Telstra Internet Protection
Web and Mail

Proactive, in-the-cloud protection against phishing, malware, ransomware and impersonation attacks.

Malware, phishing and ransomware continue to threaten businesses as they grow in sophistication and frequency. Protecting your information, financial integrity and reputation from these risks is vital.

Internet Protection Web and Mail can help you do just that through proactive, network-based scanning to help defend against detected forms of malware and ransomware, including zero-day threats.

Internet Protection Web and Mail are cloud-based services that combine advanced tools from leading security vendors, the latest local and global threat intelligence and the in-built security of our world-class networks. The services can be purchased separately or together or as part of the suite of Telstra security services depending on your requirements.
Internet Protection Web

Internet Protection Web uses high performance global infrastructure to help ensure threat protection even for remote or roaming staff, prevent users accessing malicious or inappropriate web sites or content, and reduce network congestion and the bandwidth costs from unwanted traffic.

How does it work?

![Diagram of Internet Protection Web]

Internet Protection Mail

With Internet Protection Mail, you can help secure inbound email from malware, ransomware, phishing, virus and spam. You can also detect advanced threats such as spear phishing, whaling, typo domain and spoofing attacks. In addition to this, the service can help identify unacceptable content, understand risk and enforce corporate policies. It also improves email continuity to help reduce the loss of vital information if outages occur. All data is stored to strict safety standards and you’ll have complete visibility of email activity channelled through the service.

How does it work?

![Diagram of Internet Protection Mail]
World-class security on your terms

Simple
Easy to deploy and manage
• Activate within 24 hours
• Manage your TIP services via an advanced, intuitive web portal

Flexible
Pay only for what you need
• No upfront spend on bulk licenses
• Choose to purchase individual Telstra Internet Protection Web and / or Email seats on a “per month, per user” basis

Affordable
Get access to best-in-class Enterprise-grade Cisco ESA and Umbrella technology at an affordable, flexible price point

Reliable
Have peace of mind that you’ll be protected with
• The latest local and global threat management
• 100% uptime and availability
• Dedicated Firstwave support with high SLA’s and a 24X7 Helpdesk

Compliant
• All email data stored in Australia
• Policy management is centralised for better security practices, in line with your own company policies
Security

Telstra Internet Protection allows you to use the portal to easily add, change, monitor and report on content policies and monitor the email and current threat reports for spam, virus, malware and phishing, applying it to both inbound and outbound email channels.

The following security policies are available where a defined action is applied to any inbound or outbound email that matches any rule:

<table>
<thead>
<tr>
<th>Policy name</th>
<th>The defined action is applied on:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing Indicator</td>
<td>Emails containing suspicious URLs or content</td>
</tr>
<tr>
<td>Email Bounces</td>
<td>Spam mails that appear to be bounced emails (also known as ‘backscatter spam’)</td>
</tr>
<tr>
<td>Public Redirect Spam</td>
<td>Emails containing spam relayed from public mail service provider</td>
</tr>
<tr>
<td>Footer Text</td>
<td>Emails – to add the specified footer text</td>
</tr>
<tr>
<td>Suspect Spam</td>
<td>Emails suspected of being spam</td>
</tr>
<tr>
<td>Unscannable</td>
<td>Emails that cannot be scanned e.g encrypted</td>
</tr>
<tr>
<td>SPF (Sender Policy Framework)</td>
<td>Emails that fail SPF authentication</td>
</tr>
<tr>
<td>DKIM (Domain Keys Identified Mail)</td>
<td>Emails that fail DKIM check for signing and verifying email messages on a per-domain basis</td>
</tr>
<tr>
<td>Forged Email</td>
<td>Spoofing emails, that is, those with forged sender address</td>
</tr>
<tr>
<td>Virus</td>
<td>Emails containing viruses</td>
</tr>
<tr>
<td>Spam</td>
<td>Emails classified as spam</td>
</tr>
<tr>
<td>C-Level Impersonization</td>
<td>Emails classified as ‘whaling’ phishing attacks or ‘CEO impersonation fraud emails’</td>
</tr>
<tr>
<td>Typo Domain</td>
<td>Emails sent from an ‘impersonating’ domain or those classified as look-alike/homograph domain attack</td>
</tr>
<tr>
<td>Malicious URL</td>
<td>Emails containing malicious URLs</td>
</tr>
<tr>
<td>Suspect URL</td>
<td>Emails containing suspicious URLs</td>
</tr>
<tr>
<td>Clean URL</td>
<td>Emails containing RESTful/Semantic/user-friendly URLs that enable search engine optimization (SEO)</td>
</tr>
<tr>
<td>URL Categories</td>
<td>Emails containing the selected URL categories – Risky, Unproductive, Business, Unclassified</td>
</tr>
<tr>
<td>APT Categories</td>
<td>Emails that fall under Advanced Persistent Threat (APT) categories</td>
</tr>
<tr>
<td>DMARC</td>
<td>Emails that fail DMARC authentication</td>
</tr>
</tbody>
</table>

Customer Security Management Portal

Telstra Internet Protection provides you secure access to a portal, with hierarchical multi-level Role-Based Access Control (RBAC), to give your authorised users the required level of visibility, management and control of all security, content control, DLP/ Risk or Image Control security applications and service provisioning from any nominated location.

