Data security done right

The ultimate guide to keeping your data safe from cyberthreats

n NetApp

Contents

NetApp

Ransomware—a looming threat to your data

Cybersecurity is top of mind for any organization, and for good reason. With ransomware attacks hitting 66% of organizations in 2021, it's likely a matter of when—not if—you'll be a target.

And let's face it. Cybercriminals are getting smarter by the day. Over the past year, 72% of organizations saw an increase in the volume, complexity, or impact of cyberattacks.

Bottom line: The traditional approach of protecting the perimeter is no longer good enough. And the need to upgrade is more urgent than ever.

11 seconds
Average frequency of ransomware attacks globally

$1.4 million
Average cost of a ransomware attack

1 month
Average time to recover from a ransomware attack

The building blocks of data security

Ransomware. Rogue administrators. Hackers. Cyberthreats come in all shapes and sizes. That's why building the best data security defense is critical for every organization. With the right processes, solutions, and strategy, you'll be able to keep your data secure across your hybrid or multicloud environment.

Data security is built on two foundational blocks: threat detection and threat remediation. Both work together to secure your data through every stage of an attack—from the initial hand-raise that something looks amiss to the post-event forensic analysis of your response.

Threat detection
Monitor data and user anomalies to identify threats in real time
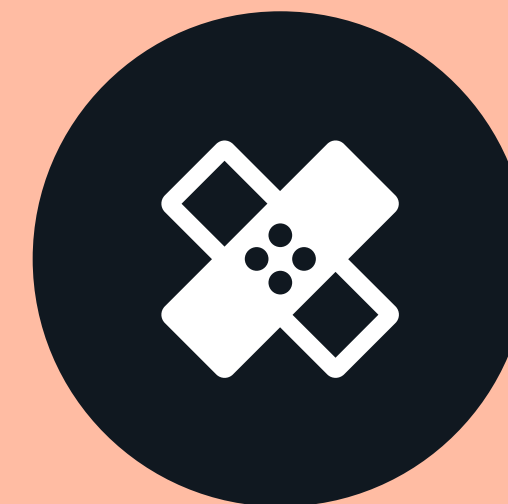
Threat remediation
Integrate layered defenses to rapidly respond to threats and quickly recover from an attack

Threat detection

An alarm that goes off after the criminals run away with your valuables isn't much help. That's why threat detection is critically important. Data security happens in real time, so you can catch threats as quickly as possible.

Threat detection focuses on monitoring and identifying threats as soon as possible—ideally before they ever touch your data. During the detection phase, your solutions need to:

1. Monitor data and users for anomalies

2. Trigger event notifications based on suspicious activity

3. Initiate threat remediation efforts

After you've confirmed that an attack is underway, it's time to mobilize the reinforcements and send that cyberthreat back where it belongs… locked outside your environment.

User access controls

Multifactor authentication

Anomaly monitoring

Zero Trust architecture

Threat remediation

Your IT has sounded the alarm—something's wrong. Now what? That's where threat remediation comes into play. Threat remediation involves responding appropriately to the threat and recovering from the attack, as quickly and cleanly as possible. During the remediation phase, your solutions need to:

1. Assess the state of the attack

2. Contain damages

3. Eliminate the threat

Even when the threat has been eliminated, threat remediation is not done. It's extremely important to conduct forensic analysis too, so that you can identify what went wrong and take the necessary steps to make sure you don't make the same mistakes twice.

Risk assessment

NetApp® Snapshot™ copies

Forensic analysis

∏ NetApp

Data security solutions you can count on

It all comes down to data. And with NetApp, data protection and data performance go hand in hand. We specialize in storing, managing, and protecting data on premises and in the cloud—so that no matter where your data lives, it's safe and secure.

Our solutions provide an integrated and unified approach to addressing everything from data loss to site outages; application or hardware failure; accidental deletion; and malware, ransomware, and virus attacks.

Basically, NetApp solutions can handle whatever threats come your way.

