



Career Education Corporation

Protects Systems, Databases and Applications from Internal and External Attacks with "Security Layering"

“NitroGuard DBM's tight integration with netForensics means we have centralized monitoring from the perimeter to the application layer. It is a very powerful tool from a security perspective. This is the trend for the future.”

Career Education

Few organizations attract would-be hackers like schools, colleges, and universities. Overzealous youths—eager to show off their newly acquired technology skills or change a failing grade to an “A”—like to see how far into a system they can get. Fortunately, IT security has been a top priority at most educational institutions for many years now, and IT managers routinely stay abreast of leading-edge security capabilities to thwart internal mischief makers.

For Career Education Corporation, a publicly traded post-secondary education firm with 80 campuses across the US, Canada, UK and UAE, IT security is a critical ingredient in its mix of online and classroom educational services. More than one-third of its 95,000 students take classes online, approximately 3500 students, faculty and staff are online at any one time, and more than 10,000 people have access to online information.

Michael A. Gabriel, director of corporate security, knows that layering security is the best way to protect an IT environment. Sarbanes-Oxley regulations virtually mandate it, with its many requirements for security and internal controls. One of the first steps Gabriel took two years ago when he was hired by Career Ed to focus on SOX requirements was to add more security layers to their event log monitoring practices.

Layer One: netForensics nFX Open Security Platform (OSP)

Early on, Gabriel selected netForensics nFX OSP software to monitor the network perimeter and the operating systems. “netForensics nFX OSP captures some 30,000 types of messages and categorizes them into 100 “buckets” to support detailed correlation of activity across a large enterprise,” Gabriel said.

More specifically, nFX OSP turns event log messages from point security products and applications into real-time intelligence. It compiles messages into a single data repository, flags the most-critical issues and launches integrated incident resolution and remediation processes.

Layer Two: NitroSecurity’s NitroGuard Database Monitor¹

With netForensics nFX OSP in place to guard the perimeter and system devices, Gabriel was ready for the next layer of security: database and application monitoring.

“I wanted more visibility into the applications,” Gabriel said. Application visibility would enable his IT team to know when inappropriate activity, such as an attack or an abuse of privilege, was underway inside a database.

“Unfortunately, the application monitoring capabilities that came with the SQL database used by Career Ed had a negative impact on system performance, which made them unusable. I needed a solution with no performance impact ... and since event logs create so many messages it is impossible to review them all manually, the ultimate solution had to integrate with the netForensics software and feed into its correlations,” Gabriel said.

¹ Originally deployed as RippleTech Informant. This product has since been renamed “NitroGuard Database Monitor.”

netForensics introduced Gabriel to Mel Shakir, who at the time was perfecting a new application-level monitoring software that would become NitroSecurity's NitroGuard DBM product. Over the next year, Gabriel consulted with Shakir on performance and integration requirements. Earlier this year, following successful proof-of-concept testing, Gabriel purchased NitroGuard DBM for Career Ed's IT environment. "NitroGuard DBM is an excellent control, and it has no performance impact—none whatsoever," he remarked.

NitroGuard DBM provides continuous, real-time auditing of all SQL and HTTP activity by monitoring all access paths to sensitive corporate and customer data—whether by users, malware, utilities, "back-door" queries, LAMP scripting, ODBC, etc. Because it analyzes the underlying web and database application protocols, the so called "deep-packet" information, it is non-intrusive and does not impact system performance.

NitroGuard DBM continuously monitors logins, logouts and failed login attempts. It also monitors user activity and alerts the appropriate IT manager in real-time (by email, pager or cell phone) of unauthorized access to data and specific objects. It provides the user login, client machine, etc. so the security administrator has enough information to take action and protect corporate assets. "Should an attack occur, we can gauge its success," Gabriel said.

Since NitroGuard DBM also captures data changes originated by users, it provides a complete audit-trail of all database requests. This audit trail can be replayed in a controlled environment for forensic purposes. Thus, Gabriel can determine exactly which records were accessed and by whom.

Further, because NitroGuard DBM tracks changes made by administrators to access controls and passwords, any attempt by someone to authorize illegal access to data and then "cover his tracks" by removing the authorization is fully documented.

Gabriel is very pleased with the performance of the integrated netForensics and NitroGuard DBM platform. "NitroGuard DBM's tight integration with netForensics means we have centralized monitoring from the perimeter to the application layer. It is a very powerful tool from a security perspective. This is the trend for the future."