CLOUD GATEWAY

PRISM

Secure Access Service Edge (SASE)

Improve performance, reduce cost and complexity and strengthen security

Components Overview

CONNECT, PROTECT, INSPECT.

Flexible networking and security to rapidly and securely connect you to multiple cloud service providers, the HSCN, the PSN and the internet.

PRISM - The UK's first SASE solution

Cloud Gateway's flexible, cloud-native and agnostic SASE solution, PRISM, enables organisations of any size to choose the tools they need to improve performance, reduce cost and complexity and strengthen security.

Secure all remote access, internet and network traffic, with government grade security, rapid deployment and flexibility to future-proof your network and business.

Performance. Cost saving. Ease of management. With PRISM you can gain them all without having to let go of a thing. Now that really is SASE.

- Reduce cost and complexity
- Improve network performance
- Faster time to market for a competitive edge
- Strengthen security
- Modernise legacy systems
- Start small and scale
- Government grade security
- Full visibility and control

Get Connected.

PRISM can operate on a 'Bring Your Own Network' basis - but if you want us to look after that side, that's ok too. Connect your network ecosystem using any carrier medium(s) with no new hardware required. PRISM acts as the beating heart of your network, providing the security and performance you need today for the cloud services you need tomorrow.

You can connect to PRISM via any public or private connectivity method, it is completely agnostic to suit your needs. Seamlessly and securely bring together all of your network endpoints for full visibility and control.

PRISM brings together:

The main corporate network

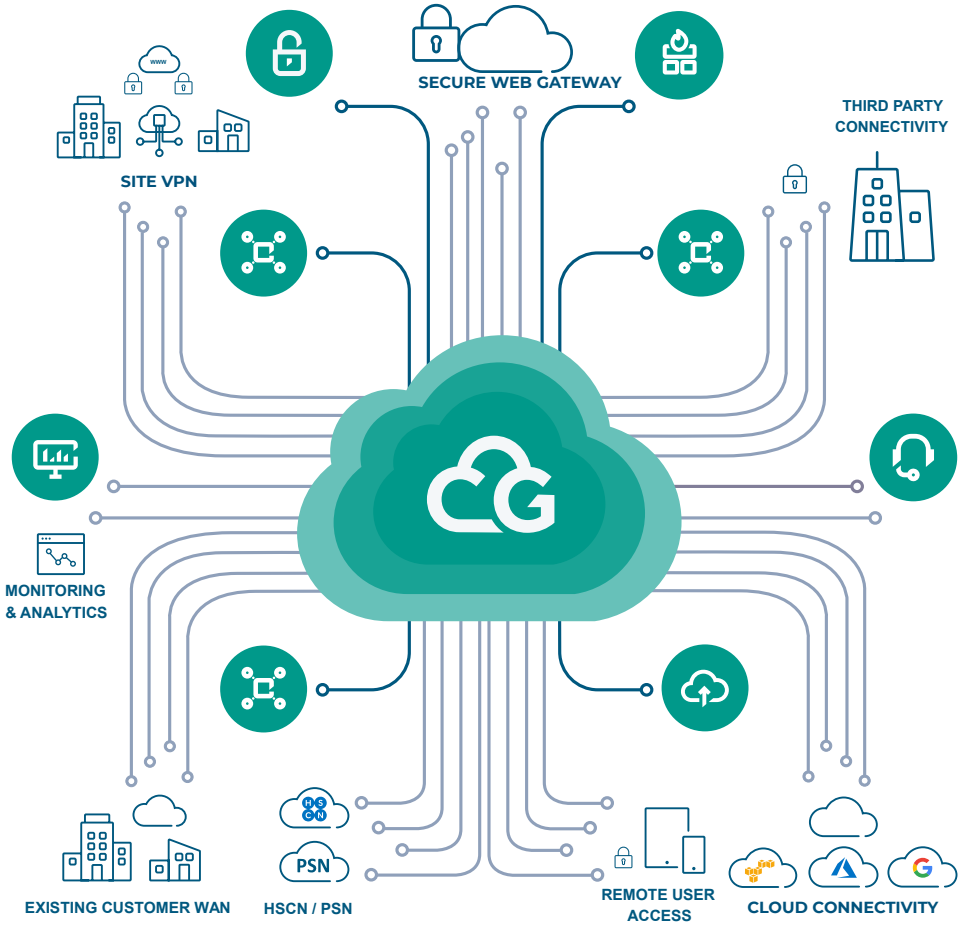
Your supply chain (including third party connections)

Cloud service providers

Remote users and home workers

The internet

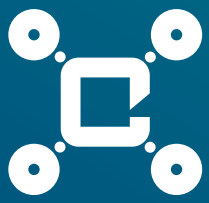
Sector-specific networks including the PSN and HSCN



Connect, Protect, Inspect.

Welcome to the three pillars of the PRISM platform: Connect, Protect, Inspect. These core pillars are essential to building a Secure Access Service Edge (SASE) solution, giving you more flexibility, visibility and control of your network.

Connect



The Connect pillar provides your organisation with a full suite of network connectivity capabilities, depending on your needs, to bring your entire ecosystem together.

Protect

The Protect pillar provides your organisation with a set of security tools, choose how you want to protect your network with granular control over policies and governance.

Inspect

The Inspect pillar gives you full visibility of your network traffic and security configurations in a single portal, allowing you to monitor the network and analyse key metrics.

Key Strengths

- End-to-end service
- Endless connectivity methods
- Born in the cloud - No harware required
- PSN and HSCN accredited
- Seamless integration: Security & connectivity
- Underpinned by broad networking expertise
- NCSC and CNSP compliant
- Security standards and accreditations
- Managed Service, 24hr support

Connect

Bandwidth

Available options

PRISM is available to purchase at the following bandwidth licence levels:

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

Do you need a single or multple links?

If purchasing a single link, with no security enabled, bandwidth is allocated to the connection purchased.

If combining a number of connectivity and/or security options, the bandwidth is allocated across the platform to all your endpoints. This means all connections have the capacity to handle the maximum bandwidth throughput of the purchased licence. The maximum throughput 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 to connect your cloud environment, data centre and 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 born in the cloud for full scalability, upgrading your bandwidth limit to the next licence level can be achieved instantly on-demand.

Simply contact the customer service team, who will work with you to uplift your bandwidth licence in accordance with your needs.

Enterprise Connect

VPN Site Connectivity

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)

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

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).

Private MPLS

PRISM can also become your MPLS or VPLS provider if required. We work with a number of selected connectivity providers to offer replacement WAN solutions as part of our platform offering. This involves delivery of physical circuits to the customer site and installation/configuration of a network device, and Customer Premises Equipment (CPE).

Remote Access

Remote Access 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 remote access traffic is encrypted and kept secure when in transit over the internet.

Commercially, you pay for concurrent users connected, not the number of users that are able to use the service.

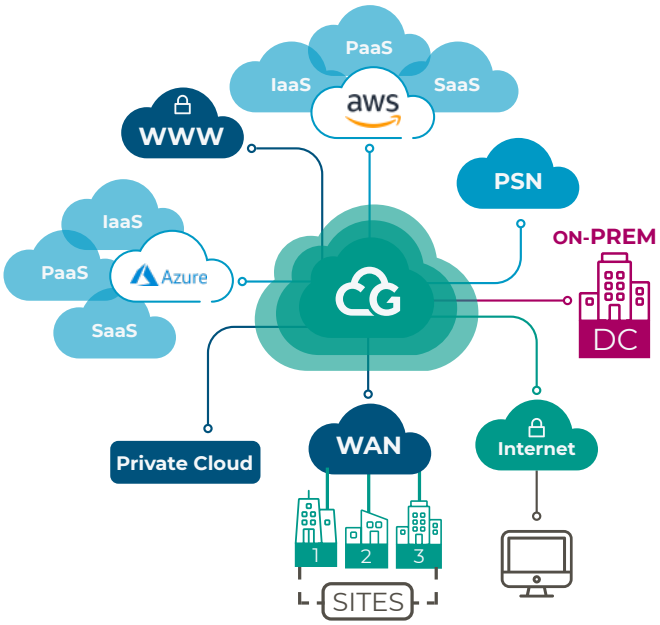
Cloud Connect

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).



Internet Connectivity

PRISM also connects to the internet so that it can perform Secure Web Gateway (SWG) and WAF functions. With PRISM, estate-wide access to the internet can be controlled to protect your users and enterprise.

Please see the 'Protect' section of this brochure for more information on the security features available as part of the PRISM platform.

HSCN

HSCN Connectivity

Connectivity to the HSCN can be added, with bandwidth allocated in isolation in bandwidths as low as 10Mbps. For more information about connectivity to the Health and Social care Network (HSCN), please get in contact.

PSN

PSN Connectivity

Connectivity to the PSN can be added, with bandwidth allocated in isolation in bandwidths as low as 10Mbps. For more information about connectivity to the Public Services Network (PSN), please get in contact.

Protect

Security Enforcement

How is security enforced?

Depending on your needs, traffic to/from the internet, your cloud connected environments, or your connected enterprise sites is forwarded through a Secure Enforcement Core.

