NETAPP ON NETAPP EBOOK

How NetApp IT Secures our Hybrid Cloud Environment

NetApp

NETAPP ON NETAPP EBOOK

Content

Authors

How ONTAP actively protects NetApp IT

By Seth Cutler
Chief Information Security Officer

Security is top of mind for any IT professional and I'm no different. Media reports of successful attacks or data breaches are becoming more frequent and new threats are arising far too regularly. NetApp is a large company with a massive amount of data, all of which must be protected.

Our security strategy starts with ONTAP. Traditional approaches to data security aren't enough to blunt threats that are ever-evolving and increasingly sophisticated. ONTAP helps us by expanding the security perimeter around our data and strengthening our posture throughout our IT ecosystem.

So, what keeps CIOs and CISOs up at night?

Most CIOs have similar security concerns. Ransomware attacks that cripple operations, data breaches that expose sensitive data, or security tools that are not well integrated frequently come up. There's not a single application that can fix everything. It takes a well-rounded approach to provide real, comprehensive protection.

How ONTAP keeps NetApp IT secure

ONTAP is our solution for many needs, security among the top. It enhances data confidentiality,

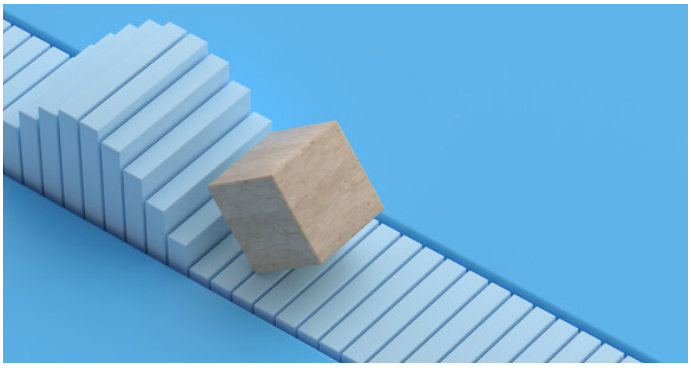
integrity, and availability, ensuring that distributed and diverse data remains protected. Security is integrated into ONTAP, meaning we have built-in protection against:

- Compromised administrator credentials through multi-factor authentication (MFA)
- Stolen data through at-rest encryption
- Ransomware attacks through immutable snapshots
- Rogue administrators through audit logging
- Lateral network attacks through secure multi-tenancy
- Disaster outages through data replication
- Guaranteed data retention through WORM storage

The platform provides world-class capabilities across four key solutions:

Encryption

Our first goal is to guard data, no matter where it is. ONTAP gives us end-to-end encryption, at rest and in transit, to provide a strong security posture throughout our hybrid cloud. Data at rest and full disk encryption are enabled by default and further enhance the security of our data fabric.



Compliance

ONTAP is built to meet standard requirements like GDPR and privacy standards by default. Additional auditing and monitoring provides an extra level of visibility.

Security

Our security standards start with MFA to guard against poor passwords. Role-based access control validates authorized users and storage-level security keeps unauthorized users from accessing or altering critical data.

Zero Trust

We are staunch believers in extending the security perimeter through Zero Trust standards – we verify and never trust. ONTAP enables NetApp IT to easily implement a Zero Trust environment and the FPolicy Zero Trust engine constantly monitors and manages file access for additional security.

Why we believe in ONTAP for security

ONTAP allows us to be proactive and stop security threats outside our walls instead of reacting to attacks after they've impacted systems. It includes over 30 data security features that keeps information safe and stops bad actors before they even get started.

