Telstra Internet Protection

Web and Mail Protection

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.

TELSTRA

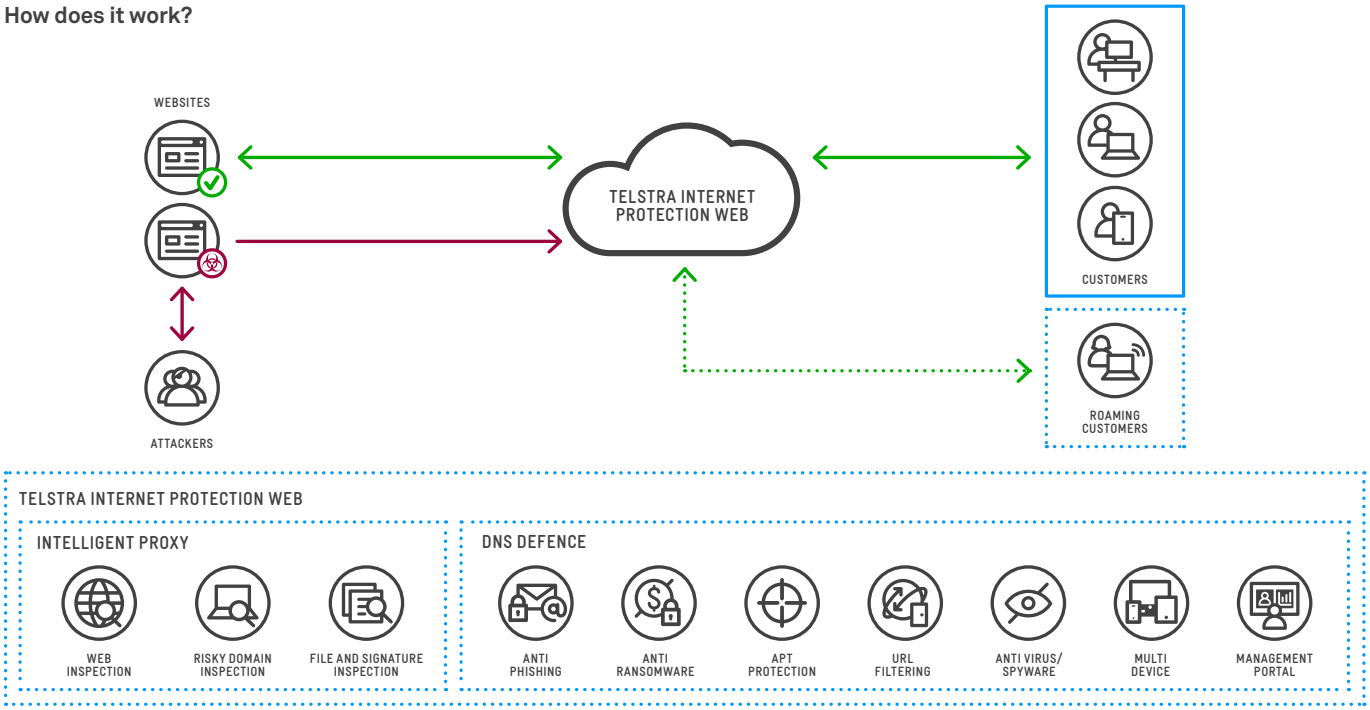
Essential protection

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.

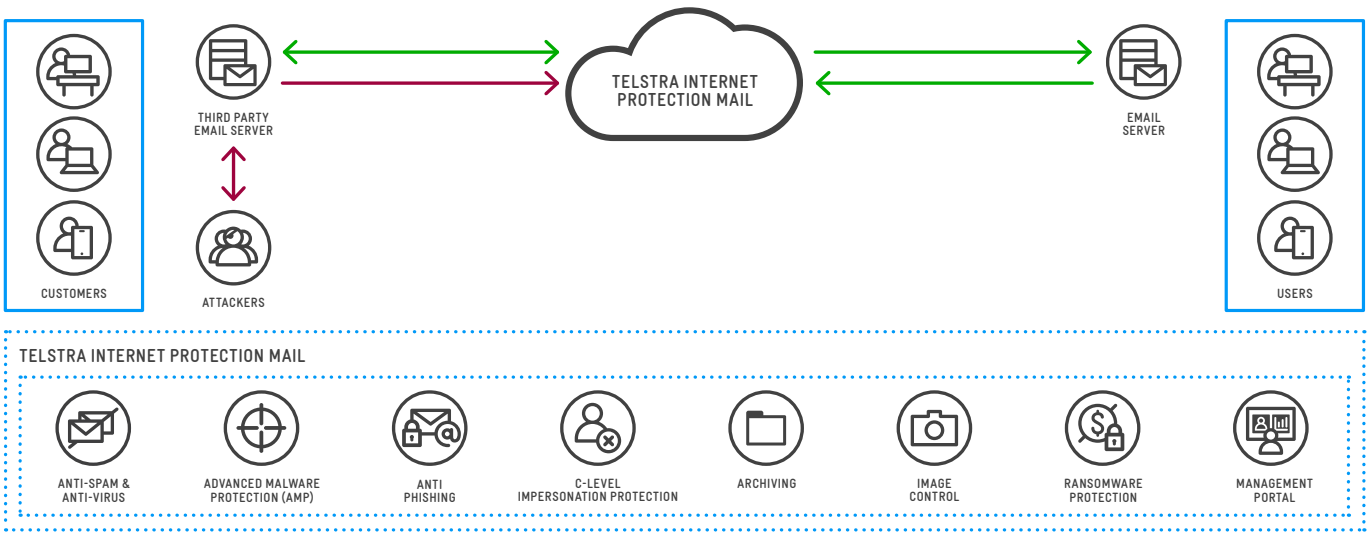
How does it work?



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?



Technical information

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:

- The access to the portal is restricted to known IPs associated with the subscribing enterprise.
- 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.
- 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.
- The system is designed to deliver the right information to the right people and to ensure them access to the right functions.
- New custom applications can be developed specific to the organisation and shared in a secure manner on the portal.
- The system allows a very granular analysis and review of email traffic and provides a full view of emails if required.
- The framework is designed to provide premium compliance and risk mitigation for the organisation; the organisation can control every access privilege.

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:

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

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:

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

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:

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

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 Actions

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 trace, track, and troubleshoot any email in case of delay, non-delivery, incorrect classification or quarantine.

The trace feature allows for:

- Search across multiple domains, emails and timescales using keywords (or part thereof) and wildcards
- Independently check delivery of emails
- Search all parts of the mail including message body (full-text indexing is supported)
- Search for the lost emails from the previous 8 days (excluding the current date) of data.
- Retain the emails longer than 8 days by subscribing to an optional service package
- From the search results, replay mails (individually or in bulk) in their original format bypassing all filters

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.

Contact your Telstra account representative for more details.

Australia

1300 telstra (1300 835 787)

telstra.com/enterprisesecurity

International

Asia +852 2983 3388 **Americas** +1 877 835 7872 **EMEA** +44 20 7965 0000 **Australia** +61 2 8202 5134

telstraglobal.com **tg_sales@team.telstra.com**