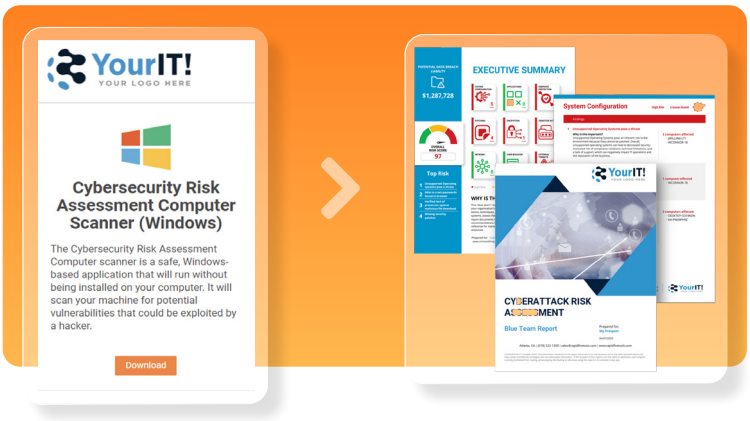
NETWORK DETECTIVE PRO

CYBERATTACK RISK ASSESSMENT
MADE FAST, EASY AND SIMPLE

The Cyberattack Risk Assessment is a special feature included in Network Detective Pro that makes it extremely quick and easy to remotely spot-check computers on any network and look for hidden vulnerabilities that could be exploited by a successful phishing attack, malicious insider or hacker who has managed to breach your firewall.



A white-labelled download page that you can brand with your logo.

A non-intrusive, self-running testing tool that end users can run on their computers, with nothing to install and no special credentials required.

A purpose-built assessment report that highlights the top risks discovered using charts and “plain English” descriptions summarizing the impact and importance of hardening the network. It also supplies supporting technical details about the specific issues it uncovers.

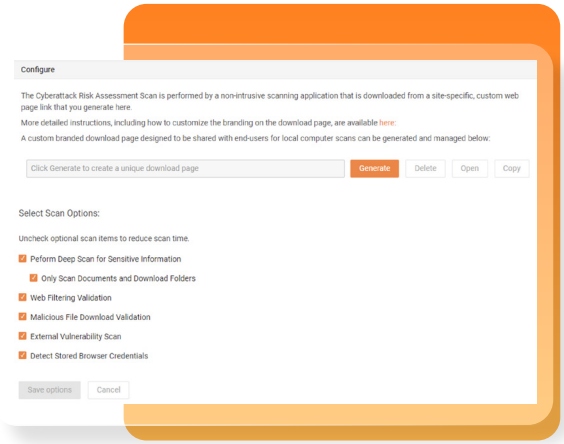
For managed service providers, the main use case for this feature is to make it easier to sell their services. With very little labor, they can remotely spot-check any prospect network and then use the report to help demonstrate the need for better risk management.

IT departments that manage their own networks can use the same tool to spot-check the cybersecurity posture of strategic partners and vendors. They can also check on remote employees who use their own computers for work and leverage the report for internal spot-check security audits.

How it **WORKS**

Generate the assessment download link

Within the Network Detective Pro software, there is an option for the IT technician to click a button and generate a unique URL to a brandable download page. This page explains the nature of the test and includes a button to download the tool.

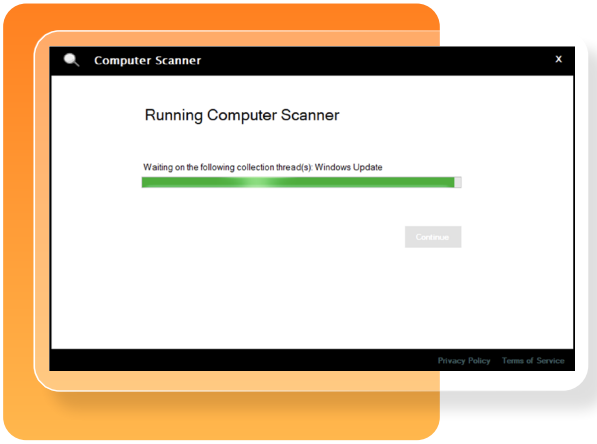


Send the link to selected end users

The URL is then sent to the end users of the computer systems included in a spot-check of the cybersecurity assessment. Ideally, this would include three to five "high target" computers belonging to upper management or critical business departments, such as the CEO, VP, HR and finance, to be tested for vulnerabilities and security issues.

End users download and run the tool

When each user clicks on the button, the tool gets downloaded onto their respective computers. The end user then clicks on the downloaded file to open it and start the test. The tool runs only that one time and doesn't install any software, agents or probes. It is designed to be non-intrusive and does not alter the computer in any way.



Merge the results and generate the report

Upon completion of the scans, the results of the tests are sent back to the Network Detective Pro site, where the IT technician can merge the results of the tested computers and generate a branded report in seconds — all with just the click of a button.

What kind of **RISKS IT DISCOVERS**

The tool tests for a wide range of common threat vectors that are likely to be targets of a cyberattack.

