INDUSFACE™

# CISO Guide for DDoS

## Prevention, Protection, and Mitigation

## List of Contents

## Abstract

Being a CISO in this ever-growing threat landscape is not everyone's cup of coffee. In recent years, with the adoption of the work-from-home culture, cyber-security attacks have taken the front seat in disrupting businesses of all sizes across the world.

DDoS attacks of any type and magnitude could cause serious damage for businesses, and mitigation and recovery could make a major impact on the balance sheets, brand reputation, business growth, and innovation.

This document is intended for CISOs and IT decision-makers who are familiar with the basic concepts of networking and security. It covers "all things DDoS" and hopefully, helps you in strengthening the security posture of your business.

## The Cat & Mouse Game

The first DDoS attack happened 20 years ago. Since then, cybersecurity professionals and vendors have risen to the challenge by formulating new and sophisticated DDoS mitigation technologies for the market. On the same note, attackers have not budged down as well. They have upped their level with sophisticated and complex attacking techniques. This has led to an escalating cat-and-mouse game to stay ahead.

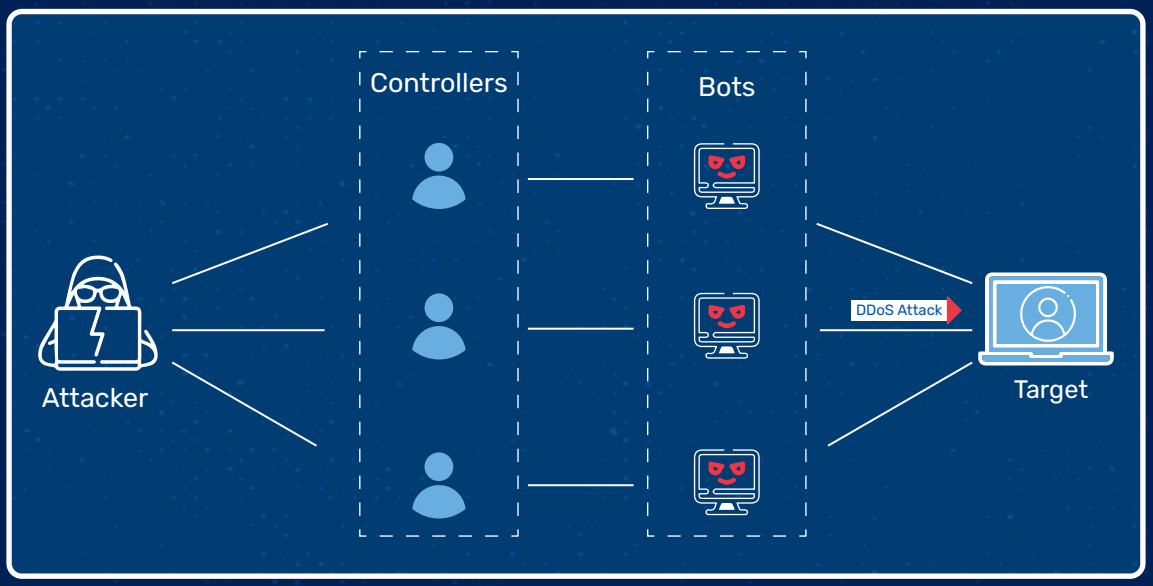
# Introduction: Denial of Service Attacks

## Not Every Traffic is Legitimate!

A DoS attack is short for Denial-of-Service attack. This attack attempts to block or deny legitimate users access to a website/ application by flooding the site with excessive, illegitimate, and unnecessary network traffic. This attack is carried out by hackers/attackers using various techniques to consume large amounts of bandwidth and thus, disrupt the website/ application access to the intended users.

