VERITAS

# Veritas Alta™ Recovery Vault Azure ExpressRoute Overview Guide

Cloud-based storage as a service.

*This paper is designed to highlight the architecture and steps Azure ExpressRoute with Veritas Alta Recovery Vault*

*For more information on Veritas products and solutions, visit www.veritas.com*

VERITAS
ALTA

# Contents

## Revision History

| Version | Date | Changes | Author |
|---------|------|---------|--------|
| 1.00 | 5/23/2023 | Initial Version | Neil Glick and Sakshi Nasha |

# Introduction

**Executive Summary**

Veritas Alta™ Recovery Vault is cloud-based storage as a service that provides a seamless, fully managed, secondary storage option for NetBackup™ users. With Veritas Alta Recovery Vault, protecting critical data in the cloud has never been easier. Seamlessly integrated with NetBackup, an easy-to-use UI simplifies provisioning, management, and monitoring of cloud storage resources and retention policies. Veritas Alta Recovery Vault offers a single, flexible repository for all your data sources—from on-premises to your public cloud workloads. Veritas Alta Recovery Vault safely stores anything that NetBackup can protect.

Microsoft Azure ExpressRoute is used to create private connections between Azure data centers and infrastructure on premises or in a colocation environment. ExpressRoute connections do not route through the public internet, and they offer more reliability, faster speed, and lower latency than typical internet connections. In some cases, using ExpressRoute connections to transfer data between on-premises systems and Azure gives you significant cost benefits.

To ensure optimal functionality between Veritas Alta Recovery Vault and ExpressRoute, Veritas purchased and configured ExpressRoute to reflect a customer's on-premises NetBackup installation. NetBackup with Veritas Alta Recovery Vault was used to back up and restore files over ExpressRoute to test functionality and performance. The goal of this guide is to show that once configured, Azure ExpressRoute is transparent to Veritas Alta Recovery Vault and NetBackup, irrespective of each other.

**Target Audience**

This document is for customers interested in learning more about how Veritas Alta Recovery Vault and Microsoft Azure ExpressRoute work together to offer a network connection that is more secure, reliable, and faster than the internet alone.

# Why Veritas Alta Recovery Vault

In just a few years, the adoption of public cloud-based data protection as a service has grown significantly. This trend has placed the onus on data owners to deliver on data protection service level agreements (SLAs), data sovereignty, security, and ransomware resiliency.

Traditional approaches to cloud data protection cannot keep pace with IT complexity, growing threats, or economic expectations.

Veritas Alta Recovery Vault provides a fully-managed cloud data protection tier that is seamlessly integrated into NetBackup. With Veritas Alta Recovery Vault, Veritas customers can be confident that their data is secure in the cloud, protected from ransomware, disaster recovery ready, and able to meet compliance and governance requirements.

Veritas Alta Recovery Vault is the right technology at the right time. Veritas Alta Recovery Vault simplifies the process of provisioning new storage in the cloud and reduces risks. All storage as a service resources are provisioned and managed from within NetBackup's locked-down security and role-based authentication policies. Eliminating separate accounts and user interfaces across cloud providers helps ensure that security and compliance policies are in check. Veritas Alta Recovery Vault is an integral feature of NetBackup, customer cloud storage benefits from all its capabilities.

With Veritas Alta Recovery Vault you can:

- **Reduce risks**: Crucial cloud security, retention, and compliance managed within NetBackup
- **Scale limitlessly**: Efficiently manage data growth without compromising manageability
- **Lower total cost of ownership (TCO)**: Predictable as a service subscription; zero hidden costs
- **Automate resiliency**: Intelligent cloud policies and air-gapped multi-cloud isolation protect data from ransomware and other threats

## Why Microsoft Azure ExpressRoute

ExpressRoute lets you extend your on-premises network into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services such as Microsoft Azure and Microsoft 365.

Connectivity can be from any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections do not go over the public internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the internet. For more information about how to connect your network to Microsoft using ExpressRoute, see ExpressRoute connectivity models.

