Shining a Light on Insider Abuse
How Luminet™ software takes the guesswork out of application monitoring

The threat of insider abuse looms large over businesses of every size. In addition to direct financial losses, insider abuse undermines customer confidence and can irreparably damage your brand. The 2010 report on occupational fraud and abuse by the Association of Certified Fraud Examiners found that firms lose an average of 5 percent of annual revenue to fraud each year, resulting in a total loss of nearly $2.9 trillion globally.*

The frustrating truth is that the people most capable of gaining unauthorized access to systems and data are also those who hold the highest degree of organizational trust—employees, contractors, and business partners. Their inside knowledge of business processes and security controls, combined with their authorized access to critical systems, puts these individuals in a unique position to manipulate data and steal assets.

Traditional fraud detection methods, such as application logging, can’t address the scale and sophistication of the threats you face today. Fortunately, modern technologies give you a whole new way to address them. Attachmate® Luminet™ software delivers enterprise-scale fraud detection and prevention capabilities—letting you see, record, and analyze user activity across all applications. Ultimately, Luminet removes the guesswork from application monitoring—giving you the intelligence you need to take informed action.

Why Insider Abuse Is Hard to Detect

Firewalls, Virtual Private Networks (VPNs), and Intrusion Detection Systems (IDSs) all work effectively to block access to information and resources from outsiders. But these security controls are powerless against malicious insiders with legitimate business reasons for accessing applications, querying databases, and changing system configurations.

Malicious insiders can exploit three factors that work in their favor:

- **Access to multiple applications**
  Employees with access to multiple applications can carry out a sequence of tasks that make their acts look legitimate. For example, an employee with the privileges to create an accounts payable record for a vendor could also create a bogus front company in the system and then issue payments to that company. One possible solution—a separation of duties—is not always possible. For example, a manager may need access to multiple applications to correct errors, approve certain transactions, or perform nonclerical operations.

- **Knowledge of business processes**
  Employees working in the same department for several years accumulate detailed knowledge about workflows and operations, including exception-handling and monitoring procedures. For example, an employee in the finance department, with experience running management reports and providing data to auditors, knows which transactions are likely to trigger review and which are likely to go unnoticed.

- **Ability to avoid detection by logging-based monitoring controls**
  Employees with detailed knowledge of logging procedures can also craft their schemes to reduce the chance of detection. For example, if manager overrides are always logged and reviewed, the perpetrator can avoid those operations and instead create false transactions that blend into the usual stream of daily transactions.

These three factors make it difficult to counter insider threats with traditional methods. Your risk management strategy must evolve to mitigate these vulnerabilities if it is going to be effective.
Where Logging Falls Short

Application logging, a fundamental tool for IT operations and systems management, was not designed for fraud management and auditing. In the absence of true application monitoring technology, however, it has become the default method used. But as enterprise applications become more distributed and encompass more complex functionality, your ability to force traditional logging to function as a modern fraud solution becomes untenable for two reasons:

- **Isolated log entries**
  
  Like your business processes, fraud is a multistep process that typically involves several applications. A transaction entered in one web application, a change to a department database through another, and a query through a mainframe system may all be part of both a critical business process and a fraud scheme.

  Traditional logging, on the other hand, is typically focused on a single application component, such as a database, application server, or messaging subsystem. Each component creates a different log with different levels of information defined in different formats. Isolated log entries about the events in one component are difficult to correlate with events recorded in other logs. Something as simple as a server with an out-of-sync clock can make it difficult to integrate data from two logs. What’s more, logs do not share common data types or formats, so linking data depends on lucky guessing as much as sound logic.

- **Incomplete information**
  
  The challenge of using logging as the foundation for detecting abuse is multiplied by the inherent limits of the information available to you. Only a fraction of the activity that occurs between employees and applications is captured by traditional logging—which means that a significant amount of potential evidence is missing from your investigations. Without complete and forensically sound information, you are unable to take informed action.

  Here’s an example: Let’s say a database trigger logs an account update, recording an original monetary value and a new value. While useful for IT system administration, this update is missing information that is crucial to investigators:
  - The identity of the user performing the update.
  - The application module used to initiate the update.
  - Links to events that occurred prior to and following the update.

