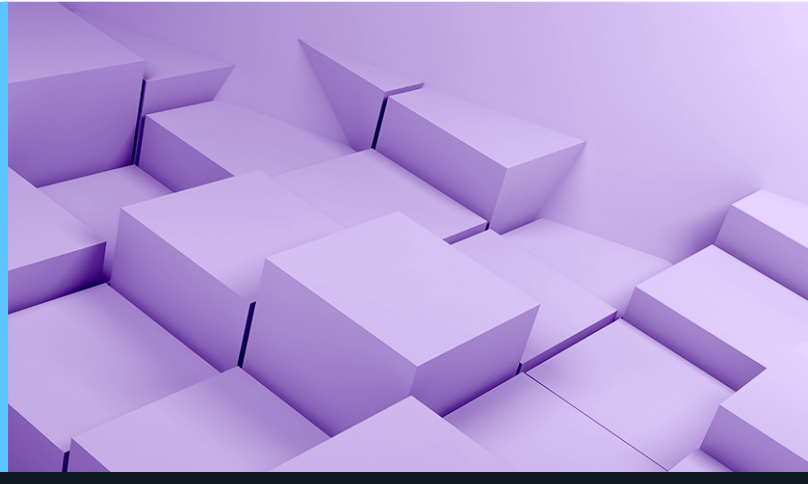
10 GUTE GRÜNDE

Schutz vor Ransomware mit NetApp



01 Logischer Air Gap

Richten Sie einen logischen Air Gap ein, um Dateien und Objekte sicher zu sperren. NetApp SnapLock Compliance und NetApp StorageGRID S3 Object Lock bieten native Funktionen für WORM (Write Once, Read Many), damit Daten während des Aufbewahrungszeitraums nicht gelöscht werden können – auch nicht von kompromittierten Administratorkonten.

02 Schnelle Recovery

Der größte Kostenfaktor bei Ransomware-Angriffen ist die Ausfallzeit. Mit den unveränderlichen NetApp Snapshot Kopien sind Ihre Daten schnell wieder online. Und entdecken Sie, wie Terabyte an Daten können in Sekunden statt Stunden wiederhergestellt werden.

03 Autonomer Ransomware-Schutz

Erkennen und beseitigen Sie Cyberbedrohungen schnell mit Machine-Learning-Technologie. Die in die NetApp ONTAP Software integrierte Technologie überwacht das Filesystem auf Anomalien, die auf sich langsam verbreitende Malware hindeuten können. Die ebenfalls integrierte Funktion zum Blockieren bestimmter Dateierweiterungen als Schutz vor Malware erkennt bekannte Malware und verhindert von vornherein ihre Ausbreitung.

04 Erkennung von Anomalien im Benutzerverhalten

Mit der Cloud Secure Funktion von NetApp Cloud Insights können Sie Anomalien in Echtzeit erkennen und so kompromittierte Benutzerkonten oder möglicherweise schädliches Verhalten aufspüren. In Kombination mit der NetApp FPolicy Komponente von ONTAP können Sie automatisch Datenwiederherstellungspunkte erstellen und sogar den weiteren Kontozugriff blockieren, um Datendiebstahl oder massenhaftes Löschen zu verhindern.

05 Zero-Trust-fähig

Nutzen Sie bei der Sicherheit einen Zero-Trust-Ansatz mit Kontrollen wie Multi-Faktor-Authentifizierung, rollenbasierter Zugriffssteuerung, umfassender Protokollierung sowie Auditing, um vor Nebenangriffen zu schützen.

06 Verhinderung von schädlichen Handlungen eines Administrators

Verhindern Sie Beschädigungen durch kompromittierte Administratorkonten mithilfe der nativen ONTAP Funktion zur Verifizierung durch mehrerer Administratoren. Bei Nutzung dieser Funktion müssen entscheidende Storage-Aktionen wie das Löschen von Volumes und Snapshot Kopien von mehr als einem Administrator autorisiert werden.

07 Erweitertes Management von Datenkopien

Verbessern Sie Backup und Disaster Recovery. Mit NetApp SnapMirror und dem NetApp Cloud Backup Service können Sie Ihre Snapshot Kopien effizient auf ein anderes ONTAP System oder einen Objektspeicher Ihrer Wahl replizieren – On-Premises oder in der Cloud.

08 Risikominimierung

NetApp Cloud Data Sense bietet Ihnen Einblick in den Sicherheitsstatus Ihrer Daten und identifiziert sensible Daten samt Speicherort. Verfolgen Sie Rechte für Ordner und nutzen Sie Optionen zum Mindern potenzieller Risiken wie Datenexfiltration.

09 Zentrales Monitoring

Überwachen Sie Ihre Hybrid-Cloud-Infrastruktur mit einer simplen UI. Das in NetApp Cloud Manager verfügbare Ransomware Protection Dashboard hilft Ihnen, Bedrohungen zu erkennen und Gegenmaßnahmen einzuleiten.

10 Nachträgliche Aufklärung

Setzen Sie bewährte Lösungen von NetApp zur forensischen Analyse vor und nach einem Ransomware-Vorfall ein. So erhalten Sie die nötigen Einblicke, um Angriffspfade erkennen, managen und blockieren zu können.

NetApp