### Key Benefits

- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider; connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange
- Connectivity to Microsoft cloud services across all regions in the geopolitical region
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on
- Dynamic routing between your network and Microsoft via BGP
- Built-in redundancy in every peering location for higher reliability
- Connection uptime SLA
- QoS support for Skype for Business

For more information, see the ExpressRoute FAQ.

## Prerequisites

ExpressRoute Prerequisites and Checklist, is a Microsoft document that provides the prerequisites that you will need before the ExpressRoute circuit can be created.

Microsoft recommends the following prerequisites:

1. A valid Azure account
2. An active Microsoft 365 subscription
3. A connectivity provider
4. Proper network requirements such as:
    a. Network redundancy
    b. Disaster recovery redundancy
    c. Proper routing between your on-site and how the provider will connect you to Azure
    d. Public IP NAT, no private IP addresses are allowed
    e. Follow QoS requirements, if any
    f. Network security

## Creating An ExpressRoute Circuit

After the prerequisites have been completed, the ExpressRoute circuit can now be installed. Microsoft provides five different methods, listed below:

Quickstart: Create and modify an ExpressRoute circuit (create using Azure portal)

Quickstart: Create and modify an ExpressRoute circuit using Azure PowerShell

Quickstart: Create and modify an ExpressRoute circuit using Azure CLI

Quickstart: Create an ExpressRoute circuit with private peering using Bicep

Quickstart: Create an ExpressRoute circuit with private peering using an ARM template

Veritas recommends and uses Microsoft Peering to configure Azure ExpressRoute with Veritas Alta Recovery Vault storage. Customers should use Azure ExpressRoute Microsoft Peering, and not Azure Private Peering. The differences are described on Microsoft's site.

In the past, with an ExpressRoute configured for Microsoft Peering, Microsoft would send all the prefixes for public IPs. Now, customers should configure a route filter first, which is a Border Gateway Protocol (BGP) community value for the prefixes you want to receive, to the storage region (such as East US, West US 2, etc.) the customer has chosen for their Veritas Alta Recovery Vault Azure storage.

Please review Microsoft's guide on setting up a route filter for the prefixes the customer wants to receive:

Tutorial: Configure route filters for Microsoft peering using the Azure portal
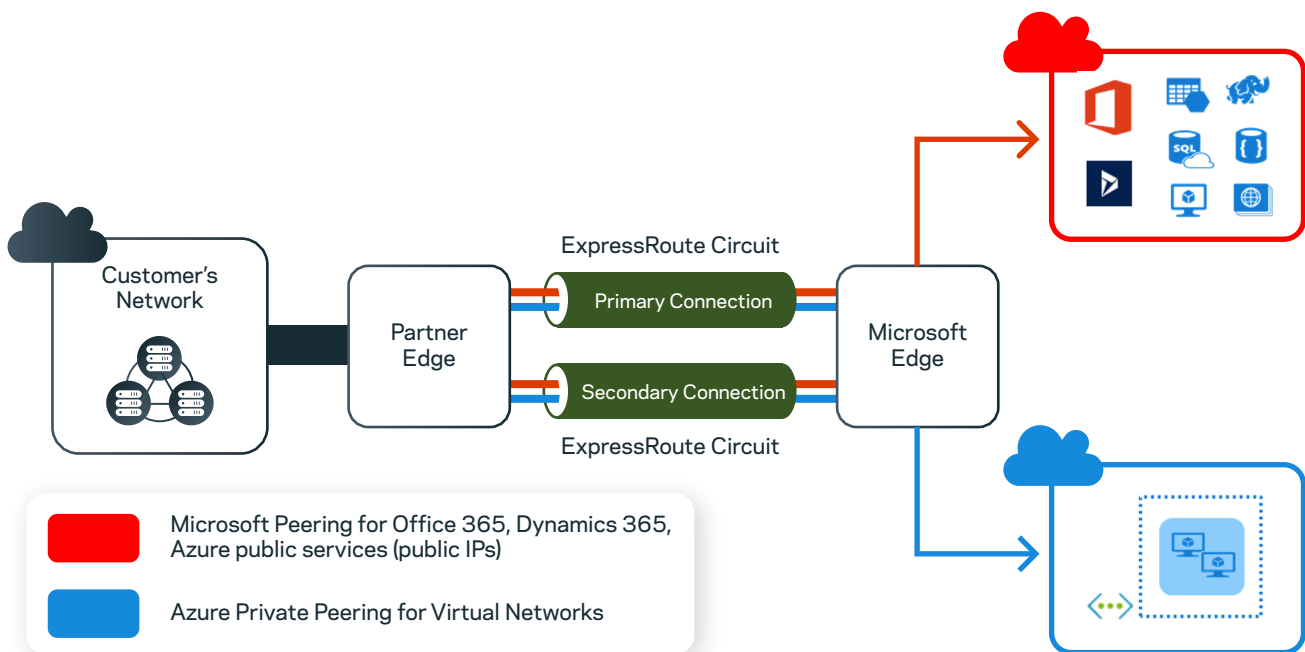


