Case Study

Security

University of Dayton

Because of the university's diverse computing environment, the IT staff had no means of performing real-time data analysis or creating reports adequate to ensure payment card industry (PCI) security compliance. The University of Dayton found its solution in NetIQ® Sentinel™ Log Manager. It has been logging, analyzing and responding to an average of three million security events a day.

Overview

U.S. News & World Report has recognized the University of Dayton as one of the 10 best Catholic universities in the nation. Founded in 1850, the University of Dayton strives to educate the whole person through community-based challenge and support.

Challenge

The University of Dayton's IT department is responsible for protecting sensitive information such as credit card transactions and personal data on more than 12,000 students and 3,000 faculty members. "The financial cost of a single security compromise could be enormous," said Randy Hardin, lead systems engineer for the University of Dayton. "But, equally important, we need to protect our technology resources without inhibiting the free communication that is an essential part of the educational experience."

The university had a central log server to collect security events across the complete network, but it had no way of aggregating the data and performing real-time analysis. "We had a huge pile of data and no way of getting to the few bits of data that were really important for security reasons," said Hardin. The university needed an effective way to analyze the data and simplify report creation for payment card industry (PCI) compliance.

> **"The essential strength of Sentinel and Sentinel Log Manager is the ability to clearly connect security events with individual identies."**
>
> **RANDY HARDIN**
> Lead Systems Engineer
> University of Dayton

Solution

The university was already using NetIQ Sentinel Enterprise to detect and log an average of three million security events a day. The IT team deployed Sentinel Log Manager for simple and speedy log data analysis.

"I was excited to see Sentinel Log Manager come out," said Hardin. "It was exactly what we'd been looking for, and we were confident that it would integrate well in our environment. We had previously looked at some open source logging and analysis products and some commercial solutions. Many of the other solutions focus on individual systems. Their capabilities simply aren't broad enough for our diverse computing environment. Only Sentinel Log Manager has the flexibility we need. It enables us to look at all information, by any parameter, and to extract the essential security information and understand its meaning."

At a Glance

- **Industry**

  Education
- **Location**

  Ohio
- **Challenge**

  The university needed an effective way to analyze log data and simplify report creation for PCI compliance.
- **Products and Services**

  Sentinel Enterprise
  Sentinel Log Manager
  Access Manager
  Identity Manager
  eDirectory
- **Results**

  + Alerts security teams to potential threats
  + Performs audits almost instantaneously

> ““Since implementing Sentinel, we have better insight into potential security issues.
>
> **RANDY HARDIN**
> Lead Systems Engineer
> University of Dayton

Contact us at:
www.microfocus.com

Like what you read? Share it.

The university has been equally impressed with Sentinel Enterprise, which it uses to collect security-related events from its firewalls, intrusion detection systems, NetIQ eDirectory™ entries, NetIQ Identity Manager and NetIQ Access Manager™. “The essential strength of Sentinel and Sentinel Log Manager, coupled with Identity Manager, is the ability to clearly connect security events with individual identities, which is critical for achieving PCI compliance,” said Hardin.

“Sentinel and Sentinel Log Manager are customizable to the nth degree,” said Hardin. “I can select the specific attributes that are important to me and see what’s going on at a glance. We can also create custom dashboards for management so they can easily understand our compliance and overall security posture.”

Results

Sentinel Enterprise has worked very well, alerting the security team to potential threats. “Since implementing Sentinel, we have better insight into potential security issues,” said Hardin. “If an unauthorized person tries to access a server, I can see the entire event within seconds. It’s mind blowing how well that works.”

The fully integrated solution quickly analyzes massive amounts of data and intelligently reports only the important security events. “With Sentinel and Sentinel Log Manager, we can very quickly analyze data from disparate sources and tie security events to individual identities.”

Previously, audits of individual queries took as much as 20 minutes, but today the IT staff can perform audits almost instantaneously. As a result, the university’s security investigations are much more efficient. “Every few weeks, several members of our team might have devoted an entire day to manually correlating events as part of security investigations,” said Hardin. “Now that we have Sentinel Log Manager, we’re performing security investigations up to 90% faster.”

The university has been very pleased with the solution’s performance versus the cost. “Sentinel Log Manager not only does an amazing job of analyzing the huge volume of data we’re throwing at it,” said Hardin. “Within this year, the solution will have easily paid for itself in reduced administrative time.”