Proofpoint Introduces its Next-Generation Email Security and Privacy Platform with Enhanced Email Encryption, Available for SaaS and Appliance Deployment

Sunnyvale, Calif. – October 5, 2009 – Proofpoint, Inc., the leading provider of unified email security, archiving and data loss prevention solutions, today introduced its next-generation SaaS and appliance email security and data loss prevention platform, Proofpoint 6. Highlights of Proofpoint 6 include the availability of Proofpoint Encryption™, a new easy-to-use, policy-based email encryption solution, data loss prevention security and workflow enhancements, support for DomainKeys Identified Mail (DKIM) email authentication, and a variety of innovative administrative features.

"To fully protect private data in email, enterprises require not just the means to accurately detect confidential information and prevent data leaks, but also the ability to automatically encrypt sensitive content," said Peter Galvin, chief marketing officer for Proofpoint. "Proofpoint's policy-based encryption features protect the security and integrity of private data in email, ensure compliance with financial and healthcare privacy regulations and help organizations avoid costly data breach notification and remediation events."

Proofpoint 6 simplifies today’s complex email environments by combining inbound anti-spam and anti-virus, outbound data loss prevention, email encryption and policy enforcement features into one affordable, easy-to-use and easy-to-manage platform for taking control of email. Some of the key features of the Proofpoint 6 platform are described in more detail below.

Proofpoint Encryption: SaaS-powered, Policy-based Email Encryption

Proofpoint’s next-generation email security platform delivers integrated data loss prevention and email encryption features powered by the new Proofpoint Encryption module and Proofpoint Hosted Key Service™. Now included as part of the Proofpoint ENTERPRISE™ Privacy suite, Proofpoint’s policy-based email encryption solution can be deployed as part of the Proofpoint on Demand™ SaaS offering or on-premises with Proofpoint’s appliance, virtual appliance and software versions.

"As an outsourced provider of human resources services, we need to be able to exchange private information via email with our clients and a variety of business partners and end-users," said Jeff Caracci, vice president of information technology at Merit Resources. "We were searching for a cost-efficient solution to enable our administrators and staff to conduct business securely over email, without placing an undue burden on users. Proofpoint Encryption fit our requirements perfectly, was easy to install and makes it simple for users to send email in a secure and compliant way. And our email administrators are thrilled that the system requires very little ongoing maintenance."

Proofpoint Encryption enables easy-to-use, easy-to-manage email encryption that’s friendly to senders, recipients and administrators. Email encryption policies are managed and enforced on an enterprise level from a single location, using Proofpoint’s administrative GUI. Once defined, enterprise encryption policies are applied automatically at the gateway, eliminating the risk of user error. Message encryption policies can be extremely granular and encryption can be triggered by any combination of:

- **Structured data matches**: Including the presence of private healthcare or financial information such as HIPAA codes, ABA routing numbers, domestic and international credit card numbers, US social security numbers, UK National Identity Card numbers and other "smart identifiers" as detected by the Proofpoint Regulatory Compliance™ module.
- **Unstructured data matches**: Such as the presence of confidential information as detected by the Proofpoint Digital Asset Security™ module.
- **Keywords** (and/or regular expression or weighted dictionary matches) found in the subject line or content of messages.
- **Message origin or destination**: Messages can be encrypted based on their destination (e.g., a specific business partner or supplier), message sender or other structural attributes.

Based on symmetric key cryptography (using highly secure AES-256 ciphers), Proofpoint Encryption solves the end-user and administrative complexities commonly associated with encryption solutions. Management of encryption keys is one of the biggest challenges in any encryption solution. Proofpoint Encryption eliminates key management, backup and administration burdens through the Proofpoint Hosted Key Service™, which uses the Proofpoint on Demand™ SaaS infrastructure to provide secure, cost-efficient, highly-available and fully redundant key storage facilities.

The combination of Proofpoint Encryption and the Proofpoint Hosted Key Service enables extremely granular, per-message
control over encrypted messages. For example, an individual message to a specific recipient can be revoked without affecting other users or other messages to the same recipient.

**Built-in reporting features give administrators complete visibility into both overall and per-policy encrypted message trends.**

Proofpoint Encryption ensures security and ease-of-use for email recipients as well. It uses a push delivery architecture that sends the actual encrypted message contents to recipients who can then decrypt messages by following a link (included with the encrypted email) to the Web-based Proofpoint Secure Reader™.

Whether Proofpoint Encryption is used with SaaS or on-premises Proofpoint deployments, messages are decrypted using an isolated instance of Proofpoint Secure Reader, hosted within the customer's own instance of the Proofpoint on Demand service or on the customer's own Proofpoint Messaging Security Gateway™ appliance.

"Email encryption has become a business and legal necessity for most enterprises and government organizations today because of the growing volume of sensitive data that is sent and stored in email, increasing corporate governance requirements and the costly consequences of data leaks," said Michael Osterman, principal of Osterman Research. 
"Proofpoint Encryption delivers robust, policy-based email encryption that can help these organizations protect confidential information and comply with regulatory requirements."

