IBM Storage Defender

Simplify data resilience for enterprise data storage

Highlights
Deploys AI-powered sensors for fast threat detection

Ensures business continuity for a variety of workloads

Enhances data resilience with IBM Storage FlashSystem

Improves cross-team collaboration to shorten recovery times

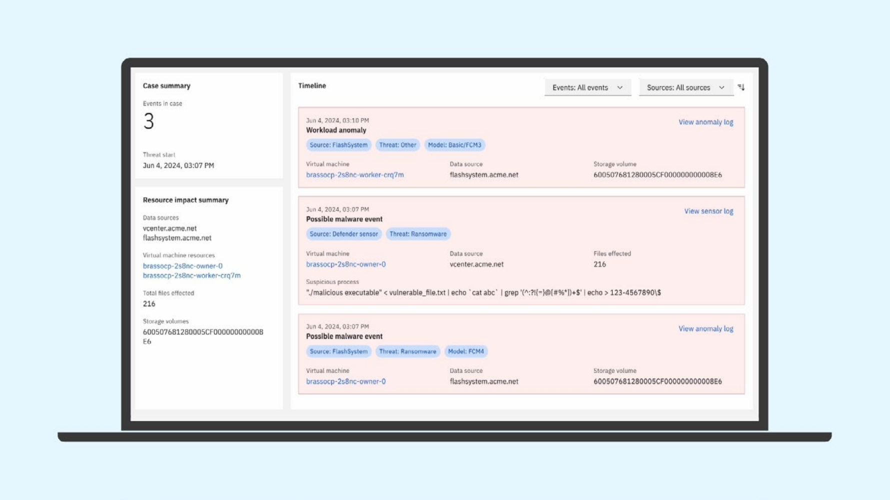
Today, organizations face severe threats to their information supply chains as cyberattacks increase and malicious actors become more sophisticated. According to the IBM® X-Force® Threat Intelligence Index 2024 report, 43% of all reported incidents involved malware, making it the most common threat, while 20% were ransomware cases.[1] In addition to malware, IT organizations are threatened by natural disasters, system failures, human errors and sabotage. These events can cause financial losses and harm customer trust if sensitive data is compromised.

IBM Storage Defender is a purpose-built end-to-end data resilience solution designed to help organizations quickly restart essential business operations in the event of a cyberattack or other unforeseen catastrophic events, minimizing the risks of financial losses or damage to the company’s reputation. It simplifies and orchestrates business recovery processes by presenting a comprehensive view of data resilience and recoverability across primary and secondary storage under a single pane of glass.

Deploys AI-powered sensors for fast threat detection

Storage Defender is designed to deploy AI-powered sensors across primary and secondary workloads to quickly detect threats and anomalies from backup metadata, array snapshots and other relevant threat indicators. Signals from all available sensors are aggregated by Storage Defender, whether they come from hardware with real-time ransomware threat detection technology or software, such as file system or backup-based detection.

When sensors identify potential threat activity, a case is automatically opened and a notification is sent to IBM QRadar® SIEM (Security Information and Event Management). In addition, incident teams receive email alerts to start coordinated actions. All open cases are presented in a comprehensive open case panel (see figure 1), which provides detailed information about the type of anomaly, time and date of the event, data sources, affected virtual machines (VMs) and the storage resources impacted by the event. This information is crucial for initiating the next steps between infrastructure and security operations (SecOps) teams and deciding whether recovery plans should be implemented immediately.



