CLOUD GATEWAY

PRISM

Hybrid Cloud and Multicloud Connectivity

CONNECT, PROTECT, INSPECT

Securely and rapidly connecting everything on your estate with multiple cloud service providers, the PSN, the HSCN and the internet.

The PRISM platform is available in 3 variations

PRISM Standard

PRISM Enhanced

PRISM Premier

The Platform

Cloud Gateway's flagship product, PRISM, provides a platform between traditional networking infrastructure and cloud services. It facilitates secure connectivity in a centralised fashion, enabling the production of reports which help ensure regulation and legislation compliance, specific to your business.

PRISM is an NCSC compliant, 100% cloud-built solution. Thanks to the intelligence of our automation, PRISM can be deployed within days, removing the burden and complexity of networking and security in a timeframe that keeps up with our clients' desire to deploy hybrid and multicloud services.

- Unique cloud-native technology
- Full visibility and control of your network
- Fully integrated network security
- Connection to any cloud service provider
- Supplier and vendor agnostic
- Rapid deployment
- Government grade security – NCSC compliant
- PSN and HSCN connectivity

Bring your own network

PRISM operates on a 'Bring Your Own Network' basis, meaning we can connect your network ecosystem, using any carrier medium(s) with no hardware required on site. You can connect to PRISM via any public or private connectivity method, it is completely agnostic. PRISM creates a routing mesh that seamlessly and securely brings together all of your network endpoints.

Depending on your specific needs, PRISM can act as the beating heart of your network, or as a spoke within a broader ecosystem. The platform reduces appliance sprawl and network aggregation points, for greater visibility and control of your organisation's traffic.

PRISM can bring together:

The main corporate network

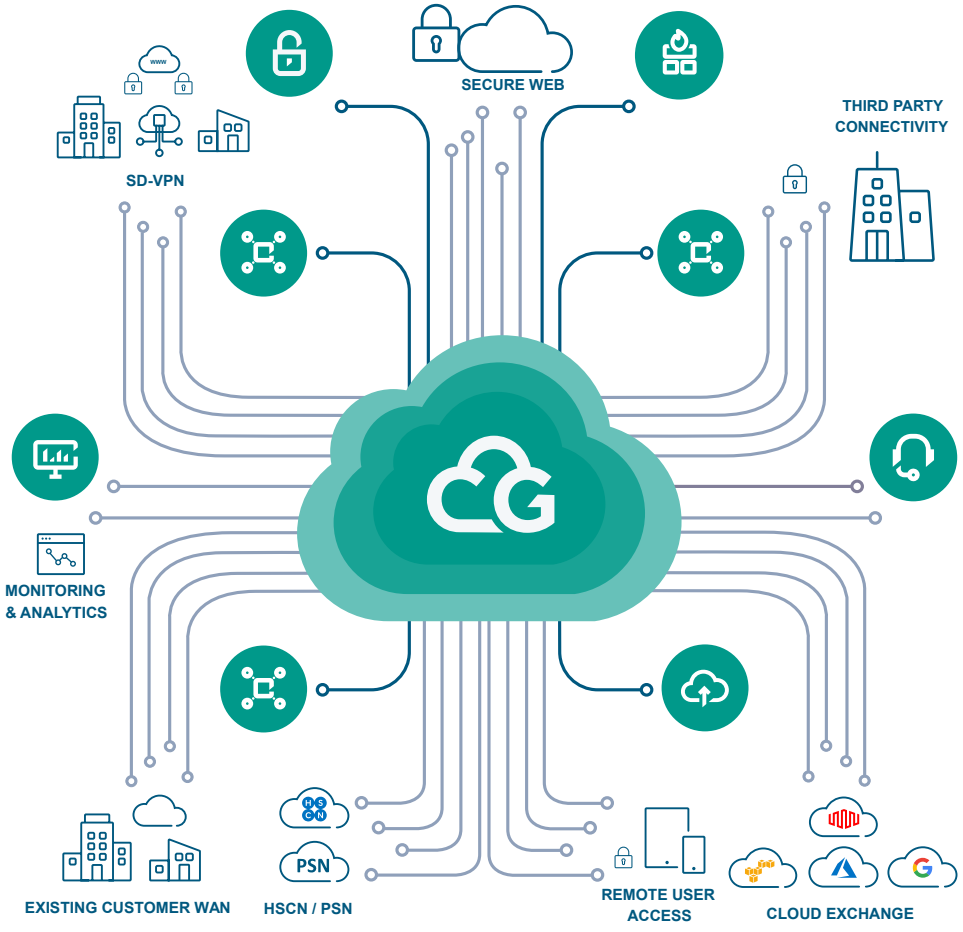
Your supply chain (including third party connections)

