SOLUTION OVERVIEW

NetApp | TD SYNNEX Public Sector | DLT

FORTIFY YOUR DEFENSE WITH NIST-ALIGNED SOLUTIONS

CONTENTS

NetApp | TD SYNNEX Public Sector | DLT

CYBERCRIME NEVER STOPS

Cybercrime generates trillions of dollars in revenue each year, making it the world's third largest economy (just behind the United States and China). With the possibility of huge financial gain, it's no wonder cybercriminals aren't slowing down.

Around the globe, there is a cyberattack every 39 seconds, 2,200 attacks each day, 800,000 attacks each year—and those numbers are not expected to slow down anytime soon, especially as cybercriminals become more adept at using AI.

How can your organization avoid becoming another statistic?

The National Institute of Standards and Technology (NIST) has created a cybersecurity framework that enables any organization of any size in any industry to build a solid cybersecurity foundation. Combined with the right solutions, this framework helps organizations prepare to manage risks and protect their critical data.

A record-breaking year

2023 was a banner year for cybercrime:

72%↑

rise in data breaches between 2021 and 2023 (a new record)

Source:

25%↑

Year-over-year increase in the number of new vulnerabilities

Source:

115%↑

Year-over-year increase in supply chain attacks in the United States (highest since 2017)

Source:

$4.45M

average cost of a data breach (an all-time high)

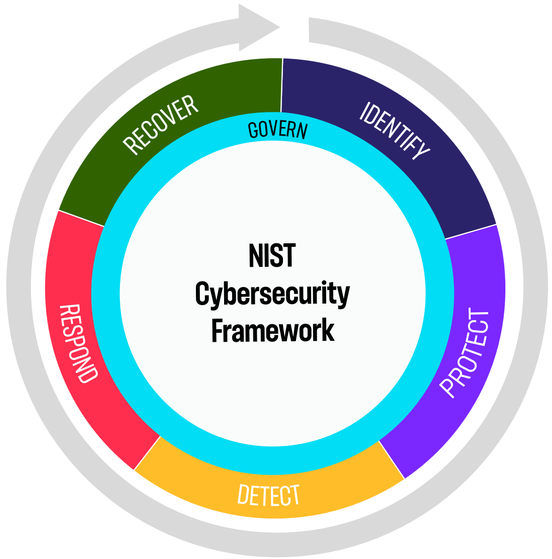
Source:

NetApp | TD SYNNEX Public Sector | DLT

SIX KEYS FOR FOR SUCCESS

The goal of a modern cybersecurity strategy is not to prevent intrusions—it is to protect your most valuable asset: your data. The NIST cybersecurity framework guidelines will help you build a strong, resilient solution that keeps all of your data safe.

The NIST framework is designed around six pillars, each of which includes its own standards, guidelines, and best practices for helping organizations effectively manage cybersecurity risk.



Is the NIST cybersecurity framework right for you?

No matter where you are on your cybersecurity journey, the NIST framework offers value. The framework is designed to complement existing business and cybersecurity operations. It can help you:

- Learn more about the uses
- Establish or improve a cybersecurity program
- Communicate cybersecurity requirements with stakeholders
- Identify opportunities for new or revised standards
- Prioritize improvement activities
- Enable investment decisions to address gaps
- Integrate compliance requirements into a cybersecurity program

Learn more about the uses and benefits of the NIST cybersecurity framework.

NetApp | TD SYNNEX Public Sector | DLT

GOVERN:
SET THE STAGE FOR SUCCESS

Success begins with establishing a cybersecurity risk management strategy, expectations, and policy. Understanding what you want to achieve will help you prioritize the outcomes of the other five framework elements.

The Govern piece of the framework establishes an overall strategy, and it also outlines roles and responsibilities and oversees the other functions to make sure that the established goals and expectations are met.

- NetApp® BlueXP™ unified management console. A single pane of glass for monitoring and administering your systems across on-premises and cloud environments.
- NetApp ONTAP® data management software. Built-in auditing and logging functions help make sure that your strategy stays on track and enable you to see gaps or vulnerabilities that may need to be addressed in other functions of the framework.
- NetApp Data Protection and Security Assessment. Assess your current data protection and security readiness and get an actionable, proactive plan to minimize risks.