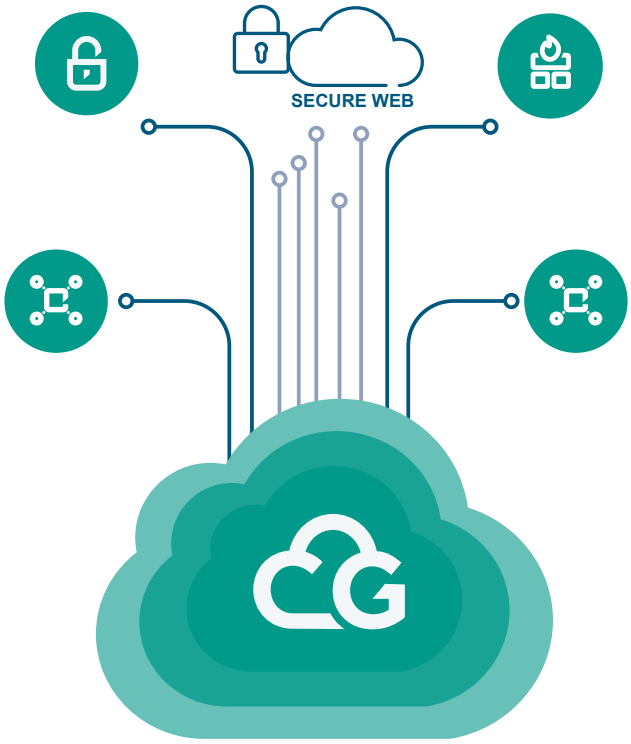
This means your security policy, posture and governance will remain in place as your corporate network changes. You can add more clouds, sites and users to the network, safe in the knowledge that PRISM will continue to apply your security policy for you.

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 SIEM / SOC, 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.

Security Options

Security components are not mandatory with PRISM if a pure connectivity solution is required. If security functions are needed however, you have the choice of either Foundation Security, or our full Firewall-as-a-Service (FWaaS) suite

The team at Cloud Gateway can make appropriate recommendations as to the most appropriate tools for your organisation, in order to protect your network and data from cyber threats.

Foundation Security

Layer 3/4 Firewall

Layer 3/Layer 4 firewall capabilities identify and block network traffic that does not conform to the standards you set.

Firewall-as-a-Service (FWaaS)

The Firewall-as-a-Service (FWaaS) module contains all the functions of Foundation Security, plus additional security functions that protect your network even further.

Anti Virus and Anti Malware

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.

Deep Packet Inspection

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. By default, DPI is enabled when utilising the advanced SEC.

IPS/IDS

Cloud Gateway integrates IPS/IDS into our advanced firewall for complete network protection from a host of threats. Proactively affect traffic in flight as it traverses your network, whilst providing granular analytics that can export to your SIEM / SOC if required.

Geo-IP blocking & IP Reputation

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.

Secure Web Gateway

The Secure Web Gateway (SWG) module contains a set of protections against internet-borne threats. SWG may be taken alongside the Foundation Security or FWaaS modules, with WAF, or on its own. DPI is enabled by default on our SWG function.

URL Filtering

URL filtering prevents 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

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.

DNS Inspection

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.

Proxy Services

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.

Web Application Firewall (WAF)

The WAF component may also be taken alongside the Foundation Security or FWaaS modules, with SWG, or on it's own.

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.

Inspect

Network visibility

Customer Portal

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.

SIEM / SOC Integration

Customers can receive logs from their protect components to their chosen SIEM / SOC solution for further analysis. By using logs exported from Cloud Gateway's platform, the customer can combine network ecosystem events with other data they may be analysing using as part of their security operations.

A real time stream of policy-controlled events is provided from our Log Aggregation Platform (LAP) to an HTTPS endpoint provided by the customer.

Log Storage

All network telemetry including logs, alerts & events, are logged then parsed with enrichment (for better search and visualisation) and available for **30 days** for retrieval. This assists with your governance and regulatory compliance.

Telemetry data may be stored for longer periods on request, please contact us for more information.

All data storage lengths are subject to storage limits.

Advanced Monitoring & Analytics

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 flexible, networking and security solutions to rapidly connect organisations to multiple cloud service providers, the HSCN, the PSN and the internet - delivered as a service at a pace suitable to the business.

Using Cloud Gateway's cloud-native Secure Access Service Edge (SASE) framework solutions, organisations of any size can choose the tools needed to improve performance, reduce cost and complexity and strengthen security. Cloud Gateway secures all remote, internet and network traffic, with rapid deployment and government grade security. Built-in flexibility ensures continuous change is future-proofed. Organisations have a single, timely and accurate source of truth, ensuring regulatory 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