

CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

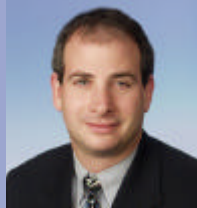
Protecting a credit union's information perimeter is absolutely critical, but it is not the sole source of danger. Employee and vendor laptops can unknowingly enable information theft via malware from behind the institution's secure and "trusted zone." Web-based e-mail systems that bypass conventional virus and intrusion safeguards also represent another direct route inside the credit union whereby staff members can unwittingly do a great deal of damage. Today's network solution requires a full time "guard" throughout the network that can deter sophisticated content threats in the form of spyware, intrusions, viruses, worms and more.

Hackers are always a threat and they are getting much more sophisticated through the use of blended threats and clever re-packaging of existing malicious software. These content threats are usually executable programs embedded within seemingly legitimate traffic. Deep packet and stateful inspection firewalls will not block these sophisticated content threats. A more thorough, proactive approach is needed in both security equipment and additive update services before malicious content enters the network itself.

At Fortinet, we deliver a unique approach that reassembles content at the network gateway to thoroughly check the entire email message or network transmission. This approach requires innovative processing power, and always current virus and intrusion updates. Only through the use of new embedded ASIC technology can complete content protection be accomplished at Gigabit network speeds so that financial staff and their clients never notice any latency. Fortinet packages its blend of hardware and software with consistent features in more than fifteen FortiGate antivirus firewall systems -- the only difference between systems is the number of users they protect and network speed requirements, e.g., a small branch office of just a few people or a very large enterprise. Our company, which has sold more than 80,000 systems, also saves financial institutions valuable capital using a per box antivirus licensing model as opposed to a per user model by tradition virus software vendors.

Our all-in-one, real-time appliances offer a choice of best in class ICSA-certified security - including antivirus, firewall, VPN, intrusion detection and prevention, content filtering, and traffic shaping. These seven wonders can all be used concurrently or selectively based upon the network environment size and speed needs. This easy to manage and update system replaces what our more than 2,000 customers worldwide call a "congo line" of disparate security devices that are inherently far more difficult to properly configure and maintain. Update services for viruses, worms and malware are offered through the global FortiProtect service; content filtering services are bundled in the FortiGuard services. Fortinet is leading a trend in the belief that Unified Threat Management (UTM) platforms are the wave of the future - research firm IDC has said that these solutions will be the norm in the next few years overtaking single function security systems within the next three years in both volume shipped and revenue sales. IDC named Fortinet the Leading UTM system provider in 2004 ahead of single function security vendors that are now trying to integrate disparate third-party software including Trend, Symantec, Cisco, McAfee, Checkpoint and Juniper.

Another valuable addition to FortiGate UTM systems is behavior-based heuristics that gives our customers the ability to stop malicious threats that are non-signature based. In practice this means that our clients will be far better prepared to detect and prevent "zero day" attacks that were previously unknown - and before the typical 12-24 hours when a virus or intrusion signature blocking agent is scripted. When used in conjunction with our FortiClient software for client-based anti-virus, spyware detection and removal, personal firewall, and VPN capabilities, our award-winning FortiGate solutions represent an integrated, holistic approach to real-time UTM security. Only by delivering content security within the network itself - at the edge and in the core and to the desktop - can credit unions truly establish a proactive comprehensive security posture.

**FORTINET**

Adam Stein is Vice President of Corporate Marketing at Fortinet, Inc. He has over 18 years of marketing and brand category creation experience focused primarily within the networking hardware, software and silicon markets. During his career, he has served as director of marketing with Juniper Networks, Broadcom and most recently as the global marketing lead for Foundry Networks. Adam has also led corporate marketing at Cisco Systems and marketing agency services for consumer goods firms. Adam has a B.A. in Distributed Sciences from the University of Colorado at Boulder, and a M.A. in Marketing from Emerson College.