VERITAS

Flex Appliances with NetBackup Security

Veritas Flex Appliances provide a complete immutable storage solution to defend your backup data and recover in software and hardware. This white paper highlights the intrusion detection and prevention, OS hardening and multi-tenancy security features in the Flex Appliances with Veritas NetBackup™ solution.

Veritas™ White Paper | October 2020

Contents

Introduction . . . 3

Executive Summary . . . 3

Scope . . . 3

Intrusion Detection and Prevention System . . . 3

IDS and IPS Overview . . . 3

Symantec Data Center Security . . . 4

Flex Appliances with SELinux . . . 4

SELinux Overview . . . 5

RBAC . . . 5

Platform . . . 6

Services and Applications . . . 6

Flex Appliance Immutable Storage . . . 7

Lockdown Mode . . . 7

Protecting Immutable Storage Servers . . . 8

OS Hardening . . . 8

Security Technical Implementation Guide . . . 9

Flex Appliance Multi-Tenant Architecture . . . 9

References . . . 10

INTRODUCTION

Executive Summary

In the wake of successful and high-profile cyberattacks against banks, technology, retail stores and governments, companies want to ensure they are not the next victim reporting a devastating breach. Today, security threats are every organization's concern. Whether a ransomware attack, hardware failure or accidental or intentional data destruction, data loss incidents can have catastrophic effects for their customers.

Veritas Flex Appliances bring agility, resilience, scalability and simplicity to Veritas NetBackup™ data protection. Flex Appliances use Security-Enhanced Linux (SELinux) to provide intrusion prevention and detection and OS hardening. NetBackup software and Flex Appliances provide a complete immutable storage solution to defend your backup data and recover in software and hardware.

Scope

The purpose of this document is to provide technical details on the SELinux IDS/IPS, OS hardening and multi-tenancy capabilities in Flex Appliances.

INTRUSION DETECTION AND PREVENTION SYSTEM

Organizations need to protect customers' data from malicious attack and destruction. The assurance of integrity and safety should be applied to network and system monitoring to prevent data loss. Alerts are needed for administrators and the security team when an incident is happening so they can respond in real time to the threat.

Veritas developed Flex Appliances with security as a primary objective. Each element of an Appliance, including its Linux operating system and the core NetBackup application, is tested for vulnerabilities using both industry standards and advanced security products. These measures ensure that exposure to unauthorized access and resulting data loss or theft is minimized. Flex Appliance use Red Hat-supported built-in SELinux to protect roles, platform, services and applications.

IDS and IPS Overview

An intrusion detection system (IDS) protects a system from an attack, misuse and compromise by analyzing system and network activity for unauthorized entries or malicious activities. IDS can monitor and audit network activities and system configurations for vulnerabilities and analyze data integrity. An IDS includes a management console and sensors. The console is for management and reporting and the sensors are agents that monitor hosts or networks on a real-time basis. An IDS has a database of attack signatures that represent patterns of previously detected attacks.

There are two common types of IDSs: host-based and network-based IDSs. A host-based IDS requires implementing a detection system on each host, and a network-based IDS funnels packets through a single device before being sent to specific hosts.

An intrusion protection system (IPS) reinforces a firewall and provides an analysis layer to select for dangerous content. An IPS actively analyzes the network and undergoes automated actions on all traffic flows that enter the network. When an IPS detects an intrusion, it blocks the traffic and prevents it from getting to its target. These actions may include dropping malicious packets, blocking traffic to a source address or resetting a connection.

The overall IPS/IDS solution on a Flex Appliance provides the following features:

- Hardened Linux OS components.
- Malware prevention or containment to ensure the integrity of the underlying host system is not harmed as a result of OS vulnerabilities.
- Data protection that tightly limits Appliance data access to only those programs and activities needing access, regardless of system privileges.
- Hardened Appliance stack.
- Locked Appliance application binaries and configuration settings to ensure changes are tightly controlled by the application or trusted programs and scripts.
- Expanded detection and audit capabilities.
- Enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations (such as PCI) as a compensating control.

