The ONTAP Advantage

Real-World Use Cases from NetApp IT

NetApp on NetApp Blog Compendium Series
Volume 1: Cyber Resilience

Table of Contents

Prologue

Unifying to Simplify: The Foundation of Cyber Resilience

Modern IT environments are more complex and fragmented than ever, with data sprawled across hybrid and multi-cloud infrastructures. But complexity shouldn't mean chaos.

In the opening blog of this compendium, Dave Blodgett, VP of IT at NetApp, shares a guiding principle for today's IT leaders: unification leads to simplification, and simplification is the bedrock of resilience. By consolidating storage management with NetApp ONTAP, organizations can gain a universal control plane that spans clouds and data centers, enabling greater visibility, control, and security. This unified strategy streamlines operations and strengthens the entire resilience posture, especially against emerging threats like ransomware.

As we explore Cyber Resilience in this first volume, Blodgett's message sets the tone: true resilience starts with simplifying what you manage and unifying how you manage it.

The Power of ONTAP

Simplifying IT through Unified Storage

Managing enterprise infrastructure at scale is a balancing act between requirements, rationalization, broad-spectrum resilience, and architectural simplicity – all essential for enabling efficient operations at scale.

Since joining the company a few years ago, I've focused on estate management and single-pane-of-glass management patterns. These systems provide:

- Centralized management
- Change execution
- Status visibility
- Instrumentation

In my view, this is the only way to manage large estates efficiently, securely, and auditably – the latter being paramount in a heavily regulated environment.

As you might imagine, one of the focus areas has been storage. In addition to lots of data (> 100PB), our infrastructure footprint is heterogeneous, spanning multiple on-prem data centers and multiple hyperscalers (e.g., AWS, Azure, GCP). Layer in storage types (block, file, object), transfer protocols (S3, FCP, NFS, iSCSI, CIFS, etc.), storage platforms (SAN, NAS, Unified, S3/-Compatible, EBS, etc.), wide-ranging performance requirements, complex data residency requirements, resilience considerations (local HA + backup vs multiple AZ vs multiple regions), etc., and you've got a good old-fashioned hairball.

My (exceptional) team and I have converged on unifying technology choices to maximize efficiency, security, and scalability. A universal approach to storage management has proven essential in reducing complexity while ensuring compliance, enabling resilience, and meeting the needs of a high-velocity business.

The Case for a Unified Storage Strategy

I have an admission to make: a few years ago – before joining NetApp – I had a similar understanding of the NetApp portfolio to that of many of my peers in the industry. It's a great company with excellent file storage, and for decades, I've been a customer of NetApp in that context. Since joining the company and experiencing the capability range of ONTAP firsthand, it's reshaped my perspective entirely. It's not just about storage – it's about unification. The ONTAP Operating System provides a common foundation for data resilience and security, something many of my peers may not realize until they see it in action or read a random blog.

While it's too late for a TL;DR, here's a punch line I whipped up before I expound a bit (pardon the amateur-hour attempt at marketing language):

ONTAP reduces complexity, simplifies management, improves security, and enables centralized control and visibility of your global storage portfolio—both on-prem and cloud-based – by providing a universal storage control plane. It allows seamless data management across hybrid and multi-cloud environments, reducing administrative overhead and simplifying operations.

Like many others, I struggled with fragmented storage environments for years – separate solutions for block, file, and object storage, often spread across on-premises and multiple cloud providers. This fragmentation creates inefficiencies, increases costs, and makes security more difficult to manage (and let's not forget my friends in audit).

With ONTAP, IT organizations gain:

- A single, scalable platform for managing all storage types across all platforms
- Seamless integration with major cloud providers
- Consistent data protection across environments – and this one is 'yuge' – more in a minute

Simplicity Over Complexity in IT

Enterprise infrastructure is inherently complex. The goal isn't to eliminate that complexity—it's to make managing it easier. A scalable infra-portfolio management strategy has to focus on unification over more decentralized patterns, leveraging solutions that consolidate management, enhance visibility, and automate operations.

