Using Software-as-a-Service to Drive Business and IT Productivity

At-A-Glance

Challenges

- Are you worried about increasing message security and compliance challenges?
- Are you struggling with rising cost of e-discovery?
- Is your IT team spending more time managing boxes and software, less time helping to grow your business?

Software-as-a-service (SaaS) solutions can help you overcome your challenges. To select the right solution you should consider the following factors:

Critical Success Factors

- Effectiveness – How effective are SaaS solutions?
- Flexibility – How can I configure and change my policies?
- Speed and ease of deployment – How quickly can I deploy?
- Scale and reliability – Can this solution handle my volume?
- Total cost of ownership – What are my IT life-cycle costs?

This paper explores these factors in detail.

LSI Corporation had been using an internal, software-based solution to keep its email channel clear of unwanted traffic, but when the volume of message traffic spiked and bottlenecks interrupted user productivity, the company knew it needed to make a change. After a rigorous review process, LSI selected Postini and now, after more than three years and six acquisitions later, the solution still requires minimal intervention.

Introduction

Leading IT organizations can improve business productivity through collaboration and real-time communications. As more employees use multiple communication channels – email, instant messaging (IM) and the web, for example – the sensitivity of the information that traverses these channels is increasing, exposing organizations to potential security breaches and compliance violations if care is not taken to protect the channels.

While many IT organizations have implemented purpose-built appliances or on-premise software to secure their electronic communications, these first-generation solutions have fallen short in four major ways (see fig. 1).

First, these solutions are expensive and carry significant hidden total cost of ownership (TCO). While the initial, upfront software license seems manageable, the associated hardware procurement, implementation, and ongoing maintenance costs can push the TCO of these solutions into the stratosphere.

Second, these first-generation hardware and software solutions are inflexible and require complicated upgrade scenarios. Each time a policy must be updated or changed, the associated downtime or latency results in security and compliance risks. In addition, the security software as well as hardware and operating system must be upgraded or updated on a regular basis, incurring unbudgeted management and custom development costs as well as undesired risk for the organization. Third, these solutions lack built-in scale, requiring additional resources to be added on an ad-hoc basis as the organization grows or even for temporary spikes in volume. This lack of scalability is also tremendously costly and risky – and can also negatively impact productivity when message volumes rise and the ineffectiveness of the solution causes a logjam in traffic flow.

Finally, these solutions are typically not integrated, creating regulatory compliance issues due to inconsistent, conflicting configurations and policies. The lack of a single command and control interface or management console complicates the problem and, because of this, these first-generation