IDENTIFY:
TAKE STOCK OF YOUR ENVIRONMENT

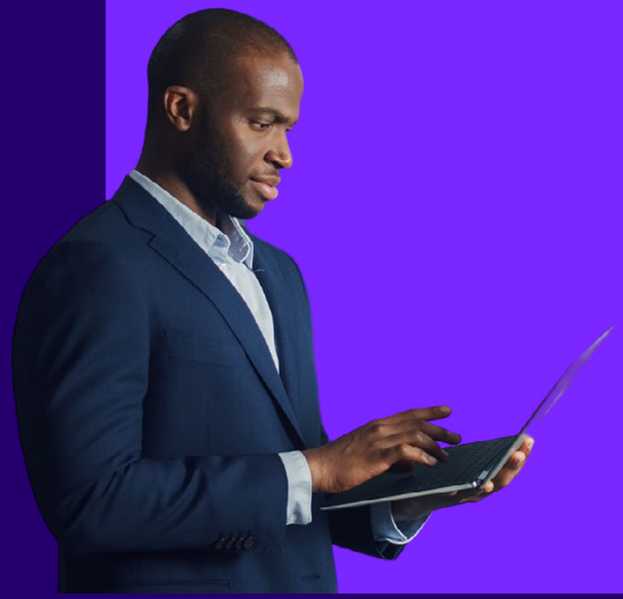
Do you know what types of data you have?
Where does that data reside in your environment?
Who has access to each type of data?

These are just a few of the questions that you'll need to answer before you can properly protect your data. From classifying and locating different types of data to evaluating permissions and assessing current data protections and security, this part of the framework can be very time consuming. But skipping over it can leave unidentified data vulnerable or put highly sensitive data at risk.

It's also important to have your data identified in case of a successful attack. If you don't know what you have, it's difficult to know what's missing after an attack. If an attack does occur, knowing the "what, where, and who" of your data allows you to quickly identify which data has been compromised. If it's an internal attack, it can also help you narrow down who the perpetrator is.

How NetApp can help

- BlueXP ransomware protection. Uses AIOps to intelligently coordinate and execute your workload defense.
- BlueXP classification. Automatically scans, analyzes, classifies, categorizes, and maps data across your cloud and on-premises storage environments. Automated reports give you a better understanding of the types of data your organization stores, where it resides, and whether it is at risk.
- NetApp Active IQ®. Continuously monitors your NetApp environment and alerts you if deviations from security best practices are detected. Lets you know what the issue is and provides guidance for how to fix it.



NetApp | TD SYNNEX Public Sector | DLT

PROTECT:
PUT YOUR DEFENSES IN PLACE

Now it's time to start building your walls—but that means more than just building a firewall around your perimeter.

