ONEMIND SERVICES

Vulnerability Assessment

DATASHEET

Don't Make It Easy

The more complicated your network is, the more vulnerabilities you have. Identifying these issues can be a daunting task for any IT department—especially when it comes to sorting through scan results to begin remediation.

With OneMind's Vulnerability Assessment, one of our cybersecurity experts will perform a comprehensive scan of your networks to determine internal and external vulnerabilities. We'll also provide expert review to help you identify which vulnerabilities are the most critical, which are easy to remediate, and which may be false positives. After your engagement, you'll have access to our Vulnerability Management platform to assist with ongoing remediation.

Our Approach

Depending on the complexity of your network and the level of testing you're looking for, OneMind offers three Vulnerability Assessment options to meet your needs. If you're seeking more manual testing of your networks, consider our Enhanced or Comprehensive Network Vulnerability Assessments, or even explore a Security Test (formerly Security Test).

New vulnerabilities are discovered regularly, so it's best practice to perform vulnerability scans at least once per month. With OneMind's Vulnerability Management software, you can perform unlimited scans, sort and prioritize results, assign tasks, and track remediation progress. The platform also helps demonstrate improvement and progress over time—ideal for reporting and compliance.

Vulnerability Assessment Offerings:

- Vulnerability Assessment (VA)
  Includes a network scan of all devices with manual false-positive testing on a sample of results. You'll receive a list of vulnerabilities along with best-practice recommendations.
- Enhanced Vulnerability Assessment (EVA)
  Adds advanced manual testing of internal and external networks, plus training on our platform for streamlined reporting and remediation.
- Comprehensive Network Vulnerability Assessment (CNVA)
  Includes all EVA features plus onsite testing of organizational practices, policy awareness, wireless networks, physical security, and data disposal procedures.

Frequently Asked Questions

Does this replace the need for a security test?
No. Vulnerability scanning doesn't determine whether a vulnerability is actually exploitable.

Is security testing included in this service?
No. Internal and External Security Testing (Security Testing) are separate offerings.

Is the scanner a hardware appliance?
No. It's an agent-less software-based scanner.

Do you conduct authenticated or unauthenticated scans?
Yes, both. We typically recommend unauthenticated scans for initial assessments.

How does the scanner connect to my network?
It must be installed on a workstation or in a virtual environment.

Will this hurt my network?
This is extremely unlikely. We do not conduct denial-of-service attacks.

Can your product integrate with my existing vulnerability scanner?
Yes. If you use Nessus, Nexpose, or Qualys, we can integrate scan results into our web platform for centralized management and reporting.

Will marked false positives show up in future scans?
No. Once a vulnerability is marked as a false positive or acceptable, it won't reappear.

Does your scanner detect rogue devices?
Yes, via our built-in network discovery tool.