
VSE NET

Produktbeschreibung

# DDoS Shield

## Der Schutz vor Angriffen auf Ihr Netzwerk

# 1. Allgemeine Informationen zum Produkt

Die VSE NET GmbH (nachfolgend VSE NET genannt) stellt dem Kunden mit dem Produkt *DDoS Shield*, im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten, einen Schutz vor volumetrischen Distributed Denial of Service (DDoS)-Attacken bereit. *DDoS Shield* wird in Form einer Automitigation bereitgestellt. Automitigation bezieht sich auf die automatische Maßnahme, welche ergriffen wird, um die DDoS-Attacke abzumildern oder zu bekämpfen. Ein manuelles Eingreifen ist nicht erforderlich.

DDoS-Angriffe zielen darauf ab, die Verfügbarkeit von Online-Diensten zu beeinträchtigen. Dabei werden Systeme und Server mit sehr großen Datenmengen gezielt überlastet. Im Falle eines Angriffs, filtert die *DDoS Shield*-Plattform den bösartigen Angriffs-Traffic heraus und verwirft ihn innerhalb von wenigen Sekunden mithilfe passgenauer Filterrichtlinien, während der legitime Traffic weiterhin an das ursprüngliche Ziel geliefert wird. Dadurch entsteht auf dem Kunden-Server, selbst während des Angriffs, keine zusätzliche Last. Die Filterrichtlinien werden automatisch auf den zentralen Routern im Netz von VSE NET aktiviert. Es bedarf keiner Konfiguration auf den Systemen des Kunden. Sobald der Angriff vorüber ist, werden die Filterrichtlinien automatisch von den Netzroutern entfernt. *DDoS Shield* bietet somit einen effektiven Schutz für Online-Infrastrukturen und Netzwerke und trägt so zur kontinuierlichen Verfügbarkeit der Kundendienste bei.

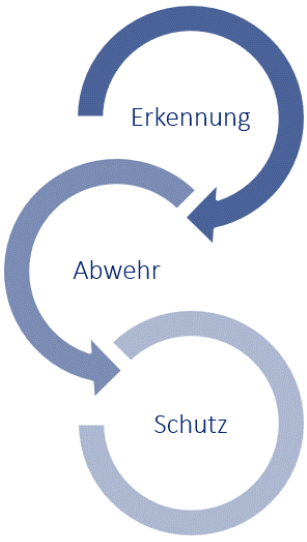
Bei dem Produkt *DDoS Shield* handelt es sich um eine kostenpflichtige Zusatzleistung zu einem Vertrag über Internetanbindungen aus dem Produktportfolio von VSE NET. VSE NET bietet folgende Produktvarianten an:

- *DDoS Shield*
- *DDoS Shield Plus*

# 2. DDoS-Schutz

## 2.1. Funktionsweise

*DDoS Shield* stabilisiert und schützt das Kundennetzwerk durch einen dreistufigen Sicherheitsmechanismus:




Erkennung:

Die *DDoS Shield*-Plattform inspiziert eingehende Datenpakete, um Anzeichen und Muster von DDoS-Angriffen zu identifizieren und bösartigen Datenverkehr zu erkennen. Kein technisches System ist in der Lage alle denkbaren Risiken abzuwenden. *DDoS Shield* dient der Minimierung der beschriebenen Risiken und kann einen wesentlichen Beitrag zum Schutz vor DDoS Angriffen leisten (vgl. 2.1)

Abwehr:

Die DDoS-Abwehr schwächt erkannte Angriffe ab und wehrt diese ab, um den Betrieb zu schützen und Auswirkungen des Angriffs zu minimieren. Dies passiert vollautomatisch innerhalb von wenigen Sekunden.

Schutz:

Der DDoS-Schutz hält durchgehend und automatisiert Gegenmaßnahmen vor, die den DDoS-Verkehr von unbedenklichen Datenpaketen trennt. So kann die Verfügbarkeit des Internetdienstes beim Kunden fortlaufend gewährleistet werden.

