Investigating Sensitive Information Leak in a Publishing Business

Customer Profile

Industry: Publishing and Book Distribution
Business Overview: A mid-sized publishing business with operations involving the creation, management and distribution of books across multiple languages and categories. Its business depended on protecting commercially sensitive information, including pricing and other internal business data.

The Problem

The organisation experienced repeated data leakage of confidential pricing information, creating significant business and commercial risk.

Preliminary analysis indicated that the leaks were originating from five possible endpoints, but there was no clear evidence identifying the responsible user or the method of data theft.

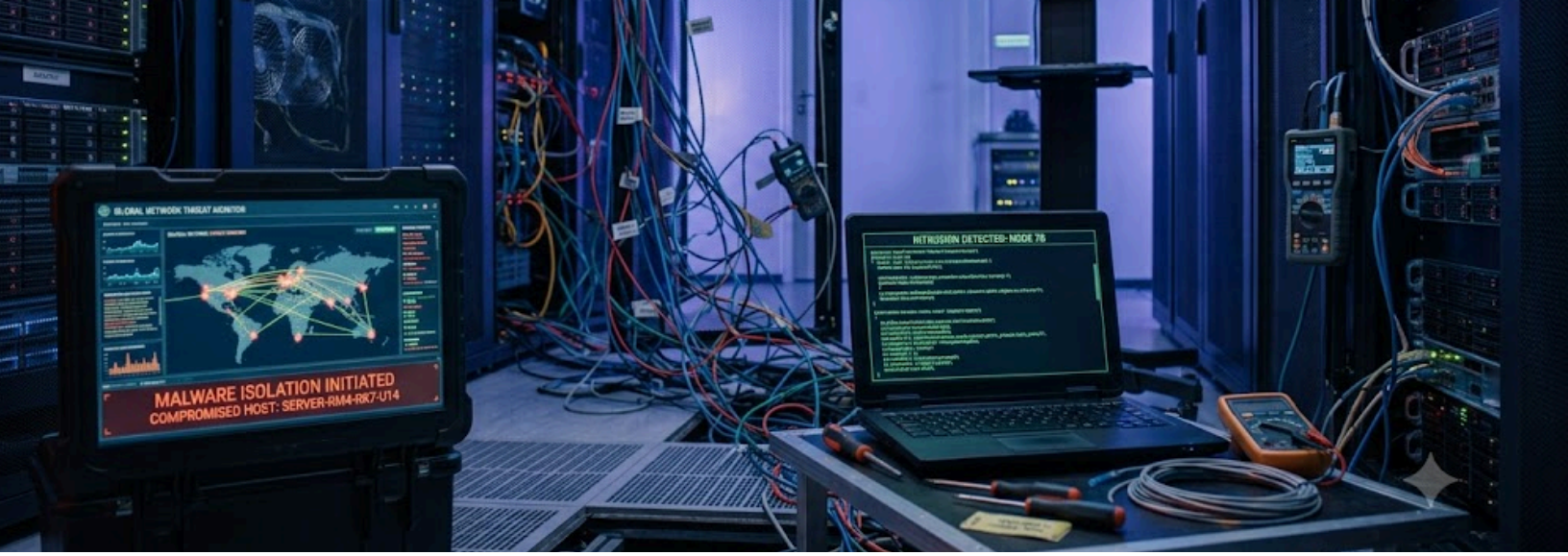
The customer engaged Eagle to perform a security investigation to identify the source of the leakage, analyze user activity, review endpoints , correlate audit logs, and determine how sensitive information was leaving the organization. The objective was to establish evidence-based findings before implementing security controls.

The Solution

Eagle conducted a forensic investigation across the identified endpoints, analysing file access logs, endpoint activity, emails, user behaviour, USB usage, audit trails, and data movement patterns to identify the root cause of the data leakage.

Based on the findings, Eagle put controls in place to monitor how sensitive pricing information was accessed, copied, transferred and shared. Alerts and controls helped identify and prevent unauthorised sharing of confidential information.

These controls helped the organisation understand where sensitive data was being leaked and take appropriate action. Data Loss Prevention (DLP) helps organisations prevent sensitive data from being shared without authorisation.



Conclusion

By combining a security investigation with data protection controls, Eagle helped the organisation identify the source of sensitive data leakage and establish stronger controls over confidential business information.

The customer gained improved visibility into endpoint activity, enhanced protection against insider threats, and a proactive framework for preventing future data leakage. The engagement reinforced a key cybersecurity principle: effective data protection begins with understanding how sensitive information moves before controlling where it can go.

- We start by understanding your business and the challenges you face. We then bring the right expertise and technology to address them, strengthen your security, and keep your business going.

Our Services

24×7 SOC Monitoring	Identity & Access Management	Application Security Monitoring	EDR & XDR
Firewall Management	IDS/IPS Monitoring	Cloud Security Monitoring	Email Monitoring
Data Loss Prevention	VAPT	Threat Hunting	SIEM & SOAR
Incident Response Retainer	**Digital Forensics**	Threat Intelligence	Security Policy & Governance Advisory