CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing the Big 3: Compliance, Fraud & Cyber Security

Doing more with less has always been a challenge to IT, but creating and maintaining a secure environment to protect both the organization and its clients has never been more important. While there are a number of essential security factors, credit unions need to prioritize their ability to comply with government regulatory standards. The cost of failure to meet these standards could mean heavy financial penalties and potentially the loss of the ability to conduct business. With this is mind, archiving and monitoring solutions to enforce compliance should be given top priority.

Fraud and cyber security are closely related issues. Effective cyber security minimizes the loss of sensitive personal identification information which is commonly the source of fraudulent activity. It is tough to determine which has more financial impact in the end, however, if you consider that prevention is almost always more cost effective than the cure, stemming the source of the problem - cyber security - should be given priority followed by fraud management.

Fortunately, there are approaches that can cost-effectively address all three problems. Consider security and compliance vendors that provide integrated platforms that can deliver a majority of these solutions in a unified service. This approach helps solve budget constraints in two ways. First, a bundled set of services can be delivered at a lower overall cost when compared to a collection of solutions from multiple vendors. Second, integrated platforms have a common management interface, making them easier to manage and freeing up IT resources to focus on other critical projects rather than trying to learn and manage disparate solutions. Realistically, finding a single vendor that fully addresses the entire spectrum of compliance and security risks is quite difficult, so your strategy should ultimately be comprised of layered solutions that effectively come together to meet your specific requirements.

The Mimecast cloud-based Unified Email Management (UEM) platform ties content control of email and secure large file transfer to a compliant archiving platform that enforces regulatory retention requirements in a secure immutable database. Content policies can be applied to enforce encryption and secure transmission requirements of sensitive information, as well as tools for actively monitoring, controlling and restricting the outflow (and inflow) of sensitive or non-compliant data. The Mimecast archive also offers rapid post-review tools for audits, investigations and legal activities including data export and legal hold. Tools are available for reviewers to manage the email review process to ensure active compliance with regulatory requirements. Policy controls can be granularly applied to users and groups that are relevant to particular archiving and oversight requirements. At the same time, granular administrator rights and roles management ensures that access to the archive is also closely monitored and controlled by administrators and compliance officers.

In terms of fighting fraud, the Mimecast UEM security platform actively protects organizations from fraud risks and provides the greatest impact on employee-centered risks. Inbound email security scans messages for malware and Trojans that can be used to compromise a user's computer and provide a beachhead to the organization at large. Multiple malware scanners are leveraged in conjunction with each other to eliminate the risk of an exploit based on a single scanning technology. Messages containing known dangerous URLs leveraged in phishing tasks are similarly blocked. In addition, innocuous appearing URLs contained in messages are redirected through on-demand security scanners to protect against zero-day threats such as spear-phishing attacks. These approaches help protect employees from unwittingly acting as gateways to external threats. The Mimecast content control technology actively prevents sensitive information from purposefully or inadvertently being sent outside the organization via email or secure large file transfer. The Mimecast secure archive allows for fraud investigations to rapidly search the entire organization's historical email or Lync® IM communications.

The Mimecast security platform is primarily email- and file transfer-focused and offers several key features to assist in securing online communication and collaboration. First, as mentioned earlier, content-based controls can enforce encryption and secure Webmail delivery requirements to ensure sensitive data is always sent safely and securely. Second, files can be transferred securely independent of the email server, including encrypted transfer, passcode access protection, access expiration, and logging. Finally, email routing policies are normally configured to always send email transmissions through an encrypted channel whenever possible using opportunistic TLS. These protections extend to most methods of end-user access, including Outlook® and Webmail interfaces such as Outlook® Web Access (OWA) and mobile devices.

Mounil Patel
Vice President

mimecast
unified email management

Mounil Patel is the Vice President of Field Enablement at Mimecast, and is responsible for the go-to-market practices for sales and pre-sales at a global level. Prior to his current role, Mounil held the position of Director of Pre-sales Engineering and Professional Services at Mimecast. Previously, he was Global Practice Director managing pre-sales and services for EMC's Telco, Media and Entertainment division for archiving and back-up products. Mounil also held pre-sales, services, and IT management positions at Iron Mountain, Endeca Technologies and Phase Forward Incorporated. Mounil holds a Bachelor of Science in Electrical Engineering from Boston University.

Contact Info

www.mimecast.com