IBM Storage Defender Sentinel

Automated recovery from ransomware

Highlights

Protects against ransomware

Creates immutable application-specific or crash-consistent primary storage snapshots

Uses anomaly detection and machine learning to identify potential threats

Orchestrates recovery from verified and validated backup copies

Supports Oracle, SAP HANA, InterSystems databases for Epic healthcare systems, VMware and Linux file systems

Organizations of all sizes, in every industry, are now threatened by increasingly malevolent ransomware and other cyber threats. Even with the strongest defensive measures, there is always the risk that some threats might circumvent every barrier and penetrate an organization's information supply chain. Beyond the financial cost and operational chaos, these attacks can severely damage a company's brand, especially in critical areas such as health care, financial services, and manufacturing.

One alarming trend is that some criminal gangs now exploit the fact that many organizations use a “30-60-90” policy for backing up data – snapshots are captured hourly and daily, with full backups generated every 30, 60, and 90 days. In response, these bad actors have come up with a new twist – they install malware and leave it dormant for 100 days or more before springing the trap. At that point, the malicious code has infected not only the target’s production data systems and snapshots, but every single one of their backup copies. The victims have few alternatives other than paying up.

IBM Storage Defender Sentinel is a cyber resiliency solution designed to help organizations enhance ransomware detection and incident recovery. Defender Sentinel automates the creation of immutable backup copies of your data, then uses machine learning to detect signs of possible corruption and generate forensic reports that help you quickly diagnose and identify the source of the attack. Because Defender Sentinel can intelligently isolate infected backups, your organization can identify the most recent verified and validated backup copies, greatly accelerating your time to recovery.

Sentinel, a turn-key solution validated per application that provides advanced data protection and recovery capabilities for a variety of workloads and use cases.

IBM extends the NIST Cyber Security Framework, emphasizing key steps like identifying risks, implementing safeguards, detecting cybersecurity events, responding to incidents, and ensuring resilience for recovery.

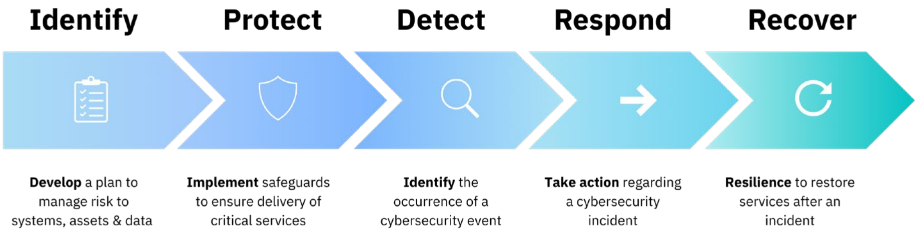

Identify
Protect
Detect
Respond
Recover
Develop a plan to manage risk to systems, assets & data
Implement safeguards to ensure delivery of critical services
Identify the occurrence of a cybersecurity event
Take action regarding a cybersecurity incident
Resilience to restore services after an incident

Figure 1. The NIST Cyber Security Framework establishes a baseline for data protection best practices

Comprehensive Data Protection

IBM has embraced and extended the Cyber Security Framework developed by the National Institute of Standards and Technology (NIST), which identifies five key steps toward comprehensive data resiliency:

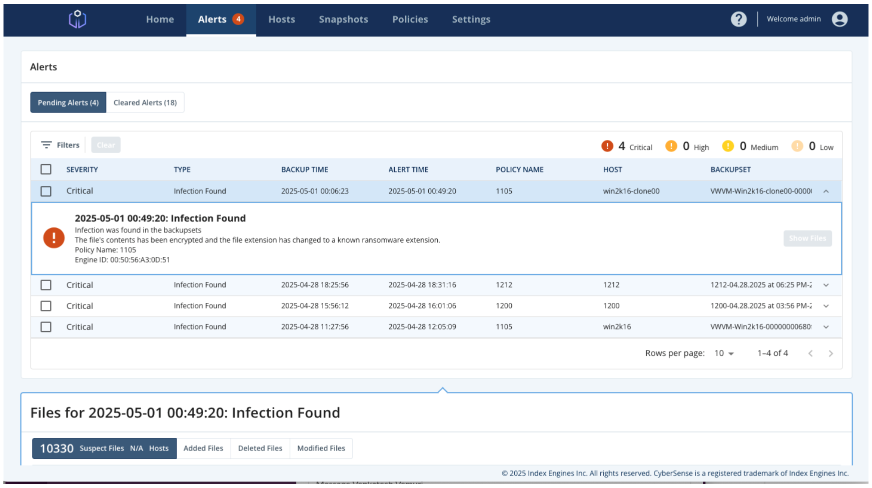
- **Identify**: Develop a plan to manage risk to systems, assets & data.
- **Protect**: Implement safeguards to ensure delivery of critical services.
- **Detect**: Identify the occurrence of a cybersecurity event.
- **Respond**: Take action regarding a cybersecurity incident.
- **Recover**: Resilience to restore after an incident.