Decentralized management, distributed patterns, and avoidable complexity just don’t work efficiently at scale, and those things are the breeding ground of unseen risk.

With ONTAP, engineers / managers have visibility and management of storage workloads in AWS, GCP, Azure, and a range of on-premises systems in a single management console. This isn’t just a convenience – it’s a necessity. SPOG management provides the ability to:

- Monitor and manage data movement across platforms, enabling seamless data portability
- Enhance security and compliance with multiple built-in protections
- Simplify disaster recovery and ransomware resilience

Ransomware Resilience: A Business Imperative

Ransomware attacks are no longer a matter of if but when. But as we all read about (and some of us lose sleep over), many organizations only realize their vulnerabilities during audits or worse – when something terrible happens. Even security-conscious businesses often have gaps in their ransomware defense strategies due to the endless permutations of storage types, infrastructure class, location, etc.

NetApp’s ransomware protection allows organizations to mitigate these risks across storage types (various on prem and cloud-based storage), and with single pane of glass simplicity, offering:

- Autonomous Ransomware Protection (AI-based technology)
- Tamperproof snapshots for rapid recovery
- Multi-admin verification (MAV) to prevent unauthorized

changes (work like the two launch keys)
- Data Infrastructure Insights Storage Workload Security

Each technology performs a different, complementary role in mitigating ransomware risk. They can be applied to on-premises and cloud workloads.

If I can offer advice, go deep on immutability in your storage portfolio. I can't tell you how many times I've heard of, in various contexts, scenarios where people believed they had immutable backups only to learn that they weren't truly immutable.

Defense in depth of your data isn't just about compliance – it is existential.

Key Takeaways for IT Leaders

Unification and centralized management are the paths to simplicity: Consolidating storage management of your on-premise and cloud-based workloads under ONTAP reduces complexity, enhances operational efficiency, and enables broad security coverage – all in a single pane of glass.

A universal storage control plane streamlines multi-cloud management and security.

Ransomware resilience must be proactive: IT leaders need to advocate for comprehensive security strategies before threats materialize.

Automation is the future: IT skill sets are shifting toward IaC, making technology rationalization more critical than ever.

IT environments are only growing more complex. The key to navigating this reality isn't adding more tools – it's choosing the right ones. A unified storage strategy that enables simplification and resilience ensures that IT teams can confidently scale, secure, and automate their operations.

