NetApp

SEPARATING FACT FROM FICTION

A guide to true cyber resilience for your block storage

THE MYTH

Your cyber defenses are complete with basic network protection, identity security, and application safeguards.

THE TRUTH

Today's cyberthreats are relentless. The sheer volume of threats is overwhelming, and although ransomware protection is top of mind, true resilience requires a data infrastructure that's prepared to protect, detect, and recover in real time.

If you overlook storage-layer protections, especially for your SAN data, you leave yourself open to threats like ransomware that bypass endpoint and perimeter security to directly target your data.

DEBUNKING THE TOP 5 MISCONCEPTIONS

1 MISCONCEPTION: WORKING WITH A SPECIALIZED VENDOR MEANS THAT YOU'RE 100% PROTECTED

FACT: Protecting against cyber incidents encompasses multiple layers of defense to protect against a wide range of threats. It's not just about the partner. You need an interconnected strategy that integrates security at every layer.

NETAPP'S comprehensive data protection integrates seamlessly with your existing security suite, complimenting perimeter, network, and endpoint security measures.

2 MISCONCEPTION: NETWORK AND IDENTITY PROTECTION ALONE IS SUFFICIENT

FACT: Specialized vendors provide essential perimeter, network, and endpoint security, but these measures alone are not enough. Ransomware attacks often bypass these defenses and directly target the data. A robust data-centric defense starts at the storage layer, especially when it comes to block workloads.

NETAPP'S ransomware protection capabilities are built into the data layer—not bolted on. This protection minimizes the chance of successful attacks and avoids tool sprawl by implementing security measures directly where the data resides.

3 MISCONCEPTION: RANSOMWARE AFFECTS ONLY NONCRITICAL DATA

FACT: Ransomware often targets the most sensitive and valuable data. Mission-critical assets, especially those stored in block storage, need to be protected by advanced anti-ransomware solutions.

NETAPP'S AI-powered detection algorithms continuously monitor data patterns, swiftly identifying potential ransomware threats on primary storage with 99% accuracy.

4 MISCONCEPTION: BACKUP SOLUTIONS ALONE SECURE DATA AT THE STORAGE LAYER

FACT: Although backups are crucial, they aren't foolproof. Attackers can compromise backup systems, leaving organizations vulnerable.

NETAPP'S holistic storage layer approach goes beyond traditional backup by incorporating built-in security measures with real-time detection and response capabilities.

5 MISCONCEPTION: RECOVERY FROM RANSOMWARE IS A LENGTHY PROCESS

FACT: A staggering 44% of data breaches are caused by ransomware, and 86% of these attacks result in total business disruption with significant operational downtime.

NETAPP'S comprehensive ransomware defense capabilities enable swift and efficient recovery in the event of a catastrophic attack. Locked-down NetApp® Snapshot™ copies with a cyber vault isolate critical data backups, so you can restore in minutes instead of days to maintain business continuity, especially for critical apps running on SAN storage.

GO FROM MYTHS TO MASTERY WITH NETAPP

By combining specialized vendor solutions with NetApp's data-centric protection, you can elevate your cyber resilience to achieve a robust defense against ransomware and advanced cyberthreats.

Talk to a NetApp security specialist to evaluate your current SAN infrastructure and explore how NetApp's AI-driven, real-time detection and response capabilities, along with our Ransomware Recovery Guarantee, can protect your organization's most valuable asset—your data.

Contact Us

NetApp