Cloud service providers

Remote users and home workers

The internet

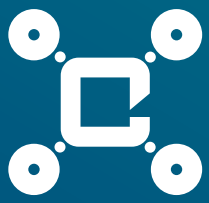
Sector-specific networks including the PSN and HSCN



Connect, Protect, Inspect

Welcome to the three tenets of the PRISM platform, Connect, Protect, Inspect. These core pillars are essential to building secure connectivity infrastructure, giving you more visibility and control of your network.

Connect



The Connect tenet provides your organisation with a full suite of network connectivity capabilities, bringing your entire ecosystem together.

Protect

The Protect tenet provides your organisation with a set of security tools, protecting your network with granular control over policies and governance.

Inspect

The Inspect tenet gives you full visibility of your network traffic and security configurations, allowing you to monitor the network and analyse key metrics.

Key Strengths

- Multi-award winning platform
- Connectivity from anywhere-to-anywhere
- 100% cloud-native solution
- PSN accredited and NCSC compliant
- Vendor & technology agnostic
- Underpinned by cloud expertise and credibility
- Experience within the UK Public Sector
- Security standards and accreditations
- Managed Service, 24hr support and white-label options available

Bandwidth

Available limits

All levels of PRISM are available to purchase on the following bandwidth licences:

100 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps

How is bandwidth measured?

Your bandwidth is allocated across the platform to all your endpoints. This means all connections have the capacity to handle the maximum bandwidth throughout of the purchased licence. The maximum throughout across PRISM is limited to the licence. This gives you the flexibility to be running workloads between end points as you require, without being penalised.

As part of your managed service, Cloud Gateway works with you to monitor your collective traffic throughput, ensuring the total throughput at any given time does not exceed your licence limit. Your traffic throughput data is also available to view on your own customer portal, and through telemetry data reports, available on request. See the 'Inspect' section for more details.

You may purchase a 100Mbps licence for PRISM Enhanced, with various connections to cloud, the internet and your enterprise sites. All individual connections to these endpoints can handle 100Mbps throughput each.

At any given moment, you may consume up to 100Mbps traffic across any/all your connections, without needing to notify Cloud Gateway, or make a conscious decision to allocate chunks of your licence to different endpoints. It is automatic, flexible and scalable.

Increasing bandwidth

As your company grows and your bandwidth demands increase, our cloud-native platform grows with you. As PRISM is built on software, in the cloud, upgrading your bandwidth limit to the next licence level can be achieved immediately.

Simply contact our customer service team, who will work with you to uplift your bandwidth licence in accordance with your needs. It is not possible to scale back your licence mid-term. Please consult our Service Definition documentation for more details.

Enterprise Connect

SD-VPN™

Available in: 

We can connect your site using your existing internet circuits and hardware. All we need you to do is build a secure tunnel to your Cloud Gateway tenant; it is based upon IPSec standards, with some BGP configuration and using a set of credentials we provide.

From there, we will quickly connect you to the PRISM ecosystem, which in turn provides links to all the other connected endpoints on your network estate.

These SD-VPN connections adhere to, and improve upon the Foundation Profile cryptographic parameters as laid out by the National Cyber Security Centre (NCSC).

Third Party MPLS NNI (Network-Network Interface)

Available in: 

PRISM can also connect to your enterprise MPLS in our carrier-neutral co-location facilities* using a Network-Network-Interface. We will work with you or your MPLS provider to create this connection and associated design.

* assuming that your MPLS WAN provider has a presence in our facilities - Equinix LD8 (London), Equinix MA3 (Manchester), Ark Cody Park (Farnborough), Ark Spring Park (Corsham).

