

E-BOOK

Fortify cyber resilience for your evolved cloud

Cyber-resilience solutions for the public sector



Contents

Introduction	03	→
Evolved cyber resilience	04	→
Double the security and compliance	05	→
The building blocks of data security	06	→
Protecting your data	07	→
Evolving for the future	08	→
Fortify your cyber resilience today	09	→



An evolved cloud strategy requires evolved cyber resilience

The cloud journey that we've been talking about for the past decade (or longer) is over. Every organization now has cloud in some way, shape, or form, thanks in part to the pandemic, which forced many organizations to embrace remote and hybrid work and simultaneously accelerated the shift to the cloud.

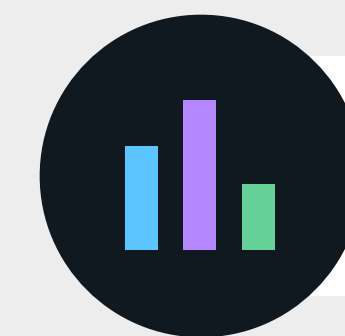
At the same time, on-premises IT still has an important role to play. In fact, for many government organizations and agencies, a hybrid cloud composed of on-premises and public cloud solutions is the way forward.

As a result, instead of focusing on getting to the cloud, organizations are now focused on evolving their hybrid cloud environments—making them simpler, more connected, and fully interoperable. With an evolved cloud, organizations can unleash the full benefits of the cloud. No chaos—just agility, flexibility, and freedom-fueled innovation.

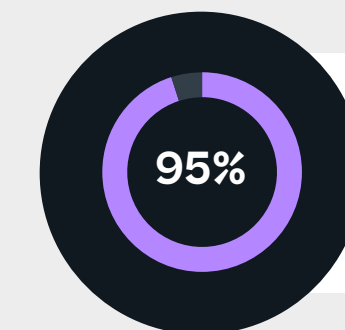
To be successful, an evolved cloud strategy requires evolved cyber resilience that builds a fortress of data protection and data security—from the inside out.



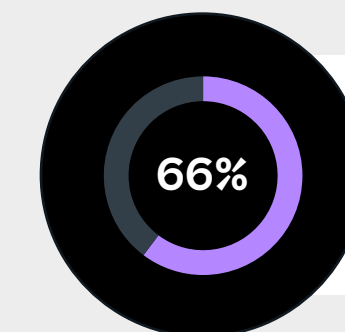
The cloud is here to stay



A **2020 study** found that cloud services are becoming an essential component for modern digital services delivery within the U.S. infrastructure industry.



Gartner predicts that by 2025 more than **95%** of new digital workloads will be deployed on cloud-native platforms, up from just 30% in 2021.



Gartner also predicts that by 2025 almost **66%** of spending on application software will be directed toward cloud technologies.

If you're still transitioning to the cloud, CISA updated its Cloud Security Technical Reference Architecture to help guide organizations in securely transitioning to and operating cloud services to comply with Executive Order 14028.



Fortified cyber resilience— why it matters

With data distributed across on-premises and cloud infrastructures, already overwhelmed IT teams are tasked with protecting hundreds or even thousands of endpoints against malware, ransomware, rogue administrators, and hackers. A cybersecurity strategy that aims to keep attackers out by securing the perimeter is no longer effective. To keep their data safe, organizations need to take their cybersecurity strategies and techniques to the next level: cyber resilience at the data layer.

Cyber resilience starts by protecting your data from the inside out. You can't rely solely on tools that are a step or two from the data. Backup software can look at your data after the copies are made but has little view into what's happening in real time. Perimeter security and network security can monitor unexpected traffic. But what if that traffic is from an admin account or an infected or compromised employee? To perimeter tools, that behavior might look normal.

The last line of defense, and the most critical defense, happens where the data resides: the storage layer. When combined with other layers of protection, storage-native protection presents a powerful approach to safeguard data against theft and encryption.