## DDoS (Distributed Denial of Service) Attack -

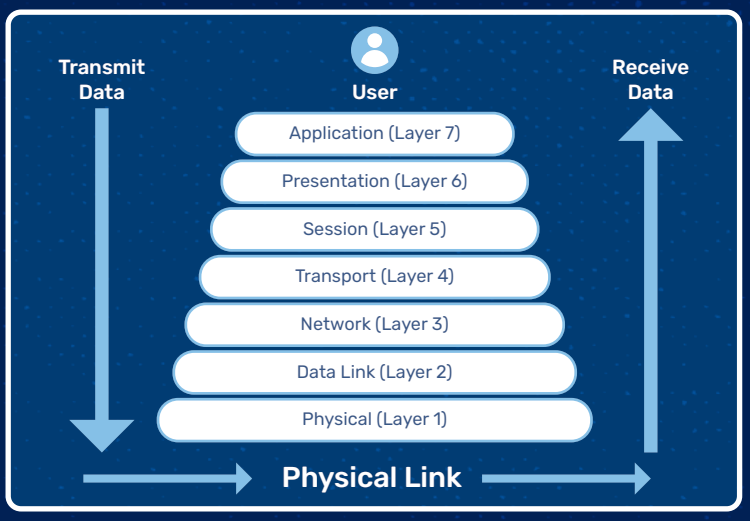
DDoS attack is short for Distributed Denial of Service attack. In this type of attack, to orchestrate an attack against a target, an attacker utilizes multiple sources such as distributed groups of malware-infected computers, IoT devices, routers, etc to flood the website/ application with excessive, illegitimate, and unnecessary network traffic.




## OSI Model & DDoS Attacks -

The OSI model, short for Open Systems Interconnection model, was created by the ISO (International Standards Organization) that conceptualized the seven layers in computer networking. Out of these seven layers, layers 3, 4, 6, and 7 are susceptible to DDoS attacks.

## The 7 Layers of OSI




Generally, attackers use the following DDoS attacks at the infrastructure layer level (layer 3 and layer 4):

- User Datagram Protocol (UDP) reflection attacks
- Synchronize (SYN) Floods

The attacker uses these methods to generate volumetric traffic that can overload the network capacity or tie up resources on systems such as firewalls, servers, load balancer, or intrusion prevention system (IPS). Though these attacks can be easily identified and mitigated, your business must have networks or systems to scale above the incoming volumetric and unnecessary traffic. This extra capacity helps free the system and application for legitimate users/traffic.

### User Datagram Protocol (UDP) Reflection Attacks

These attacks exploit based on the fact that UDP is a stateless protocol. Here, the attacker spoofs/falsifies the UDP request packet's source IP by crafting a valid UDP request packet listing the attack target's IP address as the UDP source IP address.

This UDP packet containing the falsified source IP is sent to the intermediate server. Thus, tricking the server into sending its UDP response packets to the target IP. As this intermediate server generates a response larger than the request packet, it effectively reflects/amplifies the illegitimate traffic.

The amount of amplification can be calculated based on these factors:

- Response size/ Request size.
- The protocol used by the attacker (DNS, SSDP, QOTD, etc)

Generally, the amplification factor for DNS can be 28 - 54 times the original number of bytes.

## Synchronize (SYN) Flood Attacks

In this type of attack, the attacker sends a large number of SYN packets without sending the final ACK packets to complete the handshakes. This leads to making the server wait for a response to the incomplete TCP connections. Soon, it won't have the capacity to accept new TCP connections. The attack tries to tie up the available server connections so that resources are not available for the intended and authentic connections.

## Layer 7 – Application Layer Attacks

These attacks are similar to SYN flood infrastructure attacks – the attacker floods the specific functions of an application to make it unavailable to legitimate users. These attacks can be carried out with very low request volumes that generate only a small volume of network traffic. Examples of such attacks are:


## HTTP Floods

Here, an attacker sends HTTP requests to the target that appear to be from a legitimate user of the web application. Commonly used mitigation techniques find it difficult to mitigate some complex HTTP floods that attempt to emulate human interaction with the application.


## WordPress XML-RPC Floods

This attack is also known as WordPress pingback flood. In this attack, the target is a website hosted on WordPress CMS. The attacker generates a flood of HTTP requests by misusing the XML-RPC API function.


## Cache-Busting Attacks

Cache-busting attacks are a type of HTTP flood attacks that use variations in the query string to avoid CDN caching.


## DNS Query Flood

Domain Name System services could be a target of these application-layer attacks. In this DNS query flood attack, the attacker uses many well-informed DNS queries to exhaust the DNS server resources.

## The Latest DDoS Statistics & Trends

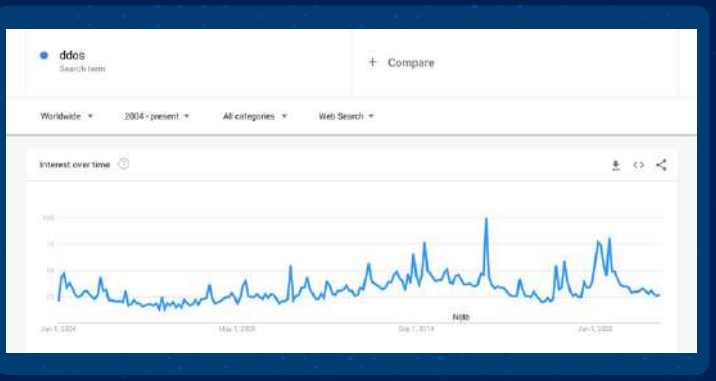
As a CISO, one needs to keep an eye on the latest DDoS statistics and trends. Data-driven decisions are always welcomed by the management. It becomes easier and prudent to communicate the DDoS threats to the management.