Data Centre Cross-Connect

Available in: 

PRISM can also connect to your enterprise using a simple data centre cross-connect in one of our carrier-neutral co-location facilities*. This essentially is “running a fibre” between our racks and yours, allowing direct physical connectivity into the PRISM fabric, and onwards to your tenant.

* Equinix LD8 (London), Equinix MA3 (Manchester), Ark Cody Park (Farnborough), Ark Spring Park (Corsham).

Cloud Connect

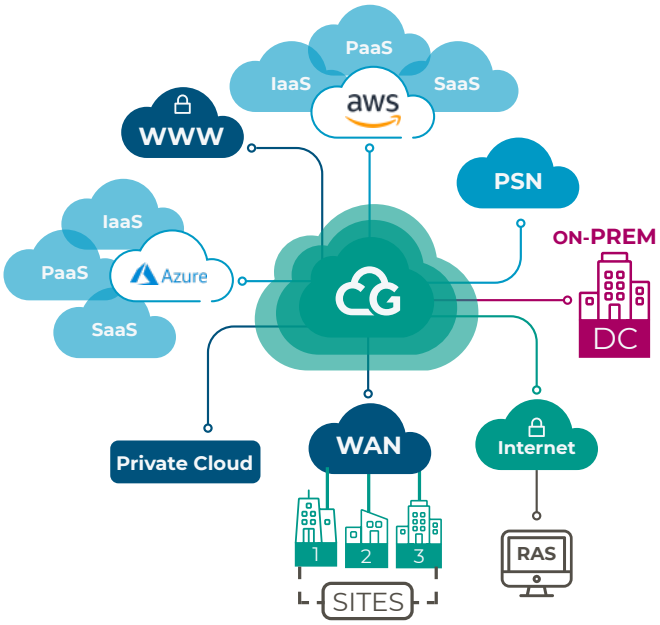
Available in:

On the 'cloud side' of your estate, PRISM has on-net/ on-ramp connectivity to many public and private Cloud Service Providers. This allows us to connect you privately to multiple cloud service providers.

Establishing a connection to a cloud environment can be done within minutes with Cloud Gateway doing the heavy lifting.

One of the benefits of private cloud connectivity is security, predictable performance and deterministic traffic paths. From a latency perspective, we have seen between 1 and 5 milliseconds* by going cloud to cloud via PRISM, which is very low latency compared to piping the same traffic over the internet.

*measured in-region (i.e. London Cloud Gateway to London AWS/Azure etc).



Secure Web Gateway (Internet)

Available in:

PRISM can also perform Secure Web Gateway (SWG) functions. This allows centralised controlled access to the internet to protect your users and enterprise; such features include:
- URL filtering based on category
- DNS inspection
- IP reputation
- Forward proxy services
- Anti-Virus and Anti-Malware
- And more

HSCN Connectivity

HSCN

Available in:

For more information about connectivity to the Health and Social care Network (HSCN), please get in contact.

PSN Connectivity

PSN

Available in:

For more information about connectivity to the Public Services Network (PSN), please get in contact.

Protect

Centralised Security

How is security enforced?

PRISM operates on a centralised security model. Traffic to/from the internet, your cloud connected environments, and your connected enterprise sites is forwarded through the Secure Enforcement Core.

