CYBERSCOPE®

Best Practices to Minimize Site Cybersecurity Vulnerabilities

CyberScope provides visibility to site access layer vulnerabilities.

PROBLEM STATEMENT – WHY SITE ACCESS LAYER ASSESSMENTS ARE NECESSARY

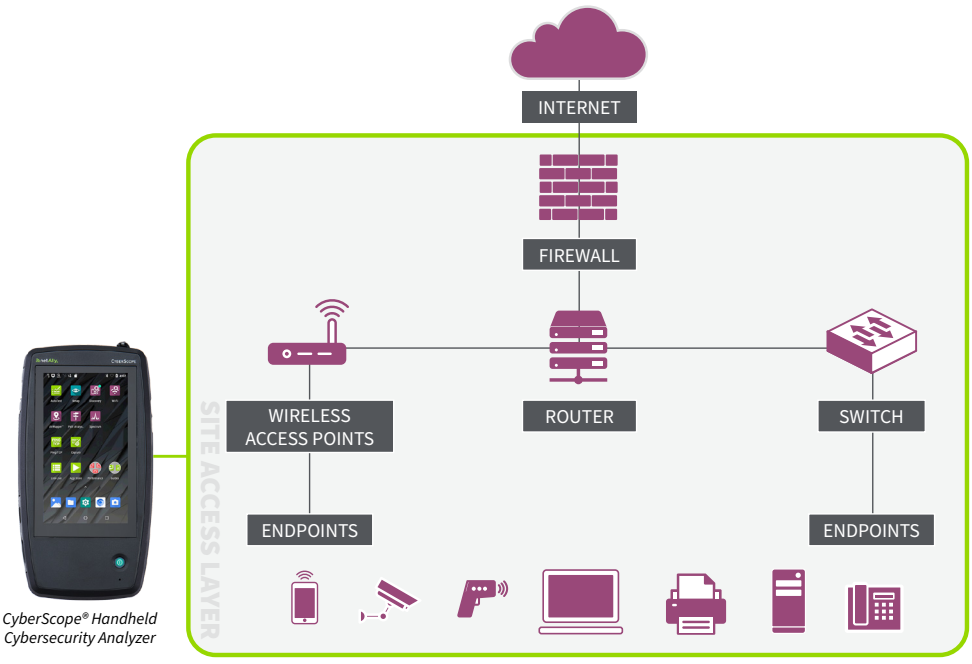
The site access layer ("the last 100 meters") of a network is ill-served by existing cybersecurity tools which cannot provide comprehensive, tactical (on-site) visibility required to reduce risk and enhance attack surface management. It is here that potential attack vectors converge including:

- Increasing complexity
- Enormous scale - growth of unmanaged devices enlarging the attack surface (IT/OT)
- Wide range of technologies in a less controlled environment
- Ubiquitous connectivity multiplies threats
- Frequent network/IT asset updates
- Numerous users accessing services (some known, many unknown)
- Close physical/Wi-Fi proximity to uncontrolled IT resources.

This list is repeated across every site within the organization. The result is elevated levels of risk and exposure associated with:

- Undetected vulnerabilities including rogue/incorrectly configured devices
- Unsecured Wi-Fi and wired connections
- Misconfigured network segmentation/provisioning

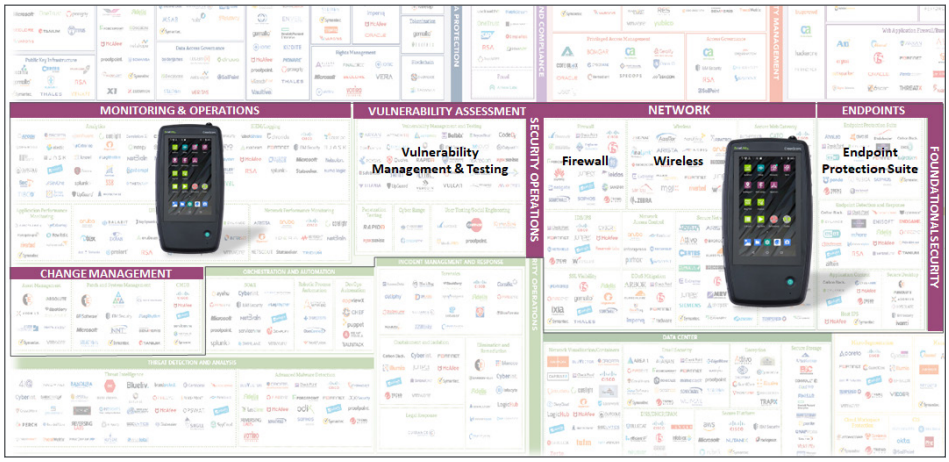
This daunting landscape can cause significant cyber-turbulence and provide numerous threats to IT assets and sensitive data.



CyberScope® Handheld Cybersecurity Analyzer

CYBERSECURITY TOOL ECOSYSTEM OVERVIEW & WHERE CYBERSCOPE FITS

The cybersecurity landscape is complicated and crowded with solutions that address individual or multiple threat vectors. There are many available security landscape frameworks, here is one simplified example and the two segments where CyberScope can add site-level visibility and enhanced vulnerability detection.



