JOINT SOLUTION BRIEF

Data Loss Prevention That Stops Exfiltrations Without Making Users' Lives Difficult

The Challenge

You need to help ensure that sensitive data isn't exfiltrated from your network, either by insider threats or outside attackers who breach your perimeter. Traditional DLP solutions require extensive management resources and make things cumbersome for legitimate users.

Integrated Solution

ITsMine uses the visibility into SMB traffic that the Gigamon Security Delivery Platform provides and its own AI capabilities to determine which folders in your file system are most at risk for data exfiltration. Disposable endpoint agents generated by ITsMine monitor risky user behavior, and when exfiltration is detected can block illicit copying to external media and record forensics data for future prosecution.

Joint Solution Benefits

- Pervasive visibility: Traffic from physical infrastructure and Azure/AWS can all be analyzed by ITsMine
- Filter out irrelevant traffic: Helps ensure that only the SMB network traffic ITsMine uses to perform its analysis is delivered
- Inspect encrypted traffic: Decrypts SSL traffic for out-of-band inspection and analysis
- Scalable threat protection: Can distribute de-duplicated, high-fidelity network traffic from multiple network links

Introduction

There are a staggering number of ways your organization's sensitive data could end up in the wrong hands. It could be transmitted by email, sent in an instant message, posted on a website or saved to a USB drive. Data loss prevention (DLP) solutions aim to prevent those leaks.

Legacy DLP solutions are often cumbersome productivity killers, both for users and IT. They require an endpoint agent installed on all computers in the organization, and creating accurate policies is so complex that customers often need extensive professional services for as long as a year after initial deployment, as well as expertise to maintain and constantly manually fine-tune the product.

DLP solutions can also trigger false positives and block legitimate business efforts, which leads users to switch to a monitor-only mode that doesn't block data leaks, rendering the solution ineffective. With the consumer data protection mandates set down by the GDPR, you can't afford to ignore these types of breaches.

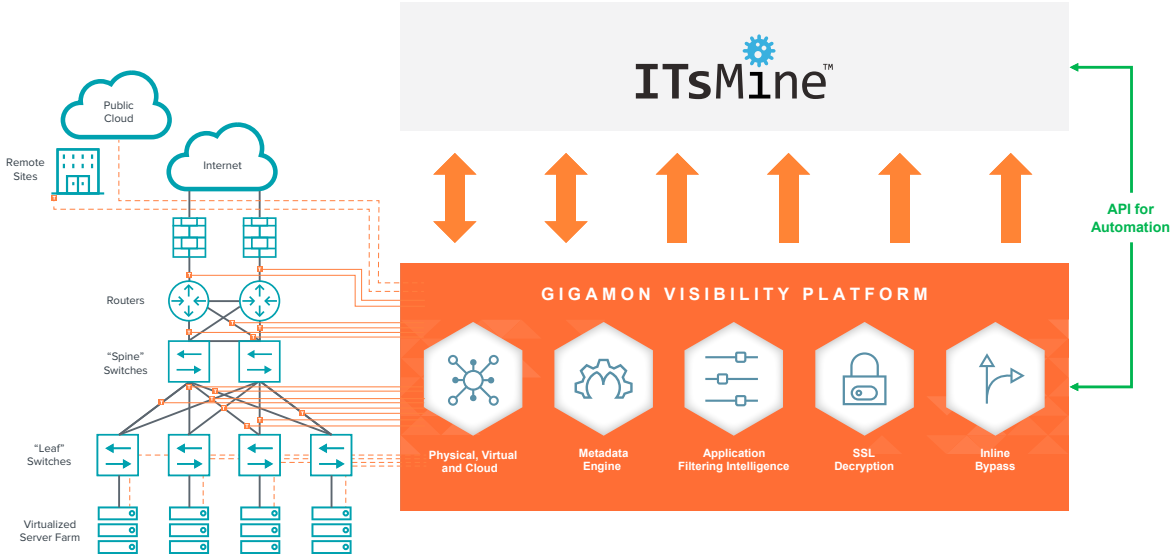
The Gigamon-ITsMine Joint Solution

ITsMine offers a DLP solution that requires no policies and no permanent endpoint agents, proactively protecting data and generating alerts. When integrated with the Gigamon Security Delivery Platform, ITsMine provides the ability to detect a breach in the middle stages of the attack lifecycle while providing the real-time forensics and actionable intelligence you need to block exfiltration of sensitive data. The solution also can detect data leakage and provide critical forensics information, including IP address and location, that will allow proactive responses to a breach.

The Gigamon Security Delivery Platform enables other tools — security, analytics, and performance monitoring products — to function efficiently and effectively. Aggregating traffic across the network, optimizing the flow of packets to individual tools, offload tasks from those tools, and use a variety of techniques to increase the availability of networks and applications. These capabilities allow enterprises to maximize network availability, improve security, and reduce costs, even as network traffic surges and computing environments become more complex.

Here the platform filters out irrelevant packets ensuring ITsMine focus entirely on the SMB (Server Message Block) network traffic it needs, to track down breaches. Using data about folder permissions, active directory groups, and the pattern of traffic to and from your company's file servers, ITsMine's Machine Learning algorithm determines the folders in your filesystem that contain the most sensitive data. ITsMine installs SoftwareMines in these folders, which when triggered deploys a disposable endpoint agent to risky users in order to track and calculate their risk level.

If the user is conducting only legitimate business, the agent will dissolve within hours. If, on the other hand, the user is deemed malicious, they can be blocked from saving to external storage. If an internal employee is harvesting sensitive data, the forensics are captured for future prosecution. Thanks to the Gigamon Security Delivery Platform's cloud capabilities, the joint solution can spot data exfiltration not just from your local physical network, but also from AWS and Microsoft Azure instances as well.



Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com