VERITAS | aws

Enhance Data Security and Resiliency with Veritas and AWS

Protect against downtime, data loss, and regulatory penalties with the reassurance of recovery at scale across your data estates.

Executive Summary

Today, cybersecurity is not just about prevention. Data lives everywhere. The attack surface for cybercriminals has grown significantly. Which means more data vulnerabilities, more risk, and more opportunities for data to be compromised—in more ways than ever before. As data grows and sprawls across your on-premises, cloud, and edge devices, protecting it isn't as straightforward as it once was. It is easy to lose control of your data.

Cybercriminals, now savvy and highly organized, have found themselves the perfect environment to gain access, do harm, and cause disruption. They regularly breach even the best prevention solutions on the market, and the numbers prove it. Last year, more than 15 ransomware attacks occurred every second. That is more than 493 million attacks globally.[1]

Old techniques such as phishing are still prominent. Typically, bad actors target unsuspecting employees with sophisticated phishing attacks, often gaining passwords, and placing malware in the environment. The goal is often to gain access to backups or even lay dormant, waiting for the optimal time to attack. Additionally, new and sophisticated methods are gaining popularity. These involve social engineering, and targeting Internet of Things (IoT) devices and infrastructure, as well as software vulnerabilities. Other forms of cyber threats such as malware attacks, intrusion attempts, and encrypted threats are also showing spikes in activity.

To make matters worse, successful cyber incidents also result in extensive downtime, lost revenue, and compliance and governance issues including violations or even hefty fines. Five of the world's key regulators issued more than $7B in regulatory fines last year.[2]

What Can You Do?

This paper focuses on the importance of integrating your Veritas and AWS solutions, adopting a multi-layered cybersecurity strategy to enhance data security, reduce risk, and keep your business resilient. It is designed for business and technical audiences who wish to learn more about how Veritas can help you:

- Protect IT systems and safeguard data integrity
- Detect, monitor, and mitigate threats
- Recover rapidly in the event of a cyberattack
- Reduce downtime and keep applications resilient
- Stay compliant with proactive data governance and control

Introduction: Veritas and AWS, the Dream Collaboration

Building on more than nine years of collaboration, Veritas and AWS are engineering and innovating together to tackle ransomware and cyber threats with a unified approach. Our strategic collaboration provides integrated solutions across our ecosystems with the goal of providing:

- Data security and ransomware resilience with integrated visibility, threat detection, immutability, access management, and orchestrated recovery
- Agile and operationally scalable data protection on AWS
- Reduced compliance risk by delivering unified visibility and agility across on-premises, hybrid, AWS data, and workloads— all with integrated analytics

Resilient, Compliant, and Secure by Default

Veritas is a global leader in secure multi-cloud data management. Simply put, Veritas puts you in control of *all* your data in the cloud, on-premises, and on edge devices. Proper data security requires the right tools. Veritas solutions were developed with business resiliency top of mind, and data security at their core. Secure by default is foundational to who we are as a company. We provide solutions for all areas of data at risk, and we do it at scale.

Veritas offers five co-sell solutions in the market, in addition to public listings on AWS Marketplace. Our collaboration enables the optimal multi-layered cybersecurity strategy that extends across data protection, application resiliency, and compliance.

Let's dive into the details of the three areas of our data risk solutions.

Data Protection: Secure by Default

True resiliency against any unforeseen event such as a cyber incident, natural disaster, hardware failures, or even human error requires that your most important assets—your data and your IT infrastructure—are protected from the unknown and the unexpected. Proper data protection requires the right tools to quickly restore business operations, minimizing downtime and potential damages. With the current cyber threats, optimizing your entire IT for the recovery process is vital. We empower our customers to break down their defensive strategy into three areas: protect, detect, and recover. This is aligned to the broader NIST Cybersecurity Framework.