Die Internetrouter im Kernnetz von VSE NET erzeugen Samples von Header- und Nutzlastinformationen des gesamten Netzverkehrs und senden diese Daten zur Auswertung an die DDoS Shield Plattform. Die so gesammelten Datenproben werden mithilfe einer Kombination aus regelbasierter und systemischer Analyse überprüft. Potenzieller DDoS-Verkehr kann dadurch rasch und präzise identifiziert werden.

Die DDoS-Mitigation Appliances sind in der Lage, sich bei einem Angriff dynamisch anzupassen und ihre Kapazität innerhalb gewisser Grenzen entsprechend der Größe der Bedrohung zu ändern.

Die *DDoS Shield*-Plattform erkennt anhand dieser Analysen die Angriffsmethode einer DDoS-Attacke innerhalb von wenigen Sekunden und erstellt vollautomatisiert anpassbare Firewall-Filter, welche den Angriff über die Router im Kernnetz mithilfe eines Netzwerkkonfigurationsprotokolls abwehren.

Diese temporäre Konfiguration umfasst Filtermechanismen, welche die DDoS-Pakete am Eingangspunkt, welcher der Quelle des störenden Datenverkehrs am nächsten liegt, blockieren. Gleichzeitig wird unbedenklicher Datenverkehr ohne Beeinträchtigung zu seinem regulären Ziel geleitet.

Die kontinuierliche Telemetrie auf den Routern sendet Verkehrsstatistiken zu erlaubten und blockierten Datenströmen an die *DDoS Shield*-Plattform. Diese gewährt, während und im Anschluss an eine DDoS-Attacke, einen umfassenden Einblick in den Netzwerkverkehr. Dieser Ablauf bleibt während der gesamten DDoS-Attacke aktiv, bis die gesammelten Daten anzeigen, dass keine weiteren Angriffe auf die betroffenen IP-Adressen mehr erfolgen. Infolgedessen hebt die *DDoS Shield*-Plattform die auf den Routern eingerichteten Filter auf und kehrt zum Normalbetrieb zurück. Die gesammelten Samples und Telemetrie-Daten werden weiterhin von den Routern an die *DDoS Shield*-Plattform übertragen, um sicherzustellen, dass der Datenverkehr ungestört verläuft und um zukünftige Angriffe schnellstmöglich zu erkennen. *DDoS Shield* stellt ein vollständig automatisiertes Betriebsmodell dar, welches eine sehr hohe Sicherheit des Geschäftsbetriebs mit größtmöglicher Transparenz verbindet.

## 2.2. Umfang des DDoS-Schutzes

VSE NET stellt mit *DDoS Shield* im Rahmen der technischen und betrieblichen Möglichkeiten einen Schutz gegen potenzielle DDoS-Attacken zur Verfügung. Hierfür verwendet VSE NET eine Technologie, die DDoS-Attacken bereits an den Netzwerkgrenzen von VSE NET erkennt und abwehrt.

Optional kann der Kunde proaktiv über laufende DDoS-Attacken informiert werden und ein zyklisches DDoS-Reporting beauftragen (s. Abschnitt 3.7).

Im Rahmen seiner DDoS-Abwehrmaßnahmen setzt VSE NET eine hochleistungsfähige Sicherheits-Appliance von Corero Network Security ein. Corero ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als qualifizierter Anbieter von DDoS-Schutzdiensten anerkannt und erfüllt somit die gesetzlichen Anforderungen gemäß §3 des BSIG.

## 2.3. Wirkungsbereich des DDoS-Schutzes

*DDoS Shield* kann nur DDoS-Angriffe auf Ziele abwehren, die sich im IP-Adressbereich von VSE NET befinden. Insbesondere bei Kunden mit mehreren Uplink-Providern kann durch *DDoS Shield* nur der Netzwerkverkehr analysiert und gefiltert werden, der zum Zeitpunkt der DDoS-Attacke tatsächlich über die Netzinfrastruktur von VSE NET geroutet wird. *DDoS Shield* wertet dabei, je nach Applikation, die OSI-Layer 3-7 aus. Der Schutz umfasst die Erkennung und die Abwehr der Attacke sowie den Schutz vor zukünftigen Attacken im Rahmen der technischen Möglichkeiten und nach dem jeweiligen Stand der Technik sowie, auf Wunsch, die Information des Kunden über den Angriff.