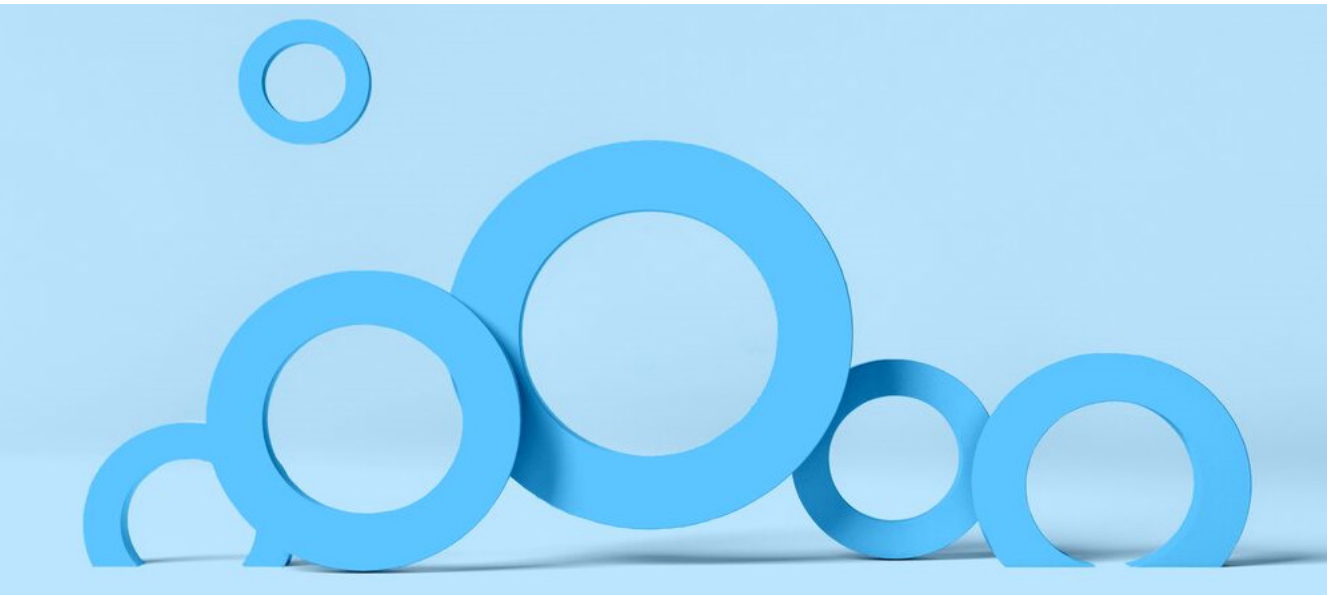
Lessons Learned

We were fortunate to have an SAP expert on the team who knew how to take full advantage of the SAP feature sets and UI microservices architectures. His expertise and knowledge had a significant impact on our success and ability to make improvements.

We learned to spend extra time on the UI when building an app with very specific designs. Although our DevOps framework made it easy to change the UI, a good first pass was important for technical engineers who love information-intensive screens.

It was challenging to rewrite a system for a user base that is technically savvy, highly opinionated, and enamored by details.

Although we found the TSEs reticent to give accolades, they did express appreciation of the single data-entry screen, embedded knowledge articles, predefined templates and pulldown menus, and the training videos and instructions on the new system. address requirements, because we were dealing with massive amounts of data that came from the former spreadsheet dashboards. This approach was especially important in building a system.



Security in NetApp IT's Hybrid Multi-Cloud

By Mike Morris
Senior Director, Platform, Cloud, and

CloudOne is NetApp IT's internal hybrid multi-cloud platform that serves as the home for all cloud services used by developers. It uses public and private clouds and is where application development and operations reside.

When building CloudOne, we placed security high on the list of requirements and that's why it's built directly into the platform. Legacy IT environments traditionally rely on a hard and complex network perimeter. They often suffer from collections of poorly designed applications, poor administrative control, unpatched servers and network port ambiguity. This leads to firewalls that are unnecessarily complex, rigid, and are very difficult to automate or even work with.

However, for CloudOne, we wanted to implement security by default. We simplified perimeter security and built security into the applications themselves. This allows for greater automation to be integrated into workflows.

To achieve security by default, we adopted five specific principles:

- **A Zero Trust model** – We assume that nowhere inside the firewall is safe. Every piece of the

environment must be secure.