Symantec Data Center Security

Veritas NetBackup Appliances use Symantec Data Center Security (SDCS) to protect servers in data centers. The SDCS software is included on Appliances and is automatically configured during Appliance software installation. SDCS offers policy-based protection and helps secure the Appliance using host-based intrusion prevention and detection technology. It uses the least-privileged containment approach and also helps security administrators centrally manage multiple Appliances in a data center. The SDCS agent runs at startup and enforces the customized NetBackup Appliance IPS and IDS policies. SDCS uses a central SDCS manager to provide you with an integrated view of security across multiple Appliances as well as any other enterprise systems managed by SDCS.

Flex Appliances with SELinux

The Flex Appliance 2.0 OS includes multiple features to ensure the security of your data. Each element of the Appliance is tested for vulnerabilities using both industry standards and advanced security products. These measures ensure that exposure to unauthorized access and resulting data loss or theft is minimized. (See Table 1 for a comparison between SDCS and Flex Appliances with SELinux.)

The security features in the Flex 2.0 OS include the following:

- OS security hardening, including SELinux.
- Lockdown mode and WORM storage support, which let you set additional access restrictions and block data deletion during a specified retention period.
- Password policy enhancement:
  - Forced password changes during initial configuration ensure the default password does not remain active on the system.
  - The ability to set your own password policy, including the option to use the Security Technical Implementation Guides (STIGs) for validation.
  - Additional password protection in the Flex Appliance Shell that locks the hostadmin account for 15 minutes after three incorrect login attempts.
- Session timeouts that automatically sign users out of the Flex Appliance Console and the Flex Appliance Shell after 10 minutes of inactivity.

SELinux Overview

SELinux is a Linux Security Module (LSM) built into the Linux kernel and loaded at boot. Driven by an administrator-controlled security policy, SELinux defines access controls for the applications, processes and files on a system. When an application or process, known as a subject, makes a request to access an object like a file, SELinux checks with an access vector cache (AVC), where permissions are cached for subjects and objects. Figure 1 explains how the subject gets access to an object.

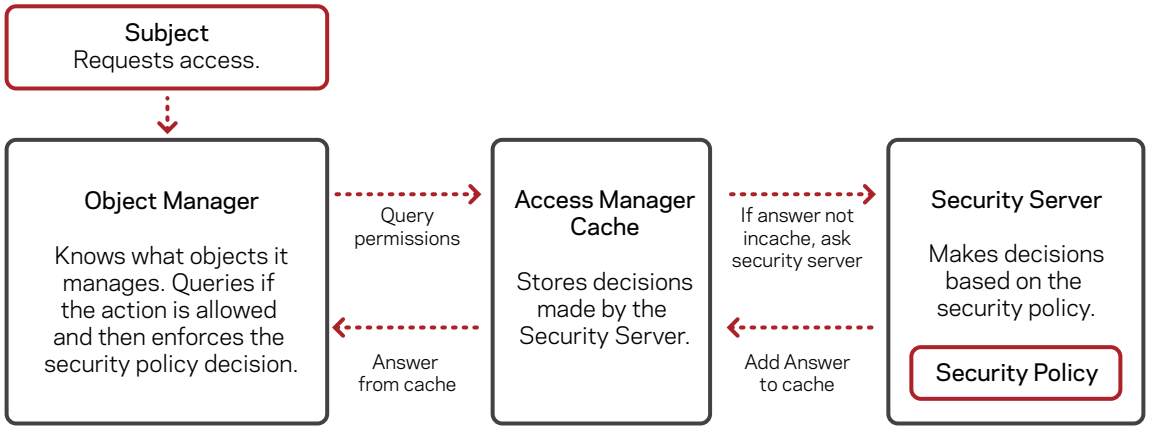

Figure 1. An overview of how a subject gains access to an object in SELinux.

SELinux is used for container separation to prevent container attacks against the host file system. The standard Linux security model allows the superuser "root" to bypass all security checks, including the possibility of using setuid bit to allow users to run an executable file with the permissions of the executable file owner. Doing so could cause security issues on systems. SELinux is a labeling system and views each object on the system—every file, directory, socket file, symlink, shared memory, semaphore or fifo file—and also every subject—a running process or Linux user entity—with a SELinux label.