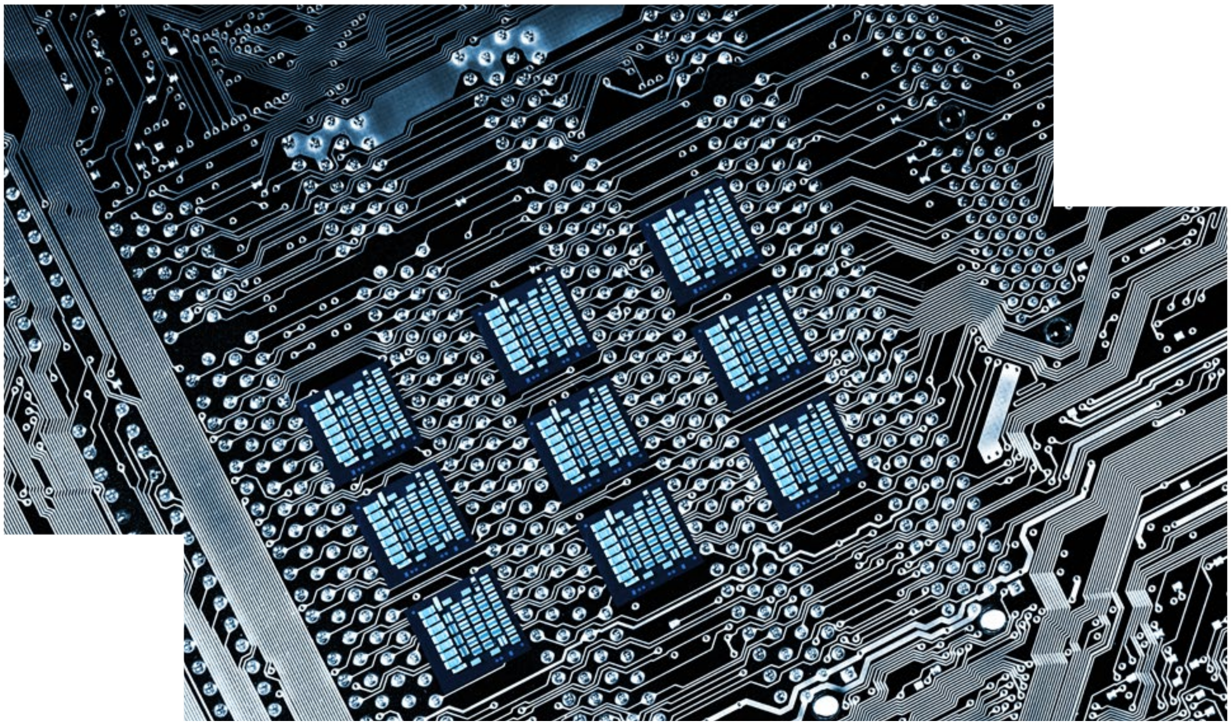
By embracing simplicity and unification, IT leaders can transform their infrastructure, making it more resilient, efficient, nimble, and future-ready.

About the Author

Dave Blodgett

VP IT, Cloud Infrastructure Operations

Dave Blodgett is NetApp IT's VP of Cloud Infrastructure Operations. He began his career as an engineer, in roles ranging from systems & network engineering, security systems, and enterprise architecture, before transitioning into management. At NetApp, he focuses on technology and management modernization methods, migrating from legacy to cloud environments, the shift from manual administration to infrastructure as code, along with creating high-velocity developer platforms while enabling security and governance.



Shielding Against Ransomware

Role of NetApp ONTAP + Data Infrastructure Insights

Now more than ever, sophisticated ransomware attacks pose a significant danger to businesses. The threat only continues to escalate in this ever-evolving digital landscape, which is why NetApp IT has implemented automated and advanced solutions, leveraging capabilities within ONTAP and Data Infrastructure Insights (formerly Cloud Insights) to help protect against ransomware attacks and the inevitable calamity that follows.

These solutions offer multiple layers of defense and coverage for our storage environment, safeguarding every critical point from perimeter security to storage. This ensures protection against threats like compromised storage administrator accounts and malicious users, while also incorporating technologies that mitigate damage in the event of an attack.

The Risk and Impact of Ransomware

Nearly 75 percent of organizations have experienced an attempt or successful ransomware attack in the last 12 months. Yet only half of that percentage has admitted to having a well-defined and thoroughly tested ransomware attack response strategy. With the advancement of artificial intelligence and related technologies, criminals can quickly launch attacks now better than ever. Extending far beyond the purview of any IT department, this issue has quickly become a board-level problem for all large enterprises.

NetApp Ransomware Solutions

NetApp's storage engineering team has identified crucial enterprise needs to improve recovery strategies and help prevent attacks. NetApp IT has delivered thorough solutions that meet these necessities - offering ransomware solutions like Snapshot, SnapVault, and SnapLock, in addition to other protective measures featured in ONTAP.

NetApp Snapshot

NetApp Snapshot offers remediation and restoration services, defeating ransomware head-on with Snapshot copies. This solution provides protection by preventing data deletion, allowing only those with administrative access to delete vital Snapshot copies.

NetApp IT uses Snapshots on most data volumes across every landscape. Each volume has a read-only Snapshot copy that is retrievable in the event of a data breach, helping to rapidly recover data from attacks and restore the base volume to a specific point in time.