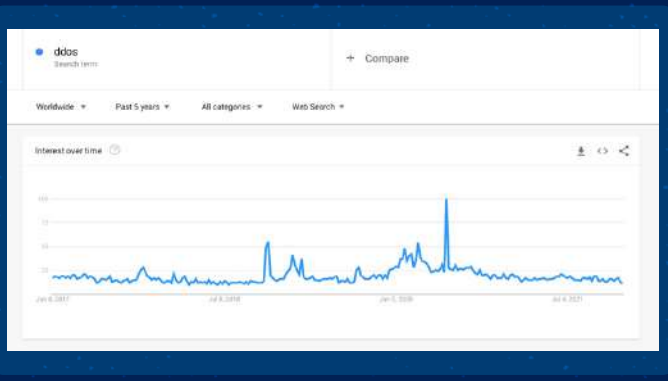
The following stats show a steady increase in both the quantity and complexity of DDoS attacks worldwide!

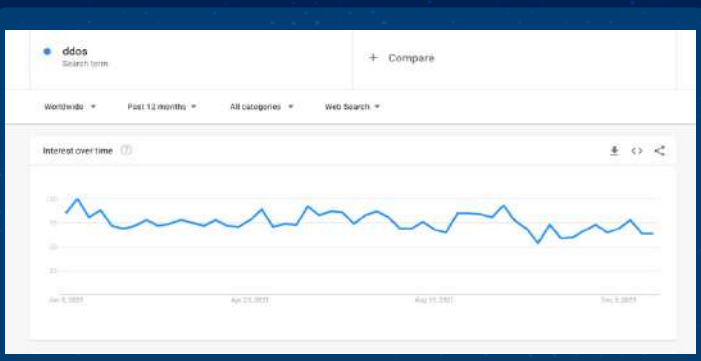
Here are some search trends w.r.t the term “DDoS” -

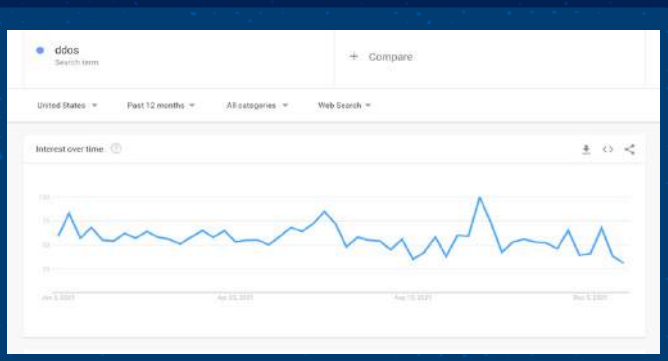
*Note: In these graphs, Interest over time means -*

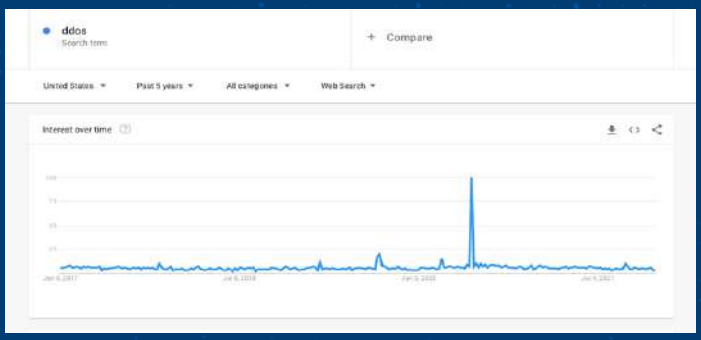
*The search interest is relative to the highest point on the chart for the given region and time. A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means there was not enough data for this term.*