Case summary

Events in case
3

Threat start
Jun 4, 2024, 03:07 PM

Resource impact summary

Data sources
vcenter.acme.net
flashsystem.acme.net

Virtual machine resources
brassocp-2s8nc-owner-0
brassocp-2s8nc-worker-crq7m

Total files effected
216

Storage volumes
600507681280005CF000000000008
E6

Timeline

Jun 4, 2024, 03:10 PM
Workload anomaly
Source: FlashSystem · Threat: Other · Model: Basic/FCM3

Virtual machine	Data source	Storage volume
brassocp-2s8nc-worker-crq7m	flashsystem.acme.net	600507681280005CF000000000008E6

Jun 4, 2024, 03:07 PM
Possible malware event
Source: Defender sensor · Threat: Ransomware

Virtual machine	Data source	Files effected
brassocp-2s8nc-owner-0	vcenter.acme.net	216

Suspicious process
```
"./malicious executable" < vulnerable_file.txt | echo `cat abc` | grep '(^:?!{=}@[#%*])+$' | echo > 123-4567890\$
```

Jun 4, 2024, 03:07 PM
Possible malware event
Source: FlashSystem · Threat: Ransomware · Model: FCM4

Virtual machine	Data source	Storage volume
brassocp-2s8nc-owner-0	flashsystem.acme.net	600507681280005CF000000000008E6

Figure 1. Open case panel

You can install Storage Defender sensors on one or multiple VMs to monitor and detect ransomware and other anomalies in real-time. The following table shows the Linux distributions installed as guest operating systems in VMs where sensors are currently supported.

Linux distribution	Starting from version	Required packages
Red Hat Enterprise Linux	9.0	– bash – kernel >= 5.9 – libgomp – python3
SUSE Linux Enterprise Server	15 SP5	– bash – kernel >= 5.9 – libgomp1 – python311
Ubuntu	24.04 LTS	– bash – Linux-image-generic >= 5.9 – libgomp1 – python3

Ensures business continuity for a variety of workloads

Storage Defender provides advanced data resilience for primary and backup storage. It includes immutable point-in-time snapshots, logical and physical air gap protection, encryption, clean room isolation for thorough threat analysis and anomaly scanning. Additionally, it utilizes cost-saving technologies such as incremental forever, deduplication and compression. It also delivers flexible data retention and protection options on write once, read many (WORM) tape and immutable object storage.

Storage Defender offers data resilience capabilities to protect your modern IT environments including VMs, physical servers, databases, applications, storage area networks (SAN) and network-attached storage (NAS). Easy-to-use policies can be configured to automate the entire data protection process, including backup, replication, and secure data retention on premises and in the cloud across a wide range of workloads. Some of the most relevant are shown in the following table.

Source type	Protected workload
Virtual machine	VMware, Nutanix Acropolis Hypervisor, Microsoft Hyper-V and Red Hat Virtualization (RHV)
Cloud virtual machine	AWS Elastic Compute Cloud (EC2), Azure VM and Google Cloud Platform (GCP)
Database	AWS Relational Database Service (RDS), AWS Aurora, IBM Db2, Microsoft SQL, Oracle, SAP HANA, SAP Sybase ASE, SAP Sybase IQ, MySQL Enterprise Edition and CockroachDB
NoSQL and Hadoop service	MongoDB, Cassandra, Couchbase, Hive, Hbase and Hadoop Distributed File System (HDFS)
Physical server	Microsoft Windows Server, Linux (Red Hat Enterprise Linux, CentOS, Oracle Linux, Debian, Ubuntu, SUSE Linux Enterprise), IBM AIX and Solaris
Network-attached storage (NAS)	Pure Storage FlashBlade, Dell EMC Isilon, NetApp, Elastifile Cloud File System (ECFS), IBM Storage Scale and Generic NAS
Storage area network (SAN)	FlashSystem, Pure Storage FlashArray, HPE Nimble and Cisco Hyperflex
Application	Microsoft Active Directory, Microsoft Exchange Server and Microsoft 365

Storage Defender includes management tools that can identify the most recent trusted recovery point and its location, whether from primary storage, object, tape or the cloud, making it readily available for near-instant recovery. Additionally, when Storage Defender detects potential threats, it streamlines business recovery activities by providing recommended actions and built-in automation to further accelerate the return of vital operations to their normal state.