RBAC

Role-based access control (RBAC) refers to the idea of assigning permissions to users based on their role within an organization. Flex Appliances use SELinux RBAC to authorize users to achieve OS hardening. User permissions are granted through roles to gain rights. A Flex Appliance login account is mapped to an SELinux user. Figure 2 shows that the Flex accounts hostadmin, root user and any use accounts are mapped to SELinux user staff_u and guest_u with staff_r and guest_r roles.

Note:

- Flex root account and any customized accounts are reduced to SELinux user guest_u that has next to non-privileges.
- An SELinux user is allowed one or more roles, restricting which roles a particular user can have.
- Roles are mapped to permissions and allowed certain domains and runtime privileges for one or more applications.

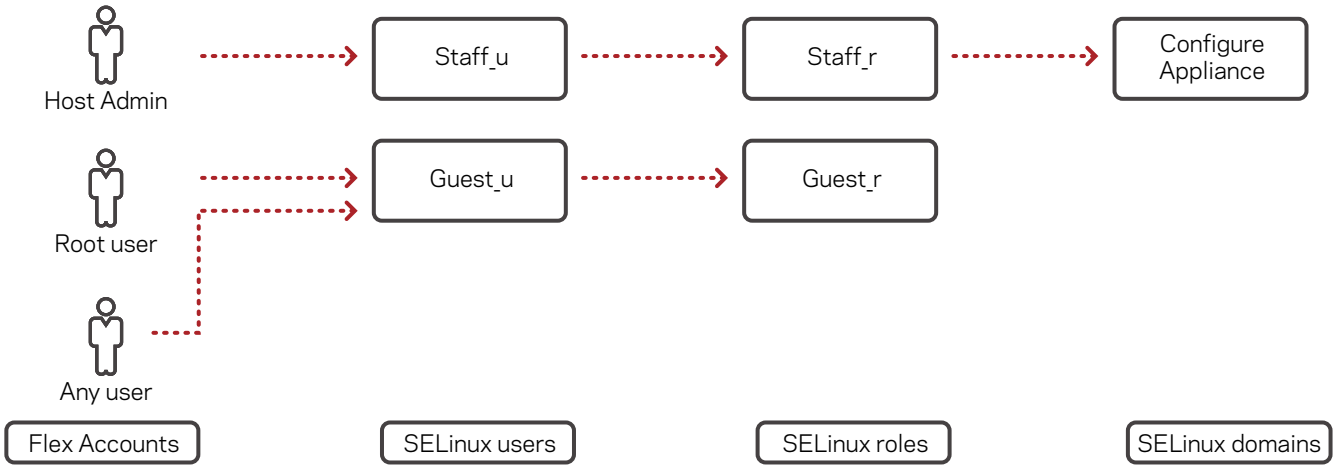

Figure 2. An overview of how Flex Appliances use RBAC to map accounts to SELinux users.

Platform

To secure a Flex Appliance platform, the worker service is run by a non-root user. The Flex Appliance applies infrastructure certificates during configuration. Applications logs track any changes during installation. The Flex Appliance also integrates with Veritas InfoScale™ device modules to allow elevated shell basic InfoScale management.

Services and Applications

SELinux Multi-Category Security (MCS) allows users to label files with categories to further constrain Discretionary Access Control (DAC) and Type Enforcement (TE) logic.

In Flex Appliances, applications and services are containerized and run with MCS turned on for exclusive data access. The Docker engine assigns a unique category pair (C1, C2) to provide isolation between the containers. Flex Appliances present dedicated file systems mounted with security context for exclusive access to each container.

There are some design considerations regarding certificates and log files:

- For certificates, MCS is disabled to allow file sharing.
- Logs go to /log/containers/service-name.
- MCS policy allows log rotation.
- Container services are allowed to access the log files.

