

Don't just scan for vulnerabilities - start *managing* them

Scan for Vulnerabilities Using Tracelnsight's Authenticated Scanning Engine

Tracelnsight includes a vulnerability scanning appliance built into the application. It is delivered as a virtual machine that sits on your network and runs authenticated scans against your devices. The authenticated scanning functionality increases scan speeds, greatly reduces false positives, and eliminates the risk of the scan negatively affecting systems during a scan.

Key Features:

- Scanner Appliance Virtual Machine can be deployed in common virtual environments (VMWare, HyperV, VirtualBox)
- Authenticated scanning - reduces false positives and gives pass and fail results
- Fast engine allows for more frequent scans of your environment
- Scan for hosts to determine all devices, including rogue devices on your network
- Create Scans and schedules to run scans daily, weekly, monthly, or quarterly

You Have Scanned for Vulnerabilities.... Now What? *Manage* Them!

You can't fix every vulnerability; there's just not enough time in the day with all of the other tasks you have on your plate. So, you must create a plan to prioritize the vulnerabilities that you can address and document the decisions you make on the vulnerabilities that you don't have time to address. Tracelnsight solves this problem.

Key Features:

- Use Tracelnsight's search, sort, and filter functions to prioritize the vulnerabilities that pose the most risk.
- Document your remediation action plan; identify the vulnerabilities you plan to fix, assign the remediation work to your team members, and document the reasons for not fixing the other vulnerabilities.
- Vulnerabilities include CVE ids, CVSS scores, and remediation reference information to aid in prioritization and remediation.
- Notation of vulnerabilities to demonstrate to management and auditors your plan for addressing vulnerabilities.

Report to Your Boss, Board, Auditors, and Regulators Your Vulnerability Management Plan

Ultimately, a board, boss, or regulator is going to ask about your vulnerability management program and you need to show your plan and your progress. Tracelnsight includes the necessary reports to show how you are addressing vulnerabilities, including how many new vulnerabilities are found and how many you and your team have remediated. Through these reports, it is easy to show that your vulnerability management plan addresses the most critical vulnerabilities in a resource-conscious way.

Key Features:

- Pass/Fail results from scanner show positive improvement over time - not just focusing on the failures
- Breakdowns help to show that the most important issues are addressed
- COncise way to prove that a meaningful vulnerability management process is in place - not just scanning