The IBM data resilience framework identifies six key capabilities that organizations can implement to help minimize their exposure to potential data breaches, keep the business operational, and control costs.

These capabilities include:

- Ensuring applications in the environment have identity and administrative security that can help manage credentials and data access. This capability can protect against the biggest of the threat vectors; compromised credentials and the malicious insider, together accounting for 26% of data breaches.
- Monitoring and identifying data in the data protection environment for ransomware or malware, determining data pattern anomalies by taking advantage of machine learning capabilities, and containing a threat before it can harm all the data.
- Ensuring the business has extensive encryption, starting at the primary storage layer all the way through backups in flight to where it is stored on backup devices.
- Having multiple layers of backup and utilizing the 3-2-1-1 methodology for protecting data to help ensure the business can be back up and running quickly.
- Protecting information in an isolated environment and using a physical or logical air gap to ensure data can’t be compromised.
- Putting capabilities in place automating recovery so it is effective, rapid, and accurate.

IBM Storage Defender Sentinel brings together the power of IBM Storage Defender Copy Data Management integrated with an anomaly scan engine powered by Index Engines CyberSense software, leveraging Safeguarded Copy immutable snapshot technology from IBM Storage FlashSystem and SVC.



□	SEVERITY	TYPE	BACKUP TIME	ALERT TIME	POLICY NAME	HOST	BACKUPSET
□	Critical	Infection Found	2025-05-01 00:06:23	2025-05-01 00:49:20	1105	win2k16-clone00	VWVM-Win2k16-clone00-0000
□	Critical	Infection Found	2025-04-28 18:25:56	2025-04-28 18:31:16	1212	1212	1212-04.28.2025 at 06:25 PM-
□	Critical	Infection Found	2025-04-28 15:56:12	2025-04-28 16:01:06	1200	1200	1200-04.28.2025 at 03:56 PM-
□	Critical	Infection Found	2025-04-28 11:27:56	2025-04-28 12:05:09	1105	win2k16	VWVM-Win2k16-00000000680

2025-05-01 00:49:20: Infection Found
Infection was found in the backupsets
The file's contents has been encrypted and the file extension has changed to a known ransomware extension.
Policy Name: 1105
Engine ID: 00:50:56:A3:0D:51

Files for 2025-05-01 00:49:20: Infection Found

10330 Suspect Files N/A Hosts

© 2025 Index Engines Inc. All rights reserved. CyberSense is a registered trademark of Index Engines Inc.

Figure 2. IBM Storage Defender Sentinel scans immutable application consistent copies and reports anomalies around corruption and cyber-attacks

IBM Storage Defender Sentinel

IBM Storage Defender Sentinel is a cutting-edge cyber resiliency solution meticulously designed to safeguard organizations against the ever-evolving landscape of ransomware and other cyber threats. In today's digital age, where cyber-attacks are becoming increasingly sophisticated, traditional defenses may not always suffice. Sentinel steps in as a robust front of defense, ensuring that your data remains secure and recoverable even in the face of the most insidious threats.

What it does

The solution automates the creation of application-consistent immutable backup copies of your data, which are crucial for maintaining data integrity. It also supports the creation of crash-consistent immutable copies. These backups are unchangeable, meaning they cannot be altered or deleted by ransomware or other malicious actors. This immutability is a cornerstone of Sentinel’s defense strategy, providing a secure foundation for data recovery.

Beyond just creating backups, Sentinel employs advanced machine learning algorithms to continuously monitor new backup copies for signs of corruption or malware. By analyzing data patterns and detecting anomalies, it can identify potential threats before they cause widespread damage. This proactive approach ensures that any signs of compromise are swiftly addressed, minimizing the impact on your operations.