	NetBackup Appliance SDCS	Flex Appliance SELinux
Hardened Linux OS implementation	The policy contains a set of rules and each rule contains subjects, resource path and access rules.	All processes and files are labeled. SELinux policy rules define how processes interact with files as well as how processes interact with each other. Access is only allowed if an SELinux policy rule specifically allows it.
Container protection	Not preferred.	Better support, integration from Red Hat and more flexibility.
Centralized managed mode operation	Available	Will be available with Syslog forwarding in the future.
Integration and supportability	Less granular and not enough integration.	More granular runtime options, more friendly to developers and administrators.
OS protection	User needs to understand OS and policies.	Red Hat provides OS policies by default.
Public sector requirement STIG	Not preferred.	SELinux is the preferred approach per the STIG DISA profile.
Vendor	Third party.	Red Hat support, embedded in the kernel.
Elevation	IPS will be disabled.	IPS will not be disabled.

Table 1. Comparison Between SDCS and Flex Appliance SELinux

FLEX APPLIANCE IMMUTABLE STORAGE

NetBackup software and Flex Appliances provide a complete immutable storage solution to defend your backup data and recover in software and hardware. Immutable and indelible data cannot be changed for a determined length of time to protect data against cybercriminal intrusion, internal threats and random disk failures given insufficient redundancy. Any data saved on these instances is protected with the following security measures:

- **Immutability**—Ensures the backup image is read-only and cannot be modified, corrupted or encrypted after backup.
- **Indelibility**—Protects the backup image from being deleted before it expires. The data is protected from malicious deletion.

Lockdown Mode

The NetBackup 8.3 Master Server communicates with storage units to gather immutability and indelibility capability and WORM (write once, read many) minimum and maximum retention period settings. Then the Master Server sets up immutability controls on the storage units and applies the WORM retention period policy. NetBackup software provides backup image management with visual representation of immutable lock, image deletion after the WORM retention period (via the command-line interface, CLI) and honor legal hold on the catalog.

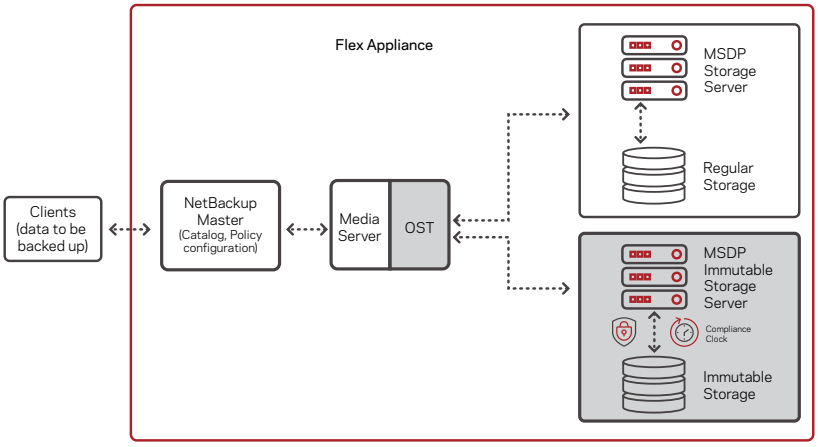

Figure 3. An overview of how the Flex Appliance protects data using immutable storage.

The Flex Appliance runs the immutable storage server to provide WORM capability, retention locks and platform hardening against ransomware and malware threats. Compliance Clock is used for retention period and is independent from OS time. The Flex Appliance has two lockdown immutability modes: Enterprise and Compliance. The Appliance lockdown state can be enabled at any time. You can choose a Compliance-mode or Enterprise-mode MSDP storage container, but you cannot mix them. (See Figure 3.) Table 2 lists the differences between Enterprise mode and Compliance mode.

	Enterprise Mode	Compliance Mode
WORM storage instance creation	Can create WORM storage instances.	Can create WORM storage instances.
WORM storage instance deletion	Any administrator can delete WORM storage instances if there is no immutable data. However, only the default admin user can delete them if immutable data is present.	Any administrator can delete WORM storage instances if there is no immutable data. No one can delete WORM storage instance if there is immutable data.
Lock deletion	Deleting an enterprise lock with the Flex Appliance MSDP solution is a two-step process: 1. The storage "security admin" removes the retention period (existing storage admin is not authorized). 2. The NetBackup admin requests image deletion via the catalog.	N/A
Security level change	To change from Enterprise mode to normal mode, you must first delete all WORM storage instances.	To move down to Enterprise or normal mode, you must first expire all data on the WORM storage instances and then delete the instances.

