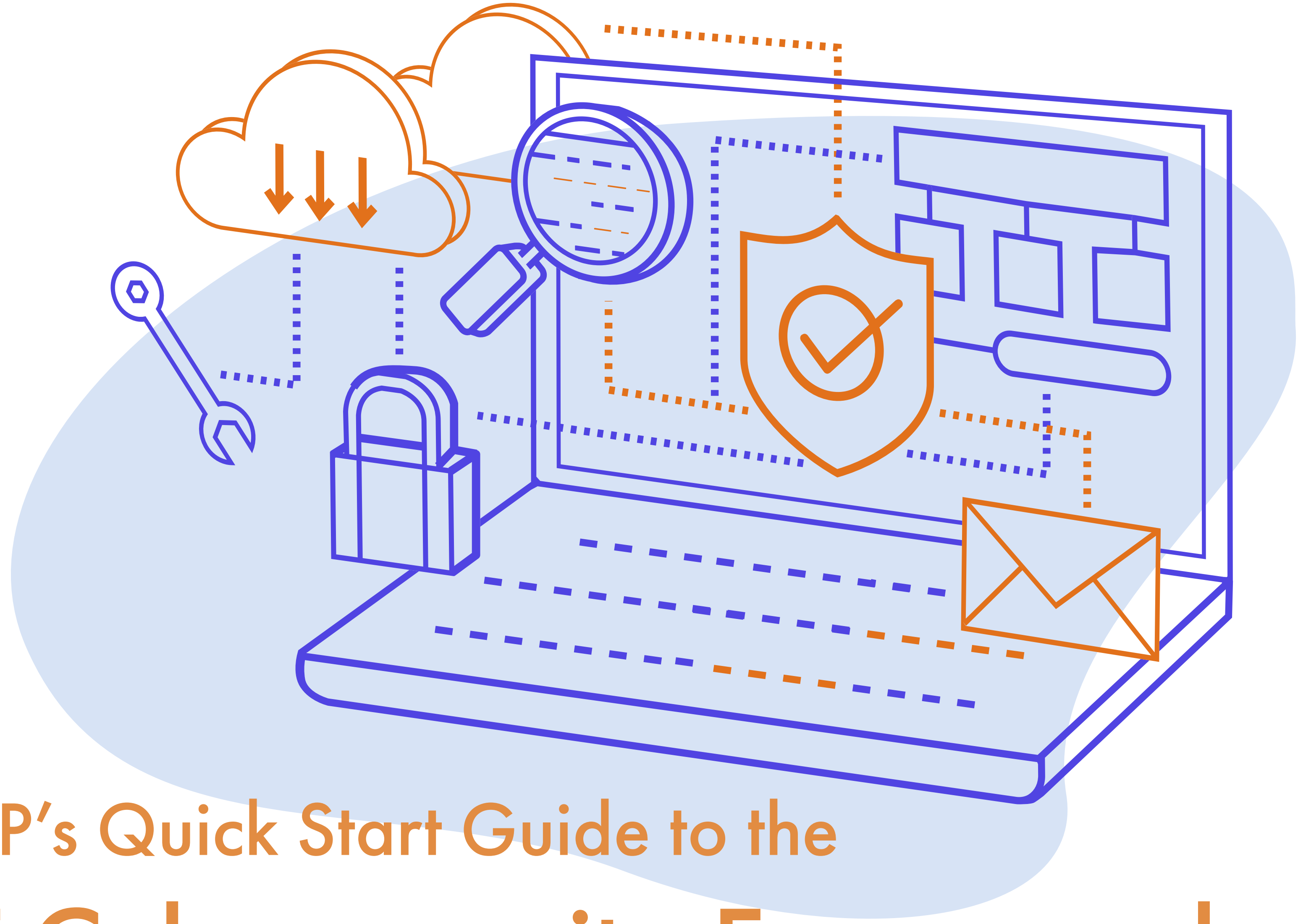


The MSP’s Quick Start Guide to the NIST Cybersecurity Framework

RapidFireTools®
A Kaseya COMPANY

Introduction:

When YOU Become the Scapegoat

It's bad enough to be the victim of a data breach. It's even worse when regulators and lawyers representing customers who are suing blame you for not adequately protecting their data. In today's dangerous digital world, companies are looking to solidify their defenses against the various potential attacks, leaks, and breaches lurking in the shadows.