Protect

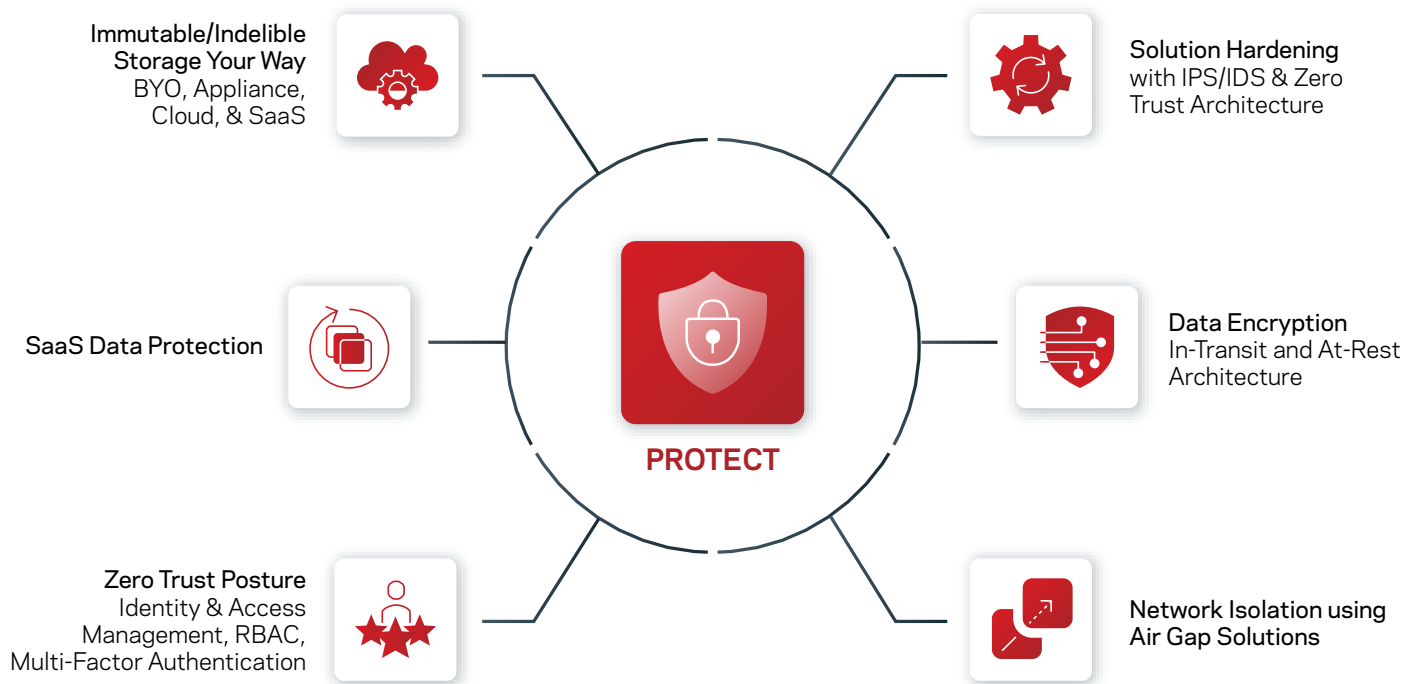Veritas protects and safeguards data integrity in six key areas:

Figure 1. Protection safeguards for cloud

Veritas efficiently protects all data sources, regardless of where the data resides. We store consistent copies of data, across multiple locations (and clouds), with powerful deduplication technology and data lifecycle management solutions to help you save only what you need. Our solutions, engineered with Zero Trust posture, provide valuable safeguards such as identity and access management (IAM), multi-factor authentication (MFA), and FIPS encryption in-transit and at-rest. Extra safeguards help reduce the attack surface, provide additional layers of protection, and prevent large-scale disruption.

Integration with the broader cybersecurity ISV ecosystem is paramount, and enables security operators and DevSecOps teams to better analyze threats and successfully recover from ransomware incidents.