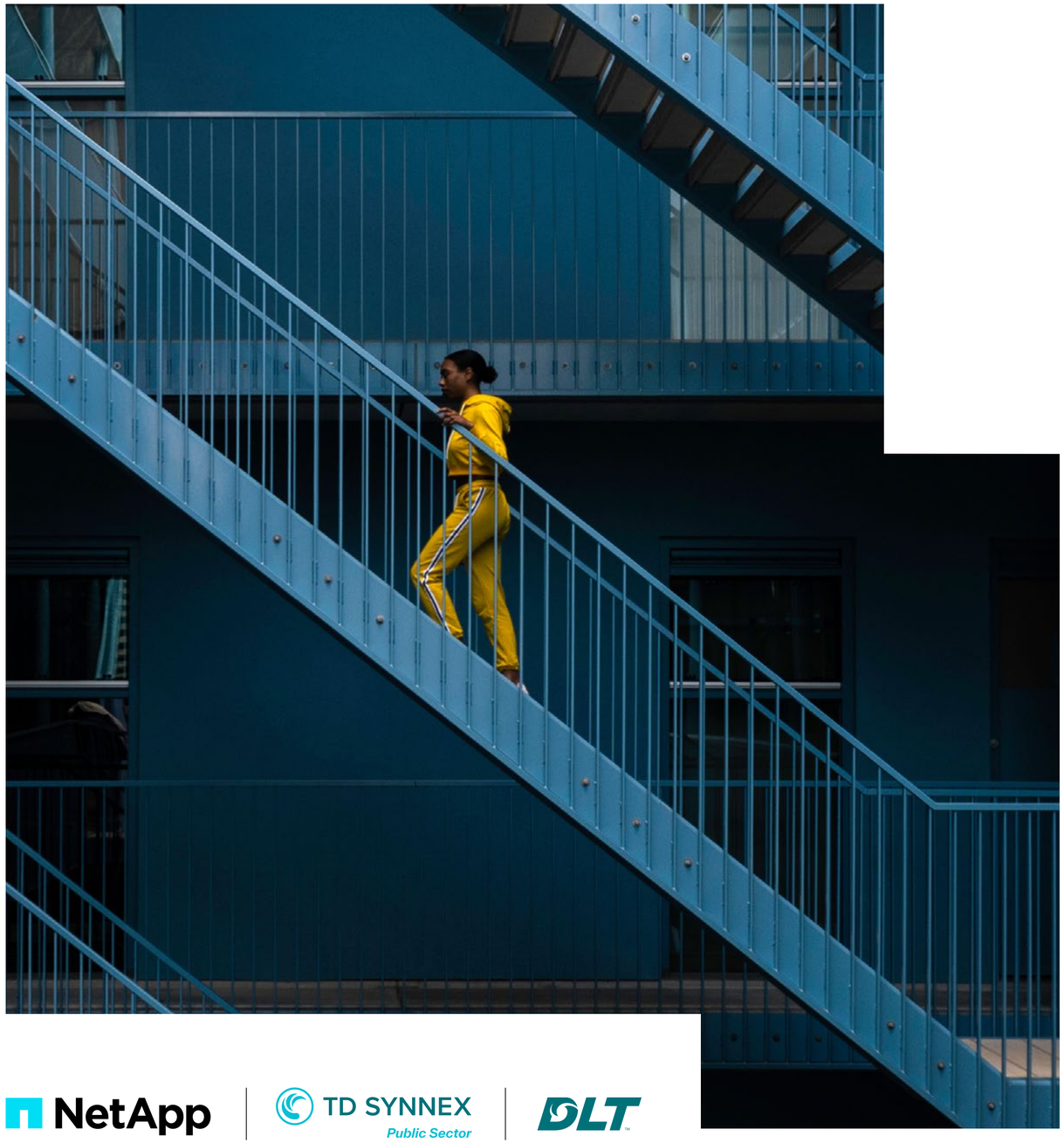
To have a fighting chance against modern cyberthreats, you need to encrypt your data, conduct regular backups, put access controls in place, update vulnerable operating systems and applications, and train your users in cybersecurity best practices.

You'll also need to be able to block malicious users, quarantine potentially bad data, prevent unauthorized data from being written to a disk, create granular, immutable copies of your data to prevent infection, and create indelible backups to prevent data deletion.

NetApp | TD SYNNEX Public Sector | DLT

How NetApp can help

- BlueXP ransomware protection. Actively monitors workload protection posture and enables you to apply protection policies with one click.
- BlueXP disaster recovery for VMware. Replicates vSphere apps and data to a VMware Cloud disaster recovery site using NetApp SnapMirror® replication software.
- BlueXP backup and recovery. Automatically backs up on-premises and cloud-based ONTAP data to object storage. Uses block-level incremental-forever technology to achieve backup windows that are 100x faster than standard backups, while preserving data efficiencies. Enables you to easily implement a 3-2-1 backup strategy.
- FPolicy. Monitors and blocks file operations based on the file's extension.
- SnapLock®. Makes your backup copies indelible, preventing deletion and renaming to protect your data and meet compliance regulations.
- Snapshot™ technology. Creates near-instant, incremental, immutable backup copies of your data
- Multi-admin verification. Helps make sure that certain operations such as deleting volumes or Snapshot copies are done only after approvals from multiple designated administrators.
- Multifactor authentication. Requires users to provide two authentication methods to log in.
- Encryption. Protects data at rest and in flight. NetApp uses both hardware and software encryption so that data at rest cannot be compromised.



