RACKTOP

10 Must-Have Cyberstorage Features

BUYER'S GUIDE

The emerging cyberstorage market offers many options for deployment. When evaluating cyberstorage and cyber secure storage solution providers, we recommend that you ask vendors to demonstrate the following features and capabilities so you can validate claims concerning a product's ease of use and typical response time.

1. Real-time active defense against data theft and data-oriented attacks

Active defense is the single most important Cyberstorage feature. Vendors who claim to have this capability must be able to demonstrate how it works in real time. The solution should not be reliant on logs or third-party integrations that delay response time and decrease overall effectiveness of detecting and stopping attacks. Many NAS and file server protections claim to stop ransomware by detecting changes in data itself, but this approach fails to detect user or application context, which is derived from pattern behavior. With data theft being the most prominent attack (91%), the data, users of the data, and the external factors which contribute to that activity must be considered in order to detect and stop advanced ransomware, insider threats, and other advanced data oriented attacks.

2. Quick recovery and restoration

In the event of a cyber incident, can the vendor's solution identify what files and user accounts were impacted? Will it automatically help you restore to the correct pre-attack version from backups or snapshots? Is it a manual or automated process? What recovery point objective (RPO) and recovery time objective (RTO) have their customers met? Is it minutes, hours, or days?

3. Zero trust-based data access

Traditional storage systems use implicit access controls for data access by trusting user credentials and permissions. But since most attacks stem from credential misuse or compromise, implicit ACL based controls are no longer sufficient. Vendor solutions should implement a zero trust based system for continuously validating and verifying a user or application's activity beyond the access control alone, much like your credit card company does for transactions. Vendor solutions should implement additional layers of verification and validation such as attribute based access, credential abuse detection, and real-time usage behaviors.

4. Real-time user behavior analytics

Identifying potentially destructive or malicious behavior in real time is critical for preventing your data from being lost, damaged, or stolen. If the vendor can't demonstrate the ability to investigate user activity logs in real time, the response will be too slow and your data could be stolen and permanently destroyed.

5. Insider threat detection and prevention

33% of data breaches originate from insiders. Can the vendor demonstrate how they will stop a privileged user from stealing data, launching a destructive data-oriented attack, or recover from an attack?

6. Incident management

How does the solution log administrator activities and provide communications to stakeholders and management? Does it provide a record of attack source, actions and remediation? Does it have an incident management workflow that can tie into your existing Security Operations Center (SOC) and infrastructure tools and communication platforms like Service Now, Microsoft Teams, and Slack?

7. SIEM integration

To find the root cause of an issue, does the solution require exporting data to an external SIEM or log analysis tool?

8. Audit-ready compliance reporting

Look for a customizable solution that can complete this task on schedule and with the click of a button so you can participate, customize, and report on demand.

9. Cyber resiliency

Keeping operations online even while under attack and quickly restoring to a pre-attack state is critical to organizational operations. Will the solution block client IP's and client accounts that were implicated in the attack? If it only blocks one or the other, it will likely be ineffective at shielding data from the attack because the adversary will use multiple machines and accounts to continue the attack.

10. Five 9's data availability

Many storage vendors talk about system uptime with high availability (HA) features, but with the modern data oriented attacks, system availability and data availability are no longer one in the same. Organizations that suffer a ransomware attack often have less than one 9 of data availability. In other words, the system is online, but the data is not usable. Vendor solutions should disclose and demonstrate how many 9's they can maintain for *data availability*, where data is 100% intact and available for users and applications.

Experience End-to-End Cyberstorage with the BrickStor Security Platform

Protect data at the core, in the cloud, or at the edge. RackTop's solution provides unique capabilities of the first unified cyberstorage solution with active defense. Simply enroll in the complimentary Jumpstart program to validate the technology in your own environment.

Start protecting your data from cyber threats today!

www.racktopsystems.com/jumpstart