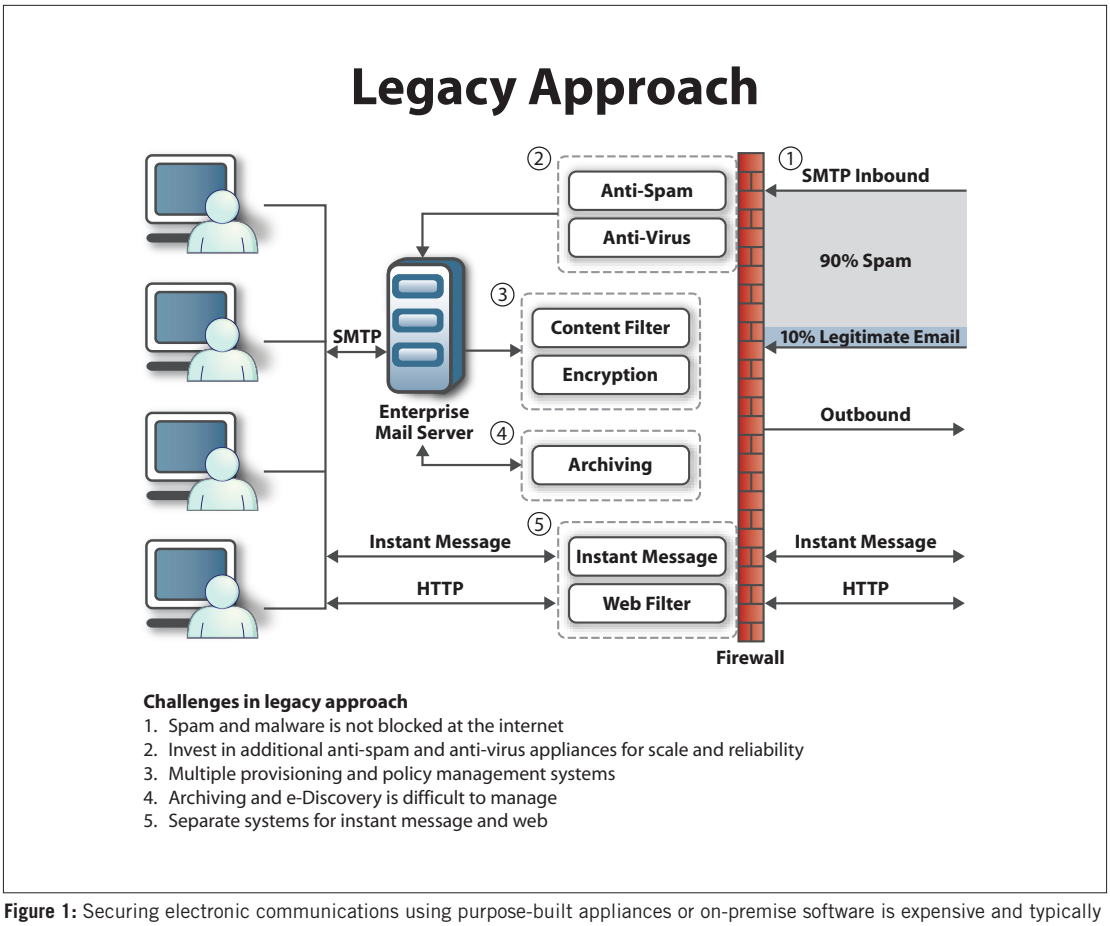

Figure 1: Securing electronic communications using purpose-built appliances or on-premise software is expensive and typically not integrated, requires multiple solutions, and is difficult to manage and support within the firewall.

The San Francisco-based accounting firm of Harb, Levy & Weiland LLP relies heavily on Postini Email Security service to improve the productivity of its more than 100 employees. By filtering out all undesired traffic well before it ever reaches the end-user, Postini helps the firm minimize the time employees waste cleaning out spam from their inboxes. Additionally, the firm relies on Postini's encryption services to ensure the privacy of sensitive client information in all of its electronic communications.

solutions actually contribute to the very problem they are intended to solve.

More recently, Software-as-a-Service, or SaaS, solutions have emerged as a viable alternative to expensive, inflexible, and difficult-to-use on-premise software and hardware appliances. Delivering software functionality in the form of a service instead of the traditional on-premise approach, SaaS has become a popular alternative in all types of business-critical software. In fact, industry analyst firm, Gartner Group, expects the growth of SaaS to more than double that of traditional installed software applications through 2011[1].

But not all electronic communications security and compliance solutions built on the SaaS model are the same, and IT organizations need a solid set of criteria to evaluate on-demand solution providers and determine the solution that is right for their specific business requirements.

This paper outlines the five key requirements CIOs should look for in an on-demand communications security and compliance solution in order to enable the IT organization to better contribute to the company's bottom line.

How to Evaluate an On-Demand Communications Security and Compliance Solution

There are five major areas IT organizations should consider when evaluating an on-demand solution provider for communications security and compliance.

1. Effectiveness

The ability of the communications security and compliance solution to be highly effective is a crucial factor in the selection process. Organizations need to know that the solution can evolve to meet changing needs and still provide effective communications security and compliance. Critical questions to have the potential on-demand vendor answer include:

- Is the solution built on a platform-based approach that enables security and compliance across all communications channels (e.g., email, IM, and web)?
- Does the solution allow for the quick and easy addition of new services or applications without service downtime?
- Can the vendor easily make changes to the solution to ensure that it is current with new regulations and legal standards as they evolve?
- Is the vendor able to quickly adapt to the changing security threat landscape and incorporate protection to minimize the customer's risk exposure?
- Does the vendor have a history of delivering reliable and high quality Software-as-a-Service solutions?

2. Flexibility

In selecting an on-demand communications security and compliance solution, it is important to remember that one size does *not* fit all. Organizations should look for an easy to administer and manage solution that fits their specific requirements and allows technical staff to focus their efforts on value-added activities that directly contribute to the bottom line. Some of the questions to ask the solution vendor are:

- How are similar policy triggers – or 'dispositions' – managed across different channels?
- Can I use the same policy settings or do I need to create a unique profile for each disposition?
- How quickly can urgent policy changes, due to a new security threat or regulatory requirement, be put into effect? Do I need to wait for minutes or hours?
- Can different departments within the organization create their unique security or compliance requirements without disrupting message flow?
- What level of granularity exists for message tracking and forensics?