*DDoS Shield* schützt darüber hinaus nicht vor Hacker-Angriffen sowie vor Angriffen auf Sicherheitslücken oder anderen Gefahren wie SPAM, Viren, Trojaner etc.

## 2.4. Beeinträchtigung der Qualität der Internet-Anbindung

Werden Gegenmaßnahmen zur Abwehr von DDoS-Attacken durchgeführt, kann es zeitweise zu Beeinträchtigungen der Qualität der Internetverbindung kommen (z.B. durch Paketverluste oder Erhöhung der Latenzen). Beeinträchtigungen dieser Art stellen keine durch VSE NET verursachte Störung der Internetverbindung dar.

## 2.5. Einschränkungen

Die mit der Nutzung des Internets verbundenen Gefahren und die sich hierdurch für die Kundenumgebung ergebenden Sicherheitsrisiken sind sehr vielfältig und unterliegen einer laufenden Änderung und Weiterentwicklung. Der in diesem Dokument beschriebene Dienst wird von VSE NET auf Basis der Hard- und Software des Herstellers Corero Network Security erbracht. Die Systeme des Kunden werden durch den Dienst, nach dem jeweils technisch möglichen Stand des Herstellers, bestmöglich geschützt. VSE NET schuldet dabei keinen Erfolg. Es ist, wie bei allen technischen Systemen, nicht möglich, einen vollständigen Schutz gegen alle denkbaren Angriffsszenarien zu erreichen. Die Wahrscheinlichkeit und die möglichen negativen Auswirkungen eines erfolgreichen Angriffs können mit *DDoS Shield* jedoch deutlich reduziert werden. VSE NET übernimmt für die Folgen von Angriffen und Fehlfunktionen, die durch z.B. noch unentdeckte Sicherheitslücken der Soft- und Hardware oder durch Angriffe, die von den Systemen nicht erkannt werden, entstehen keine Haftung.

# 3. Leistungsmerkmale

*DDoS Shield* besteht aus einer Basisleistung sowie weiteren kostenpflichtigen Zusatzleistungen (s. Abschnitt 3.1). *DDoS Shield* beinhaltet die Erkennung und die Abwehr von DDoS-Angriffen sowie den Schutz vor erneuten Attacken der gleichen Art.

VSE NET übernimmt im Rahmen des Produktes *DDoS Shield* die Konfiguration, die Überwachung und die Wartung der eingesetzten Plattform.

## 3.1. Produktvarianten

### DDoS Shield Basisleistung:

Als VSE NET-Kunde profitieren Sie automatisch vom *DDoS Shield* Basisschutz. Dieser Schutz nutzt modernste Technologien, um Ihre Verbindung kontinuierlich zu überwachen und bei Bedarf automatisch gegen Angriffe vorzugehen.

### DDoS Shield:

- Individualisierter Schutz vor DDoS-Attacken
- Monatlicher, ausführlicher Service-Report per Mail

### DDoS Shield Plus:

- Individualisierter Schutz vor DDoS-Attacken
- Bis zu drei Portalzugänge für real-time Monitoring
- Event-Mail im Falle einer laufenden DDoS-Attacke
- Service-Report per Mail (wahlweise täglich, wöchentlich oder monatlich)

## 3.2. Vor-Abstimmung

### DDoS Shield:

Zur Bereitstellung des Servicereports muss der Kunde vor Einrichtung von *DDoS Shield* VSE NET einen Ansprechpartner mit Namen, Rufnummer und E-Mailadresse benennen. Die Angaben werden im individuellen Angebot dokumentiert. Bei einer Änderung des Ansprechpartners oder der Kontaktdaten hat der Kunde dies VSE NET unverzüglich anzuzeigen.

