Everything you wanted to know about securing your storage...

but were afraid to ask

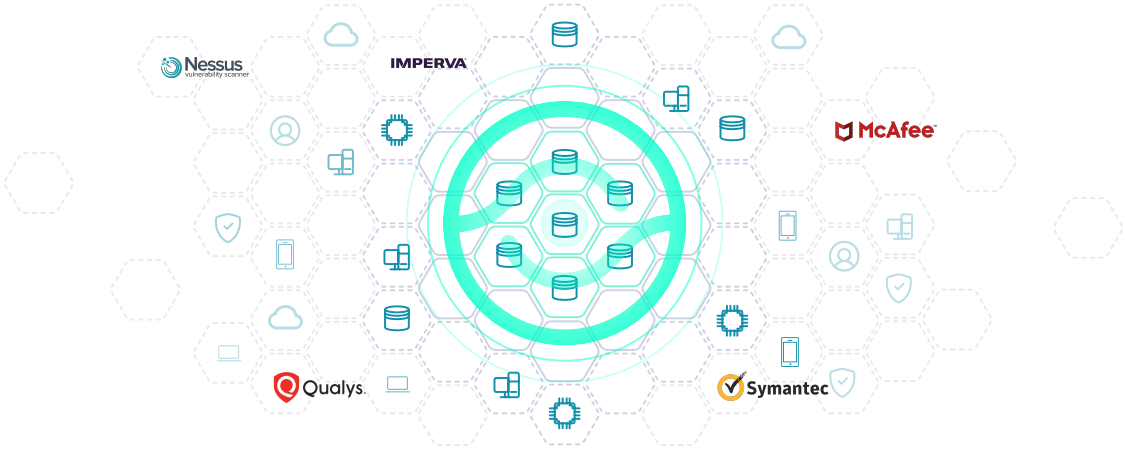
CONTINUITY

Background

Data-targeted attacks have been in the public eye for quite a while now, with Ransomware damage costs predicted to grow more than 57X from 2015 to 2021.

Growth is propelled not only by the surge in the number of cybercrime groups specializing in ransomware, but to a large extent, also by the continual increase in attack sophistication. ransomware has evolved into a fully-fledged industry, with competing groups that continually introduce new capabilities and techniques.

Some of the new trends in data crimes, such as data leak, threat of data exposure and shaming techniques have ignited the media attention, though other, potentially even more devastating are still not widely discussed, which we'll attempt to correct here.



My prediction for the remainder of 2021 is that there will continue to be more ransomware attacks. It's not exactly a radical statement. I didn't see a ton of it last year, during COVID, but this year it has been absolutely crazy. I can't tell you how many emergency incident response phone calls and Teams meetings I've had this quarter. I've probably had as many this quarter as I had the whole of last year. So my prediction for this year is much more of the same.

serco

Garrett Smiley
CISO

The Security gap explained

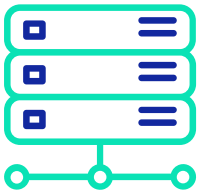
IT is a combination of infrastructure, configuration, and code – all of which are susceptible to attack (admittedly cloud technologies can sometimes blur the boundaries between configuration and code, or between configuration and infrastructure).

Zooming in on infrastructure, reveals a further division into compute, network, and storage (some also add facility and environmental controls). Significant progress has been made over the last two decades in increasing the security of the network, compute, and code layers.

However, security innovation for storage and data protection remains low, especially for solutions aimed at the large enterprise. This is under the assumption that they are far too deep in the datacenter core to reach, and far too obscure to pose a meaningful attack surface.

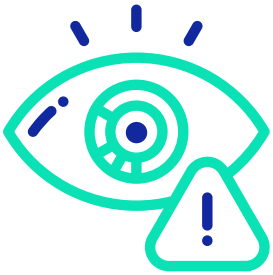
WITH THE ASSUMPTIONS NOW PROVEN WRONG BY CYBER CRIMINALS, CISOS NEED TO CLOSE THE GAP.

Unlike an attack on individual endpoints or servers, which can be highly inconvenient to a large enterprise, one that targets central storage or backup can be ruly devastating. This is because a compromise of a single storage fabric can bring down thousands of servers.



