at: www.netally.com/terms-of-use)*

- Repairs require prior qualification troubleshooting by our Customer Experience & Solutions Center. Damage covered is from normal wear and does not cover accidental product damage or loss. Accessories covered are those included with the original product purchase.
- Products that are sold with 1-year AllyCare Support included have certain features and capabilities enabled. At the end of your existing contract, you must renew your AllyCare Support contract to continue utilizing the enabled features.
- AllyCare membership may not be available in all countries. Please confirm with your NetAlly representative before purchasing.

For information about AllyCare Premium Support visit: netally.com/allycare-support

![NetAlly logo]
simplicity • visibility • collaboration