NetApp SnapVault

While Snapshot offers remediation and restoration, SnapVault provides data protection and disaster recovery. These are immutable and long-term backups, available on-site and off-site, to a separate cluster. While Snapshot focuses on primary storage, SnapVault allows businesses to have backups on a remote cluster.

NetApp IT uses SnapVault to safeguard production volumes, providing yet another level of protection from harmful threats. Based on Snapshot copies, SnapVault offers storage efficiency that is preserved over the wire and is leveraged with SnapMirror to sub-prod secondary data centers for offsite data recovery.

NetApp SnapLock

To ensure secure protection against ransomware, SnapLock compliance prevents the deletion of vital Snapshots. For optimal ransomware protection, both SnapLock and NetApp's SnapVault help lock backups and provide immutable and indelible Snapshot copies for NAS and SAN volumes.

SnapLock compliance ensures that Snapshots cannot be tampered with or deleted, offering additional security options to add a recovery cluster at the primary or secondary data center. These volumes are virtually "air-gapped," which provides optimal detection and prevention services for data. This level of protection is why NetApp IT uses SnapVault with SnapLock compliance for several Tier One applications, specifically any data protected under Sarbanes-Oxley regulations for maximum security.

NetApp on NetApp

December Partner Webinar

Strengthening Ransomware Defense: NetApp IT's Advanced Security Measures

Presented by:
Senior Storage Engineer at NetApp
Ram Kodialbail

Other Ransomware Protection Capabilities

In addition to NetApp's primary ransomware solutions, other protection capabilities are available within ONTAP. These include Tamperproof Snapshots, Multi-Admin Verification, and Autonomous Ransomware Protection (ARP). Each of these technologies provides a layer of security that monitors and protects the system from potential threats.

Tamperproof Snapshots

- Near SnapLock Compliance-level protection for Snapshot copies.
- Building on the level of protection offered with Snapshot, they assign volumes an expiration time to prevent deletion or modification for a specified active retention period.
- NetApp IT utilizes Tamperproof Snapshots for all volumes, excluding volume managed by Trident and some LUNs, to leverage on-prem and in the cloud.

Multi-Admin Verification (MAV)

- Prevents compromised, malicious, or inexperienced admins from making undesired configuration changes or deleting data.
- Ensures certain operations, such as vol or Snapshot deletion, can only be executed after approval from one or more designated administrators.
- NetApp IT leverages MAV on all ONTAP clusters, which are enabled to approve changes to ARP policies and other config modifications.
- MAV challenges bad actors from infiltrating data storage and helps protect your information from unprecedented attacks.

Autonomous Ransomware Protection (ARP)

- Provides autonomous detection of potential attacks by identifying and responding to threats in the primary storage location.
- ARP does not require additional software or hardware requirements; it's built-in and silently learns the volume activity (i.e. file level activity, extensions in use, and entropy)
- When ARP goes active, it reports in real-time if anything deviates from the benchmark statistics.
- If anomalous behavior is observed, Autonomous Ransomware Protection automatically takes early Snapshots and alerts administrators about the imposing danger to minimize attack impacts.

Data Infrastructure Insights

NetApp has elevated its security measures by incorporating anomaly and threat detection services to safeguard data with actionable intelligence. NetApp IT utilizes this technology for all on-prem NAS volumes, enhancing data protection and offering robust recommendations to prevent future attacks. Data Infrastructure Insights and Cloud Workload Security deliver valuable insights and visibility into your NAS workloads. This system alerts administrators to potential misuse or theft of key intellectual property based on usage patterns, making it highly beneficial for Enterprises looking to manage and secure access to sensitive data.

What Next?

In today's advanced technological environment, where threats are more prevalent than ever, it is crucial to implement effective measures to safeguard your information and data. The NetApp solutions discussed offer comprehensive defense across nearly every storage service layer and are continually improving.

