CITEC

Secure Web Access Services

CYBER SECURITY SERVICES – DATA SHEET

Service overview

Browsing the web can be a hazardous activity. Among other things, a well-meaning user can be compromised by clicking on a link in a malicious email, navigating to a malicious website or even through malicious advertising on an otherwise legitimate website. Any of these compromises could then leverage that access to compromise other users, or more secure data.

CITEC offers the following services, some at no additional charge, that help mitigate these risks.

RPZ DNS

CITEC's DNS service is offered at no additional cost to all CITEC clients. The RPZ DNS service includes malware feeds from a range of authoritative sources, identifying millions of malicious websites and automatically blocking them before the user connects.

RPZ DNS is one platform with a single list of URLs that is applicable to all CITEC clients, it is not customisable for client-specific requirements.

ISP Firewall

See CITEC’s *Firewall Management Service Description* for full details of the ISP Firewall service.

Threat Protection

CITEC's ISP Firewall service, which separates your internal networks from the untrusted internet, includes a threat protection component, which can be activated at no additional charge. This is the same threat protection that the whole-of-government IDP offers, protecting against viruses, spyware and a range of other threats. However, at this layer it can be configured to any level of granularity.

Want to block executable downloads to your servers, but not your desktop fleet? This is where that happens.

URL Filtering

An add-on to the ISP Firewall service is URL filtering. This is applied to your firewall instance on the ISP firewall and allows you to customise your filters for your requirements. The service is more configurable than RPZ DNS, it delivers more features and allows for finer control, such as the option to black and whitelist URLs.

URL filtering protects against web-based threats by giving you a way to safely enable web access while controlling how your users interact with online content.

With URL filtering enabled, all web traffic (HTTP and HTTPS) is compared against the URL filtering database, which contains a listing of millions of websites that have been categorised. You can use these URL categories as a match criterion to enforce security policy. For example, websites categorised as high risk (such as social media) can be blocked or have a deeper inspection requirement by passing them to stricter anti-virus, malware and other protections. You can also use URL filtering to enforce safe search settings for your users and to prevent credential phishing based on URL category.

URL filtering can integrate with your Active Directory, authenticating and reporting on individual users and groups as required.

SSL Decryption

Normally your ISP firewall is unable to read encrypted traffic, because it's encrypted. This is normally considered a good thing, since we don't want to inadvertently see people’s personal data, but it does limit what the threat protection service can detect.

With the SSL Decryption service, your ISP firewall can be configured to decrypt and scan whatever traffic you like. For example, you could choose to decrypt all traffic to your servers, while only decrypting user traffic to high-risk websites.

SSL Decryption is configurable to the same level of granularity as your security policy.

Web Proxies

Threat Protection, URL Filtering and SSL Decryption combine to fill the same role as a traditional web proxy (forward proxy). With these services enabled, you no longer need any other web proxy solution.

If you have a requirement for a web proxy that cannot be avoided, CITEC can offer a range of web proxy solutions on request.

Whole-of-government IDP

CITEC's whole-of-government IDP is a centrally funded Intrusion Detection and Prevention service, automatically applied to any users transiting CITEC's internet connections. By default, this service is ‘alert only’, which will report on malicious traffic, but it will not block any connections.

‘Blocking mode’ can be enabled on request and will provide broad-based threat protection on your internet connection. Blocking mode is an additional service that attracts additional fees.

Find out more

For more information, please contact your CITEC representative or connect at service@citec.com.au – 07 3222 2555.

About CITEC services

CITEC is a key supplier to the Queensland Government for ICT services.

CITEC's vision is to provide innovative, secure, cost-effective, efficient and accessible services that connect and benefit its partner agencies.

With a focus on transformation and continuous improvement, CITEC is committed to developing its highly skilled workforce and putting Queensland Government agencies the centre of its service design and delivery. CITEC manages key Queensland Government assets including data centres, networks, infrastructure and essential ancillary services that enable agencies to deliver better front-line services.