datiphy™

CASE STUDY
Education

UNIVERSITY USES DATIPHY DATIDNA SYSTEM TO SECURE DIGITAL ASSETS

In recent years it has been widely reported that several universities suffered severe data breaches which caused extensive damage. Consider the nature of universities and the data security risks they are exposed to. Firstly, they have periodic influxes of data in high volume due to enrollment and student activities, like exams. Furthermore, the data must be preserved even after students graduate. Such repositories of personal data are often targeted by hackers. Secondly, their infrastructure has to support diverse functions of education, research, student activities and community services. Large universities usually have on campus classrooms, laboratories, dormitories, cashiers, gymnasiums, cafeterias, shops, clinics or theaters, and these facilities all require IT support to deliver a wide variety of services. On top of that, the user group changes frequently. For example, professors often assign system administrators for their labs and give grade reporting access to their teaching assistants. In such complicated IT environments, Datiphy helps our university customers secure their digital assets.

KEY BENEFITS:

- **Continuous and complete monitoring**
- **Real-time email, SMS, syslog, and SNMP alerts**
- **Configurable script execution for network or database management**
- **Complete and independent record of database status**
- **Instant queries and intelligence for heterogeneous environments**

Here are two common customer incidences. Case One: Students bribed the administrator who had privilege to change their grades (for the better, of course). Due to the large class size, such falsification went unnoticed by the busy professor. With Datiphy's platform, any change after an initial grade submission will trigger alerts via emails or text messages to the proper jurisdiction, thus catching the violation. Case Two: Freshmen received emails and phone calls soliciting business from local services to open accounts with them. Alarmingly, students' personal information was already pre-filled. One can deduce that the source of their contact information was from a data breach. While universities can implement strict security perimeters to prevent external threats such as hacking, insider threats prove more difficult to prevent. The leak may come from a rogue employee or compromised credentials of certain IT staff. Datiphy's system, based on data-centric methodology, can detect suspicious activities and generate alerts in real time.

Let's compare the difference - with and without DatiDNA - before, during and after the perpetration of the two cases above.

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

The school may audit its IT system to prevent security violations but such audits usually rely on the data provided by the administrator. In both cases above, the insiders likely know about the audit practice and can circumvent them. Datiphy DatiDNA runs out of band and independent of regular IT operation so the audit can be conducted without involving the monitored staff.

DURING	Without Datiphy	With Datiphy
Alerting	Limited alerting and logging capabilities from databases or applications	Real-time email, SMS, syslog, and SNMP alerts
Action	Limited capability or logging of database or application activity	Configurable script execution for network or database management

Without Datiphy, it would be cumbersome to set up alert triggers for insiders, who could potentially circumvent them, if any. Datiphy DatiDNA offers configurable alerts and the triggering policies can be managed by an independent security team; therefore, the insider's violations are more likely to be exposed. The Datiphy system can set alerts based on any combination of who, what, how, when or where, and further extend the coverage with behavior policy and signature-based content policy. In the event of security violation, DatiDNA can send out alerts in real time and execute a pre-configured script to mitigate the damage.

AFTER	Without Datiphy	With Datiphy
Forensics	Insider may delete logs and destroy evidence	Complete and independent record for non-repudiation
Analytics	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, it is important to investigate the incident fully and find the party responsible for the act. Unfortunately, an extended amount of time may have passed before such investigation begins and the inside perpetrator could cover their tracks by deleting logs and altering data. DatiDNA provides a record that cannot be changed which enables organization 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.

Universities face both internal and external threats to their data security. While more stringent administrative rules, such as requiring multi-level authorization for access to sensitive data, may help prevent the cases described above; in practice, universities must also consider the impact on cost and efficiency. Datiphy DatiDNA is a technology-based solution for universities to tackle data security issues.

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™