TELUS Business Solutions | Security and Risk Management
Business. Backed by TELUS.

managed intrusion prevention

zero-day protection for your business

proactive network security

MyDoom…Slammer…Sasser. Viruses and worms like these are notorious for the speed at which they caused damage across the Internet. They are examples of next-generation attacks launched within days of a vulnerability announcement. Their "success" has highlighted the shortcomings of traditional security measures such as intrusion detection and firewalls. Now the concern is focused on attacks that are even faster – zero-day attacks that exploit computer system vulnerabilities within hours of the vulnerabilities being reported to the security community. This leaves very little time for IT professionals to patch and protect their environment.

TELUS has a better way to combat evolving threats. TELUS Managed Intrusion Prevention is proactive – it detects and blocks both known and unknown attacks. The solution addresses the primary shortcomings of conventional intrusion detection systems and firewalls.

Firewalls depend on defined hard-coded rules that allow or deny certain types of traffic. But a firewall on its own may not have the capability to block new or unknown exploits not based on these pre-set rules. An intrusion detection system (IDS) will detect possible intrusions into a network and generate reports on them. However a skilled security expert must be available to analyze these reports to verify the validity of the alarm. Meanwhile, the intrusion may already be successful and the network compromised.

Given the limitations of these systems, organizations around the world are turning to intrusion prevention systems (IPS) to enhance their security. An IPS adds the real-time blocking capabilities of a firewall to the already strong detection capabilities of an IDS. With an IPS, the attack/intrusion is detected as well as blocked. This removes the human component required to analyze logs and execute a prevention or mitigation action.

While much more effective in preventing attacks than an IDS or a traditional firewall, IPS solutions are more complex and require deep specialization to set up and maintain. That's one critical advantage of TELUS Managed Intrusion Prevention. With our managed service, TELUS security experts take care of implementation, monitoring and management. Their expertise is unparalleled. With TELUS as your partner, your enterprise gains more comprehensive security and a higher level of protection.

unparalleled performance

TELUS Managed Intrusion Prevention proactively defends against zero-day virus and worm attacks. The solution protects network infrastructure and critical systems by using advanced algorithms that can differentiate between malicious and valid traffic. As a core element of your security strategy, TELUS Managed Intrusion Prevention provides key business benefits:

Worry-free security management. TELUS has assembled the advanced capabilities, knowledge, skills and services to provide comprehensive security solutions. You don't have to develop operational procedures, or create and deploy your own IPS. That's our job. So is monitoring and maintaining your network to ensure that it delivers the performance and reliability you require. And you don't have to deal with recruiting, hiring, training and retaining personnel with the required security experience. TELUS has the expertise you need.

Access to the TELUS team of security experts. Our team deals with a broad range of constantly changing security challenges across our network and our clients' networks. Our experts will work with you to enhance your security posture through continuous monitoring, management, and immediate response to potential security threats.

Flexible cost models. Our monthly subscription models can be structured to meet your specific needs. We offer fully bundled solutions including all hardware, software, remote management, monitoring and maintenance. If you've already invested in equipment, we can manage that too.

Improved efficiency. TELUS Managed Intrusion Prevention increases employee productivity by reducing downtime due to security threats.

Compliance with regulatory and legal requirements. Many regulations require organizations to ensure the security and confidentiality of information such as financial records. TELUS Managed Intrusion Prevention will protect your network from unauthorized access, malicious content and attacks that target mission-critical financial servers and networks.

turnkey solution

TELUS Managed Intrusion Prevention delivers security, performance and ease-of-use:

- Keeps your network environment secure from external attacks
- Maintains and monitors your intrusion prevention system
- Notifies you about threats
- Implements patches before your internal environment is affected

TELUS
the future is friendly®

managed intrusion prevention

the better way to secure your network

Conventional firewalls provide protection only up to Layer-4 in the OSI model. While these measures have historically been adequate to filter out the majority of attacks, the current situation is radically different – hackers and virus writers can easily bypass firewalls by finding intrusion mechanisms above Layer-4. This renders firewalls ineffective and leaves an open door for your critical systems to be compromised.

TELUS Managed Intrusion Prevention is much more proactive than firewalls and antivirus solutions. The algorithms in our solution allow it to inspect a stream of network traffic and determine which network packets are part of an attack. TELUS Managed Intrusion Prevention provides complete protection up to Layer-7 via three intelligent mechanisms:

- **Protocol normalization and anomaly detection**. All packets entering the sensor are scrubbed; protocol is compared against rules; deviation from rules triggers a response.
- **Signature detection engine**. Signatures created for both known and unreleased attacks; anomaly detection helps prevent false positives.
- **Statistical anomaly detection**. When an attack is detected, the system determines what packets belong to the attack and drops them.

leading-edge expertise; state-of-the-art technology

TELUS managed security professionals have training and certifications from SANS, (ISC)2 CISSP, and security technology vendors. Because the field of information security continues to change at a rapid pace, our security professionals are constantly updating their knowledge and experience.

We utilize the most powerful network management systems and tools to ensure superior performance from your network. At our Security Operations Centre, TELUS network professionals continuously monitor IPS appliances for availability, performance and security. Our practice is based on input from numerous security standards and best practice organizations and industry alliances (e.g. NIST, SANS, CERT, etc.).

Our Web-based reporting tools give you the system visibility you need to run your business. Remote and on-site support is included with our service. Our commitment is to ensure that all issues are completely resolved within time frames relevant to the severity of the issue.

managed service features

design, configuration and installation

- Initial design, configuration, and installation of the IPS infrastructure
- Environmental assessment and design of an IPS solution
- Configuration and project management of solution installation to ensure compliance with scheduled turn-up dates

monitor and action

- 24x7 remote monitoring of IPS infrastructure via the TELUS Security Operations Centre including:
- State of the device
- Possible device failure
- Possible intrusions
- Proactive response to resolve specific alarmed events

maintenance

- TELUS assumes responsibility for maintenance of the IPS infrastructure
- Includes configuration changes and scheduled maintenance to implement firmware patches and updates – a critical feature because the IPS will require updates and new signatures implemented on a continuous basis as new vulnerabilities are discovered

monthly event summary

TELUS will provide a summary of events including:

- Device(s) uptime
- Possible intrusion attempts
- Alarms
- Configuration changes
- Details for all ticketed troubles and changes

service levels

- Service availability of devices: 99.95% (HA Configuration)
- Customer notification of high priority events: 15 minutes
- Signature updates: every 4 hours
- Average time for non-critical configuration changes: 4 hours