Veritas supports:

- Password access management (PAM)
- Industry-leading key management services (KMS)
- Popular malware scanners
- SIEM/SOAR/XDR vendors that receive data from log-forwarding interfaces
- Integration with SAML 2.0-compliant single sign-on identity providers

Data Immutability and Network Isolation using Air Gap Solutions

Veritas provides extra safeguards with immutable and indelible storage your way, with flexible, storage-agnostic options including BYO, appliance, cloud, and software as a service (SaaS) immutability to keep your data secure and compliant, regardless of location. Intrusion prevention and an independent compliance clock are built in for added security. Veritas also provides a simple, turnkey, pull-based isolated recovery environment or data vault. By isolating data, logically or physically, data is segmented away from the rest of the environment, leveraging the pull method. This ensures a clean copy of data for predictable recovery.

SaaS Data Protection

Veritas provides a unified data management and protection solution, delivering a single, fully managed, and cost-effective platform for SaaS workloads, including AWS. With the *shared responsibility model*, it is up to businesses to protect and secure their own cloud-based data. Our solutions consist of a cloud-native backbone that runs in AWS data centers as a fully managed SaaS deployment. Veritas provides a storage platform for enterprise organizations to centrally protect, analyze, archive, search, tier, recover, and manage all types of SaaS application data—at any scale.

Solution Hardening

Veritas offers a secure data protection platform that provides immutable storage and several hardware security features:

- OS security hardening, including Security-Enhanced Linux (SELinux)
- Intrusion detection system (IDS) and intrusion protection system (IPS)
- Robust role-based authentication
- Locked-down immutable storage
- A secure, robust, and hardened Veritas File System (VxFS)

Detect

Data Visibility

Veritas provides tools for complete visibility of your entire environment including physical, virtual, and cloud workloads ranging from storage, to compute, to every major data protection solution. Cross reporting ensures that no system falls through the cracks. In addition to shining a light on the dark areas of your environment, Veritas solutions provide comprehensive insights; and alerting and reporting correlated across on-premises, cloud, data protection, and storage.

Anomaly Detection and Malware Scanning

AI-powered anomaly detection flags out-of-the-ordinary data and user activity across your data protection environment, and alerts you to suspicious anomalies—in near-real-time. The technology can mine an enormous amount of data, automate monitoring and reporting, and provide actionable insights into what is happening in your environment. Alerts could be things such as unusual file write activity that could indicate an infiltration; it can also detect known ransomware file extensions, file access patterns, traffic patterns, code downloads, access requests, storage capacity surges, external traffic paths, and even an unexpected jump in activity compared to individuals' typical patterns.

Malware Detection

Veritas can help you detect multiple types of malware as part of the data protection workflow, such as the encrypting type and the exfiltration type, providing automated and on-demand scans. The automated malware scanning feature will remove human dependencies and allow AI and machine learning technology to scan for malware. The automated malware scan is automatically triggered by a high anomaly score. Scanning includes unstructured data, Windows, Linux, and VMware. This inclusion is vital because malware often enters your environment in a home directory—typically where large sets of unstructured data exist.