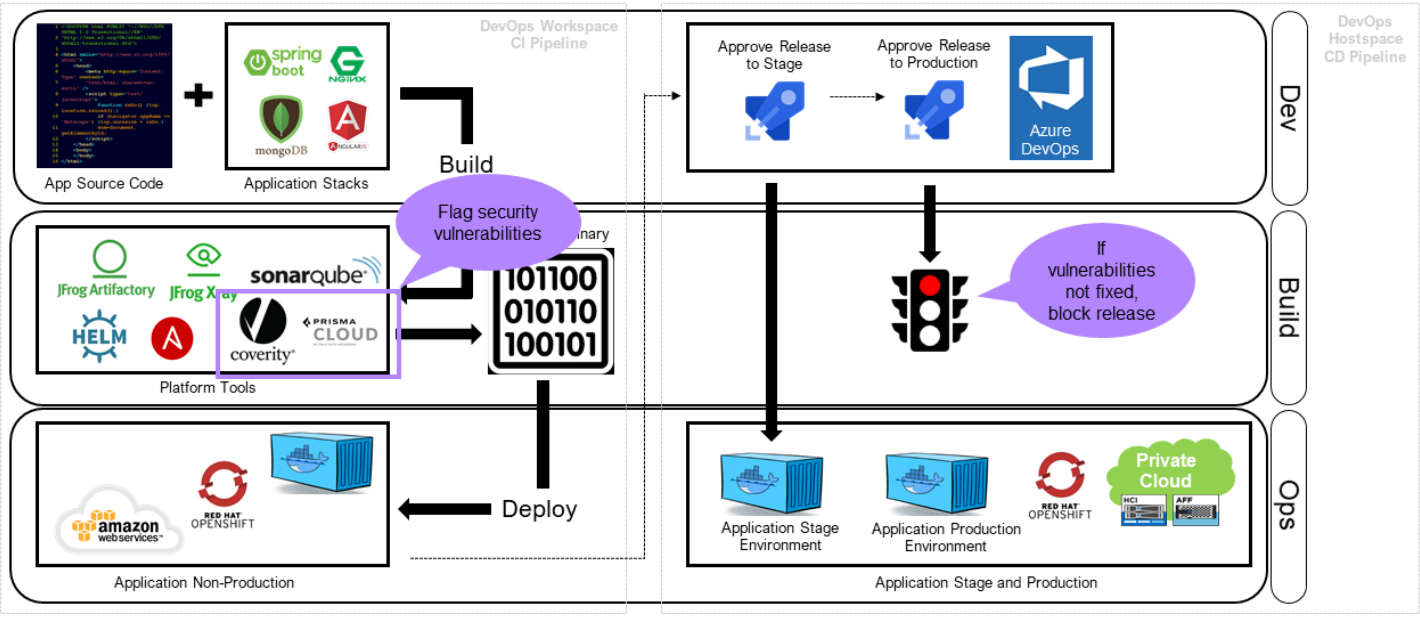
- **Applications are secure by design** – Because security is integrated into the platform, applications are more secure by default.
- **Green bucket list for common network traffic** – Custom traffic ports are not allowed. Applications are developed to use the green bucket list of network traffic ports.
- **Shift left** – Security tools are built into platform automation, including vulnerability detection and management in CI/CD pipelines.
- **Use existing cybersecurity processes** – Processes used by NetApp enterprise, including vulnerability management, incident response, and risk management are used in this hybrid cloud environment as well

We're building security into the CI/CD pipeline to make applications - and the process for building them - secure by default.

By prioritizing security when CloudOne was built, we've built a foundation that produces secure applications. We no longer depend on perimeter security only, but believe in an environment in which security is part of the entire platform.

CloudOne Architecture (DevSecOps)

Security Tools Integrated into CI/CD Pipeline



Building the NetApp IT Storage Security Program

By Faisal Salam
Senior Storage Engineer

Data hacks and ransomware are making security and resilience an ever-higher priority for IT professionals. Scrolling through any IT-focused timeline clearly shows how much importance is being placed on thwarting "the bad guys."

That's part of why NetApp IT has launched our storage security program. The program focuses on the security of NetApp ONTAP storage, the resilience of data if something bad happens, and actively monitoring for threats and breaches. It's proactive and stops threats before they become a reality.

We've already made several improvements, but the storage security program is designed to be iterative. Work will really never stop, as we research and implement new technology and tools for continuous improvement.

Our identified risks

We've identified 14 primary risks covering seven tracks that we are focused on.