  Even if application developers wanted to include some of this information, it might not be available at the database level. For performance reasons, database connections are typically pooled and associated with a single database account, and that one account may be shared for all connections. The identity of the application user is inaccessible to the lower levels of the database transaction. With only limited ability to track and record a subset of all potentially useful information, logging will perpetually fall short of meeting enterprise monitoring requirements.

Given the limitations of traditional logging, a fundamentally different approach is required.

Multichannel Monitoring with Luminet

Attachmate Luminet fraud management software extricates us from the constraints of single component logging. Luminet captures a complete history of user activity, straight off the network, so you can collect the clear and legally actionable forensic evidence—without costly modifications to existing applications.

**An over-the-shoulder view.** Luminet captures a real time, over-the-shoulder view of all user activity, which means insiders can no longer avoid detection by splitting their activities over multiple applications. For example, a user might be able to avoid triggering alerts in a single application or bypass a user interface to make changes to a database without logging an event. These actions might avoid detection by conventional log monitoring, but they still leave traces in the stream of network traffic.

Another advantage of Luminet is its breadth of coverage. Users can interact with applications through complex workflows, middleware, messaging services, and even direct access to the database. Luminet records that
Shining a Light on Insider Abuse

How Luminet™ software takes the guesswork out of application monitoring activity and stores it in a secure repository. You can easily search, retrieve, and replay any part of a user’s complete history at any time. You can also use Luminet to create detailed and aggregate reports, alerts, and dashboards to help you detect, understand, and investigate suspicious activity.

Connecting the dots. Businesses generate enormous volumes of network application traffic every day, and sifting through it for illegitimate activity is daunting. Luminet addresses the challenge with robust behavior pattern analysis and profiling capabilities that detect suspicious patterns and pinpoint anomalies—even with thousands of users accessing dozens of applications.

Is a manager accessing confidential customer information at two to three times the rate of other managers? Does one financial clerk exhibit an unusual pattern of payment activity with a particular vendor? Automatic alerts on these comparisons with profile baselines can feed directly into Luminet’s risk-scoring engine and help investigators focus on the cases that truly warrant further investigation.

Once isolated, the true anomalies can be investigated immediately—no waiting for IT to retrieve cryptic log files, no hours of manual log review. With Luminet, you can drill down directly from the automatic alert or risk-scoring reports and instantly search, analyze, and replay exactly what the suspicious users were doing—step by step and screen by screen—connecting the dots needed to build a solid case.

The extensive data Luminet collects via network monitoring, combined with Luminet’s robust set of rules, makes it possible for investigators to distill volumes of raw data into actionable information.

Visualize complex patterns of behavior and collusion with dynamic link analysis.
Luminet: Changing the Threat Landscape

Traditional approaches to new threats perpetuated by malicious and increasingly sophisticated insiders no longer work. What’s needed is a way to eliminate the risks presented by incomplete silos of information and the inability to connect the dots between multiple channels. That’s where Attachmate Luminet comes in. Designed from the ground up to address the unique challenges of modern fraud management, Luminet provides a complete view of user activity on enterprise applications—highlighting suspicious behavior and giving you the intelligence you need to take informed action.

* Association of Certified Fraud Examiners, 2010 Report to the Nations on Occupational Fraud and Abuse

Supporting Regulatory Compliance with Fraud Management

Like everyone else, you have probably bumped up against increasingly stringent industry and government regulations. These regulations were created to reduce identity theft and customer data breaches—the same types of security violations you’re tasked with detecting and preventing in the fraud management world.

In fact, why not leverage your fraud detection and prevention tools to support the auditing required for regulatory compliance? In the past, the limitations of traditional auditing methods would have made that impossible. But now, with Luminet, the same continuous monitoring and auditing you employ for investigations can be easily transferred to your compliance work.

For example, you can use the data collected by Luminet to show that only authorized users are accessing a particular legacy application. You can identify activities that fall outside the expected range, such as one employee reading the details of VIP health records significantly more than other employees in the same role. What’s more, Luminet’s flexible auditing and reporting capabilities will allow your compliance officers to quickly adapt to the ever-changing requirements they receive from external auditors and regulators.