IBM Storage Defender Sentinel

AI-Driven automated recovery from ransomware and other emerging threats

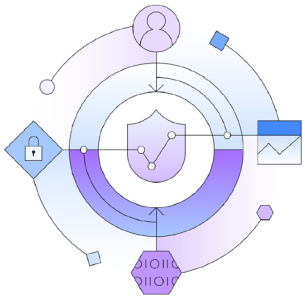
Highlights

- Defends against ransomware and sophisticated cyber threats
- Creates immutable, application-specific or crash-consistent snapshots to secure primary storage
- Leverages machine learning and anomaly detection for early threat identification
- Orchestrates rapid recovery with verified and validated backup copies
- Available for Oracle, SAP HANA, Epic Healthcare Systems, VMware and Linux file systems

Organizations of all sizes and industries are increasingly threatened by malevolent ransomware and other cyberattacks. Even with the strongest defensive measures in place, the risk remains that some threats can bypass security barriers and infiltrate an organization’s information supply chain. Beyond the financial toll and operational disruption, these attacks can inflict severe damage to a company’s brand, especially in critical sectors such as healthcare, manufacturing, and financial services.

A particularly alarming trend is the exploitation of common backup policies like the "30-60-90" strategy, where snapshots are captured hourly and daily, and full backups are created every 30, 60, and 90 days. Cybercriminals have adapted by embedding dormant malware that remains inactive for 100 days or longer. By the time the malware activates, it has infiltrated production systems, snapshots, and every backup copy. At this point, victims are left with few options other than paying the ransom.

IBM Storage Defender Sentinel offers a robust cyber resiliency solution to enhance ransomware detection and incident recovery. It automates the creation of immutable backup copies of your data and leverages machine learning to detect signs of corruption. Forensic reports generated by the solution help diagnose and identify the source of an attack quickly. By isolating infected backups intelligently, IBM Storage Defender Sentinel enables organizations to locate the most recent verified and validated backup copies, significantly accelerating recovery time.



IBM Storage Defender Sentinel

IBM Storage Defender Sentinel complements existing real-time security applications by serving as a vital last line of defense to protect data integrity during an attack.

Building on the powerful capabilities of IBM Safeguarded Copy, it regularly analyzes data copies to identify signs of corruption caused by malware or ransomware. By creating application-aware or crash-consistent immutable Safeguarded Copy snapshots, the solution ensures backups remain secure and isolated, preventing unauthorized modification, deletion, or encryption, even by users with administrative access. In the event of a cyberattack, these trusted restore points enable rapid and reliable recovery.

Designed for enterprise environments, Sentinel provides specialized protection for critical workloads and is currently available for SAP HANA, Epic Healthcare Systems, Oracle, VMware and Linux file systems.

SAP HANA

Sentinel for SAP HANA supports one of the leading enterprise databases and application servers relied upon by many of the world's largest organizations. SAP HANA enables the development of applications based on real-time data, in-memory computing, and machine learning. This powerful solution is available both in the cloud and on-premises, providing organizations with flexibility and scalability to meet their business needs.

Epic Healthcare Systems

Sentinel for Epic offers protection for both InterSystems Cache and IRIS databases, which are integral to the Epic healthcare system. In the healthcare industry, where ransomware attacks can have devastating consequences, including risks to patient safety, robust protection is essential. The solution helps safeguard critical healthcare data, ensuring secure, reliable operations even in the face of cyber threats.

Oracle

Sentinel for Oracle offers ransomware detection for Oracle databases. An enterprise database that is used for managing and storing large amounts of structured data. Its scalability, reliability and support for transactions and concurrent users is why it is commonly used among multiple industries such as finance, healthcare and government.

VMware

Sentinel for VMware enables ransomware detection on VMware virtual machines. It can scan both Windows and Linux VMs for anomalies and signs of corruption. VMware, a global leader in virtualization software, allows multiple virtual machines to run on a single physical machine, optimizing hardware usage. This capability empowers organizations to create, manage, and scale virtualized data centers efficiently and cost-effectively.

Linux File Systems

Sentinel for Linux file systems offers ransomware detection for Linux file systems. The Linux file system that are supported are Red Hat and SUSE Linux. It scans crash-consistent Safeguarded Copies of Red Hat and SUSE Linux file systems. Red Hat is a commercial license Linux distribution that is widely used among multiple industries. SUSE Linux is another Linux distribution used for servers and mainframes.

Conclusion

IBM Storage Defender Sentinel is a powerful cyber resiliency solution designed to protect organizations from ransomware and cyberattacks by serving as a critical last line of defense. It leverages immutable snapshots, advanced machine learning, and proactive anomaly detection to safeguard data integrity and enable rapid recovery from cyber incidents. Tailored for enterprise environments, including SAP HANA, Epic Healthcare Systems, Oracle, VMware and Linux file systems, it provides specialized protection for critical workloads in industries where operational continuity and data security are paramount. With IBM Storage Defender Sentinel, organizations can confidently mitigate risks, ensure business continuity, and maintain trust in an evolving threat landscape.

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.

For more information

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

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
September 2025