Quick Answer: How to Use Data Access Governance Solutions to Thwart Ransomware

Published 14 September 2021 - ID G00757978 - 4 min read

Joerg Fritsch

Initiatives: Security of Applications and Data

As ransomware continues to wreak havoc on organizations, security and risk management leaders must take a data-centric view of this data-focused threat. This research highlights how data access governance solutions can offer protection.

Quick Answer

How can data access governance solutions be used to protect against ransomware?

- Take a blended, data-centric approach to combating ransomware — a common form of data-centric malware that needs access to files and file repositories — by using multiple data security tools, including data access governance (DAG) solutions.

- Use DAG solutions to gain insight into, and more control over, who or what accesses your enterprise’s unstructured files and repositories. These solutions offer enhanced detection of, and mitigation against, ransomware.

- Review and revise user and service entitlements periodically. Understanding identity, access and data governance is key to minimizing ransomware attacks. Ransomware typically works by penetrating and compromising end-user devices via, for example, phishing attacks. Well-aligned entitlements shrink the attack surface.

More Detail

Ransomware continues to plague organizations across the world, so much so that it is one of the most searched-for topics on gartner.com.¹
Protection against ransomware requires a blend of cybersecurity tools, including DAG solutions, endpoint protection platforms (EPPs), identity access management (IAM) and data security technologies, along with behavioral analysis (see How to Prepare for Ransomware Attacks).

There are two key elements to DAG as it pertains to ransomware and other forms of data-centric attack: a static element and a dynamic element.

**Static Element: Rightsized Access**

This element concerns user rights and entitlements. Breaches and other damage caused by data-centric attacks can be mitigated by rightsizing access for users and other entities:

- Ransomware attacks unstructured data with the aim of accessing and encrypting it. The attacker then offers to provide the decryption key in return for ransom (the attacker may also seek to exfiltrate data as a means of further monetization). Ransomware is malware that is typically delivered by phishing, but ultimately requires access to files and file repositories if it is to be effective. As such, ransomware is a data access issue. This means you must pay proper attention to user access within your environment.

- Limiting data access is key, but it must be done with a focus on minimizing adverse impacts on productivity. This demands rightsized access for users. The goal is to shrink the attack surface from a data access perspective.

- DAG solutions, such as those of Netwrix (now part of Stealthbits), SailPoint and Varonis, can help align access and entitlements with identity and access repositories such as Active Directory (AD). Undertaking periodic hygiene of AD and other directories is a best practice to ensure user rights are aligned and up-to-date. Furthermore, DAG solutions help with the periodic alignment of access rights, specifically file and file repository access rights. Additional alignment of data and app classification should be layered in to ensure an appropriate risk-based approach.

- Rightsizing access is the first step, but the overall aim is to limit the amount of data that ransomware can access. Real-time detection is therefore still needed — see below.

**Dynamic Element: Real-Time Detection and Monitoring of User Behavior From a Data Perspective**
Ask yourself what “normal” looks like from a user behavior perspective. How many files do users normally access during a certain period? Over an entire system, 10,000 file requests every two hours may be normal. But would 30,000 file access requests in less than one hour seem usual? No, but this is typical behavior for ransomware. Many Gartner clients have detected ransomware merely by using DAG solutions to monitor user behavior. ²

DAG solutions typically have a deep view into file access, as they are generally embedded at the kernel level. They can control and log all file-based access (some EPPs and endpoint detection and response [EDR] tools also use file-based insights). This gives them a unique file-centric perspective that, when combined with user behavior analysis derived from the application of machine learning analytics to file access data, can identify potential indicators of compromise by, and threats from, ransomware.

DAG solutions combined with user behavior analytics can baseline what looks normal for users. If access exceeds what appears normal, alerts may be issued and manual or automated actions taken. It is this functionality that has enabled Gartner clients to mitigate the impact of ransomware. For DAG solutions to realize their potential to protect against ransomware, they must include user behavior monitoring.

Recommendations:

- Take a data-centric view of ransomware protection and mitigation. Use DAG solutions to help govern and monitor enterprise data and protect it from data-centric attack.

- Determine whether your current IAM solution has data security control capabilities natively or via integration:
  - Some IAM solutions, such as SailPoint’s, offer DAG capabilities that align with identity-first security.
  - Inquire about user behavior tools that might be available as add-ons to existing security tools (such as IAM tools and EPPs); these could provide additional insight into user access.

- Develop data security governance that is consistent with IAM policies:
  - Prioritize controls to mitigate risks and threats.
  - Conduct periodic reviews of entitlements and overall access.
Monitor behavior:

Whether or not you can see the data, monitor the behavior. Overall, for the best protection against ransomware, you need more than just DAG solutions, even though many of these also offer behavior analysis and other threat protections. You must also use tools that cover endpoint security, security information and event management (SIEM), security orchestration, automation and response (SOAR), and data backup and recovery.

Recommended by the Authors

Hype Cycle for Data Security, 2021

Use the Data Security Governance Framework to Balance Business Needs and Risks

How to Prepare for Ransomware Attacks

Designing and Implementing a Ransomware Defense Architecture

Quick Answer: Ransomware — What Happens if You Pay?

You’ve Got Cloud Security All Wrong — Why Identity and Data Security Are Paramount in a Cloud World

Top Security and Risk Management Trends 2021

Evidence

1 Gartner.com search analytics, August 2021

2 Information from approximately 560 Gartner client inquiries from August 2019 through August 2021.