The "Swiss Army Knife" of Cybersecurity

In regulated industries, adhering to industry standards and only working with compliant partners and solutions is required. Other businesses may choose to implement security programs based on a multitude of choices. Small businesses don't have the financial or technical resources of larger organizations. Where do you begin?

The NIST Cybersecurity Framework (NIST CSF) is "the Swiss Army Knife" of cybersecurity. It is a framework that covers all areas of cybersecurity and is affordable and achievable for organizations of all sizes. Only businesses that are required to comply with other standards, such as defense subcontractors, and government contractors, should use a different approach.

The NIST CSF aligns with HIPAA and other federal regulations. States like New York have based their requirements for financial service organizations on the framework. Ohio allows businesses that implement the NIST CSF to use it as a defense in lawsuits. CompTIA, the IT industry association, has based its Security Trustmark+ accreditation on the NIST CSF.

What is NIST?

NIST is the National Institute of Standards and Technology, an agency in the US Department of Commerce. It provides guidance and standards that are then referenced in laws and regulations, but NIST has no regulatory authority on its own.

The NIST Special Publications (SP) on Technology are designed for government agencies, government contractors, and the public. NIST SP 800-53 has been the framework for government contractors and government agencies other than Homeland Security. It is 460 pages and includes approximately 1,000 individual security controls. NIST SP 800-171 is a framework for protecting Controlled Unclassified Information (CUI) stored at private companies. It is 83 pages and includes approximately 110 security controls.

What is NIST CSF?

Because NIST SP 800-53 and SP 800-171 were considered too expensive and difficult for smaller businesses, NIST worked with the private sector to create the NIST Cybersecurity Framework (CSF).

The NIST CSF started in 2013 as the result of a presidential order to protect data in the private sector. The latest update is a 55-page document that helps an organization determine their current cybersecurity state, set their end goal, identify opportunities to get there, track progress and communicate status to stakeholders.

Who Uses the NIST CSF?

The NIST CSF is a voluntary framework. Businesses of all types and sizes use it to assess their cybersecurity and prioritize which improvements to make first.

Some regulations require adoption of the NIST CSF. The New York State Department of Financial Services requires organizations it supervises to include NIST CSF implementation in their compliance with its security standards. A New York law requiring protection of student data specifically references the NIST CSF.*

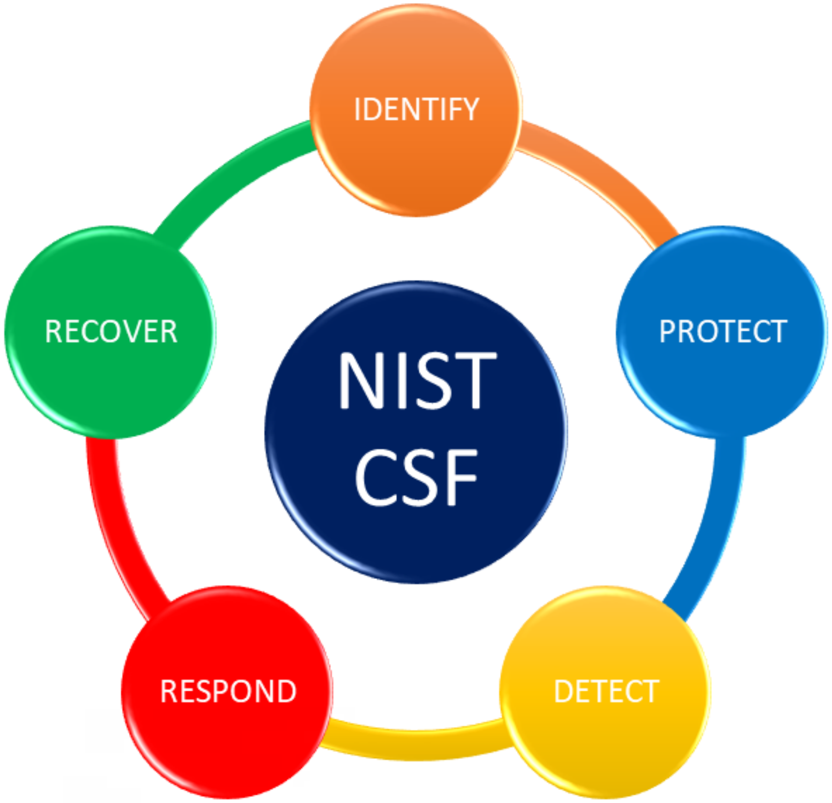
Ohio and other states provide protections if you adhere to "reasonable security standards." The key word is *standard*. What could be easier than justifying your use of a government framework as your standard?