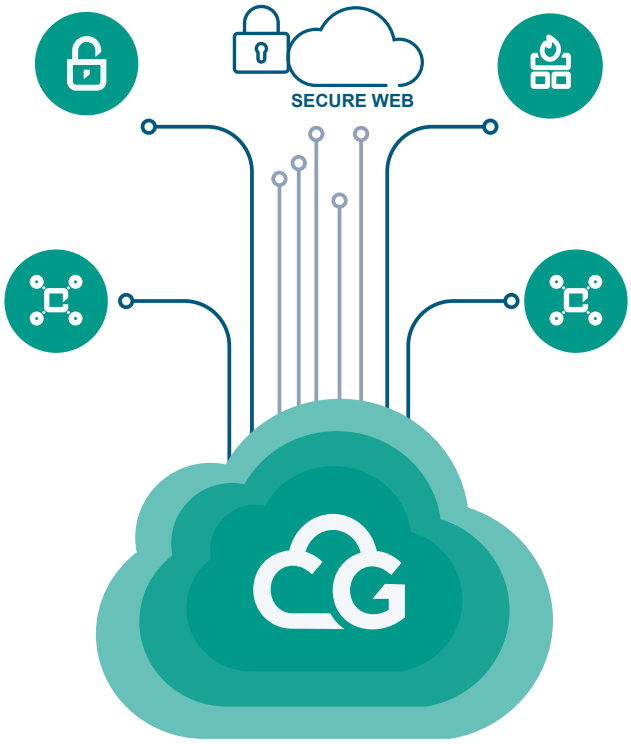
This means your security policy, posture and governance will remain in place as your corporate network changes. You can add more clouds, sites and users to the network, safe in the knowledge that PRISM will continue to apply your security policy for you.

The policy itself can be as granular or as high level as you wish, depending on how you need to manage your various traffic flows, and the sensitivity of your workloads.

Security is not just about protection, but visibility through logging and auditing.

By forwarding all traffic through our Secure Enforcement Core, we are able to feed granular detail about your network activity into our telemetry platform, integrate with your existing SOC / SIEM, and provide insight into how your network runs.

See the 'Inspect' section for more information.



Amending Security Policy

As part of your managed service, Cloud Gateway becomes the custodians of your security policy, but you have full control over the access and protection you require and desire.

We will work with you to set your initial security policy when you enter live service, through workshop sessions and conference calls, as appropriate. Amendments to security policy are done via a simple change request, submitted to our service team.

Secure Enforcement Core

Layer 3/4 Firewall

Available in: 

By default, all levels of PRISM have Layer 3/Layer 4 firewall capabilities to identify and block network traffic that does not conform to the standards you set at the basic, yet most common and efficient manner.

DNS Inspection

Available in: 

Another feature of our Secure Web Gateway is DNS Inspection, which captures the contents of DNS queries and inspects the request; the request can be permitted or denied based on IP reputation, known BotNets, known Malware sites. This service is complementary to URL filtering as this is enforceable for non-web-based applications.

URL Filtering

Available in: 

URL filtering is a component of our Secure Web Gateway module, to prevent end-users from accessing potentially harmful websites.

URL filtering at the heart of the network means our customers can enforce safe browsing practices, with all internet traffic passing through the secure enforcement core regardless of source or destination.

URL filtering can be performed using major categories (gambling, adult, IT etc) or reputation; these category databases are automatically updated every hour to ensure a robust filtering process.

Our customers can also customise their URL filtering policy as much as they like, by adding explicit sites to an allow or deny list.

Application Control

Available in: 

With Cloud Gateway's application controls, you can identify and control which applications are trusted in your IT environment; such examples are "permit Zoom via the browser" but "deny the Zoom application". You can also prevent all other unauthorised applications from running. These unauthorised applications may be from an unknown source, potentially malicious, or could simply be blocked to eliminate Shadow IT or duplication.

Proxy Services

Available in: 

Cloud Gateway's proxy services act as a gatekeeper between you and the internet. Our intermediary server separates end users from the websites they browse where an explicit proxy has to be defined (rather than native default routing to the internet). This feature is usually combined with the URL filtering and DNS inspection services.

Deep Packet Inspection

Available in: 

Cloud Gateway can use DPI (sometimes known as TLS intercept) to give control based on information within the payload that may not otherwise be seen due to encryption (i.e. HTTPS traffic flows).

This enables greater control with URL filtering, DNS inspection, Anti-Virus, Anti-Malware etc as we can create policies based on the data inside the packet, whereas previously, we would just see an encrypted packet which may or may not include harmful intent.

Anti Virus and Anti Malware

Available in: 

Cloud Gateway's Anti Virus and Anti Malware systems deal with both established, lingering viral threats, and new, dangerous exploits. Our signatures and threat intelligence is updated hourly to ensure ongoing protection and mitigate zero-day and new exploits.

This protection is not just for internet services, it can be deployed in-line for internal traffic flows in order to capture and identify threats that may exist in your enterprise.

