VERITAS

Cloud Data Security Best Practices

Implement these 10 best practices with your cloud teams today.

In recent years, the frequency of cyber security attacks and the sophistication of cyber criminals has increased dramatically. Last year, more than 19 cyber attacks occurred every second. That's more than 623.3 million attacks globally. It is safe to say that cybercrime is everywhere. There are no safe countries, industries, or companies anymore. Additionally, long gone are the days of safe technologies. Cloud is now the most common attack vector for cyber criminals, according to Tech Targets Ransomware Preparedness Research Report, published in March 2022[1].

Cyber attacks are also not limited to data or systems exclusive to any one type of infrastructure, be that on-premises, in the cloud, in multiple clouds, or all the above. Everything is now a target. Old techniques such as phishing are still prominent, but new, sophisticated methods involving social engineering, targeting internet of things (IoT) devices and infrastructure, as well as software vulnerabilities, are gaining popularity. Additionally, 2022 has experienced a spike in other forms of cyber threats: malware attacks are up 11 percent, intrusion attempts are up 19 percent, crypto-jacking attacks are up 30 percent, and encrypted threats are up 132 percent[2]. The bottom line is that cyber security is now everyone's concern.

Cloud-native capabilities meant to protect the organization's data and systems are nowhere near robust enough to handle today's threats. That's why it is critical for all IT teams, especially those using cloud technologies, to realize they can't achieve true business and operational resiliency with standard cloud-native security tools. Instead, all teams must prioritize and adopt a multi-layered cyber security strategy that extends into their cloud technologies to keep data safeguarded, keeping the business resilient and the teams in control. The best cloud data security solutions offer 99.999 percent uptime. Here are Veritas' top 10 recommended best practices to implement with your cloud teams immediately:

Cloud Data Security Best Practices

1. Understand the shared responsibility model and know your responsibilities in the cloud.

The shared responsibility security model varies according to each service provider and differs while using IaaS or PaaS. A clear-cut shared responsibility model ensures there is no gap in the security coverage of a system. Otherwise, obscurities in your shared responsibilities may leave certain areas of the cloud system unguarded and exposed to external threats.

2. Gain full infrastructure and data visibility across your entire IT ecosystem.

For data to be secure, compliant, protected, and resilient, you must have complete visibility. No dark data allowed. Cyber criminals are looking for your weakest links, the dark corners where there may be limited security or oversight in your environment, and they know that it is difficult to keep an accurate inventory of all applications and data. Shining a light on all the dark data in your environment, and ensuring that you know where all your data and sources are, provides valuable assurance that you are in control.

3. Evaluate built-in and cloud-native data security tools.

Every organization should ask their public cloud providers detailed questions about the security measures and processes they have in place, and scrutinize them. It is easy to assume that the leading vendors have security handled, but the methods and procedures they use vary drastically. Do you know how your data is being accessed and stored? Do you understand the provider's disaster recovery plan? What is their protocol for security incidents, and what level of technical assistance is available in the event of a data breach? Within their organization, who has access to your data stored in the cloud and where servers reside geographically? If any of these answers are unclear or unsatisfactory, it's best to move on to a more reputable provider.

4. Adopt a zero trust posture.

Adopting a companywide zero trust mindset has been proven to reduce the risk of a devastating attack. Further, if a breach happens, it reduces the attack surface or the blast radius because it provides multiple layers of security that minimize impact. For example, once in your systems, cybercriminals often move across your environment searching for business-critical data, confidential information, and backup systems. Strengthening your identity and access management (IAM) with multifactor authentication (MFA) and role-based access control (RBAC) for users, tools, and machines, will limit access to highly sensitive data and backups. Only users that need to access the data should be permitted. Password hygiene is a top priority. With strong IAM controls, privilege controls, hardening, and secure hardware all built on zero trust, access to these areas is prevented.

5. Encrypt data—in transit and at rest.

A key part of any cloud security strategy is understanding and managing your shared responsibility of data protection from an encryption point of view. Ensuring that your data in transit is encrypted from cloud and storage provider settings is essential. As a premium storage provider, Veritas offers encryption on storage for optimal data protection. If cybercriminals get your data, encryption protects it from being exploited.

