IBM Storage Sentinel

Automated recovery from ransomware and other threats

Highlights

Create immutable application-specific primary storage snapshots

Use anomaly detection and machine learning to identify potential threats

Choose versions for Oracle Database, SAP HANA and Epic healthcare systems

Organizations of all sizes, in every industry, are now threatened by increasingly malevolent ransomware and other cyberthreats. Even with the strongest defensive measures, there's always the risk that some threats might circumvent every barrier and penetrate an organization's data. 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 ransomware 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 ransomware 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® Storage Sentinel is a cyber-resiliency solution designed to help businesses enhance ransomware detection and incident recovery. IBM Storage Sentinel automates the creation of immutable backup copies of your data. Then it 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 Storage Sentinel can intelligently isolate infected backups, your organization can identify the most recent verified and validated backup copies, which can accelerate your time to recovery.

Create immutable application-specific primary storage snapshots
IBM Storage Sentinel uses the power of the IBM FlashSystem® solution to create immutable snapshots. This process 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 Storage Sentinel automatically scans the Safeguarded Copies, created regularly by the IBM FlashSystem solution, looking for signs of data corruption introduced by malware or ransomware. This scan helps identify a classic ransomware attack rapidly once it has started. In addition, it's designed to help identify which data copies have not been affected by an attack. This information improves an organization's ability to more quickly identify that an attack is underway and to identify and recover a clean copy of its data more rapidly.

Use anomaly detection and machine learning to identify potential threats
IBM Storage Sentinel isn't 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 Storage Sentinel frequently checks data copies for evidence of data damage caused by malware or ransomware. IBM Storage Sentinel then uses Safeguarded Copy snapshots to create a secured and isolated backup. Ransomware can't remove, alter or encrypt Safeguarded Copy snapshots, even with administrator access. In the event of a cyberattack, these authenticated restore points aid in a speedy recovery.

Choose versions for Oracle Database, SAP HANA and Epic healthcare systems
IBM Storage Sentinel for Oracle provides support for one of the most widely used databases among companies around the world, offering ransomware detection that helps protect a company's most important and sensitive data assets. IBM Storage Sentinel for Oracle supports stand-alone Oracle databases only.

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

IBM Storage Sentinel for Epic supports both the InterSystems Caché and Integrated Risk Information System (IRIS) databases used by the Epic healthcare systems. IBM Storage Sentinel for Epic has also added support for the IBM AIX® operating system, providing even greater security and resiliency. Protection from ransomware is especially critical for healthcare providers because a successful ransomware attack could potentially put human lives at risk.

Conclusion

Staying ahead of a rapidly evolving and growing cyberthreat landscape is a significant challenge for every enterprise. IBM Storage Sentinel, when used in conjunction with your existing real-time security applications, helps you mitigate these threats by helping ensure that your backups aren't corrupted by malware or ransomware. Its intelligent anomaly detection identifies potential threats and orchestrates recovery from verified and validated backup copies for your Oracle, SAP HANA or Epic healthcare data.

Why IBM?

IBM offers a broad portfolio of hardware, software and services to help organizations cost-effectively address their IT infrastructure needs. This portfolio includes 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 and multisite backup to near instant recovery.

With IBM, your organization can create a flexible, robust and resilient storage infrastructure to support critical processes for smooth operations and better regulatory compliance.

For more information

To learn more about IBM Storage Sentinel, contact your IBM representative or IBM Business Partner or visit ibm.com/products/data-protection-and-recovery.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2023