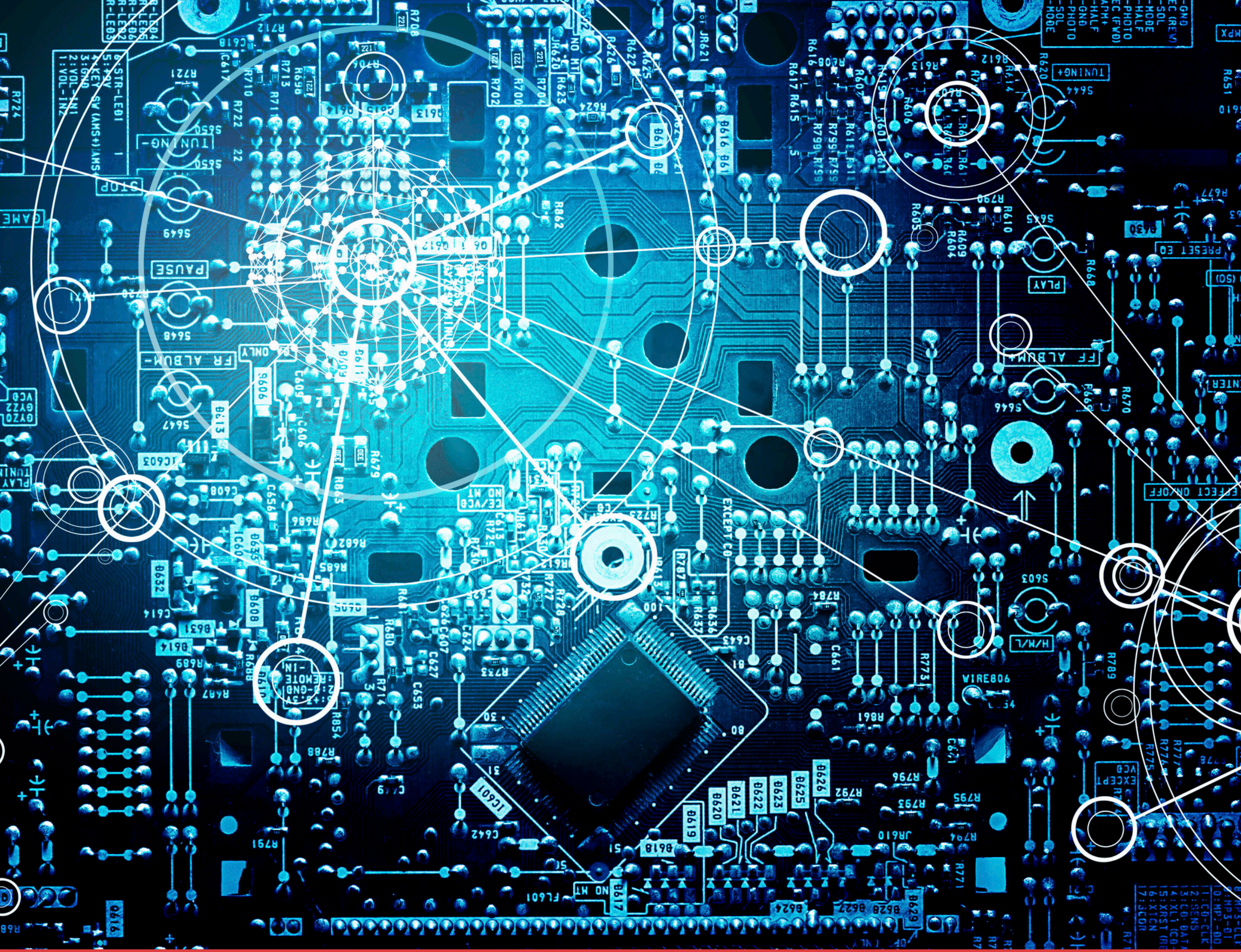


PRIMARY STORAGE SHOULD SECURE ITSELF

By George Crump

Storage Switzerland, LLC

RACKTOP®

Primary Storage Should Secure Itself

News of another data breach is becoming all too common of an occurrence. The cost to the organization is not just its reputation but increasingly results in punitive fines. The European Union's General Data Protection Regulation (GDPR) set a new standard in monetary punishment, with some fines expected to exceed $20 million for exposure. These realities are leading organizations to start investing in various defenses to cyber-threats, with ransomware being the most significant form of threat followed closely by unauthorized access to an organization's data. The problem is most of these investments build a fence around the data center instead of securing the organization at the root of the problem, the primary storage infrastructure.