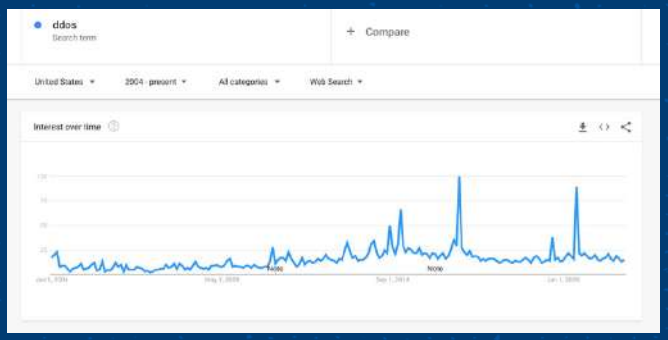


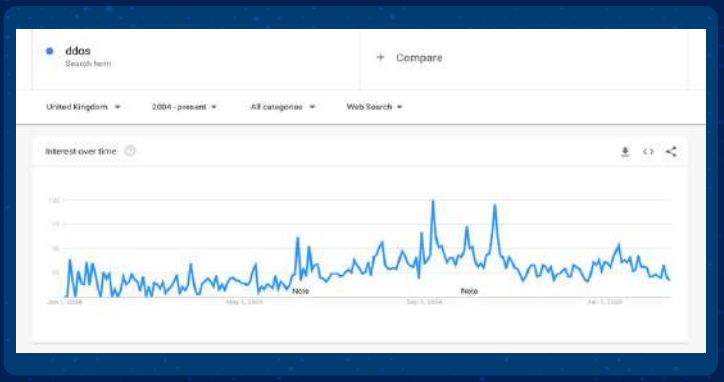



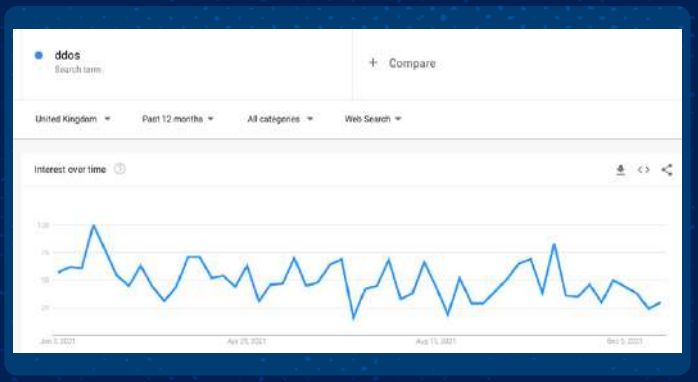






The above graphs show the interest levels to search and know about the term DDoS. And as you see, the interest levels are not to be ignored.

## DDoS Attacks Trends & Statistics 2018 – 2021

- In the first half of **(2020 vs 2021)**, there was a **151%** increase in the number of DDoS attacks
  Source: Infosecurity Magazine
- **91.06%** of the attacks in the Q3 of **2019** carried on for as long as four hours
  Source: Infosecurity Magazine
- By **2022**, experts predict that there will be **15.4** million recorded DDoS attacks
  Source: Infosecurity Magazine
- According to Amazon, in Feb **2020**, the biggest DDoS attack on record was mitigated by them. The attack reached a peak traffic volume of **2.3 Tbps** - Source: Infosecurity Magazine
- According to Neustar, the attack intensity in the first six months of 2020 increased by **81%**
  Source: Infosecurity Magazine
- There is an influx of short-lived attacks that last under **4** hours.
- DDoS activity decreased in **2018** but bounced back in **2019** - The reason could be the FBI taking down DDoS-for-hire sites in late **2018**.
- DDoS attackers are now using multi-vector attacks more frequently
- In **2020**, SYN attacks were preferred over UDP attacks
- DDoS attacks are geographically concentrated - China and the US are botnet hubs
- The decreasing order of botnets - China **(820,000)** > India **(800,000)** > Iran **(400,000)** - Source: Spamhaus
- The top **5** impacted ASN operators, mostly ISPs, have infected IP addresses due to extensive botnet malware are:
  - China Telecom / ChinaNet (China)
  - Bharti Airtel Ltd. AS for GPRS Service (India)
  - China Unicorn (China)
  - Iran Telecommunication Company PJS (Iran)
  - Telecom Algeria (Algeria)
- The majority of the attacks are launched from China, the USA, and Russia.
- In the last three years, DDoS records have been broken multiple times.
- The **2nd** largest DDoS attack on record was against Github. **1.3** Terabytes of data was sent toward GitHub's servers.

## Noteworthy DDoS Attack Examples and News 2019-2021

**Date:** May 2021
**Victim:** Government-funded Belnet ISP's network
- **Location:** Belgium
- **Impact:** More than 200 Belgian organizations, including colleges, research centers, and the country's parliament

**Date:** June 2020
**Victim:** Amazon
- **Impact:** Though Amazon mitigated this attack. Bu this was the largest DDoS attack recorded. (2.3 Tbps throughput)

**Date:** July 2019
**Victim:** Video Game Servers during Christmas 2013-14
- **Location:** USA
- **Impact:** $95,000 damages
- **Source:** US Dept of Justice

**Date:** July 2019
**Victim:** Telegram
- **Location:** USA
- **Impact:** 200-400 Gbps attack on the company Telegram
- **Source:** Security Boulevard

## Job Responsibilities & Objectives of a CISO w.r.t DDoS Prevention, Protection, and Mitigation

Now that we have established the necessary details of a DDoS attack and its trends, let's discuss the role of a CISO who is responsible for security in this context.

- Ensuring compliance across the board.
- Monitoring end-to-end security operations.
- Disaster recovery & business continuity.
- Documentation - compliance, governance, incident management, and risk management.
- Stakeholder onboarding.
- HR management (evaluating employee & organisations' behaviour).
- Financial reporting & addressing cybersecurity as a priority.
- Establishing the right governance and security practices.
- Enabling a framework for risk-free and scalable business operations in the challenging business landscape.
- Security operations management.
- Providing cyber risk intelligence.
- Data loss and fraud prevention.
- Identity and access management.
- Investigation and Forensics.
- Cybersecurity program management.

## Biggest Day-to-Day Challenges

- Project Management & Disorganization
- Professional Development
- Change Management
- Resources Management
- Problem Solving & Decision-Making Communication
- Collaboration & Creativity
- Navigating Client Relationships & Communications

## The Biggest Challenge You Face in Terms of Cybersecurity

- Communicating value to the board/management.

So,

## How to Communicate the DDoS Threats to Your Board


Being the CISO isn't easy. As you would be responsible for the entire security posture of an organization, it is your responsibility to communicate the same to your board. The board often sees security as an expense as they don't understand the intricacies as well as the big picture. Basically, they can't see what you see!

So, how do you communicate to the executive board that needs to understand the potency of DDoS attacks to the company networks and the preparation to tackle them? After all, it is the holders who grant or deny the budget for your security team operations. Thus, knowing how to convince them is one of the key challenges for any CISO.

In the past decade and especially during these work-from-home times, their focus and understanding of the importance of a robust cybersecurity program have increased. However, when a CISO starts discussing the impact of less understood threats such as DDoS, it can still be difficult to make the board agree. Some do understand the potential of DDoS attacks, primarily due to the punishing nature of the regulatory compliance regimes, but many of the board members need to understand the business impact and not just the security standpoint(s).

**Here are a few reasons why the board doesn't get DDoS or does it?**

## Turning a Blind Eye to DDoS

The threat of ransomware is visible and convincing, but the board has a tough time understanding the unique risks of DDoS. While they turn a blind eye to such attacks, DDoS, on the other hand, is becoming relevant and even more dangerous by the day. Thus, threatening the bottom lines, business growth, and innovation of any business. Many businesses are even prepared to pay large amounts of ransoms to restore operations.

## Getting Into the Shoes of the C-Suite

The board/management/C-suite likes one primary thing – business impact. As a CISO, you should speak in their language and not just in cybersecurity terms. It is all about how you connect the security posture/ defence with the business impact it has on growth and innovation. DDoS threats are ever evolving, so should your cybersecurity and business strategies to counter them. Security and business should go hand-in-hand. Back up your statements with facts, figures, case studies, and business risks too.

Here are a few key pointers to discuss with your board in terms of DDoS protection, prevention, and mitigation:

## Is Your Organization a Likely Target to DDoS Threats?

Knowing the importance of DDoS protection and the general threat of a DDoS attack is just half-job done. The other important half of this job is to know how your organization may get attacked and the impact it would have on business continuity.

As seen in recent years, DDoS attackers target internet-facing and connectivity-dependent businesses. Remote working and the dependency on the cloud should be assets to any business. But threat actors are constantly targeting these assets with varied attacking techniques.

## DDoS Threat to Business Revenue

The board doesn't understand the cybersecurity risks to the t (as you do) but surely understands the punishing effects of downtime. That is exactly what DDoS attempts to do. It paralyzes your website/ application for the intended users, and thus, the business would end-up spending time and resources on restoration rather than business profits, growth, and innovation. A DDoS attack affects each and every department of your business, not just the IT and security teams. Teams such as sales, marketing, customer support, and management are affected as well.