*Figure 1. Typical Microsoft ExpressRoute configuration It is recommended to use Microsoft Peering with Veritas Alta Recovery Vault)*

## Connecting to Veritas Alta Recovery Vault Storage with ExpressRoute

The following is an abbreviated list of steps that are needed to connect to Veritas Alta Recovery Vault storage. For an in-depth deployment guide on Veritas Alta Recovery Vault, see the Veritas Alta Recovery Vault Deployment Guide.

For an in-depth look at security and best practices for Veritas Alta Recovery Vault, see the Veritas Alta Recovery Vault Security Profile.

**Note**: Once configured, Azure ExpressRoute is transparent to Veritas Alta Recovery Vault and NetBackup, irrespective of each other.

When requesting storage from Veritas, your Veritas Alta Recovery Vault storage buckets, created by Veritas, will have immutability enabled. All NetBackup cloud storage units must be created with Governance mode immutability enabled to ensure data is written in an immutable format.

Immutability gives you the ability to write once, and read many (WORM), to your Veritas Alta Recovery Vault storage, and select how long you would like the images to be retained. In the event of a threat actor/malware compromise, immutability prevents the threat actor from expiring your backup images in Veritas Alta Recovery Vault, or manipulating the data in any way.
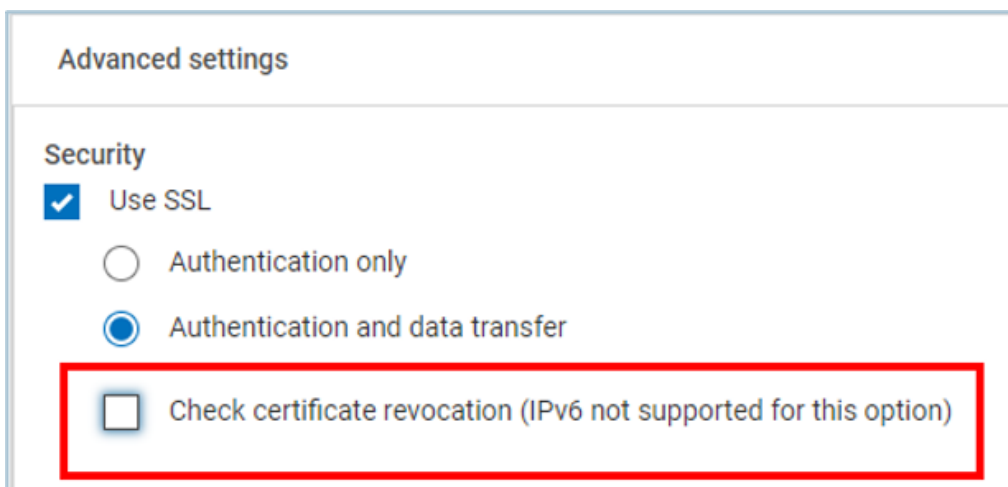
**Note**: This document is based on NetBackup 10.2 or later, for pre-10.2 steps, see the Veritas Alta Recovery Vault Deployment Guide.

**Ports**

Communication to the external storage bucket requires port 443 to be open outbound so the NetBackup API can communicate with the storage bucket through HTTPS. If outbound port 443 cannot be opened for security concerns, a proxy server can be added.

**Note**: It is a best practice that DNS and NTP can resolve correctly.

Veritas checks for certificate revocation to ensure the certificates are valid, which means that port 80 needs to be open outbound on the MSDP-C/storage server unless you do not wish to check for certificate revocation. To remove this certificate validation (not recommended), simply uncheck certificate revocation when creating the disk pool.



