DATA SHEET

GuardMode DPX

Ransomware Detection and Recovery Built-In to your Backup Software

Introduction

GuardMode provides early detection of ransomware or data-related anomalies before you backup your data. GuardMode is complementary to the endpoint and edge protection, monitoring file shares and system behavior, even over the network, instead of relying on a specific binary fingerprint. GuardMode maintains and regularly updates over 4000 known ransomware threat patterns, and assesses affected files.

While ransomware detection solutions were built for security teams to use, GuardMode was designed with the backup administrator and backup solution in mind. An easy to configure detection mechanism and the ability to guide administrators in recovering the critical affected data.

Catalogic GuardMode Highlights

- **Early Detection to Block Ransomware**
  Know what files were impacted and when. Detect, alert and act early!
- **Rollback just the Affected Data**
  Restore just the affected data without brute force reversion back to a point in time snapshot.
- **Customizable Alerting**
  GuardMode allows for customizable alerts, so an admin can be notified immediately in case of an attack.
- **Minimize Disruption**
  Integrate with snapshots and maximize customer investments in primary storage.
- **Easy to Use**
  Easy to set up and use, and can be integrated with existing security solutions, making it an effective addition to an overall security strategy.
- **Proactive Protection**
  Continuously monitors for ransomware-like behaviors and takes action to block it, providing proactive protection for data known and unknown threats.

Why Guard Mode?

GuardMode is a pre-backup solution designed to detect and alert on suspicious activity that may indicate a ransomware infection, and to prevent the ransomware from encrypting backups. This can help to minimize the impact of an attack on the user's data and systems. However, GuardMode alone is not a complete solution for protecting against ransomware infections. It works as an additional layer of protection, it can be integrated with other security solutions, like enterprise or endpoint data protection, intrusion detection/prevention systems to provide a more comprehensive defense.

CATALOGIC

GuardMode is a ransomware and data anomaly detection designed to enhances the security posture of your backup and storage teams, and therefore your company.

Distributed architecture

Data-related events are stored on the client and synced to the server. Analysis and anomaly detection happens independently from the server.

Smart Processing

GuardMode only processes active data and analyzes file heuristics rather than block heuristics (a lot fewer events).

Integration Flexibility

Modular architecture for plugin-like extensibility for data sources and targets, and making integration with SIEMs through REST API or Syslog as simple as it can be.

"It is the responsibility of every company to do all they can to harden their cybersecurity stance. This includes monitoring that the data they are backing up has not been compromised by ransomware, and that they can recover their systems and data from their backups. With the GuardMode agent in the new DPX 4.9 release, Campus and our clients' IT backup teams have a valuable tool to help ensure that their data is being proactively monitored and protected, and that they can identify and recover any data that may have been compromised." — Timo Fischer, System Architect, Campus Computer Systems.

Rapid Ransomware Detection

GuardMode uses behavior-based detection techniques to identify ransomware-like behavior, such as abnormal file access patterns, unusual process execution, and other indicators of malicious activity. This allows it to detect a wide range of known and unknown ransomware strains.

Blocklist
- Blocks file types of known ransomware
- Sourced & updated through security research bulletins

Honey Pots
- Plant files with known extensions & checksums
- Look for bites on these files

Green Lane
- Blocks all files EXCEPT allowed file list
- Accounts for automation & custom apps

Pattern Matching
- Look for known access patterns and signatures
- Look for breaches of abnormal IO thresholds

The time it takes to detect ransomware with GuardMode can vary depending on the specific implementation and configuration of the solution. Generally, GuardMode uses advanced algorithms and behavior-based detection techniques to detect ransomware in real-time, as soon as it begins to encrypt files. This means that it can detect ransomware before it can cause significant damage, and alert the user immediately. While for blocklist type of detection, an alert will be instantaneous, for threshold and behavior based detection it might be several seconds.

Conclusion

GuardMode is pre-backup solution that provides an additional layer of protection to a backup and recovery solution, specifically for ransomware and ransomware-like threat detection. It is distributed as an agent installable on Windows and Linux hosts. GuardMode is available to Catalogic DPX customers free of charge as a part of the DPX Enterprise Data Protection suite. For standalone installations pricing and licensing model, please reach out to us.

Americas: 201.249.8980
United Kingdom: +44 (0) 207 712 1667
Germany: +49 (0) 2102 307614 0
Netherlands: + 31 (0) 20 347 23 88

GuardMode

DPX

CATALOGIC