VERITAS

How InfoScale Can Help You Secure the Cloud

One of the major concerns when discussing moving applications to the cloud is that of security. The cloud, as most customers implement it, is primarily public. This is part of the allure—applications can be made available to any location at any time. However, this is also part of the problem. Along with the cloud being so accessible to your employees and customers, it is also accessible to those who wish to cause damage. When you are planning security for your cloud implementation, you should include it as a part of the architecture and design of the environment, not just something to be dealt with later.

> “
>
> *The moment something fails - any specific thing - we will be able to provide the same service in a matter of minutes.”*
>
> **Juan David Giraldo Jaramillo,**
> Leader, IT Continuity
> Bancolombia

Security is an area identified by cloud providers as shared responsibility. While the cloud providers are responsible for the security of their hardware implementation, it is ultimately up to the user as to how to secure the software installed on that hardware and how to secure the management consoles. Gartner has stated that “at least 99 percent of cloud security failures will be the customer’s fault.” (Gartner, How to Respond to the 2020 Threat Landscape)

While some security issues are as simple as implementing password protection or role-based access controls (RBAC), there are other issues that are more complex, including data-at-rest encryption (or D@RE), secure logging mechanisms, and the hardening of applications and operating systems. Securing a simple EC2 instance with an S3 bucket for storage can take several hours of work, even before securing the software to be deployed on that instance. Veritas InfoScale provides security features that help you address these issues.

The security features provided by InfoScale include the following:

- Encrypted file systems using high-strength ciphers, including US Federal Information Processing Standards FIPS 140-2 compliance
- Encrypted password files (no open-text storage of passwords)
- Enhanced logging that meets or exceeds the requirements of the new US Cybersecurity Executive Order
- Interoperability with the US Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) to harden operating systems and applications
- Implementation of clustered file systems to securely share data without using network file system (NFS)
- Payment Card Industry Data Security Standard (PCI DSS) compliance
- Penetration testing done by third-parties to ensure security and compliance with the aforementioned standards

The Federal Government has published the Federal Information Processing Standards, or FIPS, which includes the US and international gold standard for encryption—FIPS 140-2. It has been adopted by government agencies and industries around the world as their minimum requirement for encryption. InfoScale’s encryption is fully FIPS 140-2 compliant. This ensures that data is encrypted properly.

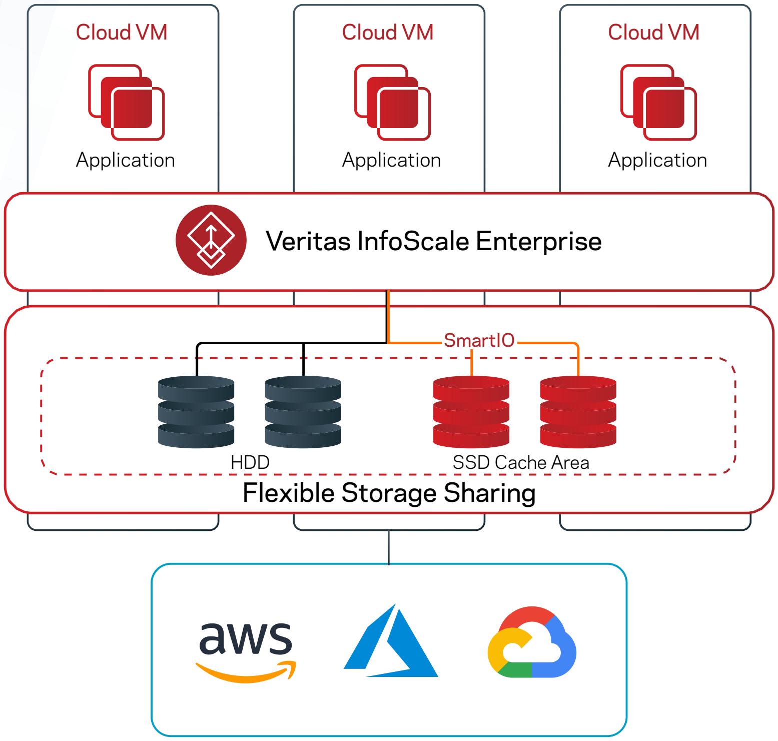

Figure 1. InfoScale clustered file system

Logging of system events, including security events, is important to forensic analysis of cybersecurity incidents that may occur. Having logs stored in a protected manner facilitates this analysis, and can not only help trace attempted cyberattacks, but can also help prepare against current and future cyberattack vectors. Effective secure logging has been recognized as a strong part of cybersecurity, even being included in a recent US Executive Order. InfoScale fully meets the requirements of this Executive Order.

Hardening operating systems and applications ensures that passwords are assigned correctly, vulnerabilities are closed, and attackable vectors are minimized in the compute environments. Leveraging clustered file systems instead of NFS ensures that file access is completely logged, and that unsecure modes of data transport are not being used to share data. PCI compliance means that our security mechanisms meet the stringent standards to handle financial data.

One last thing to mention is that, while security can be easily written into software, it is different to have that security implemented correctly when the software is deployed. Veritas contracts with several outside penetration testing vendors to verify that when InfoScale is deployed according to our best practices, the security features are active and working correctly. It's one extra step we take to provide peace of mind.

Veritas InfoScale can be a trusted partner in securing your cloud environment, just as we are to many in the Fortune 500, the US Government, and the US Department of Defense.

Let Veritas Help You Stay Secure

Learn more about InfoScale at veritas.com.

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 95 percent of the Fortune 100—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.

VERITAS™

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

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