The NIST CSF also maps to regulations like HIPAA, PCI-DSS, SOC-2, GLBA, and more. Implementing the NIST CSF will address specific, but not all, requirements in those regulations.

*From the NY Commissioner of Education in January 2020:
As required by Education Law §2-d (5), the Department adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) as the standard for data security and privacy for educational agencies.

The Five Core Functions

The framework has five core functions:



#1 Identify

What data do you have and where is it located.

What devices do you own?

#2 Protect

Safeguards to protect IT infrastructure and data, including identity management and protective technology.

#3 Detect

Instituting processes and solutions to spot potential problems, such as continuous monitoring for anomalies and events.

#4 Respond

Development of policies and procedures to react when an event occurs, including mitigation, communication and future improvements.

#5 Recover

Devising and implementing plans to restore business activities and impacted systems after an event.

The Four Tiers of Preparedness

As organizations assess their cybersecurity preparedness, they can also determine what level of preparedness is ideal for various aspects of their IT infrastructure. The framework has four tiers:

- **Partial -** Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.
- **Risk Informed -** Risk management practices are approved by management but may not be established as organizational-wide policy.
- **Repeatable -** The organization's risk management practices are formally approved and expressed as policy.
- **Adaptive -** The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators.

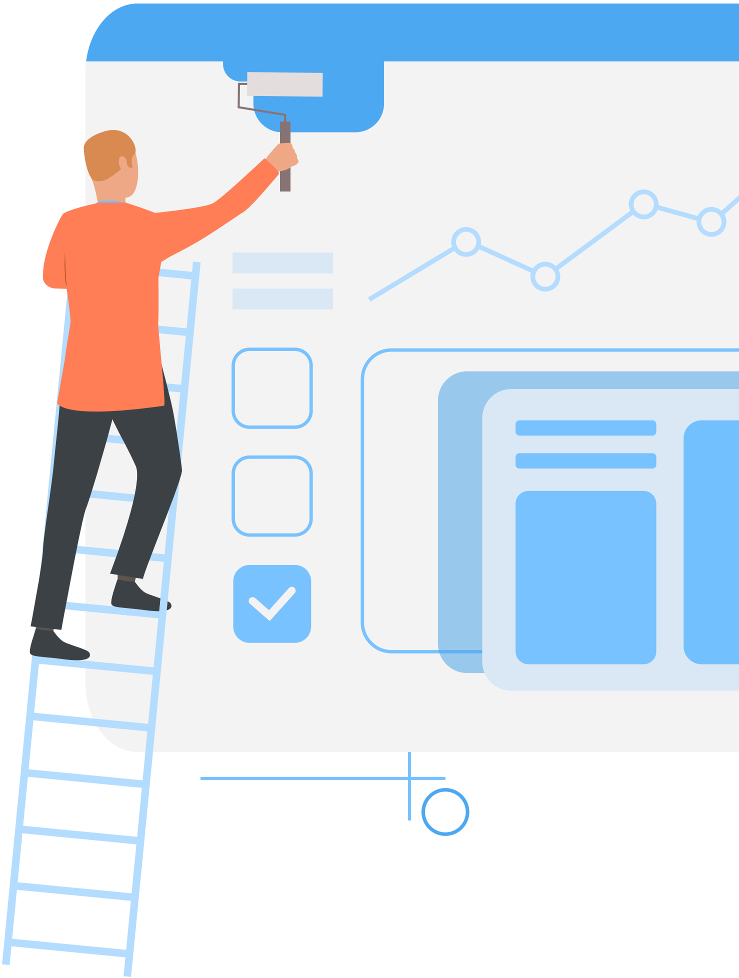
Organizations should strive for the Repeatable and Adaptive tiers to protect themselves from breaches and the resulting expensive and embarrassing after-affects.

