

## Plugging Information Leaks

### Why starting at the application level is important

Data leaks can be detected and prevented at three levels: the application level, the network level, and the desktop level. At the network and desktop levels, the tools work by looking for sensitive data created in outbound messages (e.g., email and instant messages) or in media created at the desktop (e.g., via printing, writing to USB flash disks, or writing to CDs). While these solutions may effectively curtail unintentional data leaks, they are not effective against intentional data leaks for two reasons:

- Malicious users can view sensitive information on the screen and then copy it to a piece of paper or take a picture of it, without printing it or sending it via email.
- Network data leak prevention (DLP) solutions typically look for combinations of customer fields (e.g., SSN, account numbers, and credit cards) loaded from the corporate database. But this process can be easily bypassed by users with no technical background. All they need to do is use the 'PrintScreen' command of the pages to be leaked and then paste them as pictures into an outbound email, where they cannot be analyzed by the DLP solution.

Fraudulent users can also alter the sensitive data to throw off pattern recognition. For example, a 'ChangeAll' of the digit '1' to the letter 'l', or the digit '0' to the letter o. Again, the DLP solution will not be able to identify the sensitive information.

But you can successfully prevent leaks by starting at the application level. In other words, by monitoring application usage so that you know exactly when sensitive information is being displayed on the user screen. When applications are monitored pro-actively, the fraudulent behavior that occurs prior to a leak can be detected. And the leak can then be prevented at the point of data access—regardless of the strategy for leaking the data.

### The Attachmate Luminet Approach

Unlike traditional DLP solutions, Attachmate® Luminet™ fraud management software monitors end-user activity at the application level. With Luminet you can:

- Record user activity within applications and generate a detailed forensic audit trail without relying on application log files. The Luminet audit trail includes all user queries. (While user queries are not typically logged by applications, they are critical for detecting information leaks.)
- Conduct powerful full-text searches through current or recorded activity, visually playing back every screen and keystroke relevant to an alert or a case. For example, you can search to find all the users who accessed a specific account number in a specific timeframe.
- Profile user behavior based on activity at the application level. The Luminet link analysis tool reveals user activity patterns, trends, and complex relationships across diverse enterprise applications.

You don't need to deploy any agents on the clients or the server, and there is no impact on system performance.

### Luminet Rules

With Luminet you can define adaptable business rules that pinpoint suspicious behavior based on your risk management strategy. For example, you can define rules to identify:

- Excessive number of accounts viewed by a user per day and week.
- Excessive browsing of VIP customer data performed by a user per day/ week.
- Excessive browsing through other employees' data performed by a user.
- Search for customer data by customer name (as opposed to account number).

- Excessive browsing of accounts with no action taken.
- Patterns of access to the same account over a period of time that differ from other users.
- Access to sensitive fields (e.g., identification, credit limit, transaction amount, customer address).

Once suspicious behavior has been detected, Luminet generates real-time alerts related to questionable activity patterns, allowing you to immediately zero in on anomalies.

### See. Record. Analyze. With Luminet.

Trusted employees commit more fraud and compliance violations than anyone else. The business risks—financial loss, failed audits, and brand damage—are devastating. Fortunately, Luminet can help. Unlike other fraud management solutions, Luminet sees, records, and analyzes user activity at the application level. It gives you the tools you need to connect the dots between activities and relationships—and then take informed action.

### About Attachmate

Attachmate delivers advanced software for terminal emulation, legacy modernization, managed file transfer, and enterprise fraud management. With our technologies, more than 65,000 businesses worldwide are putting their IT assets to work in new and meaningful ways. [www.attachmate.com](http://www.attachmate.com)



**Corporate Headquarters**  
1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL 206 217 7500  
800 872 2829  
FAX 206 217 7515

**EMEA Headquarters**  
The Netherlands  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

**Asia Pacific Headquarters**  
Australia  
TEL +61 3 9825 2300  
FAX +61 3 9825 2399

**Latin America Headquarters**  
Mexico  
TEL +52 55 9178 4970  
FAX +52 55 5540 4886

WEB [attachmate.com](http://attachmate.com)  
E-MAIL [info@attachmate.com](mailto:info@attachmate.com)

For regional office information, visit [www.attachmate.com](http://www.attachmate.com).