SOLUTION BRIEF

NetApp

SECURE BY DESIGN: NETAPP CYBER RESILIENCE SOLUTIONS FOR HEALTHCARE AND LIFE SCIENCES

Data is the lifeblood of good patient care and pharmaceutical development. Protect against data loss and downtime with the most secure storage on the planet.

Putting data and lives at stake

Healthcare has the second-highest rate of ransomware attacks globally. And it's no wonder. At an average of $408 per patient record on the bootleg market, healthcare data is worth three times more than data in any other industry.

Because lives are at stake, healthcare organizations are more likely to pay ransom demands. If a hospital system goes down, so do life-saving treatments. If an insurance company goes down, patients don't get approval for necessary treatments and prescriptions can't be filled. For pharmaceutical companies, an attack can bring research and development to a halt, preventing new drugs and therapies from getting to market quickly. Unfortunately, when an organization pays a ransom it puts an even bigger target on their back and makes them more susceptible to future attacks.

Cyberattacks hit healthcare organizations hard

67%	Two-thirds of healthcare organizations experienced ransomware attacks in 2024.
$9.77M	The average cost of a healthcare cybersecurity breach is $9.77M.
10X	The downtime and recovery time cost to remediate an attack is 10X the average ransom payment.
40%	Forty percent of healthcare organizations took more than one month to recover after an attack.

Why cyber resilience?
With cyberattacks becoming more frequent and more sophisticated, it's no longer a matter of if but when your organization will be the target. When not only the business but also the lives of patients are at stake, healthcare and life sciences organizations need to take a more proactive approach to cybersecurity.

To protect lives and data, healthcare and life sciences organizations need to move beyond backup and perimeter-focused security to a cyber-resilience solution that protects their data from the inside out.

Cyber resilience takes cybersecurity to the next level with a comprehensive approach to fighting cybercrime. Cyber resilience combines protection capabilities to detect and prevent attacks with recovery capabilities to keep your business running if an intruder breaches your security perimeter or if there is malicious activity from the inside.

Trust NetApp to build your data defense
Because human error is the cause of 95% of cybersecurity breaches, the most impactful way to protect against ransomware and other cyberattacks is to instill proper cyberhygiene practices. Create an environment of suspicion. Teach your users how to identify click bait and phishing scams. Train them in what to do when they get multifactor authentication errors (fault MFA). Make sure that everyone knows how to create secure passwords and how to properly handle sensitive data. Make it easy to report any suspicious links, attachments, or activity to your IT security department. But even with the best cyberhygiene practices, human error will occur—and that's where NetApp comes to the rescue.

An intelligent data infrastructure from NetApp keeps your data safe with comprehensive, data-centric cyber-resilience capabilities that are built in, not bolted on. It automatically keeps your data available and recoverable while detecting and thwarting threats in real time across your entire hybrid multicloud data estate. By implementing robust security measures at the storage level, such as encryption, access controls, and immutable backups, you can create an additional line of defense against cyberattacks.

Set the stage for success
When done well, a cyber-resilience strategy can prevent the effects of a ransomware attack from ever materializing by reducing reliance on a set of point solutions that don't integrate with or support one another. Even if your perimeter is breached, a proper cyber-resilience solution will keep your data protected.

NetApp offers the tools and expertise that you need to create a successful cyber-resilience strategy. NetApp® Professional Services such as the Data Protection and Security Assessment and tools such as NetApp BlueXP™ classification can help you build a solid cyber-resilience strategy with good data governance.

KEY BENEFITS

Set the stage for success

- Establish a cybersecurity risk management strategy, expectations, and policy.
- Identify gaps in your security coverage.
- Understand your data, where it resides, and the level of protection it needs.

Enable proper protection of your data

- Rely on the most secure storage on the planet.
- Apply data defenses such as encryption, access control, and immutable and indelible backups.
- Use a NetApp cyber vault to protect your most sensitive data.

Detect and thwart potential attacks as they happen

- Stay a step ahead of attackers with AI-driven real-time detection that is 99% accurate.
- Continuously monitor for data and user anomalies.

Recover quickly, without data loss

- Get back to normal in no time, with little to no data loss.
- Keep your guard up by continually monitoring and adjusting your protection strategies to maintain your cyber resilience.

Automating the usually time-consuming tasks of classifying and locating different types of data, evaluating permissions, and assessing current data protections and security makes it easy to get started and helps make sure that you don't leave any 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 enables 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.

Enable proper protection of your data
NetApp offers the most secure storage on the planet—no other storage solution provides equivalent security protection. Our unified data storage supports multiple data formats. With data encryption at rest and in flight, your data is protected wherever it lives and wherever it moves to.

