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**

NIST CSF 2.0 Update and Cybersecurity Awareness Month

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 Cybersecurity, Reporting obligations, Regulations, EU Directives, InfiniSafe Cyber Protection, Risk management
Paper type Research

Abstract

The global cybersecurity threat is ever constant, and its impact on enterprises can be devastating. The fact that the cybersecurity problem is very, very broad causes challenges to technology providers looking to create more secure enterprise data infrastructure, data centre, and hybrid cloud environments. As the Cybersecurity and Infrastructure Security Agency (CISA) launches a new cybersecurity program to mark October's Cybersecurity Awareness month, the author of this article looks at how Infinidat is dedicated to promoting a safer, more secure environment for its enterprise customers and the role it is playing in educating how enterprises can stay cyber secure.

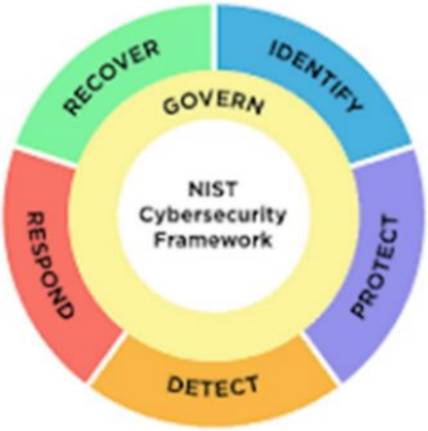
Introduction

At Infinidat we are very aware of the global cybersecurity threat and the impact that it has on enterprises, and by including cyber storage resilience and cyber storage recovery technology in all our enterprise storage solutions we can make an outstanding difference in helping companies manage their cyber risks.

NIST Cybersecurity Framework (CSF 2.0)

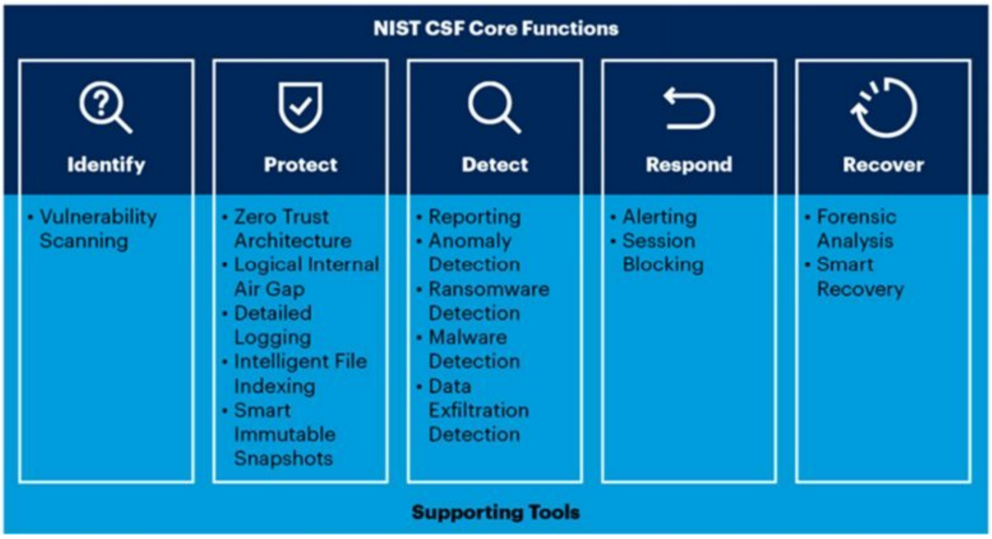
The NIST Cybersecurity Framework[1] (CSF) which was first developed and published in 2014 to help organizations worldwide easily and effectively manage cybersecurity risk. CSF 2.0[2] is an update of this framework adding the “Govern” function as a core function that informs how the other five functions are implemented. NIST CSF is one of the most widely adopted security frameworks across all industries, worldwide.

Figure 1: NIST Cybersecurity Framework (CSF 2.0)



Using the Gartner Cyber Storage capabilities mapping to NIST Cybersecurity Framework (CSF), the Infinidat InfiniVerse® Cyber Resilience Services fulfills all the NIST CSF core functions.