Access Management

- Domain authentication configuration
- Audit log management
- Account management
- Authentication
- Suspicious client identification

Data Protection

- NetApp SnapVault standards
- SnapVault relationship for production volumes

Automation

- Management of user accounts

Security Monitoring

- Enhance and Improve auditing and logging for increased forensics

Security and Compliance

- Detection of infected files
- Syslog management
- Periodic scanning to discover risks

Storage Data Encryption

- Protection of data from physical theft

Security Alerts and Review

- Share security initiatives and technology

This is our roadmap of what's important today and what we will focus on tomorrow. We're finding ways to use Ansible to automate where we can, and we're also monitoring to ensure that our configurations are still effective. Security standards are ever evolving, and we must change with them.

Our execution so far

We began the storage security program in FY 2020 and have continued adding steps to our roadmap. We've completed several parts, including some important improvements that have a significant impact on our security readiness.

ONTAP at-rest encryption

We're using a three-phase deployment to encrypt all at-rest data:

- Encrypt all plaintext volumes using a volume-level key
- Enable encryption on aggregates
- Re-encrypt volumes using an aggregate-level key

Clean up ONTAP admin accounts

A full audit was completed and unneeded accounts were removed. Additionally, unmanaged accounts were added to our CyberArk password management integration and maintenance was automated to ensure governance compliance.

CIFS/SMB auditing

We're actively auditing all operations done to a file, including saving, deleting, or modifying. Audit logs are forwarded to a third party for storage, so if there is an event that must be investigated, we have access to historical data. We are able to see what was done to files, how frequently they were accessed, when they were accessed, and by whom.

CIFS/SMB auditing is included in ONTAP, but it must be turned on and integrated into our larger system.

Immutable data recovery infrastructure

To avoid being trapped by ransomware attacks, we're securely backing up our data using a solution that includes the SnapVault ONTAP feature and SnapLock compliance software. This solution creates secure Snapshot copies of critical data and makes it impossible to alter data after the solution is executed. Our production data is covered by this solution and can be recovered if something happens.

Future enhancements

We're about two-thirds of the way through our initial roadmap, with several additional improvements planned for FY 2022. Security hardening should always be a perpetual effort.

NetApp IT's Ansible Integration with CyberArk

By Victor Ifediora
Sr. Storage Engineer

Increasingly, security has moved from the perimeter to a Zero Trust model. Assuming that every user is a potential threat and having them continuously verify themselves to get access is the new standard.

NetApp IT uses a CyberArk integration with Ansible to apply Zero Trust to our use of playbooks. We use Ansible for a whole host of automation needs, including storage deployment and volume provisioning.

What we needed was a way to protect passwords that authenticate devices that Ansible playbooks were running against. Our password storage evolved to using a password-protected password file. When we started using Ansible Tower, we protected passwords with the Ansible Tower database, until we looked into CyberArk.

CyberArk enables us to safely store passwords in a central location. It's easy to rotate passwords, adding an additional layer of security. They currently rotate on a weekly basis, but that may be expanded to daily. All passwords meet our governance standards and the reporting suite enables us to easily track what accounts are accessing systems.

Meet the NetApp IT experts

Seth Cutler joined NetApp in June 2020 as Vice President and Chief Information Security Officer (CISO). Seth is responsible for establishing and maintaining our worldwide information protection and enterprise security programs. These include security operations, incident response, vulnerability and threat management, identity management, network security, disaster recovery, risk, policies, governance, and compliance.

As the Senior Director for Platform, Cloud and Infrastructure, Mike Morris leads NetApp IT's hybrid cloud and DevOps platform strategy—orchestrated and managed by an automation ecosystem—to create a holistic environment for cloud-aware enterprise applications. Mike leads the automation, infrastructure, cloud, and service management teams for NetApp which culminate to create NetApp IT's DevOps platform, "CloudOne".

Faisal Salam is a Senior Storage Engineer in NetApp's corporate IT team and is a member of the NetApp Customer-1 team, which acts as the first adopter of NetApp solutions and services. Faisal supports software-defined storage solutions for enterprise data management including Cloud Volumes ONTAP, and has more than 10 years of experience.

Victor Ifediora, Senior IT Storage Engineer at NetApp, is a member of the NetApp Customer-1 team. Victor is the Ansible Storage Automation lead and is responsible for ONTAP provisioning and configuration management via Ansible.

For more information on the NetApp on NetApp program and how NetApp IT uses our own products, check out NetAppIT.com.

NetApp