DETECT:

STAY A STEP AHEAD OF ATTACKERS

Prevention is the best cure, but there's no guarantee that it will be 100% effective. To keep your data safe, you need to also have detection systems in place to identify suspicious activity before it becomes a threat.

Effective detection requires a thorough understanding of your regular data flows so that you can quickly spot unusual behavior. That means having a system in place for continually monitoring both user and data behavior.

One of the keys to detecting threats quickly is being able to cut through all the noise of false and low-priority alerts that security teams must filter through every day. With hundreds or even thousands of alerts coming in daily, security teams need to be able to pick out the high-priority ones so they can respond before serious damage is done.

- Cloud Insights user behavior analytics. Uses AI and machine learning to detect unusual user or file behavior. Automatically sends an alert to notify that there is unusual behavior.
- Autonomous Ransomware Protection. Uses machine learning to detect threats in real time. Automatically triggers an alert when suspicious files or activity are detected.
- Vscan. Scans for viruses when clients access files over SMB. Can scan on demand or on a schedule.

RESPOND:
KNOW WHAT TO DO IN A CRISIS

To make sure that your plan is viable, you need to continually test it. Testing means making sure that all team members know their roles and responsibilities, updating plans as threats evolve and lessons are learned, and sharing all updates with stakeholders.[7]

Having a plan in place is of paramount importance, the fact is that a truly effective response needs to be faster than the time it takes for any individual or team to manually execute a plan.

To prevent data loss, reputation damage, and financial repercussions of a successful attack, cybersecurity teams need to have automated tools that respond as soon as the detection system identifies suspicious activity.

How NetApp can help

- Autonomous Ransomware Protection. Provides automated response.
- Cloud Insights Storage Workload Security. Uses AI and machine learning to analyze data access patterns to identify risks from ransomware and insider attacks. Advanced reporting and auditing enable easy identification of possible threats.
- FPolicy. Blocks unwanted files and files with known ransomware extensions from being stored on your NetApp systems.

NetApp | TD SYNNEX Public Sector | DLT

RECOVER:
GET BACK TO NORMAL QUICKLY

If a cyberattack interrupts business operations, you need to be able to get back up and running quickly. It's imperative to be able to answer these questions:

- **What information will need to be shared?**
- Who will need access to this information?
- How will you make sure that these stakeholders get the information they need in a timely manner?
- How will you communicate the breach to the public, informing people whose information might have been compromised?
- What steps do you need to take to communicate with regulatory bodies?

In the Recover stage, you need to reduce downtime by restoring data quickly, bringing uncompromised applications back online, and applying intelligent forensics to identify the source of the threat.

How NetApp can help

- BlueXP ransomware protection. Rapidly restores workloads and their associated data through simplified, orchestrated, application-consistent recovery.
- BlueXP disaster recovery.
- BlueXP backup and recovery. Provides a single recovery console where you can view all of your backup copies and initiate a quick recovery.
- **SnapRestore® software.** Enables you to quickly restore an entire volume back to a specific Snapshot copy.
- Snapshot technology. Creates immutable copies of your data that can be used for recovery.