ONTAP

Protect your data no matter where it lives. NetApp ONTAP® has several built-in capabilities that can help detect anomalous behavior and prevent malicious or accidental changes to data, even from insider threats.

Cloud Insights

Proactively monitor your hybrid and multicloud infrastructure and keep your data a step ahead of ransomware. NetApp Cloud Insights delivers early alerts with actionable intelligence, so you can respond rapidly to threats.

Cloud Data Sense

Gain insight into what kind of sensitive data you have, where it's located, and who has access to it. NetApp Cloud Data Sense uses AI-driven technology to enable effective data governance across your entire data estate, whether on premises or in the cloud.

Cloud Backup

Seamlessly and cost-effectively back up your data, databases, and virtual machines to object storage. NetApp Cloud Backup slashes data protection costs on premises and in the cloud.

Keeping sensitive patient data safe

As one of the largest hospitals in Switzerland, Kantonsspital Winterthur (KSW) knows the importance of data security. KSW delivers primary clinical care as a consolidated central hospital, accessing 270,000 patient cases each year. This highly sensitive patient data has to be quickly available, without being vulnerable to cyberattacks.

With NetApp technology, KSW has built an infrastructure that blends performance with security:

- Converting a few large volumes to 20 smaller volumes so that restoring is faster and easier
- Hourly backups mirrored across sites and maintained for up to a year
- A 1-hour recovery point objective

Get the details

"When it comes to ransomware, you need a cool head, quick diagnoses, and reliable remedies. With the right decision, you can make IT healthy again quickly."
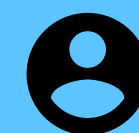
Michael Trutmann, Solution Architect and Consultant. ITpoint Systems

Safeguarding personal student data

Colleges and universities need to focus on serving student needs, not managing IT. But with sensitive information like personal student data to protect, a small college in South Florida needed solutions that didn't compromise data security during a migration.

NetApp and Veytec teamed up to support the migration, while saving big on TCO and boosting data security:

- Identifying set permissions in the original environment to correctly secure data across its new hybrid cloud location
- Deploying governance and compliance capabilities for immediate insight into all types of data
- Classifying data to create automated compliance reports for the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DDS), and privacy risk assessment

Get the details

"Cloud Data Sense provides detailed information about sensitive data and immediately tells what permissions are in place and whether sensitive information is exposed. These insights help users make informed decisions that minimize the risk of internal or external threats to the business."

Veytec, NetApp partner, Managed service provider to a small college in South Florida

Meeting critical security protocols

Protecting details of U.S. security is no small task—with no room for error. A U.S. government department upgrading IT needed solutions that would meet critical security protocols, while keeping data easily accessible.

The department turned to NetApp, building a "classified cloud" that meets those security protocols, reduces the storage footprint, and paves the way for future expansion:

- Accelerating data recovery from days to minutes
- Deploying multitenancy to carve storage into individual pieces accessible privately by users or networks as appropriate
- Embedding disaster recovery and continual-operations capabilities

Get the details

"When we started looking at this [multitenancy], the other vendors claimed they could do it. But, when push came to shove, they backed down. The only one that truly could do what we needed was NetApp."

Pat Connolly, Independent IT Contractor, U.S. Government

NetApp

Cyber resilience: Where data security meets data protection

Data security is vitally important for keeping your data safe, but it's not the whole story. To come out ahead of cybercriminals, organizations are increasingly looking at a wider picture: cyber resilience.

Cyber resilience combines data protection with data security—keeping your business running whether the threat comes from a perimeter breach or from the inside.

In protecting your business, the best defense is a good offense. Cyber resilience helps you put the right data security and data protection in place before an attack happens—so you're prepared and able to survive whatever cybercriminals throw your way.

Continue your data security journey

→ **NetApp cyber resilience solutions**

→ **NetApp data protection solutions**

→ **NetApp ransomware solutions**

→ **Cybersecurity on NetApp TV™**