Geo-IP blocking & IP Reputation

Available in: 

Cloud Gateway can filter and block communications from IP addresses that have a negative reputation, or originate from specific geographic locations. Proactively protecting the network, users and services from risk on a global scale.

IPS/IDS

Available in: 

Cloud Gateway can integrate IDS and IPS with our firewall to create a Unified Threat Management (UTM) system, for complete network protection from any type of threat. Proactively affect traffic in flight as it traverses your network, whilst providing granular analytics that can integrate with your SIEM.

Add-ons

Web Application Firewall (WAF)

Available as an add-on in: 

Many cloud providers offer default WAF services that may not be sufficient to protect the business, or cannot be configured to follow enterprise-specific rule sets.

Cloud Gateway provides a WAF that works at layers 4-7, and provides an enhanced set of protections that can be configured to secure web applications, whether hosted in the cloud or on-premise. Please refer to our WAF service definition for more information.

Remote Access Service (RAS)

Available as an add-on in: 

Remote Access Service is an optional add-on for your instance PRISM platform. It connects remote users to the network from any device over the internet, with the same level of security you would expect from an enterprise site. All RAS traffic is passed through our secure enforcement core.

Commercially, you pay for concurrent users connected, not the number of users that are able to use the RAS service. Please refer to our RAS service definition for more information.

Inspect

Network visibility

Customer Portal

Available in: 

The Cloud Gateway Portal shows your network overview at a glance, in a simple, intuitive display. Accessible via a web interface, it allows you to keep track of your network performance, utilisation and traffic flow overview.

The portal contains functionality to raise a support case with the Cloud Gateway service team, as well as keep track of existing cases.

SOC/SIEM Integration

Available in: 

For customers that have an existing SOC/SIEM, Cloud Gateway can export the collected telemetry data to provide a single pane of glass for better visibility across the estate.

Data can be exported real-time for upstream ingestion in a number of formats (standard or bespoke) as well as static files (i.e. on cloud object storage).

Log Storage

Available in: 

All network telemetry including logs, alerts & events, are logged then parsed with enrichment (for better search & visualisation) and available for retrieval. This assists with your governance and regulatory compliance.

Telemetry data is available for the following lengths of time:

PRISM Standard	PRISM Enhanced	PRISM Premier
14 days	30 days	60 days

All data storage lengths are subject to storage limits, see our Service Definition for more information.

Advanced Monitoring & Analytics

Available in: 

With PRISM Premier, you gain access to a sophisticated monitoring and analytics module, which allows you to drill down into more detail about your network traffic events.

Utilise multiple metrics and tools to dig into the exact reasons behind your network behaviour, enabling proactive troubleshooting, and analysing problems at packet level to truly understand how your network ticks.

This toolset is also used to highlight any anomalous behaviour and identify trends through the use of detailed visualisations, queries and data exports.

Connect with us

Drawing on 20+ years of experience in networking, one of the team will be happy to host a whiteboard session with you to:

- Address any challenges that you may have
- Understand your cloud strategy and security requirements
- Map out and make recommendations on potential architecture patterns for your organisation
- Discuss how PRISM can be deployed within your organisation

Contact us for tailored advice on the best solution for your specific requirements.

About Cloud Gateway

Cloud Gateway provides unique cloud-native innovation for fully agnostic hybrid cloud and multicloud connectivity. Securely connect your estate with multiple cloud service providers, the PSN, the HSCN and the internet.

Organisations of any size can harness the power and flexibility of hybrid cloud and multicloud but with greater control, pace and visibility. Cloud Gateway secures all your internet and network traffic, with rapid deployment and government grade security. Built-in flexibility ensures continuous change is future-proofed and reduces operating costs. By centralising connectivity, organisations have a single, timely and accurate source of truth, ensuring regulation compliance and protection from cyber threats.

Visit us at **cloudgateway.co.uk**
Twitter: **@cloudgatewayltd**
LinkedIn: **linkedin.com/company/cloudgateway**

ISO 27001 CERTIFIED
CYBER ESSENTIALS PLUS

CLOUD GATEWAY