Top 10 Ways that Partners Can Help Protect Their Customers’ Data

Organizations are adjusting to physical access restrictions as quickly as possible to keep their businesses up and running. How can you help them provide access to data and services for an increasingly distributed workforce without sacrificing security? NetApp empowers partners like you to protect your customers’ data no matter where it lives, across on-premises and cloud environments. To help businesses thrive and prevent costly downtime and disruption, we provide industry-leading, end-to-end solutions that avoid any issues with data security, data protection, and data recovery.

Have you ensured that your customers are using everything they have available today to manage and secure their data?

Consider the Top 10 ways that NetApp keeps your reputation and your customers’ data safe and sound

Access control

Understand where the data lives (public cloud, private cloud, on premises, or off premises such as in third-party data centers) and classify it so that you can control access to it.

Multifactor authentication

User IDs and passwords leave data access vulnerable. For stricter administrative and data access, use multifactor authentication.

Data segmentation

Use storage segmentation and network virtualization to isolate organizational data.

Locked-down access

Apply role-based access control (RBAC) and attribute-based access control (ABAC) to lock down access to the segmented data by using the principle of least privilege.

Data recovery

Be confident that your customers can recover from an attack on data with NetApp® Snapshot™ copies (instant copies), SnapLock® software (immutable data), and SnapMirror® technology (off-site backups).

Malware prevention

To prevent malware from infiltrating, use NetApp FPolicy™ file whitelisting and blacklisting based on known malware behaviors. Prevent zero-day attacks by using tools in our partner ecosystem.

Automation security hardening

Automate data provisioning, monitoring, quarantining, and remediation by using REST APIs and Ansible. Your customers cannot defend at scale with manual configuration processes.

Encryption

Protect data by using encryption for both data at rest and data in flight.

Logging

Log everything, including administrative access, configuration changes, user access to data, and aberrant activity.

Proactive monitoring

To correlate activities across your customer’s organization, use a security information and event management (SIEM) system. Alert and take action on suspicious access or behaviors.

NetApp Enables You to Better Secure Your Customers’ Data

NetApp is committed to helping you navigate these uncertain times with your customers and helping you prepare for what comes next. To answer your questions about data security and remote-access worker environments, visit our Business Continuity website on NetApp.com.

Read our NetApp blog posts:

- Achieve a Data-Centric Approach to Zero Trust with NetApp ONTAP
- Mobilizing to Stay Connected and Productive in the New Normal
- Partners: Talk to Your Customers About Ransomware Now