A Ready-Made Framework Covering All Areas

The NIST CSF is affordable and achievable because it includes common-sense recommendations and widely accepted best practices. Its primary advantages come from its comprehensive nature and its flexibility to be useful to organizations that vary widely in purpose and size.

There are multitudes of cybersecurity solutions, recommendations, and best practices out there, but most of them are only addressing a segment of an organization's overall cybersecurity profile. There are guides to prevent phishing and benchmarks for backup and disaster recovery, but they're rarely all found under the same umbrella. The framework provides an organized structure to ensure that all areas of cybersecurity are addressed. By using the framework, there's a common language and set of expectations established that makes collaboration and trust far easier.

A great benefit of implementing the framework is that it is already done for you, and you can just focus on the security controls within each section. If you are audited, investigated, or sued for a cybersecurity issue, you can show that you consistently implemented the recommendations of the US government. It will be difficult for a regulator, attorney, or jury to accuse you of doing the wrong thing.

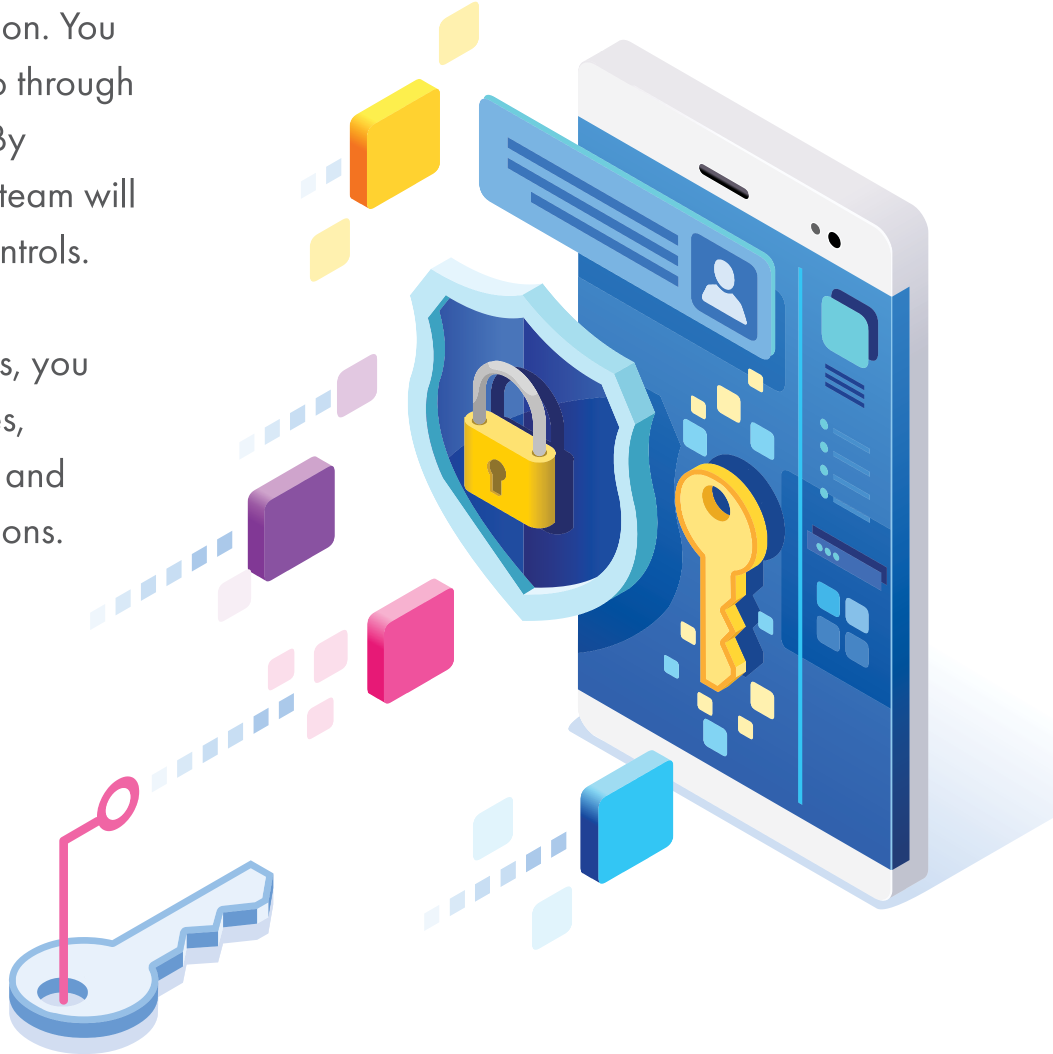


Better Protection for You and Your Clients

You should start by apply the NIST CSF to your own organization. You know that MSPs are being targeted by hackers who want to go through you to get domain administrator privileges to your client sites. By implementing the NIST CSF, you will protect yourself and your team will learn to implement the framework and live within its security controls.

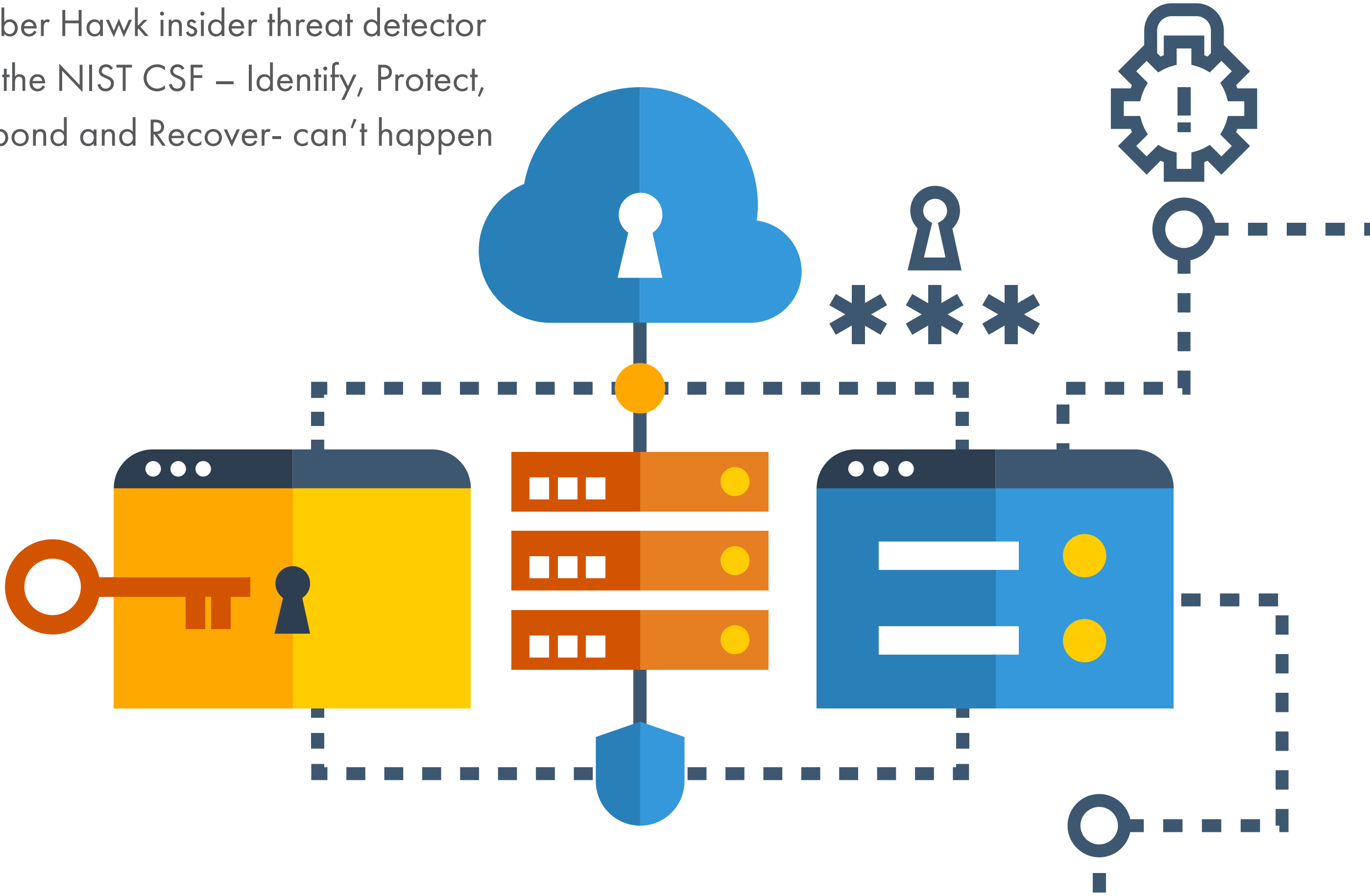
Because the NIST CSF is fully mapped out with security controls, you can use it as a basis for security assessments, managed services, and compliance services. You can align your stack of products and services with the framework and fill in any gaps with new solutions.

