datiphy™

CASE STUDY
Finance and Banking

FINANCIAL ORGANIZATION USES DATIPHY TO MONITOR AND PROTECT DIGITAL ASSETS

Financial institutions store vast amounts of sensitive data to effectively run their daily business. For that reason their operations are required to follow strict regulatory rules to maintain compliance. The banking industry must protect themselves from a range of cyber attacks while providing convenient services to customers both public and private. To keep their operations smooth and safe, one of Datiphy's flagship banking customers has adopted an industry standard perimeter defense utilizing both firewalls and Security Information and Event Management (SIEM). But, these practices are not effective at deterring internal threats coming from privileged users or compromised accounts.

The following is a synopsis of a real incident that clearly demonstrates the vulnerability of standalone perimeter defense. After servicing retail customers for several decades some bank accounts had become inactive or even dormant. This often occurs when the rightful owners of these accounts become absent for any number of reasons. At this financial organization an administrator/data base administrator (DBA) in charge of these inactive financial accounts used their privileges to authorize money transfers. An accomplice was then able to start withdrawing funds from the dormant account. Because the administrator/DBA was aware of how the bank operated, the withdrawals stayed undetected for an extended amount of time. While the bank was able to set up policies and rules for database access, a super user is often able to circumvent the rules and later cover their tracks by deleting change logs or user credentials. Crimes of this nature are very hard to detect or even prosecute due to the lack of tangible evidence. After the above incident took place the bank deployed the Datiphy solution to manage internal threats.

KEY BENEFITS:

- **Independent auditing handling**
- **Continuous and complete compliance monitoring**
- **Real-time email, SMS, syslog, and SNMP alerting**
- **Complete and independent record for non-repudiation**
- **Instant intelligence for cross-platform heterogeneous environments**

Below we compare the difference - with and without Datiphy DatiDNA™ - before, during, and after the attack.

BEFORE	Without Datiphy	With Datiphy
Auditing	Audits depended on data provided by admin/IT	Independent auditing handled by a separate team such as CSO
Compliance	Infrequent/limited checking for compliance through IT	Continuous and complete compliance monitoring

The bank regularly audited its IT systems for compliance and to prevent security violations. However, such audits relied on data provided by the IT staff, including the perpetrator. For practical reasons, complete auditing could not happen frequently thus allowing the perpetrator the opportunity to make fraudulent audit reports without revealing the violations. Datiphy DataDNA runs out of band and is independent of regular IT operations, so the compliance and audit reports can be generated, with no performance cost, and remain independent of the monitored IT system.

DURING	Without Datiphy	With Datiphy
Alerting	Limited capability, logging by DB or other applications	Real-time email, SMS, syslog, and SNMP
Action	Limited capability, logging by DB or other applications	Configurable script execution for network or DB management

Without Datiphy, an inside perpetrator may know about, or even be involved in, setting the alert triggers and log system of SIEM tools circumventing actions to evade detection. Datiphy DataDNA offers precise configurable alerts and triggering policies that can be managed by independent security teams (CISO or Risk Management Departments) making violations more likely to be exposed. The Datiphy system sets alerts based on any combination of who, what, how, when, or where database activity is happening and further extends the coverage with behavioral policy and signature-based content policy. In the event of a security violation, Datiphy DataDNA sends out alerts, in real-time, and executes a pre-configured script to prevent further violations.

AFTER	Without Datiphy	With Datiphy
Forensics	Insiders can delete logs and destroy evidence	Complete and independent record for non-repudiation
Analytics	Difficult and time consuming even if logs are available in heterogeneous environments	Organized for instant queries; Instant intelligence for cross-platform heterogeneous environments

After a security violation occurs, it is paramount to completely investigate the incident, and the party/parties responsible for the malicious act instantaneously. Unfortunately, many hours, days, or even months may have passed before a violation is noticed and investigations begin. That time allows inside perpetrators to cover their tracks by deleting logs and/or altering data. The Datiphy platform provides a record of evidence that cannot be changed which enables organizations to quickly identify perpetrators and hold them accountable for their actions. This precise and organized analysis of information following the incident utilizes all the related activities and improves future policy sets based on the derived intelligence.

Insider threats are an important security issue that many organizations holding sensitive data need to address. While more stringent administrative rules may help prevent the case discussed above, like requiring multi-level authorization for access of sensitive data; in practice, organizations must also consider the impact on efficiency. The Datiphy DataDNA platform is based on ever changing technological innovation providing flexible and scalable solutions for data security and delivering scientific certainty by analyzing the entire data pool as events occur in real-time.

For more information or to download a trial please contact info@datiphy.com or visit www.datiphy.com

ADDRESS
2290 N First Street, Suite 204
San Jose, CA 95131

WEBSITE
www.datiphy.com

SALES
sales@datiphy.com
+1.888.343.9938

datiphy™

©10/2016 Datiphy, Inc. All rights reserved. Features and specifications are subject to change without notice. Datiphy™, CompuDB™, and DatiDNA™ are trademarks or registered trademarks in the United States and/or in other countries.