IBM Technology Expert Labs
Whitepaper

Automate, Detect and Recover from Cyber Threats Faster with IBM Storage Defender

By Parwathi Hettinga-Ayakannu and Brian Hansford

The question is not “If ?”, but rather, “When?”

Data breaches in the form of cyber threats, ransomware and other attacks have only been increasing. The concern for most organizations was previously *if* the organization would be attacked; now the reality is, *when* will the organization be attacked? According to the IBM Security® Cost of a Data Breach Report 2022[1], 83% of the organizations studied in the report had more than one data breach. The average total cost of a data breach globally is at an all-time high, at $4.35 million per data breach. This is up 12.7% since 2020. Furthermore, 11% of all data breaches are ransomware attacks, which cost, on average, $4.54 million, *which does not include the ransom paid.*

The United States has the highest average cost per data breach globally, at $9.44 million. Aside from the monetary cost of the breach, there is the additional implied cost of the security and integrity of the compromised data. This is not just inherent to the company that holds the data; instead, it impacts those whose data has been compromised. This can include Personally Identifiable Information (PII), such as Social Security Numbers, addresses, dates of birth, et. al. It can also include healthcare records, financial information, and so on. This loss can affect both those impacted, as well as the enterprise itself, as the customers will lose trust in the company that was supposed to secure and hold this information closely.

This information is not merely exposed but is also subsequently exploited in a data breach within a short period of time. Rather, in many cases, a bad actor can gain entry into an enterprises' information system and lie undetected for a significant amount of time, for months, silently wreaking havoc until the bad actor is discovered. In fact, it took an average of 277 days in 2022 to discover a breach.

Surprisingly, 56% of enterprises surveyed in this report did not have any preventative measures such as fully deployed security AI and automation in place to prevent, deter, discover and recover a data breach. However, if enterprises take the initiative to reduce risks and hedge against loss of time, security, and a public relations issue, they can save money, time and, more often, potential damage to their reputations.

In case of a data breach or attack, enterprises that proactively implemented fully deployed security AI and automation saved an average of $3.05 million versus enterprises with no security AI and automation. This is a savings of 65.2%, as the average total cost is $6.20 million for a data breach for an unfortified enterprise, versus $3.15 million for an organization that has fully deployed security AI and automation.

IBM® Storage Defender serves as a set of offerings the provide an end-to-end data protection and cyber resiliency solution that enterprises can use to help fortify their resilience, reduce costs and recover faster, in the case of a potential data breach. Traditional models of data resilience that enterprises often use consist of multiple vendor products needed to meet general functionality, cost requirements and Service Level Agreements. This can often involve multiple users in silos using different software to manage the data. As a result, businesses can take longer to recover if they are hit by a cyber attack.

What is IBM Storage Defender?

IBM Storage Defender can help companies implement an end-to-end cyber resiliency solution that automates, streamlines and facilitates their data security and recovery. Specifically, using IBM Storage Defender can help companies have a minimum viable company recovery in hours, and a full company workload recovery in days.

At a high level, IBM Storage Defender provides a “single pane of glass” view into the activity of a company’s data and information. This simple, easy-to-use dashboard provides an overview of the enterprise’s data and information. Automated alerts, chosen and tailored by the client, signal when a cyber attack has happened or an anomaly is detected in the data or elsewhere in the system. For example, a user can set alerts to be delivered via Slack and text message, or a user can choose email and a phone call instead.

Once a user has received a notification that some of its secondary data has been corrupted or possibly infected, the user can refer to the dashboard to see where the data is, whether geographically or in the file system location. And a user can assign his or her own priorities to the data, the user can then see what the priority level of the data is in this situation. The user can delve deeper into the issue and see which files have been attacked or corrupted, and then the user can also see how the information is being recovered, as well as the status of the automatic recovery in real time. The criticality level of the data involved in the incident can be seen too.

IBM Storage Defender can help a client become more resilient and get back to work, faster, through the following three pillars of Accelerated Discovery, Secure Copies and Automation.