Every move you make counts and affects the balance sheet. Not just during the attack, but post the DDoS attack, the business incurs losses in terms of brand identity and reputation, compliance/ regulatory penalties, etc.

## DDoS Threat to Innovation

A well-orchestrated DDoS attack can hurt the internal business operations. With increasing dependence on connectivity, remote working, and IoT, attackers have you right where they want you. Also, they are constantly evolving to bypass your traditional DDoS protection solutions. They are picking up speed and are timing their attacks for a shorter period. Thus, helping them to circumvent your legacy DDoS detection and mitigation solutions. These short-timed attacks cause the most damage without them getting noticed.

Clever right!

But how to become cleverer than your attackers?
How to understand their behavior, their next move?

## Introducing Behavioral DDoS Solutions -

To counter the ever-evolving DDoS attackers, cybersecurity vendors like Indusface AppTrana have developed various custom algorithms to identify malicious DDoS traffic, such as measuring the normal baseline rate and comparing it against IPs that deviate from that rate.

- Behavioural DDOS can be configured to be triggered if the behaviour of the requests to an application changes. Thus, every normal variancein the request is accounted for, and alerts are triggered only when there is an abnormality

- By default, three policies that monitor traffic on the host, IP, and session levels are configured

- When an application is onboarded, these policies are configured with default values that work for most of the applications

- Within a few days of onboarding the application, based on the behaviour observed, appropriate values are derived to provide optimal protection


## How Indusface is Helping CISOs Ace the DDoS Protection Game

We are Indusface, the leading application security SaaS company that secures critical Web, Mobile & API applications of 2000+ global customers using its award-winning fully managed platform "AppTrana" that integrates web application scanner, web application firewall, DDoS, BOT Mitigation, CDN, and threat intelligence engine.

The company has been funded by Tata Capital Growth Fund, Ranked #1 in overall ratings by 2021 Gartner Peer Insight 'Voice Of Customer' report for WAF, is 'Great Place to Work' certified, the platform is compliant with PCI, ISO27001, Soc2, GDPR, etc and has been the recipient of many prestigious start-up awards.

## Get Fully-Managed DDoS Attack Protection for Applications

Indusface ensures application availability with a guaranteed uptime of 99.99% with AppTrana's always-on, unmetered DDOS protection against layer 3, 4 & 7 DDOS attacks.

- # 1 Rated WAF (Web Application Firewall) by our Customers in Gartner Peer Insights
- Only WAF with a 100% Customer Recommendation Rating in Gartner Peer Insights

# The APPTRANA Difference

## Become Battle Ready

Built for scale, AppTrana leverages highly scalable AWS infrastructure known to block large attacks up to 2.3 Tbps and 700K requests per second to provide DDoS attack protection against the largest attack possible.

## Instant Protection

Quick and easy onboarding with the enablement of pre-configured protection in 2-3 minutes. Always-on protection ensures sub-minute detection and mitigation ensuring immediate DOS/D-DOS protection without affecting legitimate traffic.

## Comprehensive Protection

AppTrana protects against all types of DDOS attacks, including Infrastructure layer attacks (like ICMP /UDP flood attacks), protocol attacks (like SYN flood attacks, UDP reflection attacks), and application-layer attacks (like HTTP flood, Slow/low attacks etc.)

## Unmetered DDoS Attack Protection

Don't get penalized for being under attack. AppTrana provides complete DDoS attack prevention, which is unmetered. You are charged for only legitimate traffic that is passed to your origin.

## Managed DDoS Protection at No Additional Cost

Sophisticated Application attacks need special attention. Get instant access to security experts who monitor your traffic and deploy complex rules to thwart complex attacks at no additional cost.

## How Does It Work?

Once the customer makes a DNS change, all the traffic to the application is passed through

- AppTrana infrastructure and DDOS protection start immediately.
- AppTrana has multiple layers of DDOS protection.

## Content Delivery Network:

Any traffic to the application first hits the edge network which caches your application. The edge is equipped to accept only well-formed requests which automatically protects against volumetric DOS/DDOS attacks like TCP flood etc.

## Highly-Scalable WAF layer:

To protect against DDOS attacks, it is important for the WAF (Web Application Firewall) infrastructure scales to observe high load. The WAF layer built on AWS monitors the load