Lepide

How Lepide Would Have Helped to Prevent the Marriott Data Breach

CASE STUDY

ABOUT THIS CASE STUDY

This is a case study of how Lepide would have helped prevent a real-world data breach. It is theoretical. Marriott International were not asked to participate in the case study, and the information on the breach was gathered from publicly available sources.

HIGHLIGHTS

HOW IT HAPPENED

- Marriott's 2014 data breach, affecting 300 million guests, involved hackers exploiting vulnerabilities in a recently acquired Starwood brand's reservation system.

THE IMPACT

- ICO levied a fine of **£18.4 million** — more than $23 million — for violating British citizens' privacy rights under the GDPR.
- Marriott incurred costs **exceeding $30 million** for investigation, notification, credit monitoring, and security improvements.
- **Business disruption**: The breach diverted resources and attention from core business operations, impacting efficiency and potentially leading to increased costs.
- **Reputational damage**: The breach significantly damaged brand trust and customer confidence. Share price dropped by 8.7%

THE SOLUTION

- **AD Security**: Lepide could have helped to reduce the AD threat surface to mitigate the risk of the breach.
- **Data Classification**: Lepide could have helped identify and classify sensitive data within Starwood systems.
- **User Monitoring**: File Server auditing would have helped raise flags on unusual user activity.
- **DLP**: Lepide could have alerted and stopped attempts to exfiltrate data.

Lepide

WHAT HAPPENED

It's understood that in 2014 a Remote Access Trojan (RAT) infiltrated the Starwood booking systems. Starwood was then acquired by Marriot in September 2016. But Marriott was not ready to book guests at its thousands of newly acquired hotels with its own in-house reservation system, and so Starwood's old system limped on.

Due to the lack of monitoring systems in place, it was another 2 years before the attackers were detected. What stands out here is not the attack's success in breaching Starwood's systems — most security experts today believe it's almost impossible to keep all attackers at bay all the time — but rather that the attack went undetected for four years. However, it should also be noted that weak password policies and a lack of Active Directory hygiene likely contributed to the attacker's ability to infiltrate Starwood systems.

THE IMPACT

For Marriott, the 2014 data breach, exposing millions of guests' information, triggered a cascade of negative impacts. Financially, they faced hefty fines (reaching £18.4 million from the ICO alone), lawsuits, and potential brand reputation damage, reflected in a temporary stock price drop. Additionally, they incurred costs for offering credit monitoring and passport replacements to affected individuals.

Consumers, the unfortunate targets, experienced anxieties surrounding potential identity theft and fraudulent activity. Their personal details, including passport numbers and credit card information, were vulnerable, leading to concerns about financial losses and misuse of sensitive data. While some may have escaped these consequences, the breach undoubtedly caused stress and a loss of trust towards Marriott. Even those unaffected felt the sting, as heightened security measures, like stricter password requirements, added friction to future interactions with the hotel chain.

SOLUTION

How the Lepide Data Security Platform Could Have Helped

With the benefit of hindsight, there were several ways in which Lepide could have helped Marriott International reduce the likeliness of the breach and speed up detection/response. These include:

1. **Active Directory Security**: Lepide could have reduced the risk surface area by removing stale AD accounts, ensuring stronger password expiration policies and flagging up unusual changes to admin privileges. Marriott had none of these measures in place, which allowed the attackers easier access and the ability to go undetected for a significant period of time.

2. **Data Discovery and Classification**: If Lepide had been in place and effectively configured, it could have helped Marriott identify and classify sensitive guest data within their Starwood systems. This would have prioritized protection measures for the most critical information. Data classification is now an essential part of mergers, and a key use case for Lepide.

3. **User Activity Monitoring**: File server auditing would have raised flags about unusual activity patterns within the Starwood systems, leading to earlier detection of the attackers.

4. **Data Loss Prevention**: If implemented correctly, Lepide could have alerted and stopped attempts to exfiltrate large amounts of guest data, reducing the scope of the breach.