Encryption is a primary line of defense. Yet ransomware also uses encryption to lock an organization out of its data. The organization uses encryption to make sure that data accessed by unauthorized means is secure but it also must defend against ransomware's use of encryption to force the organization to pay to regain access. Data can be encrypted at two points, either as it travels across a network or while it is stored on the system.

The Problem with Bolt-on Encryption

Storage systems usually have encryption added after the fact. It is either implemented as an encrypted file system, which lies on top of another file system, or it is applied to specific components of the system by using encrypted drives, for example. The problem is these methods impact performance or do not provide complete security. For instance, after the fact installation means data movement to that file system, has to happen manually. Users need to remember to move data to it and there is a concern about how much time it will take to copy data already in place. An encrypted drive is secure only after removing the drive from the hardware.

What IT needs is a feature-rich, primary storage system that has full-time encryption as an integral component. This type of system encrypts data from the start and always keeps data encrypted. The integration of encryption into the storage software enables delivery of encryption features across all the protocols, which the storage system supports. The end result is a unified encryption strategy deployed across block, file and object.

Solving the Super User Account Security Problem

Encryption by itself is not a magic pill. If a special user account, especially a superuser account, is compromised and accessed, then the data is readable by that account even if it is encrypted. Special user accounts can and should be limited, reducing risk exposure.

The way to limit the exposure of these accounts is to eliminate the need for them. The primary storage system should be able to protect itself, so there is no need for these special accounts. For example, the storage system should be able to replicate data to another system, create snapshots for point-in-time recovery and make sure those snapshots are immutable, protecting them from ransomware. Ransomware can't encrypt data if it can't rewrite it.