Cybercrime is big business



The number of publicly acknowledged data compromises in the United States increased **68%** in 2021 compared to 2020.



The average total cost of a data breach increased to **\$4.24 million** last year, the highest recorded in almost two decades.



If it were measured as a country, then cybercrime—which is predicted to inflict damages totaling **US\$10.5 trillion globally** in 2025—would be the world's third-largest economy after the United States and China.

Delivering double the security and compliance

If you're wondering when you should start putting a fortified cyber-resilience strategy into play, the answer is easy: Now.

In today's increasingly complex threat landscape, taking a unified approach to data security and data protection across your entire data estate will help you meet the highest levels of government cloud security and compliance standards now and in the future. The NetApp® portfolio of storage, data, and application services is built for the evolved cloud and delivers a unified hybrid multicloud experience with built-in data protection no matter what your environment looks like.

NetApp has relationships with all major cloud providers, but our relationship with AWS is unique. Our portfolio of solutions for AWS includes robust data management, intelligent data and user monitoring, and professional services to help keep your data secure across hybrid environments—from edge to core to cloud.

With Amazon FSx for NetApp ONTAP, you can take advantage of a managed service with cross-region replication for an extra layer of resilience against outages and natural disasters. FSx for ONTAP is compliant with FedRAMP and DoD IL4 and IL5, so you can reduce risk while tapping into the complete NetApp management portfolio in the AWS Marketplace—all from a single management interface.

NetApp makes it simple to back up, archive, or replicate data from your on-premises file servers to AWS and keep your data available and secure. We offer cloud-native file services that include built-in capabilities for protection, threat detection, and quick recovery.

Better together: NetApp and AWS

NetApp and AWS are trusted partners that you can count on to keep your most critical data secure.

Amazon FSx for NetApp ONTAP, which is available in both AWS commercial and GovCloud regions, has achieved the following authorizations:

- ✓ FedRAMP Moderate and High
- ✓ DoD SRG IL2, IL4, and IL5
- ✓ FIPS 140-2

The NetApp ONTAP® data management system has been evaluated against the following standards:

- ✓ Common Criteria/IOS 15408
- ✓ Department of Defense Information Network Approved Products List (DoDIN APL)
- ✓ Commercial Solutions for Classified (CSfC) program



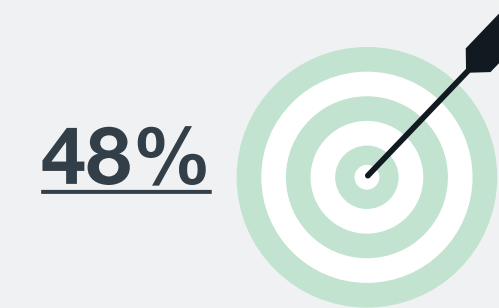
The building blocks of data security: Threat detection and threat remediation

No hybrid cloud environment is truly useful unless it's secure. With built-in threat detection and threat remediation capabilities, NetApp and AWS solutions enable agencies to defend their data against ransomware and malicious actors. The average ransom payment is nearly \$1 million and downtime costs can be up to 10x the ransom demand.

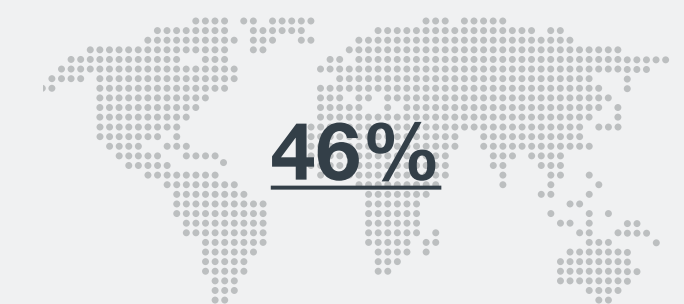
The sooner you can detect threats and suspicious behavior, the sooner you can stop an attack and prevent a long, costly recovery. NetApp solutions use AI and continuous monitoring to help detect anomalies—quickly and accurately—in user or file behavior. Built-in ML and analytics can catch malicious encryption in the act. The system can also detect when users are trying to delete large volumes of data. These features provide an additional layer of security within the AWS environment.

