

## CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

Private information and intellectual property are the "crown jewels" for any organization, comprising its most valuable assets. Organizations can not afford to be negligent with the critical data with which they are entrusted. Credit unions, specifically, face a highly competitive business environment and a highly regulated industry, so they must take every precaution to control how private and confidential information is distributed both within and outside of their organizations.

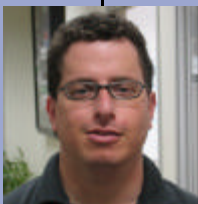
Most financial institutions have installed security solutions designed to block external attacks, like viruses, spam and hackers. While these solutions are essential, it is equally important to secure information as it leaves an organization. All too often credit unions don't have any visibility into how member information is being distributed within their own walls and don't have the tools to gain that visibility. They assume, rightfully, that the vast majority of employees are honest and do not have bad intentions, but to assume that each and every employee is not making mistakes or acting maliciously - not to mention consultants, vendors and temporary workers - is a dangerous approach.

Financial institutions need to gain visibility into their vulnerabilities to information leaks and understand what type of information is leaving their organizations. The first step is to audit and measure their outbound messages to determine if sensitive data is leaking out. That's where an Information Leak Prevention (ILP) solution comes in. Vidius PortAuthority is an ILP solution that monitors and protects any type of sensitive information from unauthorized distribution over internal and external e-mail, the Web, printers and even fax. Vidius offers free two-week risk assessments with our system, PortAuthority, to help organizations gauge their current exposure to information leaks. Many organizations are quite surprised with the details on the type of unauthorized data flow that is occurring across their communications channels.

Fortunately, it is fairly easy to build outbound barricades using the PortAuthority solution. We make it very easy to set-up rules and design policies and get the system up-and-running in just a couple of hours. Access controls and roles are set-up by the appropriate personnel within the credit union, but administrators have the flexibility to set-up the system to be user-specific as well. We can set-up the system to block employee access to external e-mail systems like Hotmail and Yahoo, if you suspect that employees may be using these channels to distribute sensitive information.

By taking a unique "inside-out" approach to security, we help credit unions prevent the leakage of sensitive member data such as Social Security numbers, credit card numbers, account numbers and much more, in both the body of e-mails and in e-mail attachments. Again, we first determine a credit union's authorized business practices and processes and then incorporate that information into our solution. And it causes no disruption to an organization as we have developed PortAuthority so that it seamlessly integrates into an organization's existing workflow and security procedures.

How do we do it? We have developed a unique identification technology, using algorithms to create digital "fingerprints" of protected content that should not be leaving the credit union. Vidius PortAuthority monitors outbound data transmissions for the protected content and blocks it, if it is being distributed to those who shouldn't have it. If it is necessary to send out sensitive data, authorized personnel can easily release the e-mails - all while creating a solid audit trail. At Vidius, we are proud that PortAuthority is the only solution on the market that can effectively monitor and, most importantly, stop leaks of member, financial and employee data.



**Assaf Litai** is Vice President of Technical Services for Vidius. He co-founded Vidius in early 2000 and plays a key role in designing and deploying solutions for customers' intellectual property protection needs. Before Vidius, he led a variety of development efforts in signal processing and advanced acoustics for military systems. Assaf has testified before a U.S. Congressional committee on the impact of peer-to-peer networks, digital piracy, and consumer privacy. Assaf regularly serves as an industry expert for publications such as Network World, InfoWorld, SC Magazine and Security Management. Assaf served in the Israeli Navy and is a member of the Information Systems Security Association. He graduated from the Israeli Institute of Technology with a bachelor's degree in Electronics and Engineering.