Furthermore, while recovery of an individual server is relatively straightforward, recovery of a storage fabric is a complete unknown to most CISOs.

Finally, far too often, the actual data, and its recovery copies are kept without sufficient isolation. Think about storage arrays that keep both the primary data and snapshots, or admin accounts that are used to manage both servers and backup.



The gap is also cultural – many CISOs and their teams are not sufficiently familiar with storage, and many storage professionals are not sufficiently security savvy. Security and storage teams are not as versed in working together, as, say, security and network, or security and server teams.

Regulation and industry awareness

Regulators are increasingly paying attention to systems and data recovery. In response, organizations, particularly in the banking & financial services sector, are investing more and more efforts in defining, measuring, and continually improving security controls for data storage and data protection.

Industry awareness is also steadily growing. In 2020, NIST released a Special ublication 800—209, titled "Security Guidelines for Storage Infrastructure", that places significant emphasis on securing and protecting data against attacks.

Most ransomware attacks still happen due to vulnerabilities: not enough patch management, not following basic security requirements, and not having basic controls. All of this leads organizations to fail.

The hackers are after our data. In a bank, data is money. This is why I'm a big believer in securing storage

standard chartered

Erdal Ozkaya
Former CISO

The top 4 storage security challenges

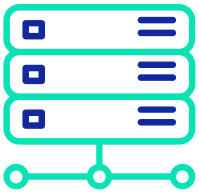
NIST SP 800-209 provides a detailed overview of storage systems threats, risks, attack surfaces and security recommendations.

While some recommendations are similar to those available for the entire IT infrastructure (e.g., physical security, authentication and authorization, change management, configuration control) other are unique to storage systems, including storage networking (which can be radically different than server networking), and areas of operations related to data protection, data isolation, restoration assurance and encryption.

The top 4 storage security challenges include:

Use of vulnerable protocols & protocol settings

Adversaries can use such configuration mistakes to retrieve configuration information and stored data, and in many cases, can also tamper with (e.g., modify, destroy, lock) the data itself, including the copies used to protect the data.

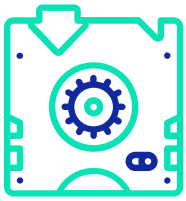


Unaddressed CVEs

Each CVE details the possible exposures and outcomes it presents – and these span a rather wide range. Among common risks include the ability to exfiltrate files, initiate denial-of-service attacks, and even take ownership of files and block devices.

Access rights issues (over-exposure)

Incorrect access rights management, can at best lead to data exposure, and at worst to compromise of the data itself and its copies, and in some cases, of the operating systems of the hosts that use the storage



Insecure user management and authentication

Incorrect and insecure configuration can allow adversaries to take full control over the storage device, up to, and including exfiltration and destruction of the data and its copies.

Storage is where our core data is stored. And so, vulnerability management, configuration management, and ensuring a strong policy around the governance of all storage devices are absolutely critical

HSBC

Sunil Varkey
Former Global Head of
Cyber Security Assessments

Summary and recommendations

In a large enterprise, data storage tends to be a security blind-spot. Analyzing data storage and data protection security posture is a new skill that IT teams must adopt in order to deal with emerging cyber-security threats.

It is recommended to evaluate existing internal security processes to determine if they cover storage infrastructure to a sufficient degree. Some questions you could ask, include:

- Do our security policies cover specific storage, storage networking, and backup risks?
- Are we evaluating storage infrastructure security on an ongoing basis?
- Do we have detailed plans and procedures for recovery from a successful attack on a storage or
- backup system? Do we test such procedures?
- How confident are we that our storage systems are sufficiently hardened?
- How confident are we that we can recover from a successful ransomware attack?

If needed, third parties and vendors could be consulted, or invited to be involved in such evaluation. Based on the findings, we recommend:

Determining if knowledge gaps exist, and building a plan to address them

Improving security program to address identified gap

Considering the use of automation to continually evaluate the status of storage infrastructure security, in order to proactively address risks.

Finally, we encourage you to learn more about storage security. A good start could be the **NIST Guide for Storage Security** – co-authored by Continuity Software. This guide provides CISOs and Heads of Storage with an overview of the evolution of the storage technology landscape, current security threats, and a set of practical recommendations.


CONTINUITY