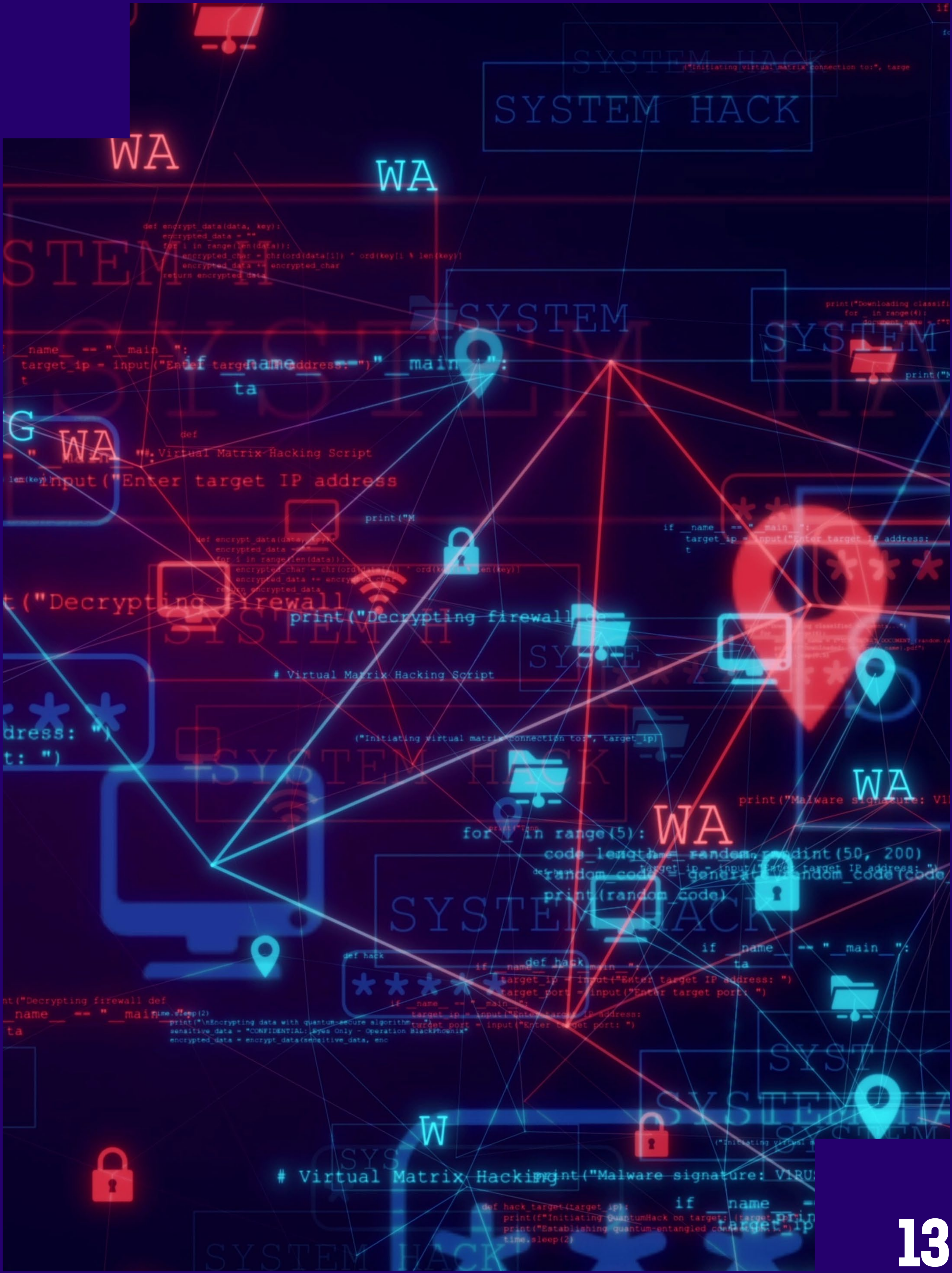
As an IT organization, we actively provide feedback to our product teams as we strive for improved solutions. You can stay updated on the latest ransomware technology advancements by visiting our website and joining future NetApp on NetApp sessions to gain insights into NetApp IT's product solutions.

