IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

What is the NIST Cybersecurity Framework and Why does it matter?

Tim Dales

 Tim Dales Product Marketing Manager Infinidat	***Biography*** *Tim Dales is a Product Marketing Manager at Infinidat (https://www.infinidat.com). Tim has over 30 years' experience in the development, marketing and sales of IT infrastructures.* *A former Senior Analyst at a storage analyst firm working with the Dell/EMC product team on APEX and creating launch collateral for Pure Storage.* *He has also held positions as an executive for networking vendor Solarflare, product marketing and sales for a CDP startup, MTI, and Emulex.* *Tim blogs at https://www.infinidat.com/en/blog/*

Keywords National Institute of Standards and Technology (NIST), Cybersecurity Framework, InfiniSafe cyber security stack
Paper type Research

Abstract

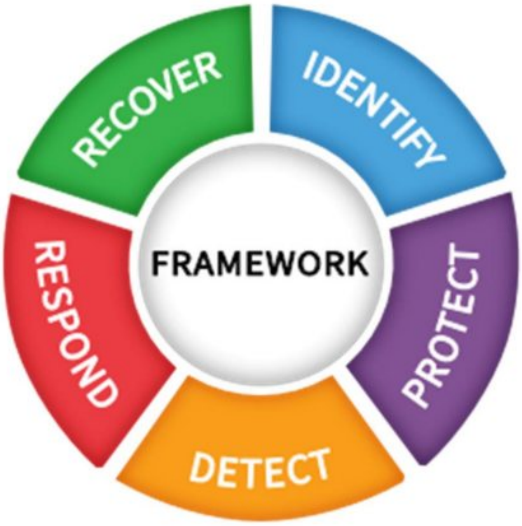
NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. The NIST Cybersecurity Framework helps businesses of all sizes better understand, manage, and reduce their cybersecurity risk and protect their networks and data. As the author explains in this article, the Framework gives businesses an outline of best practices that can help them to decide where to focus their time and money for cybersecurity protection.

Introduction

Founded in 1901, The National Institute of Standards and Technology (NIST) is one of the nation's oldest physical science laboratories and is now part of the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

You may be familiar with the NIST Cybersecurity Framework[1] (CSF) which was first developed and published in 2014 to help organizations worldwide easily and effectively manage cybersecurity risk. NIST is currently working on a new update – CSF 2.0, which we should see in early 2024. NIST CSF is one of the most widely adopted security frameworks across all industries, worldwide.

Figure 1: NIST Cybersecurity Framework



Source: National Institute of Standards and Technology (NIST)

It's worth noting that the Cybersecurity Framework came from a NIST Laboratory called The Computer Security Resource Centre (CSRC), which is focused on information related to many of NIST's cybersecurity and information security related projects, publications, news, and events. CSRC supports people and organizations in government, industry, and academia – both in the U.S. and internationally.

Figure 2: Security Guidelines for Storage Infrastructure

NIST Special Publication 800-209

Security Guidelines for Storage
Infrastructure

Ramaswamy Chandramouli
Doron Pinhas

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-209

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Source: National Institute of Standards and Technology (NIST)

One of those many projects that NIST creates is the Special Publication (SP) 800 Series, which presents information of interest to the computer security community – it developed NIST SP 800-209 (2020) Security Guidelines for Storage Infrastructure.

NIST SP 800-209 provides an overview of the development and evolution of storage technology, examines current data storage security threats, and provides a detailed set of security recommendations and guidance to address storage threats.

This is the quintessential NIST guide for any enterprise IT team that wants to have a security framework of guidelines for their storage infrastructure, including cybersecurity, to create a more compliant, hardened storage environment.

For 98% of the applicable NIST guidelines, Infinidat provides tools, solutions, features, or methods to assist an enterprise with successfully implementing a secure storage infrastructure. Of the guidelines, there are 52 that directly apply to a storage systems vendor and within the control of the storage system.

Additionally, with InfiniSafe cyber security stack, we include comprehensive cyber storage software technology – our award-winning InfiniSafe – that can be easily implemented to help enhance your cyber resilience. They include:

- **Immutable snapshots:** Whether scheduled or manually created, InfiniSafe's immutable snapshots are secure and unchangeable, point-in-time copies.

- **Logical/Remote air-gap:** InfiniSafe provides a simple way to logically separate immutable data copies from network access either locally, remotely, or both.