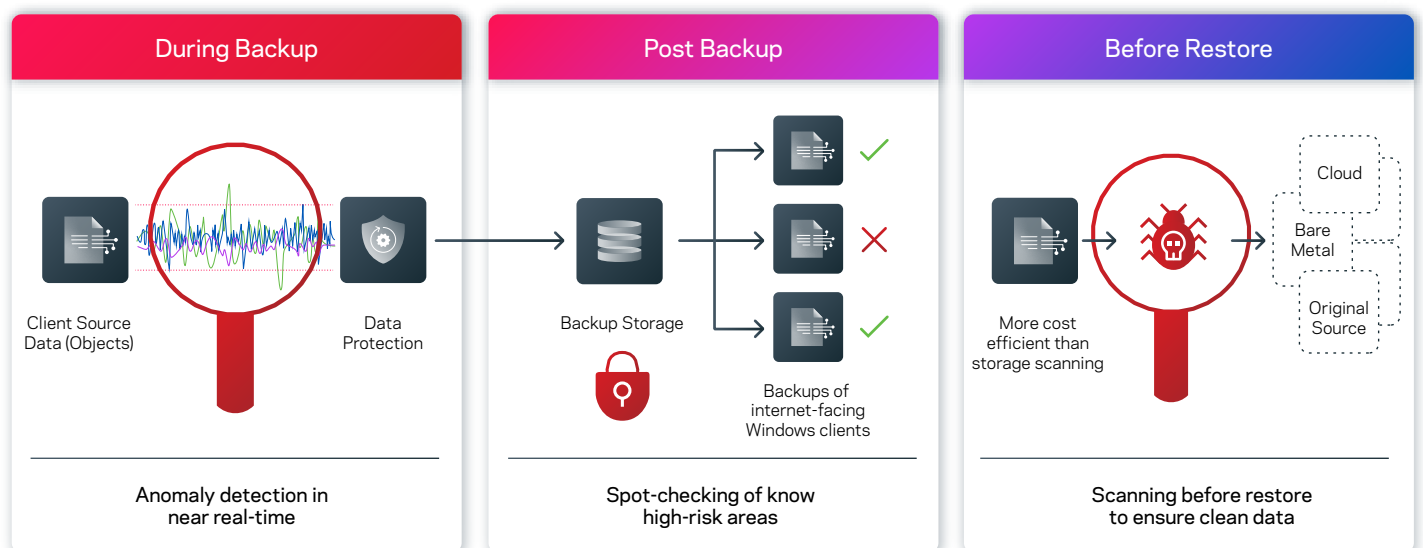| During Backup	Post Backup	Before Restore
Client Source Data (Objects) — Data Protection	Backup Storage → Backups of internet-facing Windows clients	More cost efficient than storage scanning — Cloud / Bare Metal / Original Source
Anomaly detection in near real-time	Spot-checking of know high-risk areas	Scanning before restore to ensure clean data

Figure 2. Malware scanning overview

Additionally, when recovery is necessary, backup images can be scanned using the latest malware signatures. Clear visuals and warning prompts provide awareness of infected backups, ensuring all data restored is clean and unimpacted. This practice is often referred to as restoring to the *last-known-good copy*.

Recover

Orchestrated, Flexible Recovery—at Scale

Veritas resiliency solutions are optimized for flexible, hybrid, and rapid recovery, with the ability to automate and orchestrate complete cross-zone, site, or cloud restoration with the click of a button. And we do it at scale.

Why is flexibility important? Sometimes everything is impacted in an attack, and you may need to recover an entire data center in the cloud and on demand. While other times, you may just need recovery from the object level. Still other times, you may need to recover a portion of your VMs back to production. The flexibility to recover everything—from data, to application, to an entire data center—without restriction—any size, any failure, anywhere to anywhere—is key in the event of an incident. Veritas offers many recovery solutions, including granular file recovery, bulk/instant recovery, instant rollback of VMs, continuous data protection, and bare metal recovery, to name a few. In today's ever-evolving threat landscape, with no cyber incident the same as the next, it is vital to architect an optimized and simplified recovery experience that is without restriction, so that you can get up and running in minutes instead of hours and days—regardless of scale.

Veritas makes it easy and efficient to execute automated non-disruptive DR tests with rehearsals or exercises for all tiers of business, that are automated and assured, while leveraging non-production resources such as network fencing and sandbox environments.

Disaster Recovery for Storage as a Service

Veritas also provides a virtually *air-gapped* recovery vault to ensure geographical and administrative isolation.

Application Resiliency: Multi-Cloud IT Resiliency Orchestration

Veritas helps you meet your SLAs, keep your production data and applications secure, and simplify workload mobility to drive your always-on business and ensure continuity.

Application Availability

Keep your production applications and data secure and recoverable with automated IT continuity across all environments. With the flexibility to run on any platform—including cloud and containers—you meet your SLAs with 24x7 application availability. Veritas resiliency solutions ensure that any uptime SLA is achievable. This includes architectures that span availability zones and regions, other clouds to AWS, and hybrid cloud to on-premises configurations.