**Note**: For more information about Veritas Alta Recovery Vault security, see the Veritas Alta Recovery Vault Security Profile and the NetBackup Network Ports Reference Guide regarding NetBackup client ports.

**Connection Steps**

Connection to your Veritas Alta Recovery Vault storage is simple and can be done through the NetBackup WebUI. For complete steps, see the Veritas Alta Recovery Vault Deployment Guide.

## Backup and Restore Testing

Backup and restore tests were performed with and without the ExpressRoute circuit.

The first test included a non-ExpressRoute virtual machine (VM), which was not part of the ExpressRoute VLAN. After monitoring the network traffic, we could infer that the network routing followed/traversed the public internet and reached the targeted Azure storage account, as seen in Figure 2.
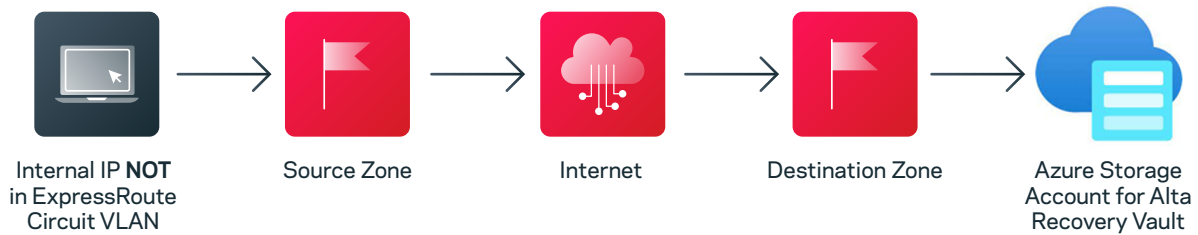


Internal IP **NOT** in ExpressRoute Circuit VLAN → Source Zone → Internet → Destination Zone → Azure Storage Account for Alta Recovery Vault

*Figure 2: Backup and restore of a VM not in the ExpressRoute VLAN, routed over the internet to connect to Azure*

The second test involved the backup and restore of a VM that was within the ExpressRoute VLAN. The network traffic followed the dedicated ExpressRoute channel over the provider's circuit and directly to Azure without traversing the public internet, as seen in Figure 3.
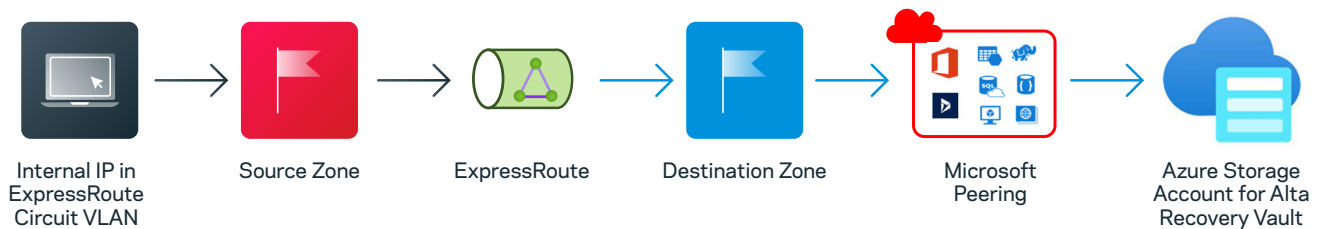


Internal IP in ExpressRoute Circuit VLAN → Source Zone → ExpressRoute → Destination Zone → Microsoft Peering → Azure Storage Account for Alta Recovery Vault

*Figure 3: Internal IP in ExpressRoute Circuit VLAN*

**Backup Tests:**

The following table shows three backup jobs that were performed on a similar-sized file. The following is a summary of the three tests:

- Test Number 1: Backup of a 3.45 GB file using an ExpressRoute circuit of 50 Mbps bandwidth
- Test Number 2: Backup of a 3.47 GB file using the standard public internet
- Test Number 3: Backup of a 3.55 GB file using a 500Mbps ExpressRoute circuit

The tests show the importance of proper bandwidth sizing and potential speed benefits of ExpressRoute.

