

Nearly every day an announcement of a new data breach or loss of corporate data hits the news. While theft of customer data continues to dominate headlines, financial institutions grapple with the challenges of protecting all types of critical information.

Financial institutions are a constant target and are well-aware that maintaining good customer relationships by keeping personal data safe is crucial to the success of their business. They not only fear data breaches, but also risk hefty financial penalties for not complying with government regulations. In fact they may face other sanctions if not compliant with mandates established by organizations such as the Federal Financial Institutions Examination Council (FFIEC) as well as the National Credit Union Association (NCUA).

As a key segment of the financial services industry, credit unions are impacted by IT security issues much in the same way as most organizations that must ensure the confidentiality, integrity and availability of customer information – security is of the utmost importance. To remain competitive, credit unions are relying more extensively on information technology to provide their customers with a wider variety of online services.

However, the ubiquitous nature of the Internet also creates new opportunities for cyber crime and other malicious activities. The huge financial loss that can be associated with network and server resource consumption causes great concern for these organizations, and any networked system that shares network infrastructure with the Internet has the potential for being compromised. Attackers are increasingly targeting the core infrastructure, focusing on the network and server infrastructure that provides access to valuable confidential data.

As information is increasingly being transmitted via the Web, governments have taken action to establish several regulations that mandate the security of confidential information and compliance. Sarbanes Oxley (SOX) and Payment Card Industry (PCI) put compliance requirements on institutions, and laws such as the Gramm-Leach-Bliley Act (GLBA) require financial institutions to ensure the security and confidentiality of customer records and related information.

Businesses such as credit unions face the same critical security and compliance challenges as larger companies,



***Today, malicious attackers have easy access to sophisticated attack tools, and IT administrators are faced with the challenge of increasing access to information without compromising security.***

and are often forced to address these issues with significantly fewer resources. Like many businesses, credit unions often do not have extensive financial resources and staff that can be dedicated to the development and implementation of information security procedures and controls. As a result, they often rely on guidance from system integrators, security consultants, and software vendors regarding which solutions would best serve their needs.

Today, malicious attackers have easy access to sophisticated attack tools, and IT administrators are faced with the challenge of increasing access to information without compromising security. Expectations of always-on access and impenetrable security are the opposite ends of

the IT spectrum that security officers must keep in sight. As such, corporate executives now look to invest a significant amount of resources to counter the threats presented by computer hackers, malware and more.

Securing critical IT infrastructure by preventing undesired access, protecting against malicious content that exposes private data, and mitigating rate-based attacks that can be employed for extortion purposes, is a key consideration in working towards fulfilling government compliance and client expectations. The risk of a data breach has prompted financial institutions to invest in Intrusion Prevention Systems (IPS) to block out undesired access from their network. IPS offers protection from malicious behavior while also enabling compliance with strict industry regulations. Over the years, IPS solutions have become a requirement for IT administrators tasked with security and availability concerns. In fact, implementing the proper IPS solution is considered a “best-practice” in the eyes of financial IT administrators.

Top Layer is the leader for Intrusion Prevention System (IPS) security solutions for financial institutions of all types and sizes. The IPS 5500 delivers the right protection, performance and reliability to provide these enterprises the confidence to ensure complete privacy of their client data infrastructure while providing proper availability. Combined with a defense-in-depth strategy, Top Layer's award-winning IPS 5500 intrusion prevention system provides credit unions with:

- Reduced risk of data breach or service outage
- Increased network bandwidth availability
- Increased network performance
- Continuation of legitimate transaction flow even in the face of brute force DDoS attacks.

The IPS 5500 is the first and only IPS solution as rated by NSS Labs that seamlessly integrates stateful firewall filters with multiple content-based and rate-based protection mechanisms on a single platform. Top Layer IPS solutions can therefore be deployed at the network



perimeter or elsewhere on the network in front of servers that host critical applications and databases .

### Customer Example

Leading financial provider, CFE Federal Credit Union, in Lake Mary, Florida leverages the Top Layer IPS solution to protect the integrity of their network and meet the strict compliance requirements that all credit unions face. The IPS 5500 enables CFE Federal Credit Union to block malicious traffic before it reaches its intended target thereby providing the organization with a much higher level of overall security. The net result is a higher level of protection of client information while at the same time reducing IT operating expenditures.

Top Layer Security offers the most innovative IPS solution for offering protection from undesired access, malicious content and rate-based attacks that target mission critical financial servers and networks. Top Layer provides IT administrators the utmost peace of mind with fast response and continual updates to protect against new vulnerabilities and potential risks. The IPS 5500 is a high-performance, scalable and reliable solution that offers the best protection mechanisms and performance for detecting and eliminating cyber threats.

**For more information on Top Layer Security and its award winning IPS  
Call +1.978.212.1500 or visit our website at [www.TopLayer.com](http://www.TopLayer.com)**

### About Top Layer

Top Layer is a leading provider of Network Intrusion Prevention Systems (IPS) that reduce organizations' risks and losses by protecting critical online assets against cyber threats. Its family of high performance IPS provides the most advanced protection against known and zero-day threats at maximum throughput rates. Top Layer is headquartered in Massachusetts, USA, with Global Sales and Support throughout North America, Europe, Asia, and Japan.

Rev 1.0 Aug-31 © 2009. Top Layer Networks, Inc. All Rights Reserved. Attack Mitigator, DCFD, Flow Mirror, IDS Balancer, TopInspect, TopMSS, SecureCommand+, and ProtectionCluster are trademarks of Top Layer. AppSafe, AppSwitch, SecureWatch, Top Layer, Top Layer Networks, TopFire, TopFlow, TopPath, TopView, and perfecting the art of network security are registered trademarks of Top Layer. Unless otherwise indicated, Top Layer trademarks are registered in the United States and may or may not be registered in other countries.

**Top  
Layer™  
Security**