3. Ease of Deployment and Use

One of the most important features of a communications security and compliance solution is how easy it is to deploy and use. The more difficult and complex the solution is from both of these perspectives, the less secure it is – and the less likely the solution will ensure the organization's ongoing compliance with regulatory requirements. Key items to look for in the solution include:

- How long does it take for the solution to be up and running?
- How much intervention does the solution require for set-up and periodic configuration adjustments?
- How invasive is the solution in processing my electronic communications? Does it require writing to disk (introducing latency and security risk) or is there a more elegant message handling process?

[1] Report Highlight for Dataquest Insight: SaaS Demand Set to Outpace Enterprise Application Software Market Growth, Sharon A. Mertz, Gartner, Inc, August 17, 2007

Norcal Waste, a California-based waste removal and waste disposal service, gives its 2,100 employees access to online applications using thin-client terminals connected to a central proxy. Switching to the Postini Web Security service from an on-premise solution, Norcal Waste can now protect its network from web-borne threats without impacting users' productivity or burdening its small IT staff with maintenance requirements.

- Can employees conduct typical tasks, such as adjusting filters themselves through self-service portals, or do users need to involve administrators in these tasks?
- What is the impact of the solution on my data center footprint?
- Will I need additional hardware or personnel to run or manage this solution?

4. Low Total Cost of Ownership

Unfortunately, the initial cost of the communications security and compliance solution can be just the tip of the iceberg with some vendors. Organizations must conduct due diligence and select an on-demand solution that keeps both the initial and incremental back-end costs down. Some of the questions the vendor should be able answer include:

- How long does it take to deploy the solution?
- What resources are required to deploy the solution?
- Is the implementation process managed by the vendor or does the customer need to hire on-premises experts?
- Does the solution require any capital investment in additional hardware, software, or resources?
- What is the upfront cost of the solution? Are there any hidden or back-end costs?
- How quickly does the solution deliver value to the organization?
- If my business grows or my needs change, how predictable are the costs of service expansion?

5. Scalability and Reliability

For today's rapidly growing business environments, scalability and reliability is of paramount importance. The communications security and compliance solution must scale to be effective at all times and deliver ongoing value to the organization. When selecting a SaaS vendor, key criteria to evaluate include:

- Does the vendor have global operations to scale as your business grows?
- Does the vendor have on-site physical security to protect the premises?
- What is the overall architecture of the operational network? Single site with back up or cluster based? For the type of architecture, why was it chosen?
- How is the integrity of the systems preserved and how is data privacy maintained?
- How will the operations network scale for future growth? Is there a growth strategy?
- What type of delays does the solution introduce to message flow?
- How is fail-over and redundancy accomplished?

On-demand communications security and compliance solutions that do not meet these five criteria shortchange the organization subscribing to the service. Why? Because they neither help the company improve business and IT productivity nor drive revenue.

The Postini Platform – Delivering Security and Compliance as an On-Demand Solution

Postini is the most effective on-demand solution provider that meets all five criteria for an effective communications security and compliance solution.

1. Effectiveness

The Postini platform processes more message requests on a daily basis than any other electronic communications security and compliance solution on the market today. This message volume enables Postini to create the most up-to-date and accurate threat intelligence on the internet in real time – and apply this intelligence to messages flowing through the Postini network, making it highly effective. For example, when the Postini identifies zero-hour virus from a sender to a customer, the entire network is alerted, updated, and protected – in real time – ensuring that the protection stays ahead of malicious individuals. This so-called "network effect" makes Postini's virus protection more effective than legacy firewalls or anti-virus software that require signature updates or downtime to reconfigure.

For every communications channel, Postini solutions process consists of the same four steps (see fig. 2):

- **Message Processing –** The Postini network accepts over two billion message connection requests daily and handles them according to the reputation and frequency of the requesting server;
- **Message Data Analysis –** Based on heuristics and constantly updated algorithms, the Postini system evaluates the content for suspect or known anomalies, including attachments and .zip files;

With constant and evolving legal and regulatory requirements, Analysts International's more than 2,500 employees provide automotive to medical consulting services to local and state governments. The firm turned to Postini not only to protect its email but also to archive all email and IM communications. Why? Because Postini's on-demand solutions made compelling economic sense from all aspects – effectiveness, cost, and support – and unburdened the firm's IT staff from the significant support and service requirements of a large user base.

