RAPIDFIRE TOOLS
A Kaseya COMPANY

eGuide

How to Discover Hidden IT Issues and Vulnerabilities Before The Hackers Do

With cyberattacks on the rise, the likelihood of a security breach occurring is no longer a matter of "if" but"when." If you haven't fallen prey to a security breach yet, consider yourself lucky. However, your luck probably won't last long — especially if you fail to detect and mitigate security risks in a timely manner.

- The average time to identify and contain a data breach is **277 days** *(IBM)*
- **83%** of organizations have suffered more than one data breach *(IBM)*
- The average cost of a data breach is a record-high **$4.35 million** *(IBM)*
- Just **54%** of businesses have acted in the past 12 months to identify cybersecurity risks *(Gov.UK)*

Simplify the Discovery of IT Security Risks

To reduce the likelihood of a data breach, IT professionals like you must be aware of the constant changes that represent threats in the network environments that you manage. You need tools that give you "X-ray IT vision" so you can get a view beyond the surface of your IT environments. With the right tools, you can easily identify security gaps and risks and implement basic cybersecurity programs to harden your network.

This eGuide reveals the simple procedures you can implement to identify and address IT issues and vulnerabilities:

- Get the 360-degree hacker's view of your cybersecurity posture
- Stay ahead of hackers by scheduling automated scans
- Reduce risk by discovering hidden internal and external network vulnerabilities
- Detect hidden threats that create risk caused by unauthorized network changes and unexpected user activity

Perform Regular Automated Network and Security Assessments

Detect loopholes before they turn into big problems

A comprehensive network assessment gives you full visibility into your organization's network to build a proactive security strategy against external cyberthreats as well as end-user vulnerabilities. Network assessments expose security loopholes in your local network, in the cloud and on devices that connect remotely. A regular automated assessment allows you to keep an eye on everything and enables you to optimize network health and defenses.

- Gain 360-degree visibility through automated data collection for on-premises, cloud and remote users and devices
- Ensure immediate web access to all the data to troubleshoot issues faster
- Focus on the most important risks and issues with dynamically generated management plans
- Build executive infographic summary reports to demonstrate value to your organization's leadership and justify increased resource needs
- Optimize the entire process to get more done without adding more staff

Bonus tip: Use a powerful IT assessment tool like Network Detective Pro to non-intrusively scan networks and individual endpoints, analyze the assessment results and generate a wide range of professionally designed reports.

Automate Network Vulnerability Discovery and Management

An average of 50 new known vulnerabilities emerge each week while the top dozen vulnerabilities continue to reoccur regularly on unmanaged networks. Conducting regular vulnerability scans reduces blind spots by detecting security vulnerabilities in networks, systems and applications that could potentially be exploited by cybercriminals. Not only is regular internal and external vulnerability scanning a must-do in today's threat landscape, it is also mandated by nearly every major data protection regulation worldwide.

Identify internal and external network vulnerabilities before they are exploited

- Run regular vulnerability scans to assess your network and identify opportunities to enhance security
- Automatically create alerts and tickets for any critical and high-severity issues
- Reduce risk by hardening every device you manage
- Meet the vulnerability scanning requirements of any cybersecurity framework
- Devise a strategy to filter out false positives
- Build both brief and detailed reports to understand the scan results and guide remediation efforts

Bonus tip: **Use a purpose-built and affordable vulnerability scanning solution like VulScan to schedule any number of automated scans whenever you want and automatically generate reports without busting your budget.**

Manage and document compliance with any set of IT security requirements or controls

IT professionals need a simple yet effective way to measure risk and meet any industry, regulatory or internal IT security requirements without adding staff or stretching budget. An IT security assurance program proves your security programs are working — and dramatically reduces the likelihood of a successful cyberattack on the networks you manage.

Automate compliance management and IT security assurance

- Measure compliance against regulations and accepted frameworks
- Identify hidden risks and compliance violations in the office, with remote workers and in the cloud
- Manage and document compliance with any set of IT security requirements or controls
- Shield your organization against business interruptions, compliance violation fines, lawsuits and monetary loss
- Keep pace with organizational changes and expansion
- Automatically create accurate evidence of compliance

Bonus tip: A compliance management tool like Compliance Manager GRC produces the necessary documents to protect your organization in case of a lawsuit, audit or investigation related to a breach. It also supplies insurance auditors with a checklist of actions that match all the terms of your cybersecurity insurance policy.

Continuous Critical Change Detection

If a critical change that creates risk is left undetected — whether it's created with malicious intent or through an oversight or misconfiguration — it can compromise the confidentiality, availability and security of an organization's systems and data. Hence, detecting anomalous IT changes early is crucial. Once an individual gains access to your network, they can have free reign to search for and steal sensitive data. It's important to implement a strategy that can help you quickly identify critical network changes so that you can act in a timely way when necessary.

Discover critical IT changes that create risk

- Detect suspicious network changes such as unauthorized network connections and logins
- Track down suspicious user activity
- Identify new-user administrator rights
- Scan daily and receive alerts for new threats
- Find misconfigurations that create risk
- Unearth hacker footholds

Bonus tip: Leverage a critical IT change detection solution like Cyber Hawk that automatically scans for threats occurring behind firewalls. It has built-in machine learning that tracks activity over time, establishing patterns and trends that – when suddenly change – can represent real threats. The longer Cyber Hawk runs on your networks, the smarter it gets.

Your Complete IT Risk Management Toolkit

Control risk across every device. Every user. Everywhere.

RapidFire Tools offers a suite of automated software tools that give IT professionals the power to reduce IT risk. Each software product is complete, automated and priced right for any organization.

They work alone or as a powerful stack through a common web-based portal, shared users and sites with deep workflow integrations that reduce risk and drive improved IT management efficiency.

Four Products. One Integrated Platform.

Network Detective Pro

Network Scanning and IT Assessments

Identify, measure and manage network issues and risks.

VulScan

Vulnerability Management

Discover network threats & vulnerabilities.

Cyber Hawk

Change Detection

Detect unauthorized network changes and suspicious activity.

Compliance Manager GRC

IT Governance, Risk and Compliance

Demonstrate your InfoSec and compliance programs are working.

Request a Demo

with one of our specialists to understand how our suite of solutions can ensure nothing about your network ever catches you off guard.