About the Author

Ram Kodialbail

Senior IT Storage Engineer, NetApp IT

Nearly 20 years ago, Ram began his career at NetApp as a Technical Support Engineer. He later transitioned to NetApp IT's Storage team, where he contributed to managing the company's corporate storage infrastructure. Currently, as part of the Storage Engineering group, he plays a key role in designing and deploying storage solutions as well as automation to meet NetApp IT's hybrid storage needs.


SYSTEM HACK
WA
WA
SYSTEM
# Virtual Matrix Hacking Script
input("Enter target IP address
print("Decrypting firewall
# Virtual Matrix Hacking Script
for _ in range(5):
WA
code_length = random.randint(50, 200)
print(random_code)
SYSTEM HACK
W
# Virtual Matrix Hacking
print("Malware signature: VIRUS
SYSTEM HACK

Enhancing Data Security

with NetApp ONTAP

In today's digital landscape, ensuring data security is paramount for organizations across various industries. As a NetApp IT Senior Storage Engineer, one of the challenges I faced was managing data protection and recovery across a large and complex IT environment. Traditional backup and recovery methods were becoming increasingly inefficient and time-consuming, significantly as the volume of data grew.

A Legacy of Innovation

NetApp has been leveraging ONTAP since our company's founding over 30 years ago, evolving from the traditional seven-mode to the current ONTAP 9. This evolution has significantly enhanced our data management capabilities, supporting diverse environments, including production, sub-production, and lab settings. Today, our ONTAP footprint extends to nearly 50 clusters, supporting both on-premises and cloud workloads. This hybrid approach allows us to consume storage as a managed service, simplifying deployment and configuration while maintaining high- performance and reliability.

From Inefficiency to Optimization

Traditional methods of data protection relied heavily on manual processes, isolated systems, and reactive measures that couldn't keep up with the exponential growth of data or the increasing complexity of IT environments. Here's how NetApp ONTAP and its suite of capabilities address these challenges:

Operational Efficiency Across Environments:

ONTAP supports both on-premises and cloud workloads, providing a unified approach to data management. This hybrid model allows us to consume storage as a managed service, optimizing performance and reliability while reducing costs.

Simplified Deployment and Configuration:

Legacy approaches required time-intensive, error-prone manual configurations for each system. With ONTAP, tools like BlueXP and Active IQ Unified Manager automate deployment and configuration, ensuring speed, consistency, and reduced administrative burden. This has allowed us to focus on strategic initiatives rather than routine tasks.

Advanced-Data Protection:

As data threats like ransomware became more prevalent, traditional backup solutions struggled to keep pace. ONTAP's SnapMirror provides automated replication, ensuring that critical data is always protected. Meanwhile, autonomous ransomware protection (ARP) uses AI/ML to detect and respond to threats, creating snapshots and restoring data without human intervention.

Scalability and Hybrid Cloud Readiness:

Traditional methods would have made managing nearly 50 clusters across production, sub-production, and lab environments nearly impossible. ONTAP's seamless scalability and hybrid capabilities simplify storage management, ensuring we can handle growing data volumes without increasing complexity.

Rapid Recovery Times:

Restoring data using legacy methods was often a slow, disruptive process. ONTAP's snapshot technology and SnapCenter provide near-instant recovery capabilities, minimizing downtime and keeping critical systems operational.

Closing the Loop: Modern Capabilities for Modern Problems

The continuing journey with ONTAP 9 reflects a consistent focus on innovation, enabling NetApp IT to address inefficiencies and complexities of the past. Each capability—from automated replication to hybrid cloud support—ties directly back to solving the core challenges of traditional methods: inefficiency, time consumption, and limited scalability.