Figure 2: Layering tools using NIST Cybersecurity Framework

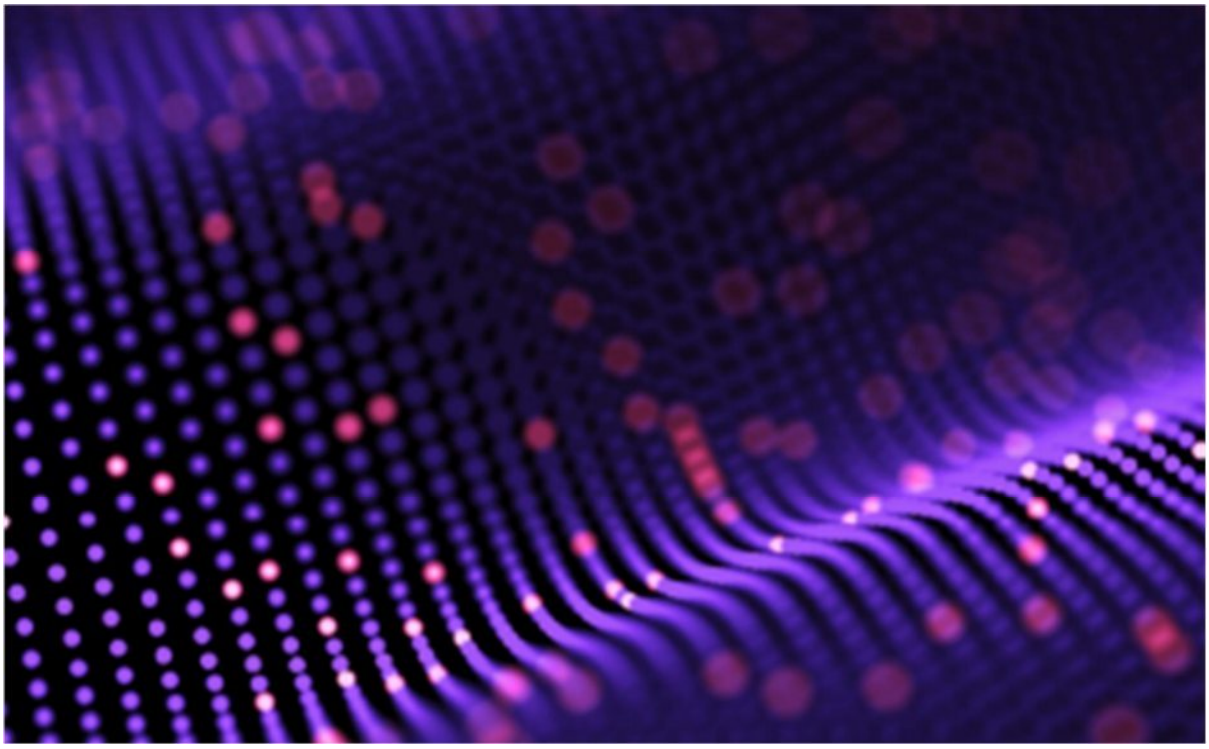


NIST CSF Core Functions

Identify	Protect	Detect	Respond	Recover
• Vulnerability Scanning	• Zero Trust Architecture • Logical Internal Air Gap • Detailed Logging • Intelligent File Indexing • Smart Immutable Snapshots	• Reporting • Anomaly Detection • Ransomware Detection • Malware Detection • Data Exfiltration Detection	• Alerting • Session Blocking	• Forensic Analysis • Smart Recovery

Supporting Tools

Source: Gartner



The Cyber Resilience Services of the InfiniVerse® Platform provides an end-to-end, multi-layered cyber stack for the creation of cyber-centric storage resilient environments focused on early detection and recovery, with guaranteed Service Level Agreements (SLAs). At the core is InfuzeOS™ software-defined storage (SDS) platform delivering advanced cyber storage capabilities. We use a secure-by-design approach to cyber-centric resilience and cyber recovery with three essential elements of the InfiniSafe® technology suite:

1. **InfiniSafe Core Cyber Stack** – Infinidat's award-winning InfiniSafe cyber resilience stack provides essential foundational capabilities in four main areas:

   - ***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.