### DDoS Shield Plus:

Zur Einrichtung des Portalzugangs sowie für die Bereitstellung von Service- und Event-Mails muss der Kunde VSE NET bis zu drei Ansprechpartner mit Namen, Rufnummer(n) und E-Mailadresse(n) benennen. Die Angaben werden im individuellen Angebot dokumentiert. Bei einer Änderung des/der Ansprechpartner(s) oder der Kontaktdaten hat der Kunde dies VSE NET unverzüglich anzuzeigen.

## 3.3. Bereitstellung

VSE NET informiert den Kunden über die Bereitstellung von *DDoS Shield* über eine Bereitstellungsanzeige. Im Falle von *DDoS Shield Plus* werden dem Kunden zusätzlich die Zugangsdaten für den Portalzugang zur Verfügung gestellt (Nutzerkennung + Token Code). Außerdem stellt VSE NET dem Kunden eine Kurzanleitung über die Bedienung des *DDoS Shield*-Portals zur Verfügung.

## 3.4. Plattform-Management

VSE NET übernimmt im Rahmen der Leistungsmerkmale von *DDoS Shield* und *DDoS Shield Plus* im Hinblick auf die verwendete Technologie die Funktionsüberwachung, das Backup der Konfiguration sowie die Softwarepflege.

## 3.5. Meldung von DDoS-Angriffen

Hat der Kunde die Produktvariante *DDoS Shield Plus* beauftragt, so informiert VSE NET ihn proaktiv im Falle einer laufenden DDoS-Attacke (Event-Mail).

## 3.6. Automitigierte Abwehr von DDoS-Angriffen

Im Falle einer DDoS-Attacke greift die Automitigation von *DDoS Shield* unmittelbar, sobald eine Anomalie im Datenverkehr erkannt wurde und setzt den Schutzmechanismus von *DDoS Shield* in Kraft (Erkennung, Abwehr, Schutz). Eine manuelle Qualifizierung oder Meldung einer DDoS-Attacke durch VSE NET oder den Kunden ist nicht erforderlich.

Durch die Automitigation von *DDoS Shield* entstehen für den Kunden im laufenden Betrieb keinerlei Mitwirkungspflichten.

## 3.7. Reporting

VSE NET stellt dem Kunden, je nach gewählter Produktvariante, mittels eines periodischen Service-Reports eine Übersicht über ggfs. erfolgte DDoS-Attacken (betroffene IP-Adressen, Art und Dauer des Angriffs) per Mail zur Verfügung.

Hat der Kunde *DDoS Shield Plus* beauftragt, so hat er darüber hinaus die Möglichkeit, über einen Portalzugang sein Netzwerk in Echtzeit zu überwachen.

## 3.8. Ende der DDoS-Attacke

Eine DDoS-Attacke gilt als beendet, sobald der Datenverkehr zu der dem Kunden zugewiesenen IP-Adresse eine unauffällige Verkehrscharakteristik aufweist. Unauffällig bedeutet in diesem Zusammenhang, dass das Verkehrsprofil etwa dem Vergleichszeitraum der beiden Vorwochen entspricht. Sind keine Vergleichswerte vorhanden, so sind die Event-Daten aus der DDoS-Plattform zur Bestimmung des Zeitpunkts maßgeblich. Im Falle von *DDoS Shield Plus* informiert VSE NET den Kunden proaktiv per Event-Mail über den erkannten Beginn und das Ende des Angriffs.

## 3.9. Zusätzliche Leistungen

Erbringt VSE NET neben den vertraglich geschuldeten Leistungen darüber hinaus gehende zusätzliche Leistungen, so sind diese vom Kunden gemäß eines separaten Angebotes nach Aufwand zu vergüten.

# 4. Mitwirkungspflichten des Kunden

## 4.1. Bereitstellung von Informationen:

Zur Bereitstellung des Dienstes hat der Kunde, in Abhängigkeit von der von ihm beauftragten Produktvariante, die nachfolgenden Informationen bereitzustellen. Die Informationen werden von VSE NET in der Angebotsphase abgefragt. Darüber hinaus können weitere administrative oder technische Angaben des Kunden erforderlich sein. Diese werden dann gegebenenfalls zusätzlich im Angebot dokumentiert.

- Name, Vorname, E-Mail-Adresse und Telefonnummer von maximal 3 Kontaktpersonen des Kunden

  Event-Mails und Service-Reports werden automatisch an die im System hinterlegten E-Mail-Adressen der Kontaktpersonen versendet.

- IP-Adressen, bzw. IP-Ranges, die überwacht werden sollen

## 4.2. Erstanmeldung am Web-Portal und Änderung des Passworts

Sofern *DDoS Shield Plus* beauftragt wurde, erhalten die durch den Kunden benannten Kontaktpersonen eine vom *DDoS Shield*-Portal automatisiert versendete E-Mail mit einem Einmalpasswort (Token). Der Kunde sorgt dafür und ist dafür verantwortlich, dass alle im Auftrag benannten Kontaktpersonen unverzüglich nach dem Versand der E-Mail ein eigenes, individuelles Passwort für ihren individuellen Zugang einrichten. Hierzu ist die Anmeldung an dem Web-Portal mit dem passenden Benutzernamen und dem dafür bereitgestellten Einmalpasswort erforderlich. Der Link zum Web-Portal wird dem Kunden im Rahmen der Bereitstellungsanzeige schriftlich mitgeteilt.

# 5. Störungen

Unbeschadet etwaiger Pflichten aus § 58 TKG gelten im Falle einer Störung der hier definierten Leistungsmerkmale die nachfolgenden Vereinbarungen.

Eine Störung des hier beschriebenen Dienstes liegt vor, wenn im Falle von *DDoS Shield* die wöchentlichen Reports nicht oder fehlerhaft bereitgestellt werden. Im Falle der Produktvariante *DDoS Shield Plus* liegt darüber hinaus eine Störung vor, wenn der Kunde sich mit den ihm zugewiesenen Zugangsdaten nicht in das DDoS-Portal von VSE NET einloggen kann.

Eine Mitigation von zulässigem Traffic bzw. ein Nichterkennen von potenziell schadhaftem Traffic stellt keine Störung des Dienstes *DDoS Shield* dar.

| | |
|---|---|
| Störungshotline | 0800 607 2221<br>(aus dem Ausland +49 681 607 2221) |
| Störungsannahme | 7/24<br>Täglich, 0:00 Uhr bis 24:00 Uhr |
| Störungsbearbeitung | 5/12<br>Werktags (Mo – Fr)<br>8:00 Uhr – 20:00 Uhr |
| Maximale Reaktionszeit | 4 h<br>Werktags (Mo – Fr)<br>8:00 Uhr – 20:00 Uhr |
| Maximale Entstörzeit | 12 h |
| Individuelle Zwischenmeldungen | x |
| Schlussmeldung bei erfolgter Entstörung | ✓ |
| Individueller Fehlerbericht | x |

## 5.1. Meldung von Störungen

VSE NET nimmt Störungsmeldungen täglich von 00:00 Uhr bis 24:00 Uhr telefonisch unter der Servicenummer 0800 607 2221 (aus dem Ausland +49 681 607 2221) entgegen. Bei Eröffnung der Störung sind Angaben zur VSE NET Projektnummer (z.B. W.58.xxxx.xx), dem konkreten Ansprechpartner beim Kunden und zur Art der Störung erforderlich.

## 5.2. Entstörfrist

Bei Störungsmeldungen, die werktags (montags 8:00 Uhr bis freitags 20:00 Uhr) eingehen, beseitigt VSE NET die Störung innerhalb von 12 Stunden nach Erhalt der Störungsmeldung, es sei denn, die Leistungserbringung ist aus vom Kunden zu vertretenden Gründen nicht möglich. Für Störungen, die freitags nach 20:00 Uhr, samstags, sonntags oder an gesetzlichen Feiertagen (Saarland) gemeldet werden, beginnt die Entstörfrist am darauffolgenden Werktag (Mo – Fr) um 8:00 Uhr. Die Störungsbearbeitung erfolgt an Werktagen (Mo – Fr) zwischen 8:00 Uhr und 20:00 Uhr und wird nach 20:00 Uhr bis zum folgenden Werktag (Mo – Fr) 8:00 Uhr unterbrochen.