- **Policy Framework –** Based on the characteristic of the communication, the Postini system looks up the specific settings required for the particular message, quarantining the message for review, refusing delivery of the message, archiving the message, or even applying encryption to the message;
- **Disposition –** The Postini network forwards the electronic communication according to the rules required by the policy. Postini can also optionally hold the communication flow if the receiving server is not available, due to maintenance, unscheduled outage, or natural disaster.

Throughout the entire communications flow, Postini does not require the message to be written onto disk (except for archiving) before any actions can be taken, conducting all necessary steps while the communication is held in memory. This not only speeds communication delivery but also eliminates security risks associated with unauthorized disk access.

2. Flexibility

The Postini solution is highly flexible to meet every organizations specific requirements and needs (see fig. 3). An administrative web-based interface enables administrators to quickly and simply create, modify, and implement policies to meet changing business conditions and evolving regulatory requirements. Changes are updated and propagated in real time, reducing security and compliance risks. And policies can be applied centrally across all channels in the entire organization – ensuring consistent security and compliance.

Another key feature that contributes to the ease of administration and management of the communications security and compliance solution is the granularity and flexibility of policy control. In other words, how narrowly can a particular rule be applied to the message flow? With the Postini solution, policies can be defined at the user, role, group, department, business unit, and organizational levels, offering highly granular flexibility. The Postini platform gives organizations a detailed and custom set of rules that can be changed on-the-fly and in real time.

3. Ease of Deployment and Use

A platform-based, on-demand communications security and compliance solution, the Postini platform is simple to deploy and use. Through its patented, real-time processing technology, it evaluates message content and attachments seamlessly – without writing to disk, which can create bottlenecks and security holes – and assigns security and compliance dispositions based on a unique combination of threat intelligence, heuristics, connection intelligence, and business policies.

Postini's unique real-time approach also ensures processing delays do not impede valid messages and no message is ever lost. Users benefit from the seamlessness of the Postini platform, which 'passes through' and instantly delivers messages that meet the security criteria, incurring zero latency. Connections from internet protocol (IP) addresses that are observed to have malicious or spam behavior are dropped, whereas messages that are known to contain spam,

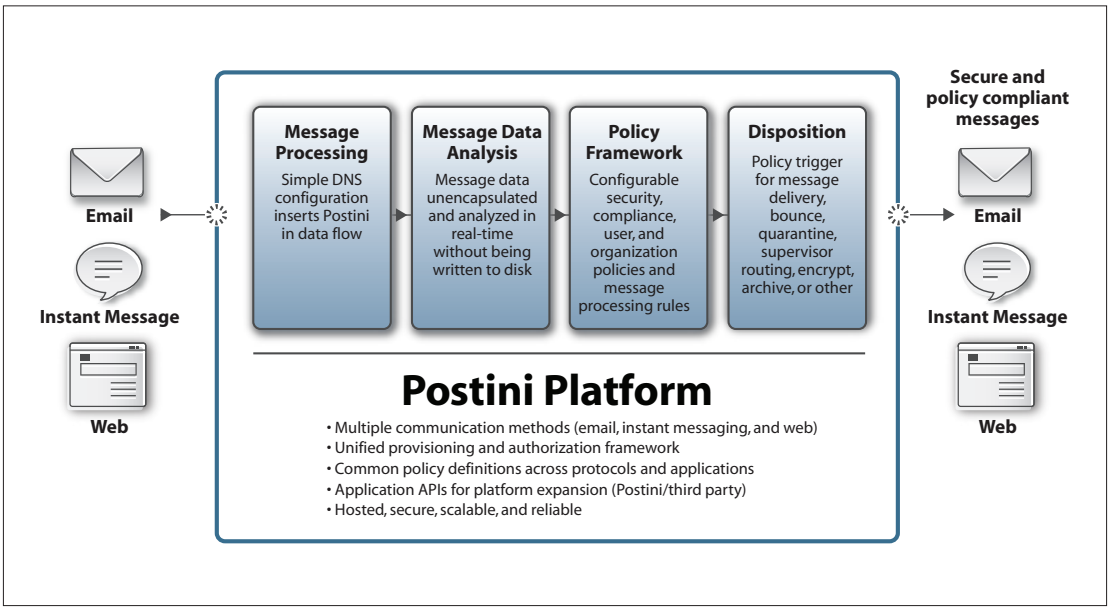

Figure 2: Postini's Software-as-a-Service platform provides an effective communications security and compliance solution.

