IBM Spectrum Sentinel

Automated Recovery from Ransomware and Other Threats

Highlights

- Protects against ransomware and other cyber threats
- Creates immutable application-specific primary storage snapshots
- Uses anomaly detection and machine learning to identify potential threats
- Orchestrates recovery from verified and validated backup copies
- Available for SAP HANA and for Epic Healthcare Systems

Organizations of all size, 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, manufacturing, and financial services.

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 little choice but to pay up.

IBM Spectrum Sentinel is a cyber resiliency solution designed to help businesses enhance ransomware detection and incident recovery. IBM Spectrum 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 IBM Spectrum Sentinel can intelligently isolate infected backups, your organization can identify the most recent verified and validated backup copies, greatly accelerating your time to recovery.

IBM FlashSystem Cyber Vault

IBM FlashSystem Cyber Vault leverages the immutable snapshots created by IBM Safeguarded Copy. IBM Safeguarded Copy lets backup administrators automatically create point-in-time snapshots that are designed to be both immutable (unable to be changed) and protected (unable to be deleted except by specially defined users).

IBM FlashSystem Cyber Vault automatically scans the copies created regularly by Safeguarded Copy looking for signs of data corruption introduced by malware or ransomware. This scan can help identify a classic ransomware attack rapidly once it has started. In addition, it is designed to help identify which data copies have not been affected by an attack. This information enhances an organization’s ability to more quickly identify that an attack is underway and to more rapidly identify and recover a clean copy of their data.

IBM Spectrum Sentinel

IBM Spectrum Sentinel is not intended as a replacement for existing real-time security applications but instead provides a last line of defense against corruption when an attack occurs.

Building on the capabilities of IBM Safeguarded Copy, IBM Spectrum Sentinel frequently checks data copies for evidence of data damage caused by malware or ransomware. IBM Spectrum Sentinel then uses Safeguarded Copy snapshots to create a secure and isolated backup. Ransomware cannot remove, alter, or encrypt Safeguarded Copy snapshots, even with administrator capabilities. In the event of a cyber-attack, these authenticated restore points aid in a speedy recovery.

IBM Sentinel is configured for specific enterprise workloads. It is currently available for SAP HANA and for Epic Healthcare Systems.

SAP HANA

IBM Spectrum Sentinel for SAP HANA supports an enterprise database and application server that is used by many of the world's largest organizations. SAP HANA helps them build applications based on real-time data, in-memory computing, and machine learning, and is available both in the cloud and on-premises.

Epic Healthcare Systems

IBM Spectrum Sentinel for Epic supports both the InterSystems Cache and IRIS databases used by the Epic healthcare system. Protection from ransomware is especially critical for healthcare providers, given that a successful malware attack could potentially put human lives at risk.

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 the IBM Spectrum Sentinel, please contact your IBM representative or IBM Business Partner, or visit https://www.ibm.com/products/data-protection-and-recovery

IBM Maintenance and Technical Support solutions can help you get the most out of your IT investment by reducing support costs, increasing availability and simplifying management with integrated support for your multiproduct, multivendor hardware and software environment. For more information on hardware maintenance, software support, solution support and managed support, visit: ibm.com/services/maintenance

© Copyright IBM Corporation 2022.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at https://www.ibm.com/legal/us/en/copytrade.shtml, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.