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

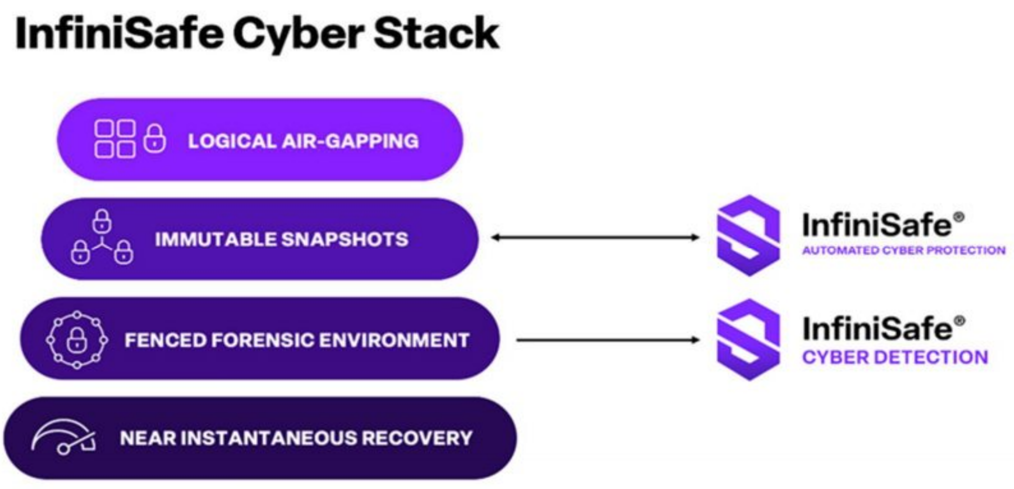
The current issue and full text archive of this journal is available on https://www.itceoscfos.com

2. **InfiniSafe ACP – Automated Cyber Protection** – at the "front end" to proactively coordinate the detection of abnormal file activity with your syslog, SIEM, or SOAR data centre-wide cyber security applications. Then orchestrate automatic event-based, immutable snapshots, file scanning, and ransomware detection to substantially reduce threat window exposures.

3. **InfiniSafe Cyber Detection powered by CyberSense** – extends cyber prevention further by validating the integrity of your immutable snapshots using powerful, AI -based machine learning scanning engines. Comprehensive machine learning detects ransomware and malware attacks with up to 99.99% accuracy so you can quickly and easily identify your data's last known good copy for rapid, intelligent recovery.

4. **InfiniSafe Cyber Detection** – adds a level of data detection to the InfiniSafe Cyber Stack that surrounds the four main layers of the stack and deepens the ability of InfiniSafe to detect cyber incidents. InfiniSafe Cyber Detection performs a deep scanning of block, file, and database stores by presenting InfiniBox® and InfiniBox™ SSA immutable snapshots to powerful AI-based scanning engines that will validate their integrity and, through machine learning, identify any malicious changes that could indicate a cyberattack.

Figure 3: Infinidat's infiniSafe Cyber Stack



Source: Infinidat

InfiniSafe Cyber Storage Guarantees build on our core InfiniSafe technology and guarantee both recoverability of immutable snapshots and recovery in a minute or less on our InfiniBox and InfiniBox SSA storage solutions and 20 minutes or less on our InfiniGuard purpose-built backup appliance, regardless of dataset size.

But we didn't stop there! Our secure-by-design approach also aligns well with NIST SP 800-209 (2020) Security Guidelines for Storage Infrastructure[3], which 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.

As malicious ransomware and malware incidents continue to disrupt critical services and businesses from energy pipelines to schools and hospitals, the total economic losses from these cyberattacks continue to climb. Implementing an effective end-to-end cyber-centric detection and recovery strategy with the Cyber Resilience Services of InfiniSafe can mitigate your enterprise's exposure and ensure rapid recovery.

Reference

[1] National Institute of Standards and Technology (NIST) https://www.nist.gov/cyberframework

[2] *The NIST Cybersecurity Framework (CSF) 2.0 (*26 February 2024). National Institute of Standards and Technology (NIST). Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[3] Chandramouli, R., and Pinhas, D. (October 2020) *Security Guidelines for Storage Infrastructure – NIST Special Publication 800-209*. National Institute of Standards and Technology (NIST). Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf