

Service Description

G-Cloud 15

Lot 2a

Colt IP Guardian

Abstract

This document is intended to describe the IP Guardian DDoS Service for prospective and current customers of the product.

Document Version	v1
Release Date	30/01/2026
Author	Colt Technology Services
Owner	Colt Technology Services

Copyright ©
No part of this document may be reproduced or adapted in any form, including photocopying or storing it by electronic means, except as is necessary for the purpose of the recipient's dealings with Colt, without the written permission of Colt. Any copies made of any part of this document shall include the notice: © 2025 Colt Technology Services. The Colt name and logos are trademarks. All rights reserved.
No information contained in this document shall be disclosed to any third party without the written permission of Colt.

Contents

Overview3

Technology platform and network access3

Colt IP Guardian Standard3

Features and Options4

Customer Roles and Responsibilities4

Disclaimer5

Service Limitations5

Definitions5

Overview

Colt IP Guardian Standard ("Service")

The Service requires customers to purchase "Underlying Services" such as IP Access, Dedicated Internet Access, or IPVPN from Colt.

Technology platform and network access

Colt IP Guardian is a network-based distributed Denial of Service ("DDoS") Mitigation Platform which uses technology platforms, software, and equipment in conjunction with the "Underlying Services" to provide customers with detection and Mitigation against DDoS attacks.

Network access supplied in relation to an Underlying Service is used for provision of the IP Guardian Service and may affect the SLA accordingly. Please refer to the respective Service Description and SLAs for details of Underlying Services.

Colt IP Guardian Standard

Colt IP Guardian Standard provides continuous monitoring and automatic Mitigation against attack. It is Customer self-service with no incident response offered. The customer is responsible for the selection of the tuning of the service countermeasures and ensuring Mitigation is initiated in the event of an attack. Colt will advise on the configurations to optimise the functions of the protection.

The service is configured for automatic Mitigation where traffic is automatically redirected to the traffic cleaning systems. When an anomaly is detected, Colt provides portal access which gives the Customer the ability to manually activate and deactivate Mitigation is required. The Customer may only start a mitigation when the Customer genuinely believes an attack is taking place and must cease mitigation once the Customer believes the attack has ceased. Mitigation must not be left activated on a permanent basis. If a Customer fails to switch the service on and off as required, Colt shall have the right, in its discretion, either to cancel the Service or amend the charges. Customer shall activate and deactivate Mitigation and track the progress of an existing Mitigation using the Colt DDoS Portal.

Initiation of Mitigation

Diversion of Attack-Traffic to a Colt DDoS Scrubbing Centre

Once Mitigation is activated, Colt will divert traffic to a DDoS scrubbing centre. Colt reserves the right to route traffic to DDoS scrubbing centres in a different region and/or country in its reasonable discretion. Customer expressly acknowledges and consents to (i) such transfer of traffic across country borders and/or (ii) Colt, its affiliates and authorised third parties accessing Customer's traffic information (e.g. port, flow, protocols, IP address) as needed for Colt to provide the Service hereunder. Customer further acknowledges and accepts that, notwithstanding anything to the contrary, it is the Customer and not Colt who is responsible for security/protection of all network traffic, including forwarded traffic and the level of security/protection of the traffic and traffic design.

Forwarding of Scrubbed Traffic

Once the Customer's traffic has been scrubbed of any detected malicious packets, Colt will forward the traffic back to its original destination.

Discontinuance of Mitigation

Where mitigation was activated automatically, it will cease automatically when the system determines that the DDoS attack has subsided. If mitigation was activated manually by the customer, they are responsible for deactivating immediately after the attack has ceased. Colt shall have the right to discontinue any Mitigation if it determines there is no active attack in progress.

System Administration

Colt will work with the Customer to resolve chronic false positives and other nuisance alerts; however, if alerting issues are not resolved satisfactorily, Colt may modify the DDoS Mitigation system configuration to reduce repetitive alarms caused by Customer system changes.

Installation of DDoS Mitigation

Colt IP Guardian includes and protects Customer IP addresses in a combination of IPv4 or IPv6 addresses and address blocks. The Customer must provide and maintain a list of IP addresses to be protected by the Service. Where Customer is using multiple managed objects/ security rule sets (a maximum of two are provided), the address space defined in each managed object must not overlap.

The Customer will provide parameters that allow Colt to determine the correct traffic alert threshold (where appropriate) and countermeasure levels to be used to detect and respond to a DDoS attack. Colt may periodically require Customer to allow traffic monitoring to update threshold levels.

Features and Options

IP Guardian Services on AS 8220

The AS 8220 network supports the Colt IP Guardian Standard Service options.

The Colt DDoS Mitigation Platform will monitor traffic being sent to the Customer's protected Internet Prefixes for signs of volumetric DDoS attacks. Where traffic volumes exceed the pre-agreed thresholds, the Service will automatically divert traffic destined to the host under attack into cleaning. This would normally result in the diversion of a single IP address into cleaning but in some scenarios, multiple IP addresses could be diverted. Mitigation can also be set so that an alert that recommends the pre-defined Mitigation is activated but waits until the Customer confirms this via the portal or by contacting the Colt support teams.

The service includes Traffic Monitoring for the identification of malicious traffic at the borders of the AS 8220 network. Clean traffic is delivered to the associated Colt service delivering traffic for IP addresses that are advertised from AS 8220 (both Provider Aggregated and Provider Independent (PA and PI). The Clean Return in this case equals the bandwidth of the associated Colt circuit.

Customer Roles and Responsibilities

The Customer must provide and maintain English-speaking security administrator contacts with valid contact information that are reachable 24/7 for any IP Guardian Incident notifications. Such administrators must be authorised to act on behalf of the Customer with regards to the operation of the Service and be able to provide Colt with any changes to the security administrator contacts.

The Customer must provide Colt with the following notifications:

- Reasonable notice of any sudden events that may cause significant traffic pattern changes in Customer's network
- Reasonable notice of any potential promotional events or other activities that may increase Customer's network or website traffic
- 24 hours advance notice via a change ticket of any additions or deletions to the list of Customer Protected IP addresses that are subject to the Service
- 24 hours advance notice via change ticket of any Customer requests to change the traffic baseline.
- At least five business days advance notice via a change ticket of any network topology or system changes that may affect the Service or the effectiveness of the Colt IP Guardian Service.

Failure to provide up to date contact information may result in the inability to monitor traffic, notify the customer of alerts or activate Mitigation.

Customer shall not:

- attempt, permit or instruct any party to take any action that would reduce the effectiveness of Service used to deliver Colt services. Without limiting the foregoing, Customer is specifically prohibited from conducting

unannounced or unscheduled test DDoS attacks, penetration testing, or external network scans on Colt's network without the prior written consent of Colt.

- attempt or allow Customer's representatives to attempt in any way to circumvent or otherwise interfere with any security precautions or measures of Colt relating to the Service or any other Colt equipment.
- misuse third-party software provided by Colt in connection with the Service (if any), including any corresponding documentation, and Customer shall use any such third-party software strictly in accordance with all applicable licensing terms and conditions. Colt makes no representations or warranties whatsoever with regard to such third-party software.

Disclaimer

Customer acknowledges that Colt IP Guardian endeavours to Mitigate security Incidents, but such may not be mitigated entirely or rendered harmless. Customer further acknowledges that it should consider Colt IP Guardian as just one tool to be used as part of an overall security strategy and is not a guarantee of security. Colt IP Guardian is a supplement to Customer's existing security and compliance frameworks, network security policies and security response procedures, for which Colt is not responsible. While Colt will use reasonable commercial efforts to provide the Services hereunder in accordance with the SLA, Colt does not warrant, that all security threats and vulnerabilities will be detected or that the performance of the Services will render Customer's systems invulnerable to security breaches or that Colt's recommendations, assessments, tests, reports or monitoring will be accurate, complete, error-free, or effective in achieving customer's security and/or compliance related objectives.

Service Limitations

If the size of a DDoS attack is such that the integrity of the Colt network is threatened and other Colt customers could be affected, Colt will retain the right to "black hole" the Customer's traffic, i.e. discard all traffic destined for Customer's IP address under attack in order to maintain the integrity of the Colt network.

For Customers who are using AS 8220 and connected to other providers in addition to Colt (multi-homed Customer); if traffic on another provider's network, due to an attack on the Customer, is redirected to the Colt network, Colt is entitled to drop all the BGP sessions to the Customer in order to protect Colt network.

Definitions

"AS" or "Autonomous System" means a group of connected networks that are managed as a single entity. Colt IP Guardian will use AS 8220.

"Incident" means any single or collection of security occurrences detected and reported by the Service, and which have been determined by a Colt analyst reviewing the data to potentially be of security consequence. Incidents may include security occurrences that are currently being investigated and actual attacks that may be in progress.

"Mitigation" means rerouting of traffic through Colt IP Guardian and initiating countermeasures with the intent to remove DDoS attack traffic identified by Colt-supplied equipment located in Colt's network.

"Traffic Monitoring" for the IP Guardian service means Flow Based Monitoring or FBM. This is a network monitoring technique that focuses on analysing the flow of data packets across a network rather than inspecting each individual packet. It provides a high-level view of network traffic patterns and allows the service to identify potential DDoS attacks.

End of Document