With customized agents developed specifically for cloud services, Veritas can manage cloud compute, network, and storage resources required for your infrastructure and applications to be online in the cloud. Veritas resiliency solutions can orchestrate the failover of apps, infrastructure, and data from an IaaS infrastructure operating in other clouds to AWS.
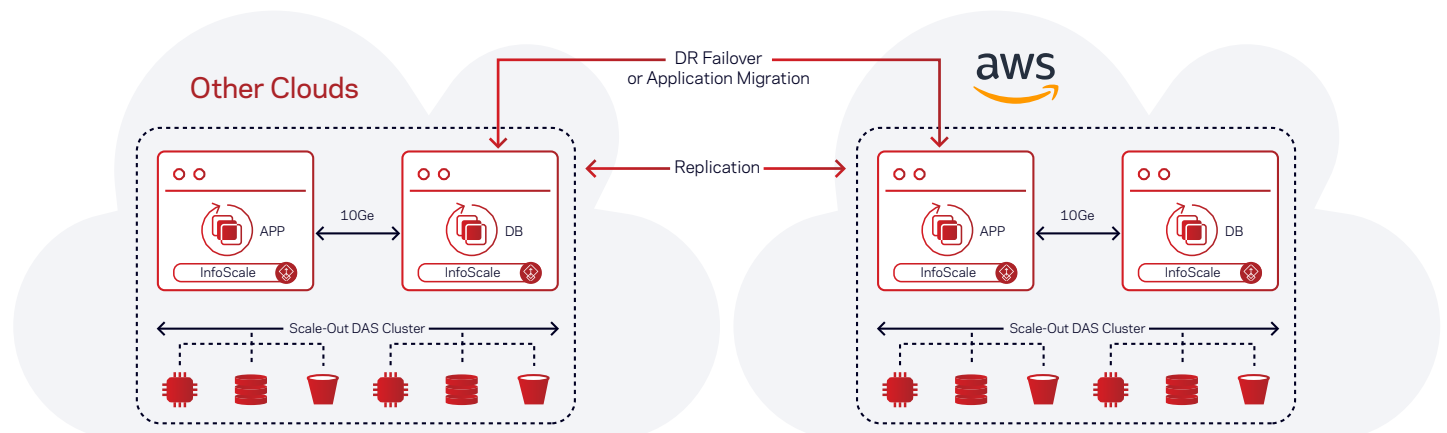

Figure 3. Veritas resiliency solutions orchestrate the failover of apps, infrastructure, and data from an IaaS infrastructure operating in other clouds to AWS

Simple AWS Workload Mobility

The ability to move your applications, data, and workloads seamlessly between on-prem environments and AWS, or between different regions within Amazon S3 is becoming more important. Veritas helps you easily move your applications within public clouds and hybrid cloud architectures. Additionally, our solutions facilitate cloud migration from on-premises systems and between different cloud providers.

For legal reasons, data sovereignty is a growing concern within data mobility. The flexibility of AWS ensures that you can optimize data storage and processing without compromising sovereignty requirements and residency laws. Data mobility enables you to adhere to these regulations by easily moving and managing data to meet requirements. AWS allows you to remain flexible and efficient to move data between environments, different cloud providers, or various regions to optimize and process in compliance with regional laws, and facilitate cross-border data transfer while ensuring compliance regulation. There are other various geopolitical considerations and implications for consumer trust and confidence to consider as well.

Autonomous Recovery Orchestration

Veritas solutions allow you to manage recovery for multitiered applications as a single consolidated entity. This facilitates completely automated recovery of complex, multitier applications that spans multiple systems. This provides easier, faster recovery with minimal application downtime when it matters most.

Data Compliance and Governance: Data Observability

Data governance should be a priority, not an afterthought. Despite this, only 62 %of organizations have implemented a data governance program.[3] With the evolving nature of threats and changes in work environments, managing data has become more complex and significant. For those in roles such as CISO, IT, network, or governance administration, the responsibility lies in tracking, managing, and interpreting data to meet legal and compliance needs.

