

With increased technology use, data security has become a priority for banks and their customers. Banks must be able to recognise and respond to all potential threats, such as hacking, phishing and spamming, as quickly as possible, says **Andre Muscat** of GFI Software.



# THE NEED FOR GREATER SECURITY

**N**etwork security is a hot issue for banks due to the growing volume, value and confidential nature of the data within their systems. While the industry has invested heavily in technology to protect that information, it must be ever-vigilant, not least because its own customers demand it.

The complexity of networks, applications and points of entry means a valuable first step is to implement security software that delivers timely, comprehensive reports that can be quickly understood and acted upon. This is one area where, in general, much work still needs to be done.

## Keep vigilant

Andre Muscat, director of the Network Security Products Division at GFI Software, says: 'Today, banks have fully digitised their main business systems and operate through technology-based transactions. As a result, they need to secure all their data, from customer details to trading records. The word "security" has been over-hyped, but often no one knows if it has been fully achieved. The best approach for banks to adopt is one of paranoia.'

GFI provides a range of non-intrusive systems, layered over banks' existing IT infrastructure. It addresses diverse data security issues, such as spam protection, defence against disruptive attacks by hackers and access control, alongside applications that enhance productivity control.

One of these systems is GFI EventsManager, which transforms network event logs into a useable form. Muscat emphasises that this is a critical area for banks in terms of compliance with regulations such as Sarbanes-Oxley and the PCI security standard, which demands that system component logs are reviewed on a regular, if not daily, basis.

Muscat explains: 'It is very important that banks know what is going on in their IT infrastructure. They need to know who has accessed which files, what data is being printed and many other things about their networks. We can help them monitor these issues.'

Among other things, GFI EventsManager also helps identify potentially disruptive network attacks, reducing system downtime and the risk that confidential customer

details are accessed or duplicated. Users can also define searches and filters on the logs collected from the whole network. It is an invaluable tool that assists in forensic investigation of suspicious events.

## Events data undervalued

Event logs and their administration are often quoted as being a big headache for systems administrators. They comprise an enormous amount of data, which is often hard to understand. Their sheer volume and complexity mean these logs are rarely used with any efficiency at all.

Furthermore, the data in these logs is often not retained long enough for it to be of value in forensic investigations or for long-term monitoring of system health and network security. A recent survey by information security training organisation SANS Institute, found that 44% of system administrators keep events logs for a month at most – indicating that event logs are undervalued.

Muscat says: 'Event logs are written by developers in technical jargon, which makes interpretation a complex and time-consuming task. This, and the fact that event logs are largely distributed across the entire IT infrastructure, makes event log management a major challenge. Our solution automatically collects logs, filters out unnecessary data and translates the pertinent information in a simple and effective visual format. This is where GFI has the edge.'

Muscat explains: 'Events management is a hot topic. It is the only way to tell what is really happening on your network. Every single aspect of it can be customised to provide different types of event logs depending on what you want to monitor. Even if you don't know this at the start you can use GFI EventsManager out of the box before you customise and prioritise the events.'

With almost 470 banking sector clients, GFI is finding a ready market for its nine security solutions, including GFI EventsManager. FBA

## Andre Muscat

Andre Muscat is director of the network security products division at GFI Software. He is responsible for leading the design and overall customer experience of the network security product range, which includes GFI EndPointSecurity, GFI EventsManager and GFI LANguard Network Security Scanner.

## Further information

GFI Software Ltd

Email: [andre@gfi.com](mailto:andre@gfi.com) Website: [www.gfi.com](http://www.gfi.com)