



# **DDoS** Mitigation

Das Leistungsspektrum zur  
Sicherung Ihrer Konnektivität  
und Internetdienste

[www.post.lu](http://www.post.lu)



# Vorbeugen ist besser als heilen

Das Risiko, mit volumen- und applikationsbasierten DDoS-Attacken konfrontiert zu werden, ist hoch und allein die Angriffsversuche können sehr zahlreich sein.

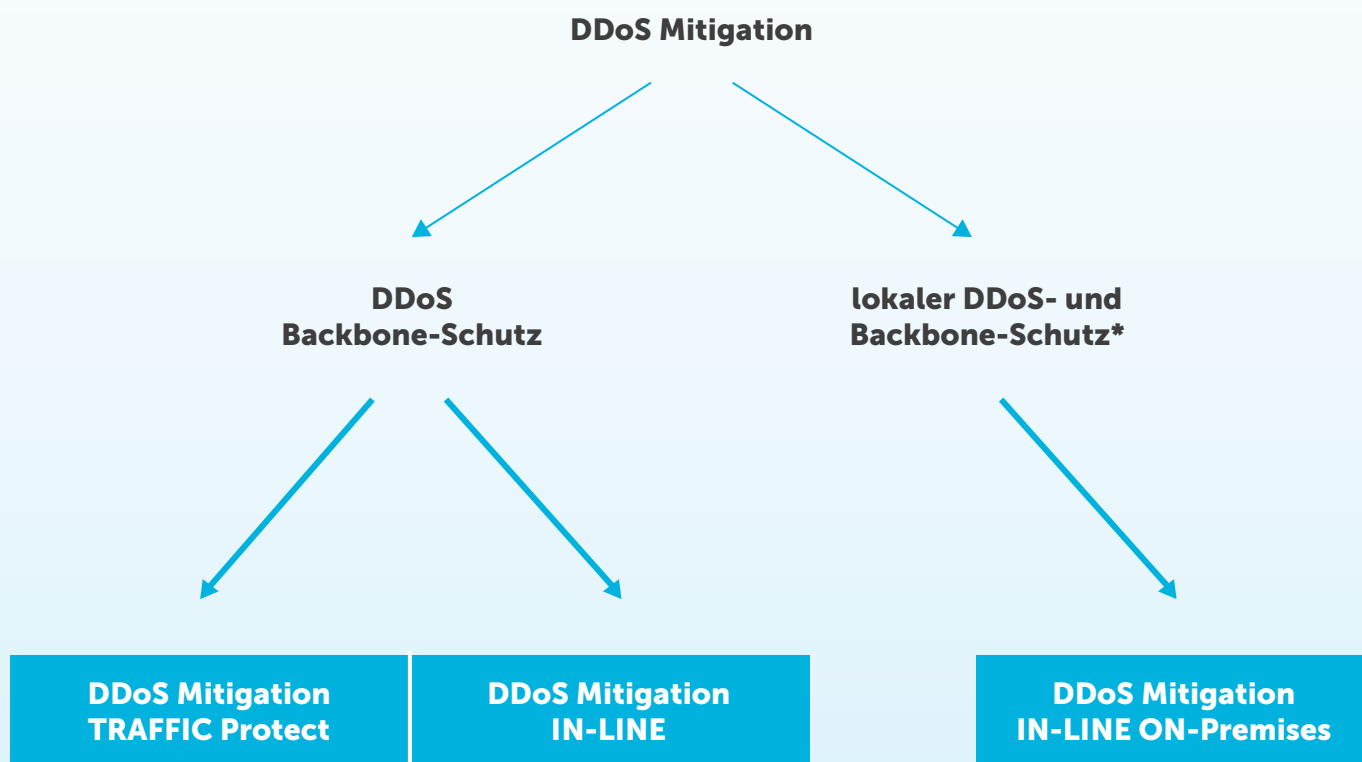
Diese Angriffe zielen darauf ab, einen Server, einen Dienst oder eine IT-Infrastruktur unzugänglich zu machen, indem die Bandbreite des Servers überlastet wird oder seine Ressourcen bis zur Erschöpfung in Anspruch genommen werden, was zur Folge hat, dass Ihre Kunden und Benutzer nicht mehr auf ihre Internetdienste zugreifen können.

In Zeiten, in denen Unternehmen im Rahmen ihrer geschäftlichen Tätigkeit auf ihre Netzwerke angewiesen sind, stellen diese Angriffe eine Bedrohung dar, die man, angesichts der möglichen Auswirkungen, ernst nehmen muss, zumal kein Tätigkeitsbereich mehr verschont bleibt.

Ein DDoS Mitigations-Dienst ist der einzige Sicherheitsdienst, der Sie vor DDoS-Angriffen schützen kann. Als wesentlicher Bestandteil Ihrer IT-Sicherheitspolitik wird er Ihre traditionellen Sicherheitssysteme wie Firewalls, Load Balancer, DNS ergänzen und schützen, da all diese Systeme keinen ausreichenden Schutz gegen DDoS-Attacken bieten.

## Unser DDoS Mitigations-Leistungspaket

Unser Leistungspaket erfüllt die unterschiedlichen Schutzbedürfnisse unserer Kunden bezüglich ihrer Internetdienste. Es schützt Ihre Internet-Infrastruktur und -Dienste vor volumen- und applikationsbasierten Angriffen anhand der Mitigation Ihres Datentraffics, indem es feindlichen Datenverkehr abwehrt und Ihren gutartigen Datenverkehr anhand unserer DDoS-Systeme filtert.



Diese Dienste sind für die professionellen Internet-Produkte DIA und IP-Transit sowie die privaten Cloud-Dienste von POST Telecom verfügbar.

\*/ Verfügbar mit den DDoS Mitigation IN-LINE-Ausrüstungen von POST Telecom.

# DDoS Mitigation TRAFFIC Protect

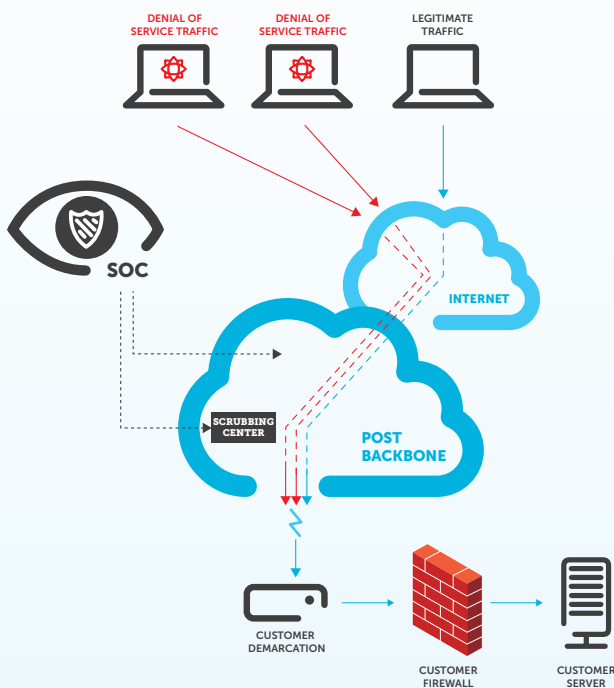
Der DDoS Mitigation TRAFFIC Protect-Dienst bietet gezielten Schutz gegen folgende Arten von DDoS-Massenangriffen:

- Bandwith Exhaustion: Überlastung Ihrer Internet-Konnektivität
- State-Exhaustion: Überlastung der Bestandteile Ihrer internetbezogenen IT-Infrastruktur wie Load-Balancers, Firewalls...

Betrieben wird dieser Dienst rund um die Uhr von unserem SOC (Security Operations Center), das spezifisch für die Sicherheit unserer Netzwerke und unserer DDoS Mitigations-Dienste zuständig ist. Das Mitigations-Verfahren wird reaktiv ausgelöst, sobald das SOC Angriffe feststellt.

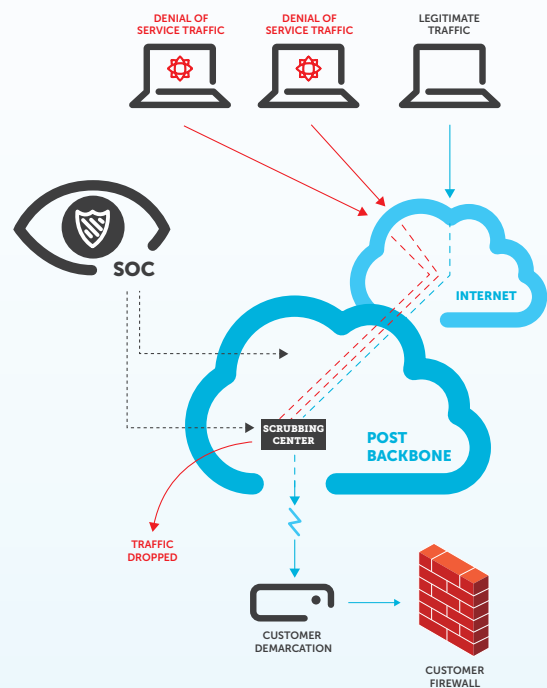
## Funktionsweise:

Ihr Netzwerk ist einem DDoS-Angriff ausgesetzt



Erkennung des Angriffs anhand der DDoS-Lösung und dem SOC von POST Telecom

Mitigation TRAFFIC Protect von POST



Routing des Datenverkehrs, Abwehr des feindlichen Verkehrs

**1. Echtzeit-Analyse** der für Sie bestimmten Internet-Pakete

**2. Überwachung und Erkennung** von anormalem Verkehr 24/7

**3. Proaktive Auslösung** der Mitigation 24/7 durch unser SOC, gemäß den auf der Grundlage Ihrer Bedürfnisse und Erwartungen festgelegten Regeln

**4. Mitigation des DDoS-Angriffs:** der Datenverkehr wird auf das zentrale Scrubbing Center umgeleitet, hier werden manipulierte Datenpakete abgeblockt und bedenkenlose Datenpakete an Ihre Dienste übertragen

**5. Information des Kunden über den Angriff** und Koordinierung, um die Mitigation zu optimieren

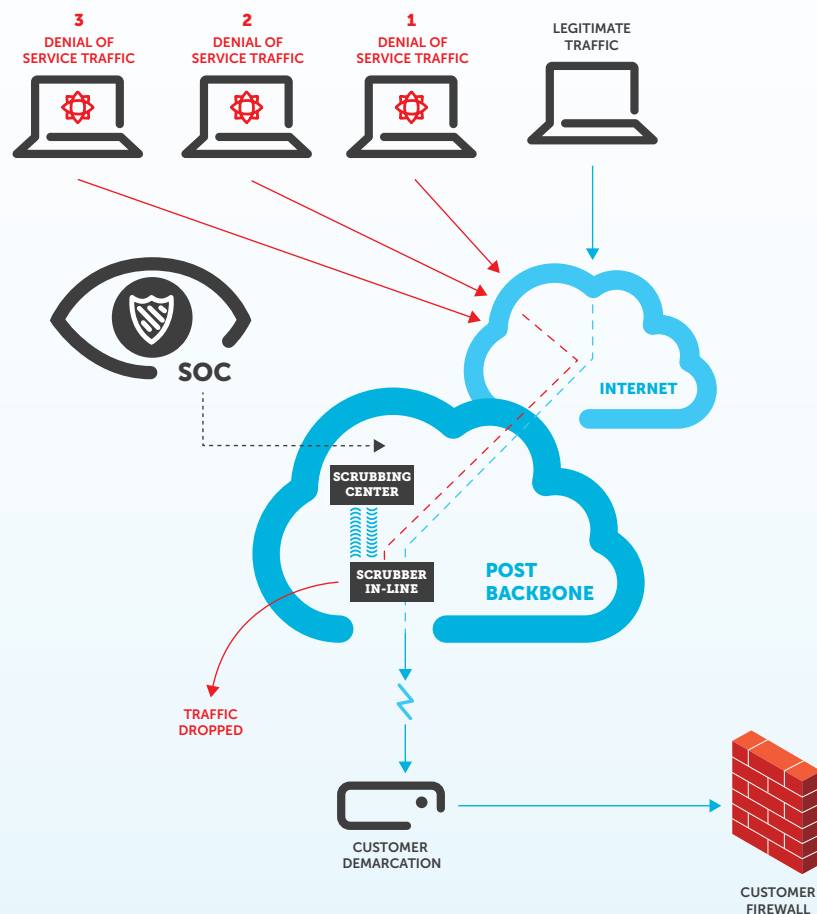
# DDoS Mitigation IN-LINE

Der DDoS Mitigation IN-LINE-Dienst deckt den Bedarf an kontinuierlichem und Echtzeit-Schutz vor applikationsbasierten Angriffen, zusätzlich zu den volumenbasierten Angriffen, ab. Er bietet somit umfassenden Schutz gegen komplexe und multivektorielle DDoS-Angriffe.

## Funktionsweise:

Sobald der DDoS IN-LINE-Dienst aktiviert ist, wird der Internetverkehr des Kunden laufend über das IN-LINE Scrubbing Center geleitet. Die Schutzmaßnahmen sind aktiv und werden in Echtzeit durch das IN-LINE Scrubbing Center auf den Internetverkehr angewendet. Ein IN-LINE-Dienst ist ein ALWAYS ON-Dienst.

## Ihr Netzwerk ist einem DDoS-Angriff ausgesetzt Kontinuierliche Mitigation



- 1. Echtzeit-Analyse aller** IP-Pakete Ihres Internetverkehrs, die in den DDoS-Dienst-Perimeter gelangen
- Sekundenschnelle **Erkennung** von anormalem Datenverkehr und DDoS-Angriffen
- 3. Automatische Mitigation in Echtzeit** Ihres Internetverkehrs
- 4. Information des Kunden über den Angriff** und Koordinierung, um das Mitigations-Verfahren zu optimieren

# DDoS Mitigation IN-LINE ON-Premises

Dieser Dienst erfüllt spezifische und komplexe Anforderungen an den lokalen DDoS-Schutz gegen applikationsbasierte Angriffe, die auch den ausgehenden Datenverkehr abdecken. (z.B. Überlastung der IT-Infrastruktur des Kunden durch Datendownload).

POST Telecom kann in den DDoS Mitigation IN-LINE ON-Premises-Dienst die Option DDoS Backbone Protection gegen volumenbasierte Angriffe, die die Kapazität des Internetzugangs überschreiten, integrieren, um den Zugang zu den Internetdiensten des Kunden zu gewährleisten.

Für eine Analyse Ihrer spezifischen Bedürfnisse kontaktieren Sie uns bitte per E-Mail unter:  
[corporate.telecom@post.lu](mailto:corporate.telecom@post.lu)

## Übersicht

	DDoS Mitigation TRAFFIC Protect	DDoS Mitigation IN-LINE	DDoS Mitigation IN-LINE ON-Premises	
Ziel des Schutzes	Schutz des Internetzugangs und der IT-Infrastruktur des Kunden	Schutz des Internetzugangs, der IT-Infrastruktur und der Internet-Dienste des Kunden	Spezieller lokaler DDoS-Schutz, begrenzt auf die Kapazität des Internetgangs Option: DDoS Backbone-Schutz	
DDoS Angriffsarten	volumenbasiert	volumen- und applikationsbasiert	volumen- und applikationsbasiert	
<b>Schutz</b>	<b>Application Layer</b>			
	Ausgehender Verkehr		✓	
	Eingehender Verkehr	✓	✓	✓
	<b>Network Layer</b>			
	State Exhaustion	✓	✓	✓
Bandwidth Exhaustion	✓	✓	✓	
<b>24/7 Traffic monitoring</b>	Inbegriffen	Inbegriffen	Inbegriffen	
<b>Mitigation</b>	Proaktiv anhand Erkennung von Angriffen durch das SOC	Permanent, in Echtzeit	Permanent, in Echtzeit	
<b>Anwendung des Schutzes</b>	Manuell	✓		
	Automatisch		✓	✓
Voraussetzungen	Keine Ausrüstung erforderlich		DDoS IN-LINE-Ausrüstung	

# Die Vorteile des DDoS Mitigation Leistungspakets

- **Ihre Internet-Zugänge sind rund um die Uhr gesichert** und sogar während eines Angriffs verfügbar: profitieren Sie von unseren Sicherheitsexperten, um Ihr Netz zu schützen und ermöglichen Sie damit Ihrem IT-Team, sich auf ihre wesentlichen Aufgaben zu konzentrieren
- **Garantierte Kontinuität Ihrer Internetdienste** für Ihre rechtmäßigen Kunden und Benutzer: Angriffe werden erkannt und gefiltert, bevor sie Ihre Infrastruktur erreichen
- **Ein einziger Ansprechpartner** für die Verwaltung Ihres Internetzugangs und der DDoS-Sicherheit
- **Kostengünstige Absicherung** gegen die Gefahr von DDoS-Angriffen
- **Finanz- und Reputationsschutz:** schützt vor finanziellen Auswirkungen durch Unterbrechung Ihrer Internetdienste oder Verlust des Kundenvertrauens
- **Flexibilität** bei der Konfiguration Ihres DDoS-Schutzes entsprechend dem Umfang Ihrer zu schützenden Internetdienste
- **Kontrolliertes Budget:** Kein Bedarf an zusätzlichem Material und Personal
- **Unterstützung rund um die Uhr** durch unsere SOC Security und Cybersecurity Experten im Falle eines Angriffs
- **Lokale Lösung,** zu 100% am Standort Luxemburg basiert und umgesetzt.
- **Lösung abgestimmt** auf restriktive lokale Datenverwaltungsrichtlinien

Weitere Informationen erhalten Sie von Ihrem Kundenbetreuer  
oder unter <http://www.post.lu/de/business>