Table 2: Comparison Between Enterprise Mode and Compliance Mode

During the MSDP immutable storage server creation, you will be prompted with minimum and maximum retention time. The minimum retention period is the shortest amount of time a WORM file can be retained in a storage unit. The maximum retention period is the longest retention period a file can have at the time it is committed to WORM. (See Figure 4.) The retention period configuration can be changed via CLI.

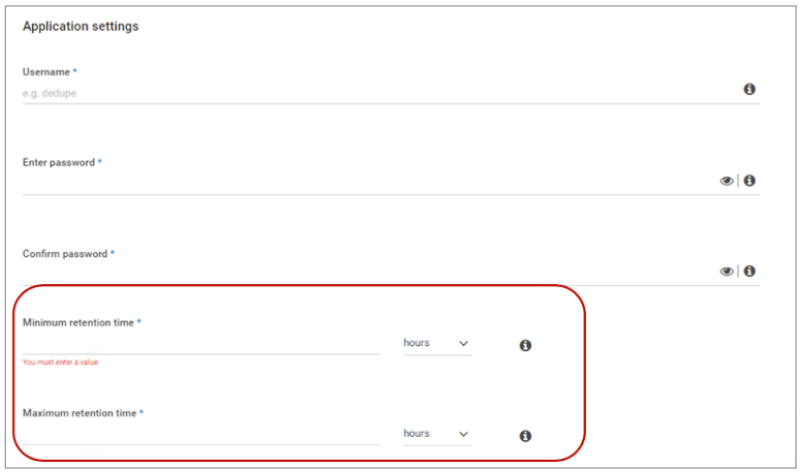

Figure 4. Setting the minimum and maximum retention times when creating an MSDP immutable storage server.

The NetBackup and Flex Appliance immutability solutions provide Cohasset Immutability assessment (in Compliance mode):

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c)
- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d)

Protecting Immutable Storage Servers

The Flex Appliance eliminates root account access to appliance OS and MSDP containers; only the host admin account can log in to compute nodes. Account policies are used to allow elevated users certain administrative commands and access to shell and web UI operations.

The following lists describe the firmware security hardening:

- Boot
  - Eliminate "single user" mode/"rescue mode" boot options.
  - GRUB (GNU GRand Unified Bootloader) menu editing disabled.
- Storage
  - No storage reset (factory reset/reimage allowed).
  - Locked down storage array.

OS Hardening

Flex Appliances use SELinux to harden platform and hosted applications and prevent unauthorized access to immutable storage. SELinux has two modes: enforcing and permissive. Flex Appliances enable SELinux in enforcing mode to set policy rules:

- Root user account privileges are reduced to next to none; only the hostadmin account can log in to compute nodes.
- The Flex Appliance keeps IPS enabled even upon elevation, and the elevated user has most of the privileges.
- Policies to allow all Flex shell and web UI operations.
- Policies to allow elevated users certain additional administrative commands.
- File labeling for platform certificates, tokens, logs and compliance clock device.
- Confine each of the instances and infra services with exclusive access to their storage.
- Policies to enable instances to run systemd and NFS services, access FUSE device and mount NFS/CIFS shares.

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Security Technical Implementation Guide (STIG) is a cybersecurity methodology for standardizing security protocols within networks, servers, computers and logical designs to enhance overall security. Flex Appliances use the STIG template to meet security requirements per the Defense Information Systems Administration (DISA) profile.

Flex Appliances implemented OS hardening with STIG by doing the following:

- Auditing enabled for low-level operations such as OS commands and system calls.
- Ctrl-Alt-Delete reboot disabled.
- SSH root login disabled.
- Maximum 10 concurrent login sessions for the hostadmin account.
- Interactive/login session idle timeout 10 minutes.
- Account lockout for 15 minutes after three incorrect login attempts in a row in the Flex Appliance Shell within 15 minutes.
- Web UI option to enforce requirements for password policy; automatically applies on each Appliance node.