**Note**: MBps is megabytes per second. Mbps is megabits per second. 1 MBps = 8 Mbps

| Test Number | Express Route Used | NetBackup Version | File Size | Start | End | Total Time | Transfer Rate | ER Bandwidth |
|---|---|---|---|---|---|---|---|---|
| 1 | Yes | 10.2 | 3.45 GB | 2:26:44 PM | 2:37:20 PM | 10 min 37 sec | 5.92 MB/sec | 50 Mbps |
| 2 | No | 10.2 | 3.47 GB | 1:47:20 PM | 1:50:10 PM | 2 min 50 sec | 64.56 MB/sec | NA |
| 3 | Yes | 10.2 | 3.45 GB | 12:14:26 AM | 12:15:45 AM | 1 min 19 secs | 58.54 MB/sec | 500 Mbps |

**Restore Tests:**

The following table shows three restore jobs that were performed on a similar-sized file. The following is a summary of the three tests. Your backup and recovery numbers will vary depending on the size of the network pipe(s) and the data that is flowing through them.

- Test Number 1: Restore of a 3.45 GB file using a 50 Mbps ExpressRoute circuit
- Test Number 2: Restore of a 3.47 GB file using the standard public internet
- Test Number 3: Restore of a 3.45 GB file using a 500 Mbps ExpressRoute circuit

The tests show the importance of proper bandwidth sizing and potential speed benefits of ExpressRoute.

| Test Number | Express Route Used | NetBackup Version | File Size | Start | End | Total Time | Transfer Rate | ER Bandwidth |
|---|---|---|---|---|---|---|---|---|
| 1 | Yes | 10.2 | 3.45 GB | 4:45:14 PM | 5:10:38 PM | 25 min 24 sec | 2.33 MB/sec | 50 Mbps |
| 2 | No | 10.2 | 3.47 GB | 2:09:26 PM | 2:11:56 PM | 2 min 30 sec | 40.2 MB/sec | NA |
| 3 | Yes | 10.2 | 3.45 GB | 12:51:37 AM | 12:52:52 AM | 1 min 15 secs | 51.76 MB/sec | 500 Mbps |

**ExpressRoute Backup and Restore Summary**

The speed of your backup and restore jobs, on an ExpressRoute circuit or not, will depend on the size of the network pipe that the data is flowing through. Typically, larger pipes will provide quicker backup and restore, while smaller pipes will become saturated and the speed will be throttled. The data transfer rate is dependent on numerous factors such as bandwidth of the ExpressRoute circuit, latency, frame size, and window size.

- Test 1 in backup and restore shows the importance of proper network sizing. The ExpressRoute circuit is throttled by how much data can be pushed through, and the backup/restore data transfer rate begins to increase as expected.

- Test 2 in backup and restore is not the ExpressRoute circuit, and shows that with no network throttle, the speeds and feeds will increase dramatically. However, speeds and feeds will greatly depend on your non-ExpressRoute circuit.

- Test 3 in backup and restore depicts how increasing the ExpressRoute circuit bandwidth speeds up the data transfer rate of backup and restore jobs. As seen in the test, the backup and restore finishes faster than the ExpressRoute circuit due to the point-to-point architecture built into ExpressRoute.

ExpressRoute currently supports bandwidth from 50 Mbps to 10 Gbps, with the price increasing as bandwidth increases. Careful analysis of your current backup network needs should be considered when purchasing your ExpressRoute circuit. See Azure ExpressRoute Pricing for more information.