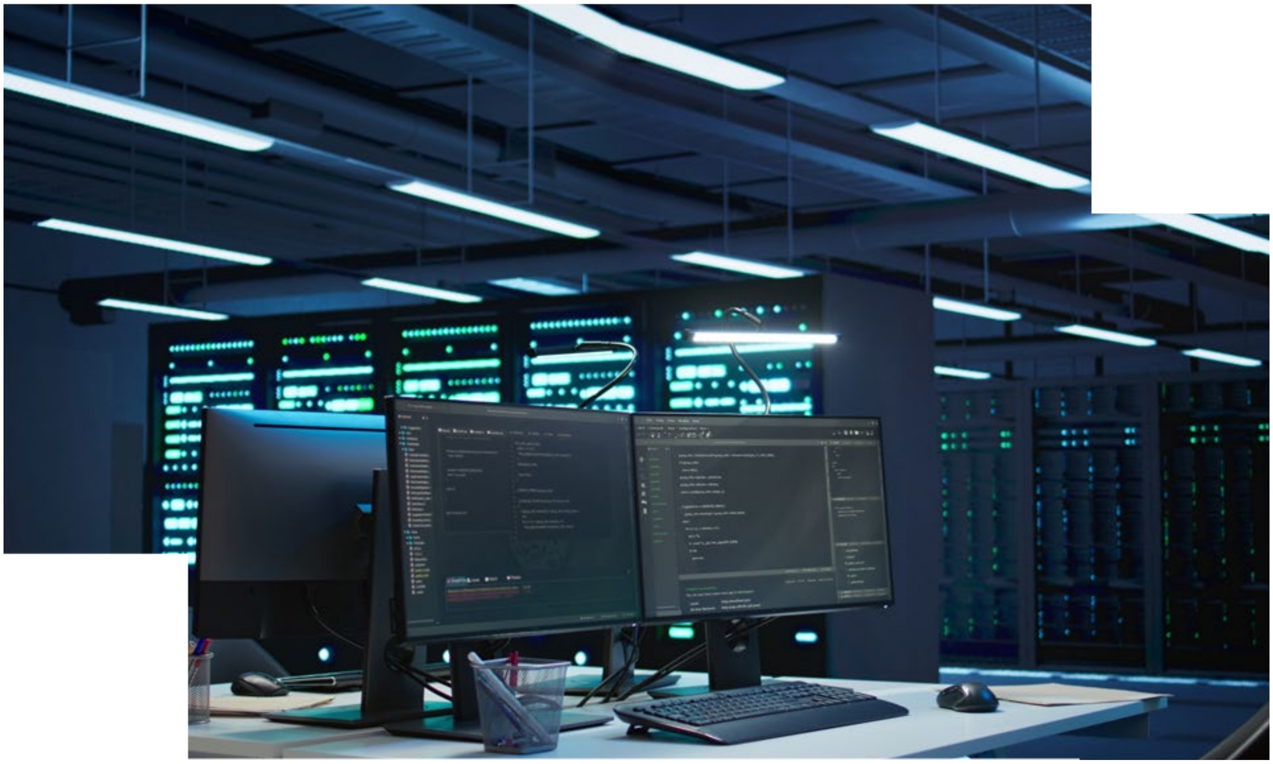
In today's fast-paced digital landscape, staying current isn't just about adopting the latest technology. It's about transforming how we approach data protection, recovery, and management. By leveraging ONTAP, NetApp has redefined data management, creating a foundation that ensures agility, security, and performance for the future.