Recognizing essential information—including what must be protected, retained, or deleted—is critical, especially when recovering from ransomware incidents. Communication monitoring has become more complex with the increase in remote work. Collaboration tools, now fundamental to many organizations, contribute to challenges in collating content, especially as legal actions become more common.

Challenges related to data compliance and governance are numerous, accentuated by today's fast-paced, multi-channel communication. This includes issues such as a lack of leadership in data, limited resources, and tight budgets. Specific industries face unique challenges; for example, financial services firms need to monitor an increasing amount of content across various channels, leading to $1.8 billion in fines for Wall Street firms in 2023 alone, due to improper usage and monitoring.[4]

Global litigation is not only increasing, but also becoming more complex. A Norton Rose Fullbright survey indicates that 44% of firms anticipate more litigation by 2023.[5] The emergence of new communication channels, many facilitated by AWS, adds complexity, necessitating the extraction of relevant content for specific cases.

Managing compliance successfully requires foresight in risk management, and refinement of data procedures. Veritas provides an all-inclusive solution for data governance, compliance, and eDiscovery. This includes automated correction tools and monitoring content across AWS. Veritas Alta™ provides a robust cloud data management solution. Products such as Veritas Alta™ View and Veritas Alta™ Capture offer integration with AWS's platforms, providing a seamless experience in data collection, archiving, and eDiscovery.

By taking a proactive approach, you can stay ahead of data challenges and gain greater control over your data. Leverage your data assets—including those managed with AWS—to foster growth and innovation, knowing that your information is secure and well-managed. Together, Veritas and AWS offer tools that ensure data protection, availability, and compliance across various platforms.

What Sets Veritas Apart

800+
Supported Workloads

Breadth of Workload Support (800+)

Today, data lives everywhere and it is *always* your responsibility to protect it. Our mission is to put you in control of your enterprise data and applications across any cloud, any environment, at any scale. What sets us apart is that our solutions help you safeguard all your valuable data, with a breadth of cloud service and workload support that covers more than 800 workloads. Regardless of where your data is stored, we have you covered.

Cloud Scale Technology

In addition to the data security and resiliency solutions listed above, Veritas provides elastic Cloud Scale Technology—a cloud-native option that delivers enterprise data protection services. This new generation architecture leverages artificial intelligence (AI), machine learning (ML), containers, and microservices, along with web scale IT techniques such as service elasticity, hyper-automation, and multi-tenancy. This technology also powers our AI-based anomaly detection.

Veritas REDLab

Veritas built an isolated REDLab to study ransomware and malware firsthand. In this lab, Veritas regularly simulates and executes real ransomware and malware infections on our products. This provides Veritas with many advantages to research and study the latest cyber incidents. The REDLab team regularly assesses features that aid in detecting malicious code or intrusions, protecting the backup repository and infrastructure, and speeding up recovery. Veritas REDLab has proven to be extremely valuable in securing the reliability of our solutions during a ransomware incident, and providing a roadmap for future innovations.

Take Control with Veritas and AWS

Together, Veritas and AWS ensure you can meet the recovery objectives required for your business, whether in response to human error, natural disasters, or cyber incidents such as ransomware. Simply put, Veritas and AWS help you take control of your data, and keep your mission-critical data and applications online, resilient, compliant, and secure—whether your data is on-premises or in the cloud.

Learn more about how to strengthen your cyber resiliency with Veritas and AWS.

1. "SonicWall Cyber Threat Report Casts New Light on Shifting Front Lines", Threat Actor Behavior, 2023
2. "Regulators Slapped Industry with Record Fines in 2022, SEC in the Lead", Finance Magnates, 2023
3. "The Strategic and Evolving Role of Data Governance in 2022 and Beyond", Mega International, October 2022
4. "Wall Street hit with $2 billion in fines over employees using WhatsApp and other unauthorized messaging apps", Fortune, 2022
5. Norton Rose Fullbright survey, 2023

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

V1946 08/23