- **Fenced forensic environment:** InfiniSafe enables you to create a completely private network that is isolated for data validation, testing, and recovery.

- **Near-instantaneous recovery from cyberattacks:** Get all of your known good and validated data back and available for restore in minutes, regardless of the data set size.

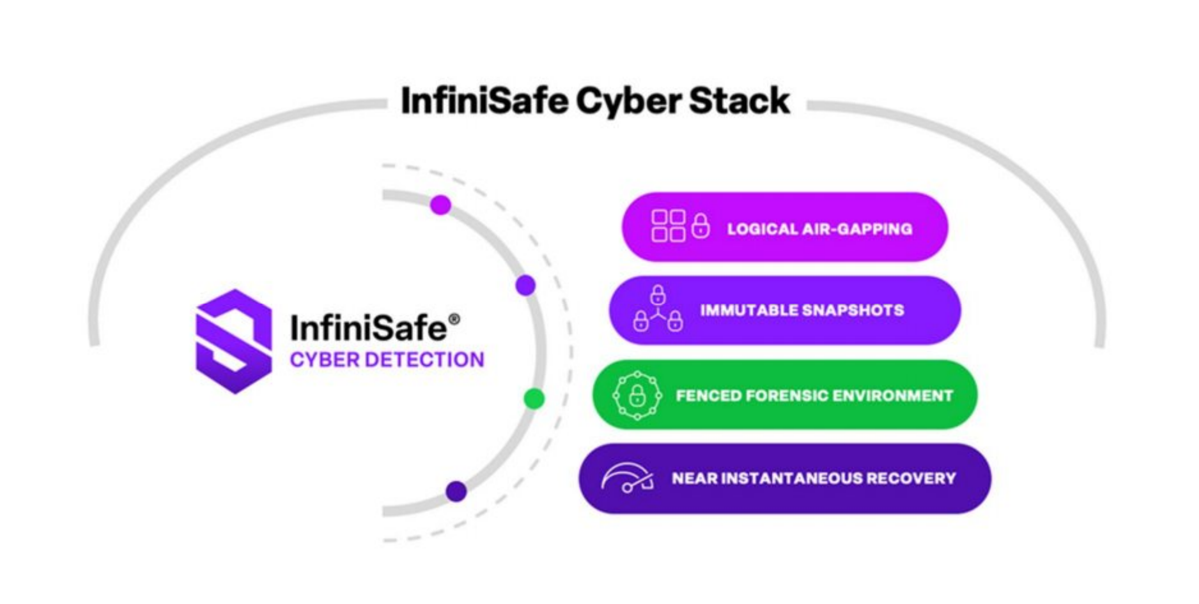
These InfiniSafe core functions are available at no additional cost to our InfiniBox®, InfiniBox™ SSA and InfiniGuard® platform customers.

InfiniSafe Cyber Detection

Taking cybersecurity one step further, we have extended the InfiniSafe® enterprise cyber storage software stack with an optional, subscription-based solution: InfiniSafe Cyber Detection.

When an attack is detected, InfiniSafe Cyber Detection provides forensic reporting to diagnose what data has been compromised and the nature of the compromise and provides critical insights to where the compromised data originated. Then, using the power of InfiniSafe technology, the IT team can quickly recover to normal business operations, once they have identified a known good copy of the data.

Figure 3: InfiniSafe Cyber Stack



InfiniSafe Cyber Detection uses a combination of over 200 full-content-based analytics that inspect the content of files and data, not just metadata. Powerful machine learning algorithms will tell you the type of variant that was used to corrupt the data with 99.5% accuracy, helping companies protect their business-critical infrastructure and content without a waterfall of false positives, so you can focus on real areas of concern and address issues quickly.

With the great number of features and capabilities provided with the Infinidat storage platforms, along with the full set of core and optional InfiniSafe technology, enterprise IT teams can ensure that their storage infrastructure meets NIST compliance and can avoid the impacts of ransomware and malware attacks.

Additionally, ask your cyber insurance carrier if you qualify for a rate discount if you are NIST compliant or have implemented cyber resilience/security/recovery measures such as InfiniSafe and InfiniSafe Cyber Detection technologies within your infrastructure?

Reference

[1] NIST Cybersecurity Framework. Available at: https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0