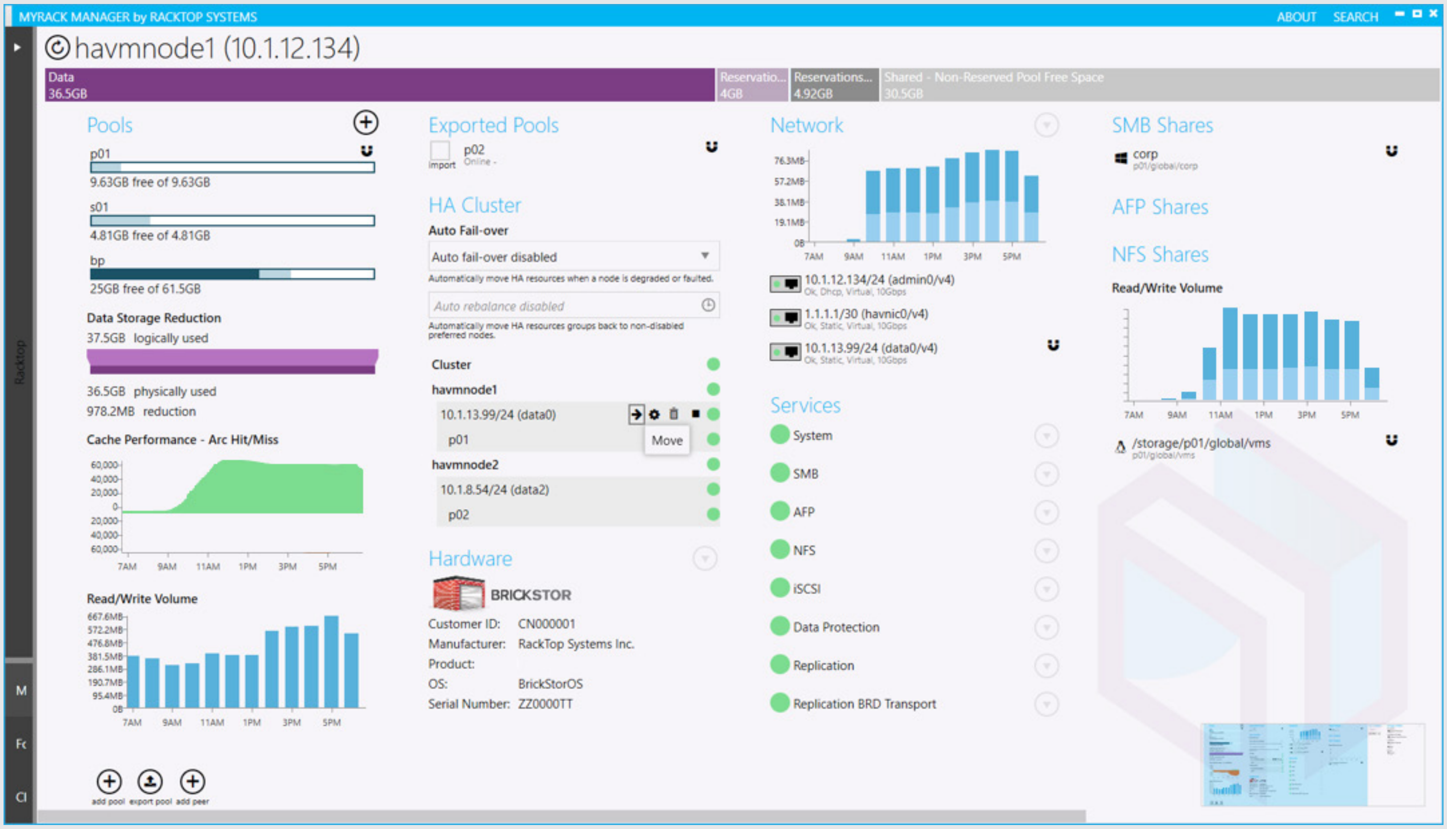
The system should be able to archive these replicas, as well as old data, to a tertiary store, with cloud storage being an ideal target.

Combining the ability for primary storage to provide both inline encryption and to protect itself means the copies made for protection and archive purposes are also encrypted and secure. And the need for special user accounts is reduced.

Implementing a Threat Assessment Process

At some point, an attack will come, and the organization needs the ability to detect, respond to and, if necessary, recover from it. The storage system also should have the ability to report on data and access exposure as well as providing user behavior tracking to identify anomalies as quickly as possible.

RACKTOP SYSTEMS'
DATA MANAGEMENT INTERFACE



MYRACK MANAGER by RACKTOP SYSTEMS

havmnode1 (10.1.12.134)

Data 36.5GB | Reservatio... 4GB | Reservations... 4.92GB | Shared - Non-Reserved Pool Free Space 30.5GB

Pools

p01 — 9.63GB free of 9.63GB

s01 — 4.81GB free of 4.81GB

bp — 25GB free of 61.5GB

Data Storage Reduction

37.5GB logically used

36.5GB physically used

978.2MB reduction

Exported Pools

p02 Online -

HA Cluster

Auto Fail-over: Auto fail-over disabled

Automatically move HA resources when a node is degraded or faulted.

Auto rebalance disabled

Automatically move HA resources groups back to non-disabled preferred nodes.

Cluster

havmnode1
- 10.1.13.99/24 (data0)
- p01

havmnode2
- 10.1.8.54/24 (data2)
- p02

Hardware

BRICKSTOR

Customer ID: CN000001
Manufacturer: RackTop Systems Inc.
Product:
OS: BrickStorOS
Serial Number: ZZ0000TT

Network

10.1.12.134/24 (admin0/v4) — Ok, Dhcp, Virtual, 10Gbps

1.1.1.1/30 (havnic0/v4) — Ok, Static, Virtual, 10Gbps

10.1.13.99/24 (data0/v4) — Ok, Static, Virtual, 10Gbps

Services

- System
- SMB
- AFP
- NFS
- iSCSI
- Data Protection
- Replication
- Replication BRD Transport