- **Accelerated Discovery:** This feature is proactive in that it detects malware, corruption, or any other nefarious activity and lets the user know immediately. Insights can also be derived through an automated data pattern scanning analysis to determine the presence of corruption or other activity. By employing proactive detection through malware scanning, the user can take appropriate action to address the issue, thwart any attack and then begin the subsequent data recovery process. Instead of being reactive after a bad actor may have already done significant damage, this feature offers the user control in being able to rapidly respond and begin addressing and recovering the data. In addition, there is significant ecosystem scanner support as well, which provides another layer of protection.
- **Secure Copies:** These provide the security in knowing that the backup copies of enterprise data are not corrupted as well, in case of an attack. The copies are immutable, meaning that they cannot be changed after they are created, which, in turn, means that a bad actor cannot corrupt or change these copies

in any manner whatsoever. This provides multiple layers of protection, supported by clean and reliable data copies.

- **Automation:** IBM Storage Sentinel is key to the entire process to simplify and streamline ransomware detection and automated recovery orchestration. Threats are automatically detected, then the alerts are sent directly to the user via the user's preferred means of communication. This then supports rapid recovery for both the primary and secondary workloads of an enterprise.

The components of IBM Storage Defender

IBM Storage Defender provides an end-to-end experience from a cyber resiliency perspective, and it is comprised of several different components including IBM Storage Protect Suite, IBM Storage Virtualize, IBM Copy Services Manager, IBM Storage Sentinel, and IBM Storage Archive.

- **IBM Storage Protect Suite:** This includes **IBM Storage Protect, IBM Storage Protect Plus, IBM Storage Copy Data Management (CDM), IBM Storage Protect Snapshot** and all other variations currently included in the IBM Storage Protect Suite.
  - -Enables scalable hybrid cloud data protection for physical file servers, applications and virtual environments.
  - -Provides recovery, replication, retention, and reuse for virtual machines (VMs), databases, applications, file systems, SaaS workloads and containers in hybrid cloud environments.
  - -Automates the creation and use of copy data snapshots, vaults, clones and replicas on existing storage infrastructure including hybrid environments.
- **IBM Storage Virtualize (Base Virtualization):** This is comprised of **IBM Storage Virtualize Metro/Global Mirror, IBM Storage Virtualize Flash Copy and IBM Storage Virutalize for Public Cloud.** It creates and secures immutable snapshots of data that cannot be changed or deleted, offering a rapid recovery point.
- **IBM Storage Sentinel:** Enhances ransomware detection and incident recovery through anomaly detection, orchestration and copy management
- **IBM Storage Archive:** Direct, intuitive and graphical access to data stored in IBM Tape drives and libraries

- **IBM Copy Services Manager:** Manages block storage data replication and disaster recovery
- **IBM Storage Protect for Containers**
- **IBM Storage Defender Data Protect**
- **IBM Storage Defender Replica**
- **IBM Storage Defender Data Management Service**

How does it help clients?

An important differentiator of IBM Storage Defender involves IBM's data reduction techniques, which can help an enterprise to significantly reduce its overall storage capacity and cost. Competitors may want to take multiple backup copies of the client data, then they may take snapshots of the data as well. This duplication of effort in making multiple copies is an unnecessary waste of time and effort.

Instead, we use the data backups we have already taken along the way, instead of taking more snapshots and backing up the same data multiple times. This minimizes the overall storage capacity and cost for a client, and also reduces the amount of potential stress that taking multiple copies of backups may incur for the client. In addition, in situations that a financial firm may encounter where there is a disposal hold that is required to be put on the backup data (in case of an investigation, for example), the client needs to be able to release the data after the investigation and return to normal. It can be difficult for a client to sort out what it needs to keep and what it needs to throw away.

Why was IBM Storage Defender created?

IBM Storage Defender was created as a direct result of listening to client feedback, as well as overall client demand. IBM clients would often purchase products from the IBM suite of tools and create their own custom architecture in alignment with their business requirements and load demands. As such, sometimes clients would buy products that they initially thought that they would need, and then some aspect of their business changed, leaving them with extra products that they may not need or use. Conversely, clients could also underestimate their needs or their capacity for growth, and underbuy products as well. Products can often be new and have to be stood up, while other products may be decommissioned.