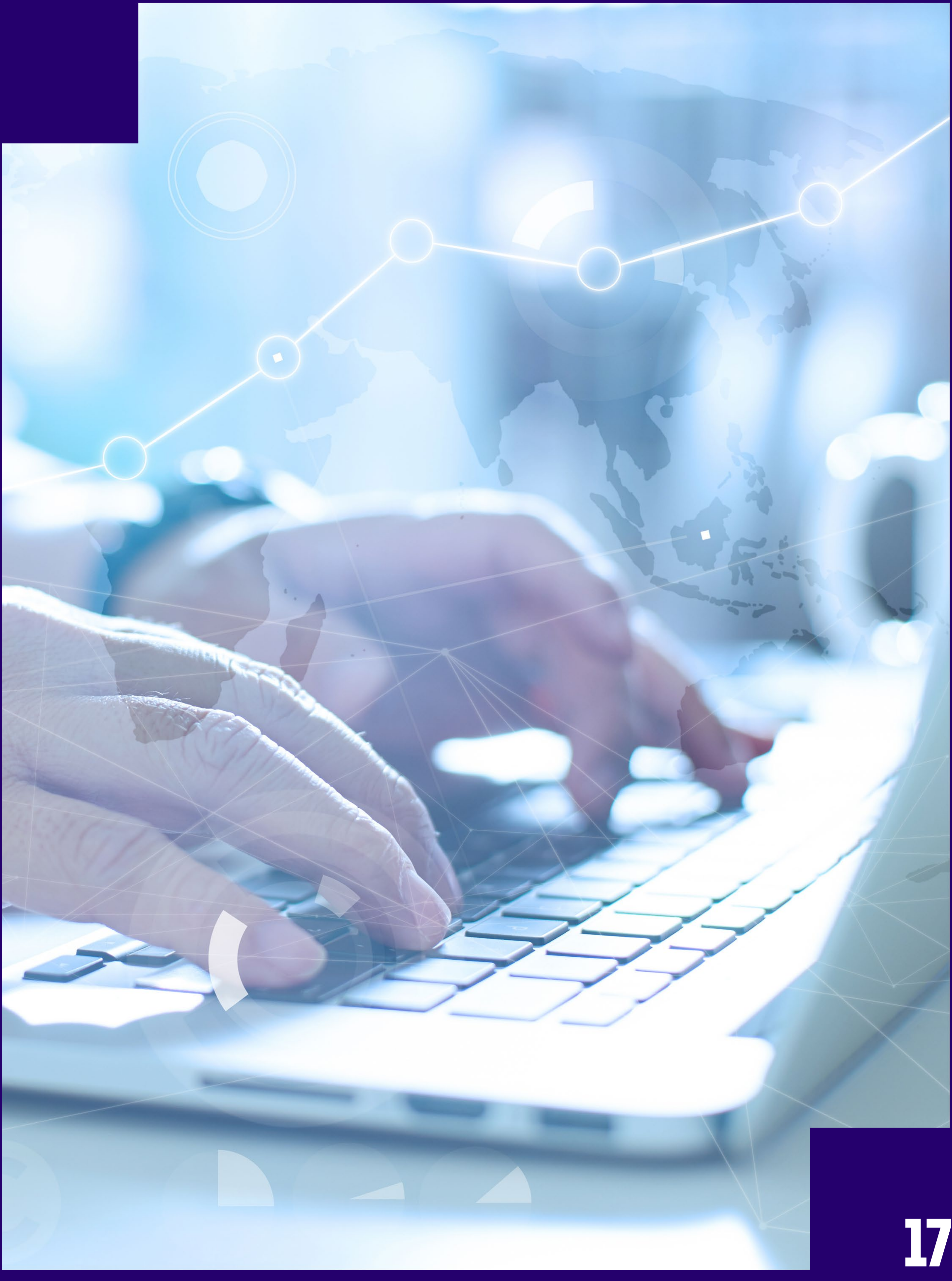
About the Author

Faisal Salam

Senior IT Storage Engineer, NetApp IT

Faisal Salam is a Senior IT Storage Engineer at NetApp and 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 in addition to the use of ONTAP Adaptive QoS.





Contact Us

LinkedIn

@cmattbrown

Email

NetAppIT@NetApp.com

Website

www.NetAppIT.com