Bandwidth size can be checked in the Azure portal as seen in Figure 4.
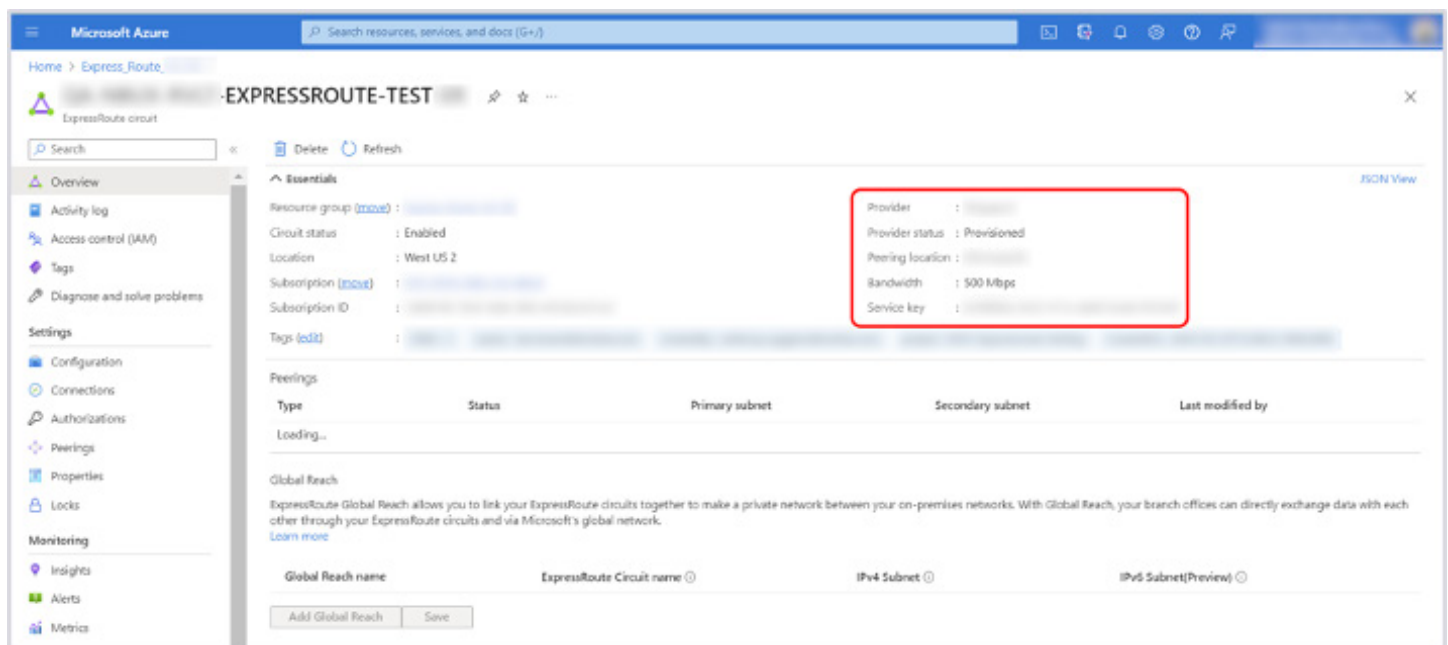


*Figure 4. ExpressRoute circuit with 500 Mbps in Azure Portal*

## Conclusion

Customers can now choose to use Azure ExpressRoute, which  offers more reliability, faster speeds, consistent latencies, and higher security than typical connections over the public internet; or customers can continue to use standard transport layer security (TLS) built into NetBackup. Both solutions are supported and provide excellent connectivity for Veritas Alta Recovery Vault.

Veritas Alta Recovery Vault simplifies the process of provisioning new storage in the cloud and allows for limitless scalability, lowers TCO, and automates resiliency. Through seamless integration with NetBackup and an easy-to-use UI, management and monitoring of cloud storage resources and retention policies, provisioning storage, and data protection has never been easier.

## References

What is Azure ExpressRoute?

Connect an on-premises network to Azure using ExpressRoute

ExpressRoute Documentation

Extend an on-premises network using ExpressRoute

ExpressRoute connectivity models

ExpressRoute FAQ

ExpressRoute Prerequisites and Checklist

Quickstart: Create and modify an ExpressRoute circuit (create using Azure portal)

Quickstart: Create and modify an ExpressRoute circuit using Azure PowerShell

Quickstart: Create and modify an ExpressRoute circuit using Azure CLI

Quickstart: Create an ExpressRoute circuit with private peering using Bicep

Quickstart: Create an ExpressRoute circuit with private peering using an ARM template

Veritas Alta Recovery Vault Deployment Guide

Veritas Alta Recovery Vault Security Profile

Azure ExpressRoute Pricing

## About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets, and 60+ clouds through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

## VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact