

## Privileged User Management and Financial System Hardening for Sarbanes-Oxley Compliance

### CUSTOMER SNAPSHOT



Moody's KMV, a subsidiary of Moody's Corporation offering credit decision support products that integrate with clients' pre-existing customer systems.

#### ► Web Site

[www.moodykvm.com](http://www.moodykvm.com)

#### ► Industry

Financial Services

#### ► Problem

Moody's KMV had just six weeks to correct vulnerabilities in its financial database system to secure Sarbanes-Oxley certification. In particular, the company needed to gain comprehensive control over the activities of back-end administrators and establish clear separation of duties in order to maintain the integrity and accuracy of financial data.

#### ► Solution

Moody's KMV implemented Digital Guardian from Verdasys to analyze system and database access and maintenance activities and implement new compliance-driven audit trails and policies that ensure proper and authorized use of financial applications, data and systems.

#### ► Benefits

With the help of Digital Guardian and the Verdasys professional services team, Moody's KMV met the expectations of Sarbanes-Oxley auditors – while preventing database access violations and information misuse through iron-clad acceptable use policies that are enforced in real-time and a comprehensive monitoring and alert system to help it remain in continuous compliance. The company is rolling out Digital Guardian to 500 users across several departments.

Moody's Corporation has a name that is synonymous with business. Moody's KMV, a subsidiary, is the leading provider of quantitative products for credit-sensitive investors, offering models that provide current default probabilities, recovery estimates, valuations, and correlations that are widely used to assess portfolio risk/return. Serving more than 1,500 clients in 80 countries, including 70 percent of the world's largest banks, Moody's KMV maintains the largest database of corporate defaults in the world and provides credit decision-support products that integrate with pre-existing customer systems.

#### **Maintaining Trust and Assuring Compliance**

Like all public companies, Moody's KMV must comply with the Sarbanes-Oxley Act, which protects investors by demanding that companies ensure the accuracy and integrity of corporate financial reporting. Since Moody's KMV's business is built on a foundation of customer trust regarding the reliability of its data, complying with Sarbanes-Oxley was more than just a legal obligation.

"Sarbanes-Oxley compliance is a critical business issue for Moody's KMV because it is vital that our company lead by example," said Mario Duarte, director of security, Moody's KMV.

To secure its financial systems from misuse by privileged users and prevent the inadvertent or intentional modification of financial data, Moody's KMV turned to Verdasys and its Digital Guardian data security platform. With Verdasys' help, Moody's KMV established a set of best practices for the operation of its back-office financial application environment and implemented the appropriate controls and audit trail around user activity to satisfy the requirements of Section 404 of the Sarbanes-Oxley Act as well as the expectations of its clients.

## VERDASYS™

Data Security at the Point of Use

## Pre-Audit Findings Highlight Challenges

In July 2004, Moody's KVM was informed that its Sarbanes-Oxley audit was scheduled for just after Labor Day. To obtain a baseline of its vulnerabilities before the formal audit, Moody's KVM contracted with a Big Four consulting firm to perform a pre-audit of its financial systems and the surrounding security environment. The pre-audit revealed two issues that had to be rectified quickly if Moody's KVM was going to receive a letter of attestation for its compliance with Sarbanes-Oxley.

The first vulnerability identified in the company's existing controls was system and database administrators' ability to freely access and modify executables and other system resources, such as dll files and OS logs – and the lack of any auditing or controls around such activity. In addition, database administrators with certain access rights had the ability to actually erase database log files for the financial system without a trace, which left Moody's KVM vulnerable.

The second issue identified in the pre-audit was a need for better separation of duties between different kinds of administrators and better auditing of routine system maintenance and change activities. Previously, when a database administrator made a change to the database software or applied a system patch, the action went unchecked. As a result, Moody's KVM could not ensure that the change was sanctioned or performed correctly. The company needed an audit trail that could track changes to the financial system software, its supporting databases and its underlying operating system, while ensuring changes were performed only by appropriate individuals.

"The pre-audit identified several questions: Who has access to our financial applications, what are they doing with the data and can we record or audit this activity?" said Duarte. "From a best practices standpoint, solving these issues was important."

Moody's KVM operates its back-office financial systems on several servers with a mix of databases, third-party applications and legacy applications. Unfortunately, the company's accounting software would not have the necessary change management and reporting capabilities needed to help

Moody's KVM satisfy its audit requirements for several years – and implementing a new accounting application was simply impossible in the available timeframe. Moody's KVM found the solution it needed in Verdasys Digital Guardian.

## Streamlining Data Security for Sarbanes-Oxley Compliance

The first solution that monitors information at the point of use – desktops, laptops and servers – Digital Guardian from Verdasys is an information security platform that provides seamless, secure monitoring and control of corporate information. Digital Guardian not only provides critical, real-time compliance policy enforcement and auditing of financial information and application use, but also allows for the ad hoc creation of reports that prove the effectiveness of controls to auditors and enable companies to respond quickly to actions that violate policies.

The Digital Guardian system consists of a web-based management server and host-based agents that can be rapidly deployed across an organization and transparently integrated with existing infrastructures. Once installed on desktops, laptops and servers, the agents track all file, application, network, clipboard and printing operations. This low-level OS and application activity is then filtered and synthesized into a reduced volume, easy-to-read activity journal that can be used for audit, forensics and compliance reporting purposes. The agents also enforce explicit information and application use rules by taking action against user activity that violates policies and puts the organization at risk of non-compliance. By operating at the kernel level, the tamper-resistant agents remain unseen while providing oversight of all users, regardless of the level of administrative rights they possess.

In addition to integrating activity information from all agents into a single, enterprise-wide activity journal, the Digital Guardian management server provides for agent deployment, audit and forensic reporting, policy definition and distribution and alert management – all through an intuitive, easy-to-use web interface.

*“Digital Guardian is a cost-effective solution for addressing virtually all of our security-related Sarbanes-Oxley compliance issues with minimal impact on our systems, servers and users.”*

*David Stanton, Moody’s KMV security analyst*

“Sarbanes-Oxley compliance requires you to tackle numerous initiatives in a relatively short time. Digital Guardian is a cost-effective solution for addressing virtually all of our security-related Sarbanes-Oxley compliance issues with minimal impact on our systems, servers and users,” said

administrators, who have elevated rights and full control over the computers. Now we are monitoring the administrators,” said Stanton. “If you’re a database administrator or another user with elevated access rights, it used to be possible to cover your tracks. For instance, an administrator could create a new user and then delete it without anyone else being notified. They could even alter the application. But with Digital Guardian, we’ve eliminated these possibilities and are now protecting the data as well as the application itself. Even the administrators who manage Digital Guardian can’t delete their actions without someone being notified.”

Today, Moody’s KMV knows instantly who accessed its financial applications, systems and data, from which machine and application, and whether the use or modification carried out was appropriate. This allows the company to hold users accountable for the appropriate use of sensitive corporate data and the integrity of financial applications and reporting processes.

With the implementation of Digital Guardian, when a user violates a rule, a member of the Moody’s KMV security team is immediately notified by an alert that appears on the Digital Guardian administrative console. This enables Moody’s KMV to immediately assess and quickly respond to all violations as needed. Digital Guardian not only notifies the security team that something is wrong, but automatically generates an audit trail in the company’s ticketing system.

“The Digital Guardian-powered alert system and audit trail directly supports our Sarbanes-Oxley certification,” said Stanton. “The auditors required us to demonstrate that we view, respond to and log all alerts in a ticketing system. Digital Guardian manages the entire process seamlessly.”

Moody’s KMV was also able to isolate and eradicate the potential exposure of confidential financial information by users who copy it to laptops, which can be easily lost or stolen, move it to removable media or attempt to transmit it using web mail and other messaging applications. “With Digital Guardian, we now see all the data coming in and going out of the system,” said Stanton.



*Using Digital Guardian’s summary and drill-down reporting capabilities, the Moody’s KMV security team can quickly and easily provide auditors with the high-level reports and forensic detail needed to verify that their controls are effective and have not been violated.*

David Stanton, Moody’s KMV security analyst. “At the same time, it is a highly adaptable solution that will enable us to easily implement new best practices as they are adopted.”

### **New Rules Thwart Database Access Violations**

With the clock ticking, teams from Verdasys and Moody’s KMV began solving the company’s Sarbanes-Oxley deficiencies by deploying a sample set of agents to collect activity data from Moody’s KMV’s IT environment. Together, the teams reviewed three days of actual application and user activity to filter out normal activity and isolate exceptions and violations to database access processes. Based on this information, they then created and deployed Digital Guardian policies that fortified the financial database environment against unauthorized access and use. “Under Sarbanes-Oxley rules, you have to watch over IT

## Meeting Auditor Expectations

With the help of Verdasys, the Digital Guardian platform and a host of new business rules implemented across a key group of engineering and IT users, the deficiencies noted in the pre-audit were addressed in time for the official audit by another Big Four firm. The audit consisted of a review of Moody's KMV's data access policies as well as a live demonstration of the system.

As part of the demonstration, the auditors instructed Moody's KMV to deliberately violate policies to see how Digital Guardian responded and displayed the resulting information on the security console. Moody's KMV users performed a series of actions in an attempt to gain unauthorized access to financial data. In every case, Digital Guardian successfully prevented the access. When a user was blocked, a real-time prompt informed them of the reason based on the company's compliance and security policies. Each attempt was also immediately logged and generated a real-time alert.

Moody's KMV's Duarte reports that auditors were satisfied with the new solution. "Digital Guardian is like having an auditor, security group and consultant all in one package," he said. "You can spend days and weeks trying to convince an auditor that your controls are adequate, but with Digital

Guardian, we were able to cut this down to hours. Every time we had an issue, we just told the auditor how we're employing Digital Guardian, and it was 'case closed.' "

## Addressing Enterprise Security Needs

Digital Guardian is being rolled out in a phased approach throughout Moody's KMV. Following a limited implementation as part of the Sarbanes-Oxley audit process, Digital Guardian was installed in the finance, human resource and IT departments in the fall of 2004. Moving forward, Moody's KMV anticipates deploying Digital Guardian to the entire company to address additional issues such as the installation of unauthorized software and intellectual property protection.

Moody's KMV credits both Digital Guardian and the Verdasys professional services team for the company's success in addressing its compliance objectives. "There was significant collaboration between Moody's KMV and Verdasys in the effort to meet the auditors' demands in such a short time-frame," said Duarte. "Verdasys went above and beyond the call of duty. We not only met the immediate challenges of Sarbanes-Oxley, but we are well-positioned to address future challenges as they arise."

## ABOUT VERDASYS

*Verdasys is pioneering a new generation of real-time compliance solutions designed to maintain the security, confidentiality and veracity of regulated information wherever users access, utilize or communicate data. Its unique Continuous Compliance Assurance capability addresses compliance and privacy requirements, namely assuring that the company is in compliance and remains in compliance on an ongoing and real-time basis.*

## ABOUT DIGITAL GUARDIAN

*Digital Guardian provides data security at the point of use and enables companies to understand all risks of exposure and misuse of their data, monitor the movement of files and the use of applications, storage and networks, and prevent unauthorized actions that can put information and compliance in jeopardy. By actuating corporate information use policies in real time, Digital Guardian assures companies that they are meeting government-mandated information privacy, security and auditing requirements and remaining in compliance on a real-time, ongoing basis.*

For more information on Digital Guardian and how it can help your organization, [visit www.verdasys.com](http://www.verdasys.com).

## VERDASYS

950 WINTER STREET, SUITE 2600 WALTHAM, MA 02451  
781-788-8180 TEL 781-788-8188 FAX

[WWW.VERDASYS.COM](http://WWW.VERDASYS.COM)