Email protection.

Ultimate security and privacy for email, hosted in Canada.

Assessing the risk.

Efficient and economical, email is today's critical business communications tool. But there's a downside to our reliance on email – extreme vulnerability to security threats and a huge drain on productivity through spam.

Consider the risks:

- **Spam.** Spam accounts for up to 80% of email traffic. If each one of your employees spends 30 minutes every week sorting through their emails to delete spam, what is the impact to your bottom line? Also consider the amount of bandwidth and email server space that is wasted receiving and storing unwanted messages. What if this waste could be eliminated before it reaches your network?

- **False positive spam.** Many anti-spam solutions are not specifically designed for business. The results are high false positive rates, meaning many legitimate emails are labelled as spam and deleted. Imagine the impact if your customers' emails were consistently blocked.

- **Malware.** Email may contain viruses and malware that can infect and shut down your critical systems and applications. If your email server is corrupted, you could potentially lose all your customer correspondence – not to mention the costs to recover your system.

- **Phishing.** Through links embedded in unsolicited emails, users are lured to seemingly legitimate Web sites. They are then encouraged to enter personal information which is in turn stolen and sold on the black market.

The better way to protect email.

TELUS offers a comprehensive solution specifically designed to protect all aspects of email communications – spam, viruses and archiving. The advantage of a fully managed solution is that TELUS takes care of all monitoring and maintenance. Your organization does not have to provide the skilled resources that are required to manage and support a growing security infrastructure. TELUS Email Protection delivers key business benefits:

- **Industry-leading uptime and message delivery.** With TELUS' superior network uptime, your filtered email will be delivered promptly.

- **Effective Spam and Malware filtering.** Our spam and malware detection and filtering rates are the best in the industry, with a catch rate greater than 99% and a false-positive rate of less than one in a million messages.

- **Unbeatable privacy protection.** Apart from filtering for unwanted content, email processed by TELUS servers is never changed, read, copied, distributed or otherwise tampered with.

- **Compliance with legislation.** Our solution can help your organization meet government and industry regulations regarding email communication. Regulations may include filtering incoming and outgoing email communications. Privacy legislation is also forcing the encryption of outgoing emails that contain private customer information.

- **No up-front capital expense.** TELUS Email Protection solution is hosted, which immediately lowers costs associated with processing spam. There is no software to buy or install, and no hardware to configure or maintain.

- **Free up IT resources.** Instead of getting bogged down with system maintenance and updates, your IT people have the time to focus on more strategic projects.

Comprehensive protection.

TELUS Email Protection comprises features hosted in Canada that can:

- Filter spam
- Scan and eliminate viruses
- Provide outbreak detection and prevention
- Enforce policy
- Provide status reports
- Provide message continuity
- Encrypt email (optional)
- Prevent the loss of sensitive data (optional)
- Advanced Malware Protection (optional)

TELUS®

Take a closer look.

TELUS Email Protection offers best-in-class features for key aspects of securing email communications:

- Spam filtering
- Malware Scanning
- Policy enforcement
- Status reporting
- Message continuity
- Email Encryption
- Data Loss Prevention
- Outbreak Detection

TELUS Email Protection Service is one component of a fully integrated, comprehensive security portfolio available from TELUS.

The benefits include:

Proven Spam Protection

Our security technology blocks all types of undesirable email messages using a multilayered scanning architecture. This enables us to deliver the industry's highest spam catch rate, greater than 99 percent, with a less than one in one million false-positive rate.

TELUS Email Protection examines the complete context of a message, including: what content the message contains, how the message is constructed, who is sending the message, and where the call to action of the message takes you. By combining these elements, the broadest range of threats are stopped with industry-leading accuracy.

Powerful Virus Defense

TELUS Email Protection provides a multilayered, multivendor approach to virus filtering.

McAfee and Sophos antivirus technologies are fully integrated to enable multiple traditional virus detection methods and to ensure maximum protection.

Outbreak detection filters prescreen messages, stopping viruses and malware hours before traditional signatures are available.

Sophisticated Outbound Filtering Protects Sensitive Information

Outbound filtering is just as important as inbound security. By applying additional message safeguards and policies, outbound filtering helps protect and secure sensitive information.

Content filtering can be used to add headers or footers to email, or to keep email with confidential or inappropriate information from entering or leaving your network.

Transport Layer Security (TLS) uses digital certificates to authenticate the user as well as the network.

Advanced Controls

Users can take advantage of the highest levels of security and control. A range of email authentication solutions are supported by the security gateway to enable the intelligent mail system to make more accurate decisions.

Sender Policy Framework (SPF) verification and signing means that messages are digitally processed to establish and protect identities with email senders and receivers on the Internet.

Bounce Verification tags messages with a digital watermark to provide filtering of bounce attacks at the network edge. Directory Harvest Attack Prevention (DHAP) tracks spammers who send to invalid recipients and blocks attempts to steal email directory information.

Comprehensive Administration and Easy Access for Co-Management

Consolidated and robust reporting options analyze traffic data from geographically diverse infrastructure deployments to provide fully integrated security reporting.

Message tracking gives customers real-time visibility into messages. This feature can help resolve help desk calls quickly by determining the exact location of a message. Instead of having to search through log files, the administrator can use the flexible tracking interface to locate messages.

Email Encryption (optional component)

Technologies to encrypt email, such as S/MIME and Open PGP, have failed to achieve widespread adoption primarily due to their deployment complexity and the burden they place on the sender and the recipient to open and manage encrypted messages.

TEPS Email Encryption overcomes the problems of earlier technologies by providing a solution that that meets compliance requirements for email encryption, while delivering powerful new email control features—all in an easy-to-use, broad-reaching, and affordable offering.

Data Loss Prevention (optional component)

To ensure compliance with industry and government regulations worldwide and help prevent confidential data from leaving customer networks, Email DLP offers easy management, comprehensive protection, and unparalleled accuracy. Email DLP has more than 100 predefined polices to cover government regulations, and industry regulations.. Subscribers can also build custom policies to look for company-specific informa¬tion. Additionally, they can choose from numerous remediation actions, such as BCC, notify, quarantine, and encrypt. Email DLP is specifically designed to virtually eliminate false positives, which means that subscribers do not need to constantly monitor and manage violations. If examining quarantined messages is required, offending content is highlighted in each message.

Advanced Malware Protection (optional component)

Email is one of the top methods for distributing malware, and email-based exploits have become more sophisticated over time. The exponential growths in new malware samples and modes of attack have made it impossible for traditional antimalware solutions and security measures to keep up. Featuring file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for the continuous analysis of threats, even after they have traversed the email gateway. You can block more attacks, track suspicious files, mitigate the scope of an outbreak, and remediate quickly.

GET THE BEST FOR YOUR BUSINESS.

Do more with TELUS solutions. Connect with us today and we'll show you how. Contact your TELUS Account Executive, call 1-866-GO-TELUS or visit **telus.com/BusinessSecurity**

TELUS