Managing a business is difficult enough, while also managing the technology infrastructure that underpins a business can be even more challenging.

More importantly, what clients were looking for was agility; the agility to scale up or down to meet demands without a lot of extra work, time and additional cost. Could a business become agile in almost any situation? This was the ideal situation for a client: enhanced agility to be able to shift the enterprise infrastructure and deal with increased business demands while also easily managing the underlying business infrastructure.

This is how IBM Storage Defender was created—the key to providing that enterprise agility that so many clients were looking to gain. IBM Storage Defender allows clients to have a suite of tools at their fingertips, allowing the client to have all of the pieces they need for various scenarios. These scenarios include hardware, on-prem, off-prem, cloud or any combination thereof.

Clients can buy IBM Storage Defender and easily add or remove any of the product's functionality where they are required. The client merely has to keep within its license limits in order to utilize any of the functionality of IBM Storage Defender versus having to go through an entire sales cycle or process to procure any additional components or products. Furthermore, the client can use what it already has; frequently, some clients are not always aware that they may already own several pieces of the IBM Storage Defender components already.

IBM Storage Defender Capabilities

IBM Storage Defender provides many capabilities for enterprises. Overall, it provides scalable hybrid cloud data protection for physical file servers, applications, and virtual environments. More importantly, it provides for the recovery, replication, retention and reuse for VMs, databases, applications, file systems, SaaS workloads and containers in hybrid cloud environments. Users can automate the creation and use of copy data snapshots, vaults, clones and replicas on existing storage infrastructure including hybrid environments.

IBM Storage Defender also enables users to create and secure immutable snapshots of data that cannot be changed or deleted, offering a rapid recovery point. It can manage block

storage data replication and disaster recovery. It enhances ransomware detection and incident recovery through anomaly detection,orchestration, and copy management. Another key feature is that IBM Storage Defender provides Red Hat OpenShift® and IBM Cloud Pak© for Data data protection designed to help protect OpenShift clusters and applications. The user can benefit from direct, intuitive and graphical access to data stored in IBM tape drives and libraries.

IBM Storage Defender provides clients with data resilience through three pillars:

1. **Data protection** occurs across multiple layers and services. This includes hardware snapshots and copy data management. Also, data backup and recovery can be scaled on a short- or long-term retention spectrum.

2. **Data immutability,** meaning that the data cannot be changed or altered once written, is in the form of immutable snapshots, as well as immutable targets in cold storage or object storage. Data can be saved either in a Write Once Read Many (WORM) format, or in a Non- Erasable Non-Readable (NENR) format.

3. **Data isolation** is important in protecting the integrity of the data. Multiple layers of data isolation that can be created include physical and logical air-gap, cold storage/object storage, data vaults, isolated infrastructures and clean rooms.

IBM Technology Expert Labs can help install and set up IBM Storage Defender

IBM Technology Expert Labs has the knowledge and expertise to help clients from beginning to end with IBM Storage Defender. The advantage of using IBM Storage Defender is that all of its components fall under the same roadmap. This eliminates the complexity of compatibility matrices between components for the client. Unlike other solutions offered by different companies, IBM Storage Defender is not parsed into separate entities; it is one solidified product roadmap. This singularity maintains the overall integrity of the solution as it is consistent and cohesive. Furthermore, this singularity is important to a client, because if a component of the IBM Storage Defender solution has an issue or does not work properly, the Technology Expert Labs team knows the solution intimately and understands that the issue can be

pinpointed within the components that comprise the solution. This is as opposed to a solution that is composed of multiple service vendors or pieces, where if there is an issue, it can take a long time to determine which piece is erroneous.