Your clients hire you because of your expertise, experience, and the special tools you use to secure their data so they can focus on their mission. By helping your clients implement the NIST CSF, you can sell them more, provide better protection, and help them protect their reputations and finances against regulatory fines and lawsuits.



The Right Tools for the Right Job

Network Detective Pro assessment modules, the comprehensive Compliance Manager platform, and Cyber Hawk insider threat detector are perfect for the first three functions of the NIST CSF – Identify, Protect, and Detect. The last two functions – Respond and Recover- can't happen if you don't get the first three right.



THE RIGHT TOOLS FOR THE RIGHT JOB

IDENTIFY

Network Detective Pro IT assessment modules and Compliance Manager help you identify the devices on a network and where data is stored.

Deep scans can be run to identify Protected Health Information (PHI) that is protected by HIPAA, and Personally Identifiable Information (PII) like Social Security Numbers that is protected by every state data breach law.

Using these tools will help you scope the security requirements.

PROTECT

There are many tools you can deploy to protect the network perimeter and set controls to protect from insider threats. But you'll need Network Detective Pro and Compliance Manager to make sure these other tools are actually working.

Both identify the status of security Controls like security patches, antivirus protection, external vulnerabilities, and password management. Both provide reports that can be used as evidence of security and compliance.

You can enhance your managed services by incorporating these tools into your daily activities.

DETECT

Network Detective Pro and Cyber Hawk help you detect unusual behavior on a network that may indicate a breach.

Seeing that an average user's account has been elevated to a network administrator, or that failed logins have increased, can be the first indicators of a compromise, allowing you to prevent an expensive and embarrassing data breach.

How to Deploy NIST CSF for All Your Clients

You already provide cybersecurity services to your clients. Now take the next step to prove your security is working, and document it. See how Compliance Manager can help.

Compliance Manager for NIST is a purpose-built platform that allows you to create a customized cybersecurity program for each of your clients based on the NIST Cybersecurity Framework. This platform allows you track ongoing compliance with the specific IT security policies and procedures you set and document any issues and remediation steps you take.

Click here to request your demo.

RapidFire Tools, a Kaseya company, creates innovative business-building technology tools for Managed Service Providers (MSPs). More than 8,000 technology service professionals worldwide use our products to close more business, offer more services, keep more customers, and make more money. Our offerings include Network Detective Pro®, Compliance Manager™, and Cyber Hawk.™

Network Detective Pro is the #1 non-intrusive IT assessment and reporting tool. With it, MSPs can quickly and easily capture a vast amount of network assets, users, configurations, and vulnerabilities without installing any software, probes, or agents. Our proprietary algorithm analyzes the data to generate dozens of professionally designed, completely brandable reports in minutes.

Cyber Hawk detects insider cybersecurity threats and generates daily alerts of suspicious network changes and anomalous end-user behaviors. Cyber Hawk empowers MSPs to create custom, brandable, and unique cybersecurity services at an affordable rate.

Compliance Manager is a unique compliance process automation tool with built-in modules to support the delivery of Compliance-as-a-Service solutions for HIPAA, GDPR, the NIST Cybersecurity Framework, as well as for most cyber liability insurance policies. MSPs use Compliance Manager to ensure that the IT policies and procedures required by industry or government regulations are being followed and, critically important, documented.

To learn more, visit www.rapidfiretools.com or call 678-323-1300.