CASE STUDY

The University of Exeter

syslog-ng™ Store Box

The University of Exeter, located in Devon, United Kingdom, is a leading UK university which combines world leading research with very high levels of student satisfaction. It is ranked 10th out of more than 100 UK universities in the Times league table. The University has 18,500 students and employs 1,800 staff.

The Challenge

With complex networks and large numbers of users, universities face a variety of IT operations and security challenges. To facilitate security investigations and monitor its core infrastructure systems, the University of Exeter's IT experts needed to centralize the collection and management of numerous large log files from multiple, disparate devices and operating systems. Searching logs on individual machines meant security investigations were time-consuming. The volume of data needed to be logged was extremely large due to the size and nature of the university's network; the network's firewall logs alone generate in excess of 20 gigabytes of log messages per day. The IT environment could generate more than 10,000 log messages per second during peak loads and this message rate was expected to grow significantly. The IT operations team needed a scalable solution that could cope with current demands but was also able to scale to future growth in the number of log sources and log messages.

Learn more

- Read more about syslog-ng™ Store Box
- Request an evaluation
- Request pricing

"WE ARE NOW ABLE TO PERFORM ANALYSIS AND INVESTIGATE ISSUES ON LOG FILES WHICH PREVIOUSLY WERE SPREAD ACROSS MULTIPLE SERVERS AND PLATFORMS, ALLOWING FOR A MUCH FASTER RESPONSE TO SECURITY INVESTIGATIONS."

- Paul Sandy, Head of IT Governance and Compliance

The Solution

To meet this challenge, the university chose to deploy a syslog-ng™ Store Box (SSB) virtual appliance. With the SSB, the university can centrally manage events from its Firewalls, DHCP servers, VPN access, Email servers and Apache web cluster logs. The high level of configurability of syslog-ng™ clients on the log sources ensured that data collection and management could be finely tuned to the IT team's requirements. In the future, the SSB deployment will include security event logging from Active Directory Domain Controllers, a Linux Server farm and Wireless Access Points as well as the university's primary student portal service.

The centralized, indexed, and searchable log files allow for a much faster response to the IT department's security investigations. Operations and security staff expect to store five terabytes of archived log messages, making efficient storage of and quick access to data essential. The speed of processing logs and ease of searching logs using the SSB appliance's web interface now enables the IT team to analyze and investigate issues on log files which were previously spread across multiple servers and platforms.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com