6. Implement immutable storage and network isolation using an air gap solution.

One of the best ways to safeguard your data against ransomware is to implement immutable and indelible storage with an internally managed compliance clock, and set up an isolated recovery environment (IRE). Immutable and indelible storage, which ensures that data cannot be changed, encrypted, or deleted for a determined length of time (or at all) prevents data tampering and unauthorized access. Isolated recovery environments and air gap solutions isolate data, logically or physically, to help ensure that data is segmented away from the rest of the environment.

7. Adopt anomalous activity detection and malware scanning.

Implement tools that detect, ideally monitoring for abnormal behaviors and mitigating malicious activity of both data and user activity. Essentially, it is vital to implement concrete and automated measures to alert if anything happens out of the ordinary in your ecosystem. This could include anomalies such as unusual file write activity, which could indicate infiltration; but it could also include detecting known ransomware file extensions, file access patterns, traffic paths, or even an unusual jump in activity compared to typical patterns. Being notified immediately of anything out of the ordinary provides a valuable advantage to act or mitigate quickly. Additionally, these tools can help to regularly conduct cyber threat hunts.

8. Optimize your environment for recovery and rehearse regularly.

The best defense is to make sure that recovery is always an option, with flexible, hybrid, and rapid recovery that can be performed in minutes, even at scale. This is achieved by having as many recovery options as possible, including alternative recovery sites such as secondary data centers, or even standing up an entirely new data center in the cloud on demand. Don't forget to test early and test often—you are only as good as your last test.

9. Understand data duplication and gain an accurate picture of your data footprint.

It is a good idea for corporations to take steps to minimize the data that they entrust to their cloud service provider. Step one is to refine business practices to collect only the data required. Next, understand if your data is being duplicated, and if so, where. Lastly, optimize for sustainability goals. Storing data in the cloud costs energy, and with some cloud providers, that energy comes largely from burning fossil fuel. Others, such as Google Cloud, are front runners in powering cloud data centers with solar and other renewable energy sources. The bottom line, storing redundant, obsolete, or trivial (ROT) digital data is environmentally irresponsible, in addition to being costly and inhibiting performance. Solutions that provide the visibility needed to optimize every aspect of data storage, deduplication engines, and resource consumption in the cloud should be prioritized.

10. Educate and empower employees.

Part of regular security hygiene includes educating and empowering your employees to play a proactive role in your organization's security practices. In today's cyber threat environment, it is vital to ensure that you keep your software and tools up to date. Make sure your employees implement these regular updates and upgrades. Continuously train and update your teams on security best practices and protocol, they are often the gateway to a cyberattack. Modern phishing attacks and social engineering are now so sophisticated they can often fool even seasoned security professionals. Focus on training employees to identify phishing and social engineering tactics, build strong passwords, browse safely, use MFA, and always use secure VPNs, never public Wi-Fi. Also, ensure all employees know what to do and who to alert if they fall victim.

Cloud data security requires a trusted partner and simply stated, Veritas is here for you. We put you in control of your multi-cloud and help you meet your end of the shared responsibility model. No one supports more immutable storage options for primary backups with deduplication than Veritas. Only Veritas can automate and orchestrate the recovery of entire business services, including multi-tiered applications and all their dependencies, not just the data. Keep the cloud-native experience your business requires, but gain better security, hardened defense against ransomware attacks, and autonomous operations with Veritas. Protect your cloud data the right way while gaining confidence in the face of threats while reducing IT costs.

To learn more best practices for cloud data security, visit https://www.veritas.com/solution/cloud-data-security or request a call from our sales team.

[1] SonicWall, "SonicWall Threat Intelligence Confirms Alarming Surge in Ransomware, Malicious Cyberattacks as Threats Double in 2021," February 17, 2022. https://www.sonicwall.com/news/sonicwall-threat-intelligence-confirms-alarming-surge-in-ransomware-malicious-cyberattacks-as-threats-double-in-2021/

[2] Veritas and Vanson Bourne, "The Vulnerability Lag." https://www.veritas.com/content/dam/Veritas/docs/reports/GA_ENT_AR_Veritas-Vulnerability-Gap-Report-Global_V1414.pdf

VERITAS

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

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

V1621 08/22