SMB Shares

corp — p01/global/corp

AFP Shares

NFS Shares

/storage/p01/global/vms — p01/global/vms

Introducing RackTop Systems

RackTop Systems' BrickStor is a turnkey storage system designed to provide secure, high-performance storage. It is available as a software-only solution, but most of their customers opt for a turnkey appliance that further enhances security. Unlike other security solutions, BrickStor is a complete, feature-rich solution. It offers all the capabilities of a typical primary storage system like snapshots and replication as well as robust protocol support like NFS, SMB, iSCSI and S3 (object).

BrickStor has two capabilities that make it unique among its competitors. First, it has complete data management features that include intelligent data movement. However, BrickStor's data movement is not limited to tiering within the system. It can also tier old data to any S3 compatible object store or cloud, like Amazon S3. The inclusion of archiving to a secondary storage tier means that RackTop provides its customers with complete archive functionality.

The customer is able to use the data management functionality to drive down storage costs. Because access to data is within a single logical operating environment, access to old data is both transparent and seamless. Retrieval times from local on-premises high capacity storage or object storage should go unnoticed by users and even most external cloud accesses should be complete before the users experience a loss in productivity.

The result of this integrated data management is that not only can organizations drive down primary storage costs, they are also able to further limit exposure. The system can automatically store old data in the cloud making it harder for an external party to gain access to it. Additionally, all data stored in the cloud is encrypted.

BrickStor's second unique capability is the built-in security features. It provides a multi-layer encryption function and includes key management. Encryption is inline and always-on, securely storing data. Additionally, because of the integration of encryption into the storage software, RackTop delivers the feature without impact to user performance.

As part of its security capabilities, it includes auditing, immutability and full ransomware protection and recovery. It also provides complete user auditing and access analysis allowing the organization always to be aware of any data exposure issues. In short, RackTop addresses all of the previously mentioned security concerns.

StorageSwiss Take

Most primary storage systems just focus on providing performance to production applications. A few will also include robust data protection functionality. RackTop is unique in that it also provides data management and integrated data security. For organizations looking to refresh their storage systems and address concerns about data security while lowering overall storage costs, thanks to its robust data management, RackTop deserves strong consideration.

The Firm

Storage Switzerland is the leading storage analyst firm focused on the emerging storage cataegories of memory-based storage (Flash), Big Data, virtualization, and cloud computing. The firm is widely recognized for its blogs, white papers and videos on current appraoches such as all-flash arrays, deduplication, SSD's, software-defined storage, backup appliances and storage networking. The name "Storage Switzerland" indicates a pledge to provide neutral analysis of the storage marketplace, rather than focusing on a single vendor approach.

About Our Partner

RackTop Systems is a leading provider of high-performance Software-Defined Storage embedded with advanced security, encryption and compliance that empowers both government and commercial organizations. With an intuitive, easy-to-use interface, RackTop's flagship product, BrickStor, is an all-in-one data storage and management platform that protects sensitive data from cyberattacks while meeting internal and regulatory compliance requirements. Fully configurable and flexible to handle growing data needs, the platform enables enterprises to easily create shared, distributed storage resources—reducing cost and complexity, optimizing operations and improving security. Headquartered in Fulton, Maryland, RackTop was founded in 2010 by veterans of the U.S. intelligence community who have been solving the most complex data and security problems for more than two decades. RackTop's technology has been deployed at numerous organizations in a variety of industries worldwide, including government/DoD/public sector, media/advertising and entertainment, financial services, healthcare, higher education and life sciences, among others.

For more information, visit www.racktopsystems.com and follow on Twitter @RackTop.

The Analyst

George Crump is the founder of Storage Switzerland, the leading storage analyst focused on the subjects of big data, solid state storage, virtualization, cloud computing and data protection. He is widely recognized for his articles, white papers, and videos on such current approaches as all-flash arrays, deduplication, SSDs, software-defined storage, backup appliances, and storage networking. He has over 25 years of experience designing storage solutions for data centers across the U.S.