

Finding a Balance between Security and Convenience

Bank employees and the IT staff that support them need simple, easy to use and easy to deploy security tools. Employees must have access to sensitive customer data, communicate with customers, and deal with third party vendors as part of day to day business processes. Any security solution that is not convenient will unfortunately not get used. While every bank has a firewall and other perimeter security devices, these network-centric devices are oblivious to sensitive data. What are needed are data-centric devices that can probe deeper into the network and catch actual sensitive data transmissions.

Banks gain a whole new layer of security when they deploy data-centric devices. However, they must be transparent to the network and support high availability so as to not disrupt a bank's normal operations. In order to help safeguard their digital assets, they need to implement the tools that can effectively manage their customer and employee personal information. Ideally, this solution would not require the use of "agents" (software that needs to be loaded on to each workstation and server) because that approach can be complicated, time-consuming, and costly.

Even though the large majority of confidential data that is leaked from a bank is unintentional, the consequences can be the same as a malicious act – mandatory disclosure generating unfavorable media coverage, upset customers, tarnished bank reputations, possible regulatory fines, expensive clean-up costs, as well as an increased risk of fraud and identity theft. At Intrusion, we have a long track record of stopping confidential customer information from leaking onto public networks. Our Compliance Commander Sentry solution can actively block customer data leaks while being completely transparent to the network. It monitors all ports, protocols, and applications, known and unknown, against confidential data leakage so that there are no weak links in the customer data security chain. High availability is supported by our Secure Tap™ with its unique fail-to-pass technology.

In addition to Compliance Commander Sentry, we add additional layers of security on top of databases and file servers. Our Database Defender protects against illegitimate database and file server access, originating from inside or outside the bank, while simultaneously having no impact on database performance. As for e-mail interfaces, we have a new addition to the Compliance Commander product family – the Encrypted E-mail Server which seamlessly encrypts sensitive outbound e-mails. This is especially important when you consider that virtually every bank relies on e-mail communications with customers and vendors, and our extensive research shows that e-mails are also a major cause of sensitive customer data leaks. We selectively encrypt e-mails that require it because there is no need to encrypt every e-mail – that would be less efficient. The Encrypted Email Server is bundled at no additional charge with Sentry to provide a complete, cost-effective solution for protecting customer data.

More and more banks are turning to our Compliance Commander product suite to help safely manage personal customer information such as social security numbers, drivers' license numbers, customer account numbers, credit/debit card numbers, etc. Our actual data matching technology completely eliminates false positives for the IT Department, and gives senior managers at the bank the peace of mind of knowing that their customers' sensitive data is not being misused by either criminals or employees. Many community banks currently have Compliance Commander deployed on their network, and this number is growing quickly as many more banks conduct our no-charge risk assessment to highlight issues that they may have with customer data.



Jay Barbour
Vice President

Jay Barbour is a CISSP and Vice President of Marketing at Intrusion Inc. Jay's responsibilities include product marketing and marketing strategy for Intrusion's line of security products. Prior to joining Intrusion, he served as Vice President of Product Management at ScanSafe, a leading managed web security start-up. Other experience included two years of consulting to security and wireless start-ups from 2003 to 2005. Jay also held various product management and marketing roles at Silicon Valley based companies including Teradyne, 3Com and Hewlett-Packard, from 1999 to 2003. He holds a degree in Engineering Physics from Queen's University, Canada, and an MBA from INSEAD, France.