The secure portal access features means:

1. The access to the portal is restricted to known IPs associated with the subscribing enterprise.
2. The user cannot see the login page if the portal doesn’t have the IP address the user is trying to log in from. However, the users can update their IP by contacting the Support team.
3. If 2FA is implemented, the user will need to enter the authorisation code sent to his/her registered mobile number on every log in to the portal.
4. The system is designed to deliver the right information to the right people and to ensure them access to the right functions.
5. New custom applications can be developed specific to the organisation and shared in a secure manner on the portal.
6. The system allows a very granular analysis and review of email traffic and provides a full view of emails if required.
7. The framework is designed to provide premium compliance and risk mitigation for the organisation; the organisation can control every access privilege.

Footer Text

Telstra Internet Protection provides you secure access to a portal, with hierarchical multi-level Role-Based Access Control (RBAC), to give your authorised users the required level of visibility, management and control of all security, content control, DLP/ Risk or Image Control security applications and service provisioning from any nominated location.

The secure portal access features means:

1. The access to the portal is restricted to known IPs associated with the subscribing enterprise.
2. The user cannot see the login page if the portal doesn’t have the IP address the user is trying to log in from. However, the users can update their IP by contacting the Support team.
3. If 2FA is implemented, the user will need to enter the authorisation code sent to his/her registered mobile number on every log in to the portal.
4. The system is designed to deliver the right information to the right people and to ensure them access to the right functions.
5. New custom applications can be developed specific to the organisation and shared in a secure manner on the portal.
6. The system allows a very granular analysis and review of email traffic and provides a full view of emails if required.
7. The framework is designed to provide premium compliance and risk mitigation for the organisation; the organisation can control every access privilege.
**Content Control**

Telstra Internet Protection allows you to use the portal to enforce specific actions on individual email filters such as email size, profanity, attachment type, and email headers.

The following content control policies are available and configurable through the portal to specify any number of content policy rules and define the action to be applied to any inbound or outbound email that matches any rule:

<table>
<thead>
<tr>
<th>Policy name</th>
<th>The defined action is applied on:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Only</td>
<td>Emails from/to the specified addresses</td>
</tr>
<tr>
<td>Email Size</td>
<td>Emails that are lower than/between/over the specified size(s)</td>
</tr>
<tr>
<td>Attachment Type</td>
<td>Emails with specified attachment types, including those often used as disguised malware payloads e.g. .exe, scripts, encrypted</td>
</tr>
<tr>
<td>Profanity</td>
<td>Emails containing profane words or language</td>
</tr>
<tr>
<td>PCI</td>
<td>Emails containing credit card information</td>
</tr>
<tr>
<td>Custom Keywords</td>
<td>Emails that contain the specified keywords</td>
</tr>
<tr>
<td>Inbound Marketing</td>
<td>Emails classified as marketing emails; also known as ´Graymail´</td>
</tr>
<tr>
<td>Email Header</td>
<td>Emails that contain the specified text in the header</td>
</tr>
</tbody>
</table>

**DLP (Data Loss Prevention) and Risk**

Telstra Internet Protection gives you the flexibility to inspect every message that leaves the organisation and apply advanced actions ranging from alerting key parties to blocking the transmission easily and effectively.

The following DLP/Risk policies are available and configurable through the portal to specify any number of DLP/Risk policy rules and define the action to be applied to any outbound email that matches any rule:

<table>
<thead>
<tr>
<th>Policy name</th>
<th>The defined action is applied on:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Only</td>
<td>Emails from/to the specified addresses</td>
</tr>
<tr>
<td>Email Size</td>
<td>Emails that are lower than/between/over the specified size(s)</td>
</tr>
<tr>
<td>Attachment Type</td>
<td>Emails with specified attachment types, including those often used as disguised malware payloads e.g. .exe, scripts, encrypted</td>
</tr>
<tr>
<td>Profanity</td>
<td>Emails containing profane words or language</td>
</tr>
<tr>
<td>PCI</td>
<td>Emails containing credit card information</td>
</tr>
<tr>
<td>Custom Keywords</td>
<td>Emails that contain the specified keywords</td>
</tr>
<tr>
<td>BCC</td>
<td>Emails containing external mail addresses in the BCC field</td>
</tr>
<tr>
<td>Email Header</td>
<td>Emails that contain the specified text in the header</td>
</tr>
</tbody>
</table>

**E-Discovery/Archive**

Telstra Internet Protection allows you to quickly search and retrieve archived email content for all of your customer domains across all nodes and associated email archives as well as across all inbound and outbound email channels.

E-Discovery/Archive employs advanced customer-specific indexing technology for:

- Faster parallel search
- Access-controlled metadata and records
- Granular separation and association with data stores (to conform with security and retention policies)
- Highly scalable (to millions of records) whilst maintaining sub-second retrieval times
- Metadata indexes that integrate automatically with the interface (specific to customer, role, or time)
- Metadata indexes that support both simple features or classification metadata from complex specific classifiers
- Metadata indexes can be associated with an ontology leaf, or can relate to entire dataset

**Continuity**

Telstra Internet Protection improves email continuity to help reduce the loss of vital information if server outages occur.

The Continuity features means:

- The domains are configured when the email solution is deployed.
- Multiple domains can be configured as per your requirement.
- You can use the portal to add or change failover configurations of any domain.
- The Portal Admin can set up email, SMS, and call alerts for emails sent to you when there are alerts associated with your domain.
**Image Control**

Telstra Internet Protection gives you the ability to configure control policies for non-business and offensive images in your email flow.

The Image Control application has two key policies:

- **The Non-Business policy** filters emails that contain graphics/ media of non-business nature, such as email marketing material, presentations, personal jokes, etc.

- **The Offensive policy** filters out emails that contain porn or sexually explicit graphics/media and those that might be considered to be in violation of the harassment policies of the organisation.

**Policy Filter Rule Action**

Telstra Internet Protection gives you a powerful, granular yet simple way to configure different actions selectable for every Security (except Spam and Virus), Content Control or DLP/ Risk policy filter rule to optimise how you enforce, monitor, respond, audit & continuously improve your security posture.

- **Copy**: choose to send a copy of an email to a designated recipient e.g. IT / Security Admin

- **Flow**: choose if and how to handle the processing and forwarding of the email:
  - **Delay** – to any specified time range in the same day
  - **Hold/Quarantine** – place in quarantine, where it can be parsed by an administrator using the Trace APP
    - **Alert/Notify** – sender, recipient or nominated Administrator with fully-configurable notification templates
  - **Redirect**
  - **Release**
  - **Reorigin**

- **Modify**: choose if and how to modify the email prior to delivery to the destination/recipient
  - Add Header
  - Add Warning
  - Remove All Attachments

- **Learn/Report**: choose a filter simulation mode to passively examine and report the match behaviour of new or modified policy filter rule on inbound or outbound email streams, and assess how it may perform against security goals and business outcomes, before deciding to actually implement the policy filter rule.

**Trace**

Telstra Internet Protection’s trace functionality allows you to use the portal to track, and troubleshoot any email in case of delay, non-delivery, incorrect classification or quarantine.

The trace feature allows for:

- **Copy**: choose to send a copy of an email to a designated recipient e.g. IT / Security Admin

- **Flow**: choose if and how to handle the processing and forwarding of the email:
  - **Delay** – to any specified time range in the same day
  - **Hold/Quarantine** – place in quarantine, where it can be parsed by an administrator using the Trace APP
    - **Alert/Notify** – sender, recipient or nominated Administrator with fully-configurable notification templates
  - **Redirect**
  - **Release**
  - **Reorigin**

- **Modify**: choose if and how to modify the email prior to delivery to the destination/recipient
  - Add Header
  - Add Warning
  - Remove All Attachments

- **Learn/Report**: choose a filter simulation mode to passively examine and report the match behaviour of new or modified policy filter rule on inbound or outbound email streams, and assess how it may perform against security goals and business outcomes, before deciding to actually implement the policy filter rule.

**Reports**

Telstra Internet Protection enables real-time reporting across all inbound and outbound email channels, various timeframes, segments, groups, and domains and allows access to top level as well as detailed view of individual emails.

The following standard reports are available:

- **DMARC** – An aggregated view of the DMARC reports (about messages that pass and/or fail DMARC evaluation) received and the number of emails reported for the selected domain.

- **Email Basic** – Online review of real-time flow. It covers usage and segment reports (for most of the policies).

- **Live** – Real-time reports that provide instant access to the current email flow; information is loaded every 15 seconds.

- **Offline Reports** – Periodic offline reports requested by the customer. You can assign a recipient for the report or enable/disable the report.

- **Threat Insight Email** – A unique insight into inbound email traffic covering blocked and delivered emails with specific drill down capability by time.

- **URL Premium Protection** – Report on inbound URL reputation and their categorization.

- **Web Basic** – Web reports covering usage and segment across all policies set in the platform. It covers web traffic that move inbound and outbound through the platform.
About Telstra

We provide network services and solutions to more than 200 of the world’s top 500 companies. They rely on us to do business across 240 countries and territories and to enable greater productivity, efficiency and growth.

Our solutions offer the best of all worlds – skilled people and a rich portfolio of services delivered on our world-class Telstra Next IP® network and Telstra Mobile Network. To ensure reliable performance, they’re monitored and maintained from our dedicated centres using advanced management and operational systems. And they’re backed by Telstra Enterprise-grade Customer Service® and one of Australia’s largest and most qualified field and technical workforce.

The spectrum device and ™ are trade marks and ® are registered trade marks of Telstra Corporation Limited, ABN 33 051 775 556.