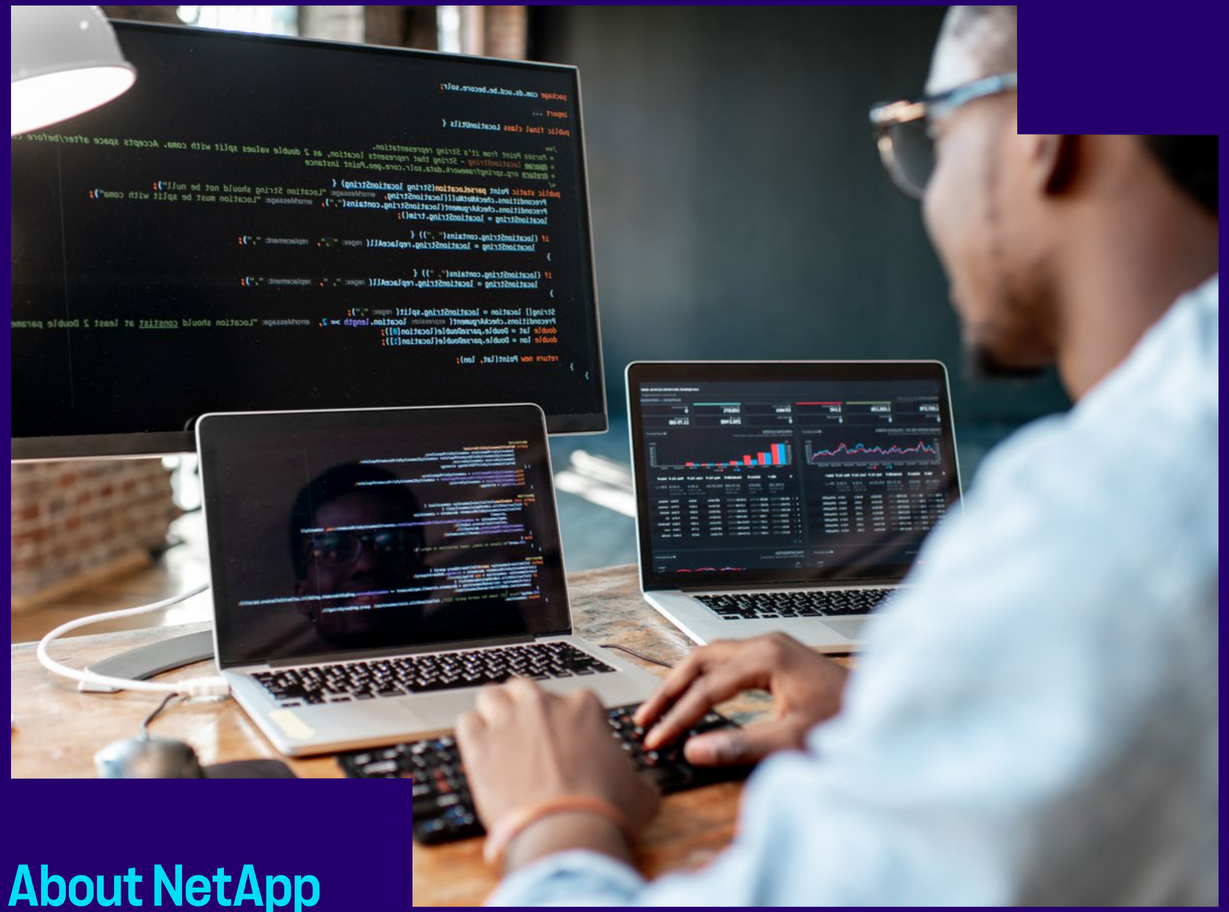
NetApp | TD SYNNEX Public Sector | DLT

START FORTIFYING YOUR DEFENSE TODAY

Aligning your cybersecurity strategy with the NIST cybersecurity framework enables you to build a stronger, more resilient solution. Wherever you are on your cybersecurity journey, NetApp has solutions and expertise to help you create a solution that adheres to NIST guidelines and helps you achieve your desired outcomes.

→ **NetApp cyber resilience solutions**

→ **NetApp ransomware protection**



About NetApp

NetApp is the intelligent data infrastructure company, combining unified data storage, integrated data services, and CloudOps solutions to turn a world of disruption into opportunity for every customer. NetApp creates silo-free infrastructure, harnessing observability and AI to enable the industry's best data management. As the only enterprise-grade storage service natively embedded in the world's biggest clouds, our data storage delivers seamless flexibility. In addition, our data services create a data advantage through superior cyber resilience, governance, and application agility. Our CloudOps solutions provide continuous optimization of performance and efficiency through observability and AI. No matter the data type, workload, or environment, with NetApp you can transform your data infrastructure to realize your business possibilities. www.netapp.com

Contact Us

NetApp | TD SYNNEX Public Sector | DLT