Threat remediation is the other side of the coin. If attackers get past your security layers, you need to be able to shut them down and get your organization back up and running as quickly as possible. The faster you can respond, the faster you can get back to business. With NetApp and AWS, unauthorized users are quickly identified and automatically blocked. An immutable snapshot of your data is automatically created, enabling you to restore to your “last-known good” state.

Threat detection and remediation are critical capabilities for government organizations and agencies



of nation-state attacks are aimed at government organizations.



of nation-state attacks target the United States (the most targeted country in the world).



Cyberattacks are more likely than missiles to bring down F-35 jets.



Cyberattacks take a big bite out of budgets, costing the U.S. government \$13.7 billion in 2018 alone.

Protecting your data: Data availability, backup, and recovery

The cost of ransom pales in comparison to the value of your data. The main goal of any cyber resilience strategy is to prevent data loss. Data loss comes in many forms—such as data leaks, data exfiltration, or data deletion—that can seriously disrupt critical government operations with the potential to compromise national security and put lives at risk.

Even after paying the ransom, organizations still lose an average of 39% of their data. A better approach to preventing data loss is to have a solid data protection plan that includes backup and recovery. If ransomware strikes, you can skip the payment, recover your backup copies, and get back to business-as-usual quickly.

NetApp has simple tools that government agencies can use to back up, archive, and replicate data from on-premises NetApp storage to AWS (or from AWS back to your on-premises storage). Data is protected with immutable NetApp Snapshot™ copies and automated, efficient, highly durable backups of every volume in your file system—enabling you to improve your cyber resilience and meet backup and recovery compliance requirements. You can quickly restore everything from complete volumes to individual files and folders when needed.

Data backup is your best protection against data loss



Only **4%**

of organizations that pay a ransom
get all of their data back.



Cyberinsurance has a **98%** payout rate on ransomware claims, but it can't prevent data loss.

81%

of cyberattacks against government entities threaten data exfiltration.