**Data Loss Prevention Workflow and Security Enhancements**

**Building on the robust DLP incident management, remediation and workflow features introduced in Proofpoint 5.5, Proofpoint 6 enhances security for messages held in quarantine.**

When messages are quarantined for further review, the sensitivity of different policy violations may require that only specific administrators, compliance officers or other business users be allowed to review certain types of content. New folder-level access control features allow more granular control over which users can see, review, comment upon and track outbound policy violations.

**Enhanced Support for Email Authentication Standards**

Proofpoint 6 adds DKIM signing of outgoing messages to help defend against email address spoofing (i.e., forged email headers, as commonly used in phishing attacks). DKIM email authentication allows organizations to digitally sign outgoing messages so that recipients whose mail servers support DKIM validation can be confident that messages are truly from that organization and not a phishing attempt.

As in previous versions, Proofpoint 6 also supports the SPF (Sender Policy Framework) sender authentication standard. SPF records can be checked for all incoming email messages and policies can be configured to take action on the success or failure of SPF record checks.

**Policy Engine and Administration Enhancements**

New domain-based administration features in Proofpoint 6 make it easy for organizations that manage a large number of domains to configure and enforce messaging policies based on a user’s domain. Domain groups can be created either manually or automatically and unique policies can be applied to messages that come to, or originate from, those specific domains.

Proofpoint 6 simplifies the process of customizing the look and feel of all end-user interfaces, including the email digest, the end-user Web interface and the Proofpoint Secure Reader. Proofpoint's administrative GUI now lets email administrators customize these interfaces with point and click ease.

Proofpoint 6 also allows for more granular handling of inbound messages that include multiple recipients. The new "envelope splitting" feature allows messages destined for multiple recipients to be processed via different policies on a per-recipient basis, allowing for better control over message dispositions.

Proofpoint continues its tradition of delivering "worry free" email security solutions with minimal administration and maintenance overhead. New features in Proofpoint 6 make updates and upgrades easier than ever, with improved feedback and reduced downtime during upgrade processes.

**SaaS and Appliance Solution Suites Simplify Email Security**
The new features of Proofpoint 6 will be available simultaneously for Proofpoint's SaaS (Proofpoint on Demand™) and appliance (Proofpoint Messaging Security Gateway™) deployments. With the introduction of Proofpoint 6, Proofpoint's flagship email security solution, Proofpoint ENTERPRISE™ is available both on-demand and on-premises with two new solution suites that support the most common inbound threat protection and outbound data loss prevention requirements:

- **Proofpoint ENTERPRISE Protection Suite**: Proofpoint ENTERPRISE Protection delivers all of Proofpoint's best-in-class inbound email security and email management components. Features include: advanced connection management; Proofpoint MLX™-powered spam detection; signature-based and zero-hour virus protection; email firewall, deep content inspection and outbound filtering capabilities to enforce acceptable use policies for message content and attachments; advanced message tracing; and TLS encryption.

- **Proofpoint ENTERPRISE Privacy Suite**: For enterprises with advanced regulatory compliance and data privacy requirements, Proofpoint ENTERPRISE Privacy provides "defense in depth" for private information of all types. It protects private information in email, defends against leaks of confidential information and ensures compliance with common data protection regulations including HIPAA, GLBA and PCI standards. For maximum data loss prevention flexibility and control, Proofpoint ENTERPRISE Privacy now includes the powerful encryption features of Proofpoint Encryption, which helps mitigate the risks associated with regulatory violations, data loss and corporate policy violations by automatically applying encryption based on your organization's unique policies.

Features include: advanced, highly accurate detection of private or confidential information in unstructured and structured data; pre-configured data protection policies; an easy-to-use administration console; integrated policy-based email encryption and robust incident management.

**Pricing and Availability**

The Proofpoint 6 platform, Proofpoint Encryption module, Proofpoint ENTERPRISE Protection and Proofpoint ENTERPRISE Privacy suites will be generally available in November 2009. Pricing for the Proofpoint ENTERPRISE Privacy bundle (including Proofpoint Encryption) is less than $17 per user, per year for organizations with 5000 to 10,000 inboxes. Contact Proofpoint for a detailed quote.

Current Proofpoint customers on maintenance can upgrade to the Proofpoint 6 platform free of charge. Contact support@proofpoint.com for details.

**Learn More about Email Encryption in Today's Enterprise**

Learn more about Proofpoint's easy-to-deploy and easy-to-use policy-based email encryption solution and why email encryption is a critical component of today's email security solutions. Register to download two new whitepapers—Proofpoint's Protecting Enterprise Data with Proofpoint Encryption and Osterman Research's The Critical Need for Encrypted Email and File Transfer Solutions—by visiting:

[http://www.proofpoint.com/emailencryption](http://www.proofpoint.com/emailencryption)

To watch a video of product marketing manager Ken Liao explaining Proofpoint Encryption, visit:


**About Proofpoint, Inc.**

Proofpoint focuses on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging. Learn more at [www.proofpoint.com](http://www.proofpoint.com).

###

Proofpoint is a registered trademark of Proofpoint, Inc. Proofpoint on Demand, Proofpoint ENTERPRISE, Proofpoint Encryption, Proofpoint MLX and Proofpoint Messaging Security Gateway are trademarks of Proofpoint, Inc. All other trademarks contained herein are the property of their respective owners.