NetApp cyber vaulting, powered by SnapLock® compliance software, is a comprehensive and flexible solution for protecting your most critical data assets. Logical air-gapping with robust hardening methodologies for NetApp ONTAP® data management software enables you to create secure, isolated storage environments that are resilient against evolving cyberthreats and internal multiadmin attacks.

NetApp offers the only hardened enterprise storage that is validated to store top-secret data. In addition to being NIST FIPS 140 and CSfC certified, our solutions feature quantum-resistant encryption. Not are the hardware and ONTAP® software certified, but NetApp software also provides extended features to help secure your environment. These features include:

- Multifactor authentication (MFA)
- Multiadmin verification
- Role-based access control (RBAC)
- Creation of write once, read many (WORM) volumes
- Data classification
- Frequent immutable, indelible NetApp Snapshot™ copies
- Built-in anti-ransomware protection

Detect and thwart potential attacks as they happen
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. NetApp's real-time, AI-powered ransomware protection with 99% detection accuracy continuously monitors for suspicious activities and anomalies, swiftly identifying potential ransomware attacks as they unfold. When a threat is detected, the system can automatically isolate affected data and prevent further spread, minimizing potential damage.

NetApp Data Infrastructure Insights (formerly Cloud Insights) Storage Workload Security offers an additional layer of defense against insider threats. By meticulously tracking file activity for every authenticated user, it generates actionable intelligence that enables organizations to identify and mitigate potential internal security risks. This comprehensive approach combines proactive threat detection, rapid response mechanisms, and detailed user activity monitoring, offering a multifaceted shield against both external ransomware attacks and internal security vulnerabilities.

NETAPP CYBER RESILIENCE SOLUTIONS IN ACTION

SAFEGUARDING DATA-DRIVEN HOSPITAL OPERATIONS

Klinikum Freising is a municipal hospital in Germany that provides superior primary care for the district of Freising and its adjacent counties. The hospital uses ProLion CryptoSpike, developed for ONTAP storage and connected per NetApp's FPolicy interface. User access to files is monitored in real time. Any threats detected are eliminated immediately according to set policies. Users are notified by email about why the access was blocked and when the file is available again. In case of a file restore or recovery, NetApp Snapshot copies are there to help fix the problem.

Read the full story

SAVING DATA SAVES LIVES

UZ Leuven, a leading European healthcare provider, protects their data estate from the ongoing threat of ransomware through NetApp cyber-resilience solutions. NetApp Snapshot and SnapLock technologies are key to helping the hospital protect their sensitive data and prevent downtime from an attack.

Watch the video

NETAPP CORE CAPABILITIES FOR CYBER RESILIENCE

- **Built-in data protection.** Over 30 built-in security features, including multifactor authentication and multiadmin verification, role-based access controls, at-rest and in-flight encryption, and immutable, indelible backups, prevent attacks from reaching your data.
- **Real-time threat detection and response.** Detect risks with 99% accuracy. Respond instantly to detected risks by automatically blocking the suspicious user and preventing questionable files from being written to disk. If needed, a Snapshot copy for recovery is automatically triggered.
- **Fast backup and recovery.** Faster, more frequent backups and the ability to recover workloads within minutes—with application consistency and little to no data loss—help you to avoid the costly downtime associated with a cybersecurity breach.
- **Cyber vault file locking.** Immutable, indelible NetApp Snapshot copies are locked on the cyber vault, with strict access controls on a hardened configuration. If attackers do make it past your perimeter, they won't be able to alter your data in any way.
- **Ransomware Recovery Guarantee.** Only NetApp guarantees recovery of your protected Snapshot copies. No data loss, guaranteed. If we can't help you recover, we will compensate you.

Recover quickly, without data loss

For healthcare organizations, downtime is never an option. If an attack does happen, you need to detect it immediately and get back up and running as quickly as possible, not only for the health of your business, but for the health of patients as well.

NetApp cyber-resilience solutions enable you to recover your protected Snapshot copies in minutes. And only NetApp offers a Ransomware Recovery Guarantee. We are so confident in our ability to enable you to recover quickly that we will compensate you if we can't.

After an attack, NetApp helps you keep your guard up with automated, continuous monitoring. The BlueXP unified control panel gives you visibility across your entire data estate, enabling better data governance and providing insights for where you need to adjust your protection strategies to maintain your cyber resilience.

NetApp cyber-resilience solutions—your prescription for success

More than 2,000 healthcare and life sciences organizations trust NetApp to secure their mission-critical data. Only NetApp solutions are secure by design, with built-in cyber-resilience capabilities at the storage layer where your data lives. Our NIST-aligned data security solutions protect you from data loss and downtime by proactively detecting potential threats and quickly recovering data and applications. There is no better way to protect and secure data across your entire hybrid multicloud environment.

Learn more about NetApp cyber-resilience solutions.

Contact Us

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

NetApp