Another aspect that is a significant differentiator is the fact that IBM Storage Defender is a pre-delivered suite of tools. In a typical services situation, a client may order one component, then add more later on as business needs of the company may change. This piecemeal ordering of services is often fraught with delays or additional paperwork, which can also cause procurement issues. Time and money can be wasted in this approach. IBM Technology Expert Labs has the deep technical skills to help integrate this suite of tools to help clients protect and recover from cyber attacks quickly using tried and tested best practices

Having a pre-delivered set of tools helps to subvert this expenditure of additional time and effort. If a client has IBM Storage Defender and wants to add an additional tool or component, it can be easily done by procuring an additional license; the client does not have to initiate or endure the process of going through another sales cycle. IBM Storage Defender was built to accommodate the flexible and changing needs of an enterprise; components can easily be added or modified to suit the needs of the client. This way, the client can be secure in knowing that it can easily adapt and change its suite of tools to meet its needs, without enduring unnecessary delays or expenses, to the detriment of its business operations.

From an administration perspective, the Technology Expert Labs team can deliver these repeatable and scalable solutions over and over again, ensuring consistency and reliability through the sheer agility of such a repeatable and solid solution. All of the components of IBM Storage Defender are there for a logical and rational reason, developed through years of client interactions and discussions.

IBM Storage Defender clients can benefit from the Technology Expert Labs team's established best practices that have been garnered over the years through many successful client implementations, performance capacity, administration and other related work.

The most interesting aspect of IBM Storage Defender is that many clients are ready to migrate to IBM Storage Defender already. This is because clients have a lot of the existing IBM products, or they are probably using it currently. Clients may not be using the latest backup techniques or repositories to store their data, because they do not know it or are not

ready or do not realize it yet. If clients do migrate their existing data, they can run backups faster or do the backups cheaper or have better recovery. More importantly, clients can discover the versatility of what can be done with the data that has already been backed up. Clients may not realize that currently they may be doing extra work, backing up data more than once; that by using IBM Storage Defender, they can save time and money by reducing duplicate work, while also protecting themselves better.

This is mostly because, with IBM Storage Defender, clients do not need to send the backup data to different locations multiple times. Therefore, they do not need such a large bandwidth for their backup data. This, then, translates to cost savings and less data being stored on the more expensive media because a user is better able to manage it on the back end.

IBM Storage Defender also provides potential cost savings through tiering options, meaning that backup data sitting on expensive media can be tiered off to less expensive data. This is because more recent—data that is a week or two old—that needs to be restored, this is located on the faster media. Older data does not need to be restored that often. Therefore, the client can efficiently store the correct backup data on the right media at an economic price.

Get started with IBM Storage Defender today

Contact your IBM sales representative or IBM Technology Expert Labs at Systems-Expert-Labs@ibm.com to engage a specialist who can help you get started today.

Parwathi Hettinga-Ayakannu is the Global Storage Practice Delivery Leader, IBM Technology Expert Labs, par@nl.ibm.com.

Brian Hansford is in Global Sales for IBM Technology Expert Labs for Software Defined Storage and Modern Data Protection, HANSFOB@uk.ibm.com.

References

[1] Cost of a data breach 2022, https://www.ibm.com/reports/data-breach

IBM Technology Expert Labs
Whitepaper

IBM Technology Expert Labs

IBM Technology Expert Labs offers infrastructure services to help you build hybrid cloud and enterprise IT. From servers and mainframes to storage systems and software, Technology Services helps you deploy the building blocks of a next-generation IT infrastructure that empowers your business.

Our Technology Expert Labs consultants perform infrastructure services for clients online or on site, offering deep technical expertise, valuable tools and successful methodologies. Our services are designed to help clients solve business challenges, gain new skills and apply best practices.

Technology Expert Labs offers a wide range of infrastructure and software services for IBM Power®, IBM Storage, IBM zSystems® and IBM LinuxONE and GDPS®. Technology Expert Labs has a global presence and can deploy experienced consultants online or onsite around the world.

Learn more

To learn more about project management services or IBM Technology Expert Labs, visit:

ibm.com/services/infrastructure

or email us at: **systems-expert-labs@ibm.com**

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
June 2023