For safekeeping, data managed by Storage Defender is replicated to offsite recovery facilities. That helps deliver fast and flexible restores from primary and remote sites, allowing the recovery of individual items, complex systems and entire data centers. In addition, workloads can be restored in an isolated clean room environment to be analyzed and validated before being recovered to production systems. This verification helps ensure that your data is clean so you can more safely re-establish business operations.

Enhances data resilience with IBM Storage FlashSystem

FlashSystem arrays are platforms built for data resilience from the ground up and designed with a cloud operations management style to simplify the protection of mission-critical data. FlashSystem with IBM FlashCore® Module 4 (FCM4) can identify threats in real-time by building into the hardware the ability to collect and analyze stats for every single read and write operation without any performance impact. Storage Defender and FlashSystem can seamlessly work together to create a multi-layered strategy that can drastically reduce the time needed to detect a ransomware attack while producing more accurate results and lower false positives.

FlashSystem offers protection through immutable copies of data known as safeguarded copies, which are isolated from production environments and cannot be modified or deleted through user error, malicious actions or ransomware attacks. Storage Defender can recover workloads directly from FlashSystem safeguarded copies to significantly reduce the time needed to resume critical business operations, as data transfer is performed through the SAN, using Fibre Channel (FC) or internet small computer system interface (iSCSI) rather than over the network.

When potential threat activity is detected, the IBM FlashCore module reports the anomaly to IBM Storage Insights Pro, which analyzes the data and alerts Storage Defender about suspicious behaviors coming from your managed FlashSystem arrays. Storage Defender correlates the specific volume in the FlashSystem associated with the VM under attack and proactively creates a safeguarded copy of the affected data for offline investigation and follow-up recovery operations. When time is crucial, this rapid, automatic action can significantly reduce the time between receiving the alert, containing the attack and the subsequent recovery.

Improves cross-team collaboration to shorten recovery times

QRadar® SIEM solution helps organizations detect cybersecurity incidents, respond to threats and comply with security regulations. Its features include event and log management, incident response and security analytics to enable effective monitoring and protection of the IT infrastructure. When a threat is detected, Storage Defender collects and sends the information to QRadar SIEM, that empowers security analysts to view storage-related incidents in their existing Security Operations Center (SOC) dashboards, extending the monitoring capabilities between storage administrators, security and other incident teams. This integration helps share crucial information and coordinate activities across all the involved teams to initiate the procedures to re-establish business operations while reducing the complexity and cost of managing security and data recovery activities.

Simplifies license management to reduce complexity and costs

Storage Defender offers all IBM Storage for Data Resilience capabilities, including data protection, copy data management and virtualization, consumable through credit-based licensing called resource units (RUs), which give you the flexibility to choose only the capabilities your enterprise needs. This acquisition and licensing approach streamlines and simplifies the management of what used to be a range of software capabilities spread over multiple licensable solutions and helps you reduce complexity and costs while optimizing resources.

Ensuring the availability of business operations is essential to building operational resilience and trust. Storage Defender is an advanced solution that helps organizations build operational resilience by bringing together multiple levels of threat detection and data protection that serve as a basis to build several advanced lines of defense across primary and secondary storage to effectively contain and control cyberattacks and other unforeseen threats. Storage Defender helps provide the peace of mind you need to successfully navigate unpredictable events and ensure the continuity of vital business operations and processes.

Why IBM?

IBM provides a broad portfolio of hardware, software and services to help organizations efficiently meet their IT infrastructure requirements. That includes reliable data resilience solutions that help accelerate business recovery from unforeseen catastrophic events. As business needs evolve, IBM solutions prioritize interoperability and the integration of new use cases or approaches, from analytics to multisite backup and near-instant operations recovery.

To learn more about IBM Storage Defender, contact your IBM representative or IBM Business Partner or visit ibm.com/products/storage-defender.

[1] X-Force Threat Intelligence Index 2024, IBM, February 2024.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.