When offering its own email hosting and delivery service became unmanageable due to the explosion in spam volumes, Dazzl, a value-added reseller based in Canada turned to Postini instead. With no hardware expenditures to accommodate growing capacity nor uptime and delivery latency concerns, Dazzl's staff experienced an almost instantaneous productivity boom after deploying Postini because its employees can now pay more attention to customers and generate revenue rather than maintaining its email security solution.

phishing, or harmful viruses are blocked. Postini quarantines suspicious and non-compliant messages and holds them for user review.

4. Low Total Cost of Ownership

With the Postini platform, organizations can deploy a security and compliance solution in hours or days rather than weeks or months. Without hardware to specify and purchase or software to implement, there are no concerns about integration with other existing infrastructure or worries about significant investment in skilled teams of technicians to implement and maintain the solution. Postini has one of the lowest operating, capital, and IT overhead costs of any on-demand communications compliance and security solution available, enabling customers to realize quick time-to-value for their Postini platform investment (see fig. 4).

5. Scalability and Reliability

Built on top of an award-winning, global infrastructure spanning 14 different data centers that process communications efficiently and reliably, the Postini network delivers scalable operations and support that is monitored around the clock for any unexpected system issues or threats. With a global infrastructure, the Postini network can easily accommodate additional capacity for customers as growth requirements dictate or when occasional spikes in network traffic occur, ensuring that network congestion or connection limits do not impact customers' business productivity.

The Postini network is not only scalable, but also highly reliable, delivering automated, immediate failover in the event of a catastrophe with a 99.999% service-level assurance for email processing. The network's reliability has been independently validated to adhere to industry best practices. In addition, each year, the Postini operations staff conducts rigorous SAS 70 Type II audits for each of the company's data centers. To-date, Postini is the only on-demand communications security and compliance provider to earn the coveted WebTrust seal for meeting the rigorous standards set forth in the SAS 70 guidelines.