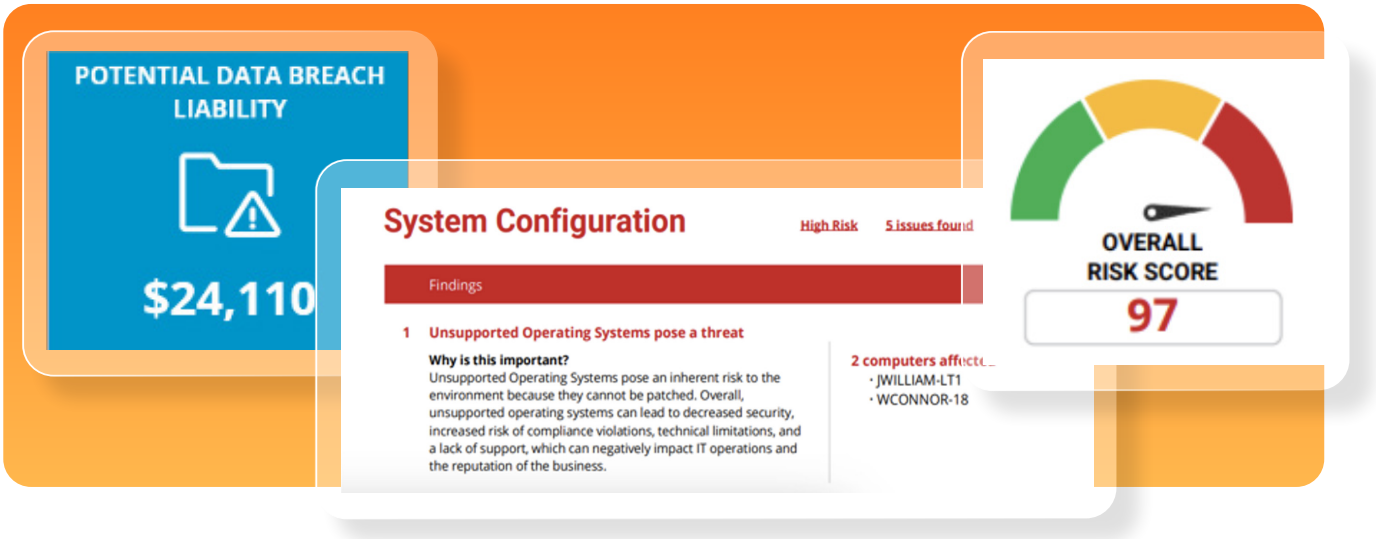
Here are some examples of the kinds of issues it can uncover:

- Missing or out-of-date patches
- Inconsistent or insecure password policies
- Sensitive data (PII) stored on systems and liability costs
- Documenting if the system is encrypted
- Checks whether a/v is installed and up to date
- Tests endpoint protection
- Checks whether web filtering is enabled
- Checks for external vulnerabilities
- System configuration issues
- Network issues
- Use-behavior issues

How the **RESULTS ARE PRESENTED**

The information is presented in the form of a professionally designed report, with a cover page that can be branded by the organization performing the assessment, including a custom logo and cover image. All key findings are presented on an Executive Summary page, with graphical elements representing nine key IT security categories. Each element is color-coded — red for high risk, yellow for medium risk and green for low or no risk — and includes the number of issues discovered for each targeted system.

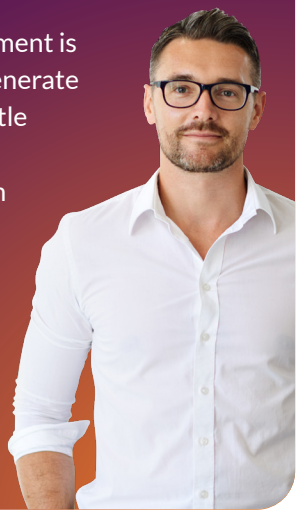
The Executive Summary is followed by supporting technical details for the findings as well as a "plain English" explanation of why it is important to be tracking each category, and the implications of not addressing the issue(s) immediately to reduce risk.



HOW TO USE this feature

For MSPs

The Cyberattack Risk Assessment is part of a proven method to generate new business. There's very little labor involved and the tests can be automatically run from remote locations. MSPs can widely advertise their offer to perform free spot-check assessments and then use the compelling reports to close the deal.



For IT departments

This tool is perfect to spot-check the cybersecurity posture of key partners and vendors who regularly access your network, as well as check the computers of remote employees who access the network from their home computers. It's also great for conducting internal spot-check security audits and reporting the current security status to the management.

Going beyond the **SPOT-CHECK**

The Cyberattack Risk Assessment feature is designed to provide a very quick and easy way to perform an initial yet comprehensive security assessment of a new environment, or a spot-check of one you manage. However, what it can reveal is just the tip of the iceberg.

Network Detective Pro also includes the IT industry's most comprehensive set of automated assessment tools, including specialized network scanners, lightweight discovery agents and cloud discovery tools. Set it up to automatically take a regular "snapshot" of your entire network — every device, every user, everywhere.

Have the risk summary report and detailed risk management plan generated automatically and sent to you for action to help harden and secure your network.

Request a demo and sample a test of your own network

Are the networks you manage secure? Do you have the tools to keep them risk-free? Contact us today for a demo of Network Detective Pro and get a spot-check cyberattack risk assessment of your own network at the same time.

Get a demo

of Network Detective Pro today.