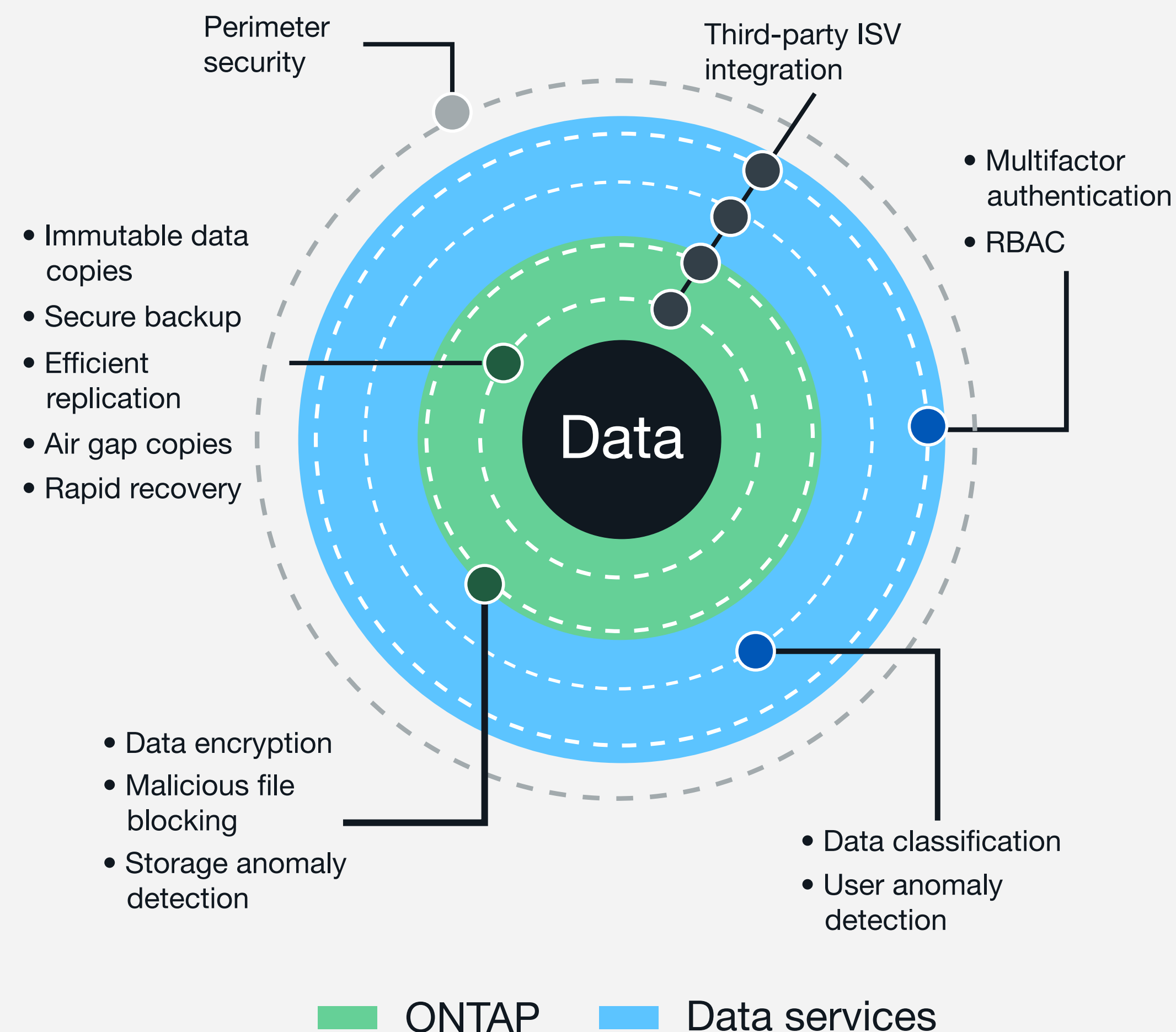
Evolving for the future: Zero Trust and cyber resilience at the edge

With cyberthreats becoming more frequent and sophisticated, evolving your cyber-resilience strategy means thinking differently about how you protect your data. To improve cyber resilience, many organizations are setting up a cybersecurity mesh with Zero Trust security as the core principle. A cybersecurity mesh takes security outside the fortress walls and builds layered security around individual devices for added defense.

NetApp brings Zero Trust to the evolved cloud with multifactor authentication and unified control of data protection and security across your edge, core, and cloud environments using NetApp BlueXP. Unlike perimeter tools, which assume that insiders are trusted, NetApp assumes Zero Trust for everyone, monitoring activity from insiders, outsiders, ransomware attacks, and rogue and compromised users across your IT landscape—from a single interface.

Trust nothing, verify everything

-  **60%** of data breaches involve the use of stolen credentials to slide past security barriers.
-  Attackers are **more likely to use stolen credentials than malware**.
-  Zero Trust can reduce the cost of a data breach by about **\$1.76 million**.
-  Organizations that use Zero Trust data segmentation are **2 times** more likely to avoid critical outages due to cyberattacks.



Fortify your cyber resilience today

Your cyber-resilience plan is just a few clicks away. Learn how NetApp on AWS can help put your data-centric cyber-resilience plan into action.

- ➔ **NetApp cyber resilience for AWS**
- ➔ **NetApp ransomware protection**
- ➔ **Building an effective cyber-resilience strategy**
- ➔ **Why you should include NetApp in your cyber-resilience conversations**

Reach out to your NetApp partner or sales representative to talk about how to boost cyber resilience in your hybrid cloud environment.



About NetApp

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services, and applications to the right people—anytime, anywhere.



+1 877 263 8277

© 2023 NetApp, Inc. All Rights Reserved. NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners. NA-994-0123