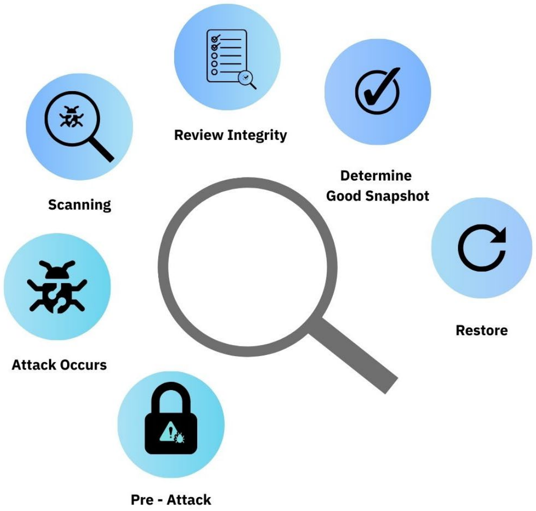


Figure 3. IBM Storage Defender Sentinel addresses six key points in the cyber attack timeline

How IBM Storage Defender Sentinel works
There are six key points on the timeline as Sentinel responds to a cyber-attack.

1. Pre-attack – IBM Storage Defender Copy Data Management creates a series of immutable snapshots called Safeguarded Copies, which are proactively scanned for threats by IBM Storage Defender Sentinel anomaly detection engine that is powered by Index Engines CyberSense software.
2. During an attack – Ransomware begins infecting production files / databases / systems with Safeguarded Copy, and those snapshots are protected and scanned proactively by Sentinel.
3. Scanning initiated – Even as the attack is taking place, Sentinel is scanning snapshots and analyzing entropy changes, file extension mismatch, and other signs of data corruption.
4. Integrity review – Snapshots can now be assessed to confirm which have been verified to be free of threats and data corruption.
5. Determine good snapshot – The most viable snapshot to restore from is identified.
6. Restore – The most viable snapshot is used to restore data to the production environment so the organization can resume normal business operations.

Value to customers

IBM Storage Defender Sentinel offers unparalleled value to customers by providing a comprehensive and automated approach to data protection and recovery. Here are some key benefits:

- **Enhanced security**: By creating immutable backups and continuously monitoring for threats, Sentinel ensures that your data remains secure even in the face of sophisticated cyber-attacks.
- **Rapid recovery**: The solution's ability to quickly identify and isolate infected backups accelerates the recovery process, minimizing downtime and operational disruption.
- **Proactive threat detection**: Advanced machine learning algorithms enable proactive detection of potential threats, allowing for swift intervention before significant damage occurs.
- **Cost efficiency**: By reducing the impact of ransomware attacks and ensuring rapid recovery, Sentinel helps organizations avoid the substantial financial costs associated with data breaches and prolonged downtime.
- **Compliance and trust**: With robust data protection measures in place, organizations can maintain compliance with industry regulations and build trust with their customers by demonstrating a commitment to data security.

IBM Storage Defender Sentinel is not just a solution; it's a strategic asset that empowers organizations to navigate the complexities of modern cyber threats with confidence and resilience.

IBM Storage Defender Sentinel offers automated, immutable backups and advanced machine learning to proactively detect and isolate threats, ensuring rapid recovery and enhanced security against ransomware and cyber-attacks, minimizing downtime and financial impact.

Workload support

Sentinel supports the following enterprise workloads:

- Oracle Database
- VMware virtual infrastructure
- SAP HANA Database
- InterSystems Caché and IRIS for Epic healthcare systems
- Linux file systems

Conclusion

IBM Storage Defender Sentinel delivers a powerful, automated defense against ransomware and cyber threats by combining immutable backups with intelligent anomaly detection. Its ability to proactively identify and isolate compromised data ensures rapid, reliable recovery, minimizing downtime and financial impact. With broad workload support and seamless integration into existing environments, Sentinel empowers organizations to strengthen their cyber resilience, protect critical data, and maintain operational continuity with confidence.

Why IBM?

IBM offers a vast portfolio of hardware, software and services to help organizations cost-effectively address their IT infrastructure needs. These include robust data-storage solutions to enable always-on, trustworthy storage, and recovery from disaster. Because business needs shift, IBM solutions emphasize interoperability and the integration of new use cases or approaches, from analytics to multi-site backup to near- instant recovery. With IBM, organizations can create flexible, robust and resilient storage infrastructure to support critical operations for smooth operations and regulatory compliance.

For more information

To learn more about IBM Storage Defender Sentinel, contact your IBM representative, IBM Business Partner, or visit https://www.ibm.com/products/storage-sentinel.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2025

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.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.