Fällt das Ende der maximalen Entstörungszeit auf einen gesetzlichen Feiertag oder ein Wochenende, so wird die maximale Entstörungszeit für die Dauer des Feiertages oder des Wochenendes bis zum nachfolgenden Werktag (Mo – Fr) um 8:00 Uhr unterbrochen. Bei Störungen, die im Verantwortungsbereich des Kunden liegen, entfällt die Verantwortung von VSE NET, die zugesicherte Entstörungszeit einzuhalten.

## 5.3. Schlussmeldung bei erfolgter Entstörung

Der Kunde erhält eine Schlussmeldung bei erfolgter Entstörung. Diese kann sowohl schriftlich als auch telefonisch erfolgen.

# 6. Wartungsarbeiten

Durch VSE NET geplante und angekündigte Wartungsarbeiten an der *DDoS Shield* Plattform können eine geplante Unterbrechung der vertraglichen Dienstleistung bewirken. In dringenden Fällen kann eine ungeplante Wartung ohne vorherige Information des Kunden notwendig sein.

## 6.1. Wartungsfenster

Das jeweilige Wartungsfenster für geplante Wartungsarbeiten wird dem Kunden im Vorfeld per Mail mitgeteilt.

# 7. Jährliche Dienstverfügbarkeit

*DDoS Shield* hat eine jährliche Mindestverfügbarkeit von 99,8%. Die Verfügbarkeit in Prozent errechnet sich aus der Gesamtzahl der Stunden eines Betriebsjahres (Zeitraum von 365 Tagen ab dem Tag der Bereitstellung) abzüglich der Stunden des Betriebsjahres, während denen das Produkt nicht verfügbar ist, dividiert durch die Gesamtzahl der Stunden des Betriebsjahres multipliziert mit 100. Folgende Zeiten und Ausfälle werden in der Verfügbarkeitsrechnung nicht berücksichtigt:

- Entstörfrist (s. Abschnitt 5.2)
- Ausfälle durch Fehler, die im Verantwortungsbereich des Kunden liegen
- Unvermeidliche Unterbrechungen auf Grund von Änderungswünschen des Kunden
- Ausfälle, die durch höhere Gewalt verursacht sind
- Ausfälle in Folge des ausdrücklichen Wunsches des Kunden, die Störung nicht zu beheben
- Ausfälle auf Grund geplanter oder vereinbarter Unterbrechungen in Folge von Wartungsarbeiten durch VSE NET oder den Kunden
- Zeitverluste, die nicht durch VSE NET verschuldet sind

# 8. Glossar

| Bezeichnung | Beschreibung |
|---|---|
| Automitigation | Ein Prozess oder eine Technologie, die automatisch Bedrohungen oder Sicherheitsvorfälle identifiziert und Gegenmaßnahmen ergreift, um den Schaden zu minimieren. |
| BSI<br>(Bundesamt für Sicherheit in der Informationstechnik) | Eine deutsche Behörde, die für die Sicherheit von IT-Systemen und den Schutz von Informationen zuständig ist, einschließlich der Entwicklung von Standards und Richtlinien. |
| DDoS<br>(Distributed Denial of Service) | Eine Art von Cyberangriff, bei dem eine Vielzahl von Systemen gleichzeitig einen Dienst überlastet, um diesen unzugänglich zu machen. |
| IP-Range | Ein Bereich von IP-Adressen, der für die Zuweisung an Geräte oder Netzwerke verwendet wird, häufig zur Verwaltung von Netzwerken und deren Sicherheit. |
| OSI-Modell | Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur. Es beschreibt die Kommunikation über sieben verschiedene Schichten hinweg (OSI-Layer). |
| Telemetrie | Die automatische Übertragung von Messdaten und Informationen von einem Ort zu einem anderen, oft verwendet in der Datenüberwachung und -analyse. |
| Uplink Provider | Ein Dienstanbieter, der Internetverbindungen und -dienste bereitstellt, insbesondere für die Verbindung von Netzwerken zu größeren Netzwerken oder dem Internet. |