FLEX APPLIANCE MULTI-TENANT ARCHITECTURE

Flex Appliances tightly integrate with NetBackup and simplify your environment by providing a common platform for Veritas applications. You can consolidate multiple NetBackup and CloudCatalyst deployments (domains) on a single Flex Appliance, substantially reducing data center costs and complexity. (See Figure 5.)

The Docker container software runs directly on the Veritas Optimized Operating System (VxOS), which is a Linux-based OS. The VxOS provides the Flex Appliance kernel, runtime library and container engine. Flex Appliances use container isolation and security technology to ensure users are kept separate when using different instances of NetBackup on a single Appliance. Between the kernel features built into the VxOS and the network and data segregation, NetBackup service users are effectively firewalled from one another. This multi-tenant architecture simplifies your NetBackup environment by allowing multiple NetBackup domains to run on this common platform.

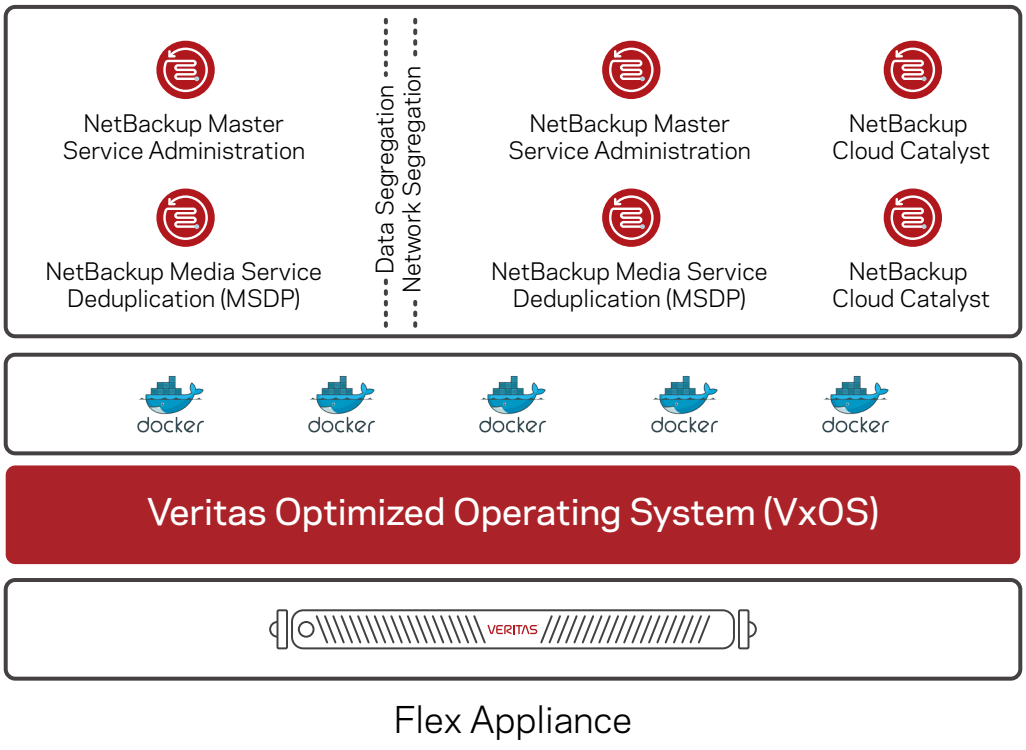

Figure 5. Consolidating multiple NetBackup and CloudCatalyst deployments (domains) on a single Flex Appliance.

REFERENCES

- Flex Appliance Product:
  https://sort.veritas.com/DocPortal/pdf/130821112-136840843-1
- NetBackup Product Documentation:
  https://sort.veritas.com/documents/doc_details/nbu/8.2/Windows%20and%20UNIX/Documentation
- What's SELinux:
  https://www.redhat.com/en/topics/linux/what-is-selinux
- Admin guide:
  https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/index
- MCS for containers:
  https://www.redhat.com/en/blog/why-you-should-be-using-multi-category-security-your-linux-containers
- Crash course:
  https://www.slideshare.net/ffri/mr201406-a-re-introduction-to-se-linux

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

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

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V1108 10/20