CLOUD GATEWAY

OBSERVE

SIEM / SOC INTEGRATION

SERVICE DEFINITION

V2.0
Issue Date: 14/10/2025
Commercial in Confidence

About this document

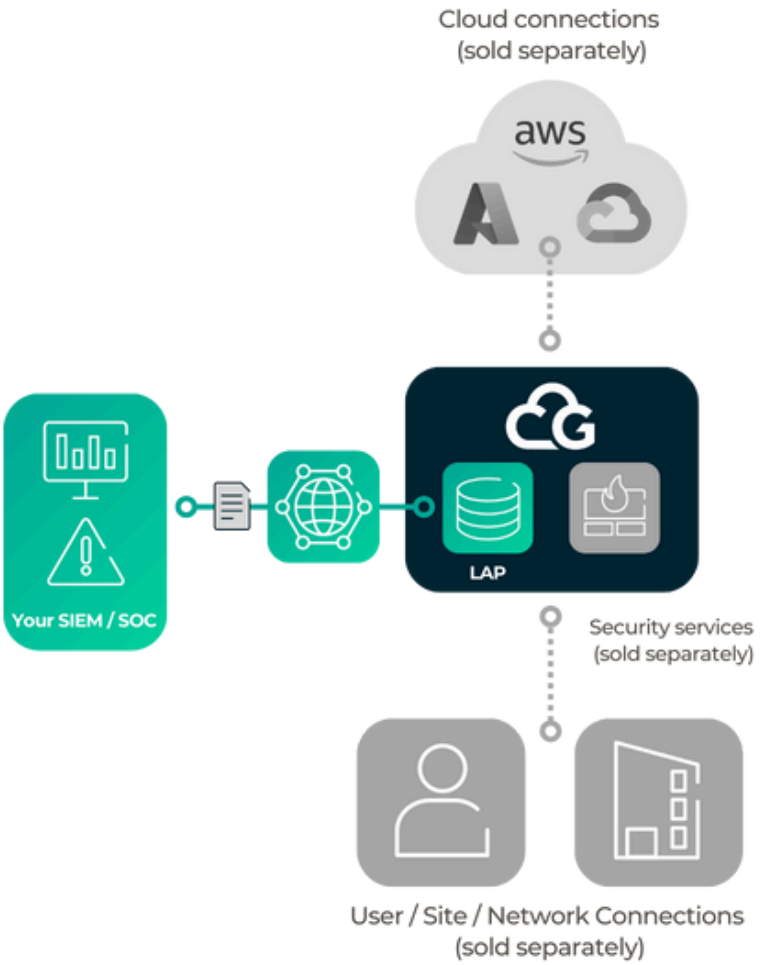
This document is designed to provide a straightforward, clear description of our **SIEM/SOC Integration** service. It covers basic operation, support, what's included and excluded. It defines your responsibilities, and our responsibilities when deploying and running the service.

What is SIEM / SOC Integration?

SIEM/SOC Integration is a component service available as part of the Cloud Gateway platform. SIEM/SOC Integration enables you to receive logs from our security components, to your chosen SIEM solution for further analysis.

Connectivity and security services that generate these logs are subject to commercial agreement and should be purchased separately to SIEM/SOC Integration.

By using logs exported from our platform, you can combine network ecosystem events with other data as part of your security operations.



Basic operation

Our data centre presence

SIEM/SOC Integration automatically pushes data from a Log Aggregation Platform (LAP) to your chosen SOC/SIEM application endpoint. You will provide us with:

- Host name
- Port number
- Server certificate
- Username and Password

A stream of policy-controlled events is provided from the Secure Enforcement Core (SEC) in SYSLOG or CEF format, to an HTTPS or TLS endpoint provided by you. If you're not sure what kind of endpoint you have, we can help you identify the requirement.

Logs are batched and pushed to your SIEM/SOC endpoint in intervals every 5 minutes.

Types of Event Logs

Events Exported

Any policy related events related to Firewall-as-a-Service (FWaaS), Foundation Security, Secure Web Gateway (SWG) and Web Application Firewall (WAF) components.

All activity related to Remote Access session activity (start, end).

Events Not Exported

Any traffic / logs that do not pertain to your usage (e.g. Cloud Gateway administrative traffic)

Event Example

Below is an example of a log record that may be exported to your SIEM/SOC endpoint - for illustrative purposes.


```
{
  "@timestamp": "2021-01-19T13:28:10.319Z",
  "dstip": "17.178.104.182",
  "eventtime": "1611062890300851067",
  "dstintfrole": "undefined",
  "srcintfrole": "undefined",
  "appcat": "VoIP",
  "<190>date": "2021-01-19",
  "eventtype": "signature",
  "incidentserialno": "198182092",
  "appid": "24426",
  "apprisk": "elevated",
  "logid": "1059028704",
  "time": "13:28:10",
  "srcintf": "port1",
  "action": "pass",
  "msg": "VoIP: FaceTime,",
  "host": "195.206.176.16",
  "tz": "+0000",
  "srcip": "172.27.101.164",
  "dstintf": "port1",
  "service": "udp/16385",
  "applist": "default",
  "policyid": "4",
  "sessionid": "20295",
  "srcport": "16403",
  "@version": "1",
  "app": "FaceTime",
  "level": "information",
  "proto": "17",
  "dstport": "16385",
  "direction": "outgoing",
  "tags": [
    "6p6-customer-siem",
    "filtered"
  ]
}
```


Format and File Types

SIEM/SOC Integration will export using the native format of our Network Virtual Appliances (NVAs). These will be sent in CEF or SYSLOG format. Other formats and log parsing may also be supported, on request.

Acceptance testing

Acceptance criteria

The acceptance criteria for SIEM/SOC Integration, as part of the platform onboarding are:

- You provide us with an HTTPS or TLS endpoint, and a valid certificate for authentication
- We provide you with set of Cloud Gateway IP addresses to permit traffic at the ingestion end
- Connection is established between the Cloud Gateway LAP and the log receiving endpoint
- You check and confirm that logs are being received

Exclusions

The service does not include:

- SIEM/SOC capabilities of any kind. This service pushes logs to your SIEM/SOC solution
- Custom security policy from which logs are generated. Custom security policies may be implemented via Foundation Security, Firewall-as-a-Service (FWaaS), Web Application Firewall (WAF) and SWG (Secure Web Gateway). These services are available as separate components of the platform
- Interpretation or enrichment of data
- Re-sending of logs after the export feed has already pushed them to the SIEM application
- Recovery of missing log data as a result of a service interruption
- Internet connectivity services between Cloud Gateway's endpoint and yours
- Administration and support of your SOC/SIEM toolset and its required internet connectivity to facilitate log ingestion

Customer responsibilities

You are responsible for:

- Security and safety of data once received and held in your SIEM/SOC solution
- All IT equipment and environments including and beyond the HTTPS / TLS endpoint to which export data is sent
- Provision of your own internet connectivity (unless otherwise agreed)
- Resiliency of the HTTPS / TLS endpoint receiving logs
- Validity of the signed certificate used to establish the connection
- Using encryption a minimum of TLS 1.2 encryption
- Providing an authentication mechanism using either (or both) certificates and username password combination

- Addition of Cloud Gateway's IP addresses to any allow list protecting your endpoint
- Backups. You are responsible for backing up your own systems. We don't hold customer data. We will back up our own platform, and will store logs as detailed in the Log Storage section below

Cloud Gateway responsibilities

We are responsible for:

- Design, installation and configuration of SIEM/SOC Integration service
- Retrieval of log data that has been lost as a result of a Cloud Gateway connectivity failure between our Log Aggregation Platform (LAP) and your endpoint

Ordering and lead time

Ordering and volume

We calculate your platform cost on a bandwidth basis. SIEM/SOC Integration is sold as a component of our platform, the cost will usually be combined with other components and quoted as a total service cost in the proposal.

Lead time

Our Service Level Agreement (SLA) to deliver SIEM/SOC Integration is 5 working days. The lead time is measured from receipt of a valid Purchase Order (PO) and contract acceptance, to live service ready for any acceptance testing. The SLA timer will be paused when there is a dependency on you to provide information or input.

Service management

Service support

We have an experienced Service Desk team who are responsible for the day-to-day operational service between you and us.

The Service Desk team's primary responsibility is to provide a single point of contact within Cloud Gateway – to which issues surrounding satisfaction of service may be escalated and resolved.

Support escalations

We strive to ensure that all incidents, service requests, or simple advice and guidance requests from our customers are fulfilled efficiently and effectively within our published timescales.

If you feel that a request is not being managed effectively or would like to escalate a particular issue, this can be raised with our Service Management team.

Complaints

We take complaints seriously and ask that any customer wishing to raise a formal complaint does so in writing to service@cloudgateway.co.uk. Full details of our complaints procedure can be found within the Cloud Gateway Customer Service Pack, which you will receive during the onboarding process.

Reporting

Various types of reports can be provided. You can request these by contacting service@cloudgateway.co.uk, or raising a ticket via the Cloud Gateway Portal. Charges may apply.

Service levels

The service levels that apply to this service are available in our Service level Agreement (SLA).

Data processing

The data processing terms that apply to this service are available in the Cloud Gateway MSA, found here: https://www.cloudgateway.co.uk/compliance/msa/.

Security arrangements

- The core platform infrastructure that supports this component service is hosted in geographically diverse UK data centres. All data remains within UK sovereignty (with exception if endpoints connect to our platform via the internet)
- We are ISO27001 and ISO9001 accredited. We are also compliant with Cyber Essentials Plus

Log storage

- All traffic logs and policy controlled events are stored in our Log Aggregation Platform (LAP)

- Logs are retained for 62 days as standard, and are used to populate graphs and visualisations in the Cloud Gateway Portal

Business continuity and disaster recovery

Cloud Gateway maintains a comprehensive approach to operational resilience, ensuring continuity of service through robust business continuity and disaster recovery planning. Our internal continuity and disaster recovery plans are reviewed and tested regularly, and staff receive training to ensure they can respond effectively to a disruption.

Our infrastructure is designed for high availability across data centres. Network component configurations are backed up regularly and can be used to recover from disruptive scenarios. Supplier relationships are governed by rigorous due diligence, including reviews of the supplier's own continuity and recovery practices. Data centres and hosting providers, where under our selection, are selected based on secure practices and continuity capabilities. Certifications held by the supplier are reviewed, such as ISO 22301, ISO 27001, ISO 9001 and ISO 14001.

Our operational model supports full remote working, whereby all staff are equipped to operate securely from the office, home or other locations.

CLOUD GATEWAY

cloudgateway.co.uk

+44 (0)20 3870 2444

sales@cloudgateway.co.uk

Cloud Gateway
The Ministry, Borough
79 Borough Rd, London SE1 1DN