Cybersecurity technology map

HOW CYBERSCOPE IMPROVES SITE LEVEL CYBERSECURITY POSTURE AND OPERATIONAL EFFICIENCIES

With so many cybersecurity vendors pushing their solutions, what are the gaps that CyberScope addresses? CyberScope is the only comprehensive cybersecurity solution for NetOps and SecOps teams that provides in-depth, tactical “feet-on-the-street” site level situational awareness in a single coherent offering. That’s why we call it the “world’s first comprehensive handheld cybersecurity analyzer”. This view looks from “inside the site” rather than from the “outside” (as with cloud or appliance-based monitoring solutions). In doing so, it can find unknown devices and detect vulnerabilities that range from VLAN provisioning errors, a rogue access point, or a device with a single misconfigured open port—any of which could be an entry point for a hacker.

The only comparable, less-efficient onsite offering is a laptop or tablet that has been loaded with various open-source tools, standalone apps, and/or in-house designed scripts. Of course, with this hodge-podge of executables there is still no overarching framework that brings it all together, causing security specialists to spend extra time consolidating, analyzing, and sharing meaningful data.

CyberScope facilitates a standardized site assessment workflow, integrating Nmap scan results in its automated testing and network/endpoint discovery, with results automatically collated in Link-Live™, NetAlly's collaboration, reporting and analysis platform. Only CyberScope combines all this intelligence in a single, coherent solution.

Now let’s dig a bit deeper into the two areas of cybersecurity tool ecosystem mentioned above, *“Foundational Security”* and *“Security Operations”* and see how CyberScope is different from, and/or can augment these other solutions at the site access layer.

Security Operations

- *Monitoring and Operations* –This is a very diverse area encompassing numerous capabilities and vendors. Broadly, CyberScope offers general/user/device analytics and compliance visibility.
- *Vulnerability Assessment* – CyberScope features built-in Nmap capabilities with AutoTest integration providing fast detection of vulnerabilities.
- *Change Management* – CyberScope Network Discovery and Nmap capabilities enable NetOps or SecOps teams to find unknown devices and potential associated vulnerabilities; network analytics and visibility provides segmentation and VLAN provisioning validation.

Foundational Security

- *Network*
  - Firewall – CyberScope can validate firewall functionality to ensure correct IT resource access.
  - Wireless – CyberScope includes robust wireless security capabilities and performance testing.
- *Endpoints*
  - Endpoint Protection Suite – CyberScope provides detailed views into site access layer endpoints by discovering, identifying, and scanning devices locally.

Looking at the broader cybersecurity tool landscape, one attribute for most of these offerings is they are all generally deployed across the organization (e.g., cloud-based, "monolithic" appliance, or agent based). Each addresses a narrow aspect of site access visibility described above but none can match CyberScope's all-in-one capabilities at the site-level with the unique perspective of being physically present in the access layer. This distinct, tactical perspective can be crucial to rooting out vulnerabilities and should a breach occur, offer intelligence on lateral network hacker movement.

The other critical variable is that many organizations simply do NOT have budgets to deploy the litany of tools that provide total end-to-end visibility and intelligence, or they remain in a constant state of "catching up" with the addition of new locations so cybersecurity visibility coverage is forever lagging. CyberScope can effectively aid them in these cases, helping gain visibility that is often completely lacking in a simple-to-use tool for all staff expertise levels.

These same organizations frequently also suffer from a severe staffing shortfall and/or lack of in-house cybersecurity expertise. The result is a continuous struggle of aligning staff to resolve current service problems, take a more proactive cybersecurity posture, and foster NetOps and SecOps team collaboration efforts. CyberScope addresses each of these challenges in a simple to use offering, providing a path to automating work processes and maximizing staffing resources.

THE UNIQUE ADDED VALUE OF CYBERSCOPE

Beyond the value mentioned above, CyberScope also facilitates a more proactive stance in reducing site level vulnerabilities.

This is because CyberScope can be deployed immediately as the site resources and services are spun up (or updated). In fact, just like the best

practice of performing a Wi-Fi survey as the wireless network is deployed or modified (and periodically thereafter to maintain reliable service levels), CyberScope makes performing a site access layer assessment to detect vulnerabilities fast and simple - enabling teams to conduct frequent assessments with minimal effort, leading to a more effective site security posture.

CyberScope empowers the SecOps team or those responsible for cybersecurity to get in front of potential problems by detecting vulnerabilities before a breach occurs.

KEY TAKEAWAYS

Given the high stakes and treacherous IT remote location environment, it's critical for organizations to reduce risk at the site access layer where other tools can leave gaps or not provide complete visibility. CyberScope is the only solution on the market that provides unified, comprehensive site access layer visibility in a single easy-to-use tool with a tactical, location-specific perspective. Regardless of the business size, CyberScope can help. In the process, it can augment or bolster existing cybersecurity solutions and efforts by finding unknown devices as well as a range of endpoint vulnerabilities that, left undetected, can quickly expose organizations to escalating cybersecurity risk. The best solution for site access layer cybersecurity vulnerability visibility is CyberScope.

netAlly
CyberScope®