1. Active Directory Security

Firstly, Lepide could have minimized dormant accounts, often referred to as "stale AD accounts." These unused accounts provide easy entry points for attackers. By identifying and removing inactive accounts, Lepide would have shrunk the potential attack vectors significantly. Additionally, it could have enforced stricter password policies; mandating stronger password combinations and enforcing regular password changes. Weak passwords were a contributing factor in the breach, and Lepide's stricter policies could have acted as a crucial barrier.

Secondly, Lepide could have detected and flagged suspicious activity related to administrator privileges. The attackers gained unauthorized access by exploiting admin rights, and their actions went unnoticed for an extended period. Lepide's real-time monitoring capabilities could have identified unusual changes in privilege elevation, triggering immediate alerts and investigations, potentially stopping the attackers in their tracks.

By addressing these two critical areas - stale accounts and admin privilege security - Lepide could have significantly bolstered Marriott's defenses and potentially prevented the devastating data breach. Its proactive approach to managing access and identifying anomalies could have made a crucial difference in safeguarding sensitive guest information.

2. Data Discovery and Classification

Firstly, Lepide could have identified and classified sensitive guest data within the acquired Starwood systems. This process involves tagging and categorizing information based on its level of vulnerability (e.g., passport numbers, credit card details). With data accurately classified, Marriott could have prioritized protection measures, focusing resources on safeguarding the most critical information. This targeted approach would have been significantly more efficient than applying generic security measures across all data, potentially plugging the gaps exploited by attackers.

Secondly, Lepide could have facilitated the implementation of stricter access controls and monitoring for classified data. Knowing exactly where sensitive information resides allows for granular control over who can access it and under what circumstances. Lepide could have helped establish stricter access requirements, potentially limiting access to only authorized personnel with a legitimate need. Additionally, it could have enabled real-time monitoring for suspicious activity around classified data, alerting security teams to any unauthorized access attempts, potentially stopping breaches before they escalate.

By enabling data classification and facilitating stricter access controls, Lepide could have helped Marriott significantly reduce the attack surface and protect sensitive guest information. Its ability to identify and prioritize critical data, coupled with robust access control and monitoring, could have been instrumental in preventing the devastating breach.

3. User Activity Monitoring

Marriott's data breach serves as a stark reminder of the importance of comprehensive file server auditing. Had such a system been in place for the acquired Starwood systems, it could have played a crucial role in detecting the breach much earlier, potentially limiting the damage significantly.

File server auditing continuously monitors activity on file servers, recording details like who accessed what files, when, and from where. In the context of the Marriott breach, this audit trail would have captured any unusual activity patterns employed by the attackers. They might have accessed sensitive guest data at odd hours, downloaded large amounts of information, or made unauthorized modifications to files. By analyzing these audit logs for anomalies, security teams could have identified suspicious activity much sooner, potentially triggering an investigation and stopping the attackers before they inflicted significant damage.

While hindsight is always 20/20, implementing robust file server auditing offers a proactive approach to data security. By providing detailed activity logs and highlighting unusual patterns, it empowers organizations to detect and respond to breaches swiftly, minimizing the potential impact on sensitive information and individuals.

4. Data Loss Prevention

Firstly, Lepide could have detected and alerted on attempts to exfiltrate large amounts of guest data. Its real-time monitoring capabilities, threshold alerting, and pre-defined threat models would have identified unusual data transfer patterns, potentially indicating unauthorized access. Security teams would then be instantly notified, allowing them to investigate and potentially stop the exfiltration before significant damage occurred. This rapid response could have drastically minimized the number of impacted individuals and the amount of stolen data.

Secondly, Lepide could have implemented data loss prevention (DLP) controls to automatically block the exfiltration of sensitive information. By defining specific threat action workflows, and enabling threat custom threat response actions, Lepide could have identified and prevented data exfiltration in real time. This proactive approach would have significantly restricted the attackers' ability to steal guest information, further limiting the scope of the breach.

In conclusion, by offering real-time anomaly detection, pre-defined threat models, and threat response actions, Lepide could have been a valuable tool in mitigating the Marriott data breach. Its ability to identify and halt suspicious data transfers could have minimized the impact on guests and protected their sensitive information.

Get peace of mind that your identities and data are secure with Lepide.

Take a look at our interactive demo to see how Lepide can help your business achieve your security and compliance goals.

Launch Interactive Demo