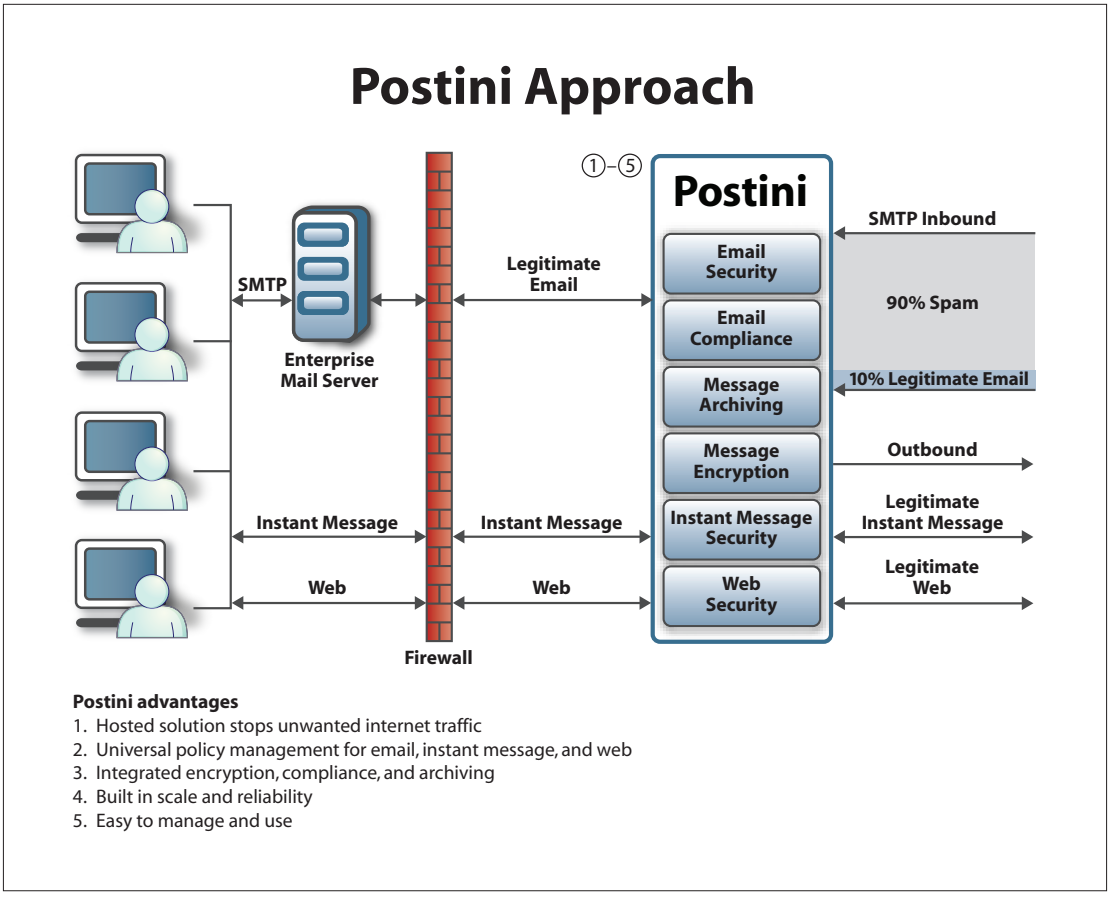

Figure 3: Postini's on-demand solution stops unwanted internet traffic before passing through the enterprise firewall.

Conclusion

Not all on-demand communications security and compliance solutions are equal. In fact, many fall far short of meeting the five critical criteria that enable subscribing customers to improve the productivity of their business and IT users while ensuring the security and compliance of all electronic communications.

Postini uniquely meets the five criteria of an effective on-demand communications security and compliance solution. Delivering ease of use, flexible administration and management, high effectiveness, low total cost of ownership, and strong scalability and reliability, Postini helps its customers improve both their business and IT productivity and drive bottom-line revenue.

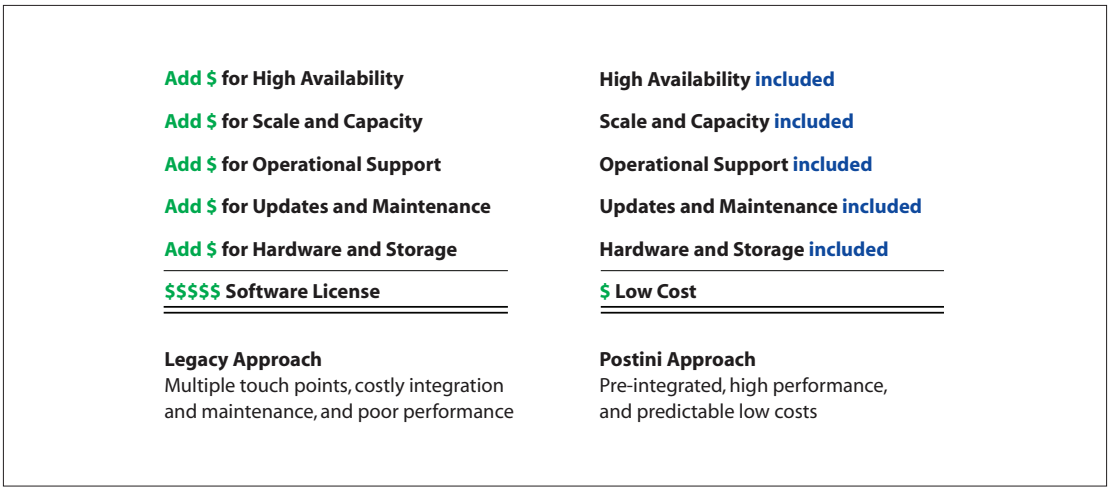

Figure 4: Postini solutions include ease of deployment, scalability, support, and high performance at a low cost.

About Postini

Postini, a wholly owned subsidiary of Google, is a global leader in on-demand communications security, compliance, and productivity solutions for email, instant messaging, and the web. Postini's award-winning services are designed to protect customers from viruses, spam, phishing, fraud, and other attacks; encrypt messages to ensure confidentiality and privacy; and archive communications to ensure compliance with regulations and to prepare for e-discovery.

More than 35,000 businesses rely on Postini everyday to protect them from a wide range of threats. Customers can ensure reliable communications, reduce compliance and legal risks, and enable the intelligent management and enforcement of enterprise policies to protect intellectual property, reputations, and business relationships. More than 1,700 business partners worldwide add value to Postini solutions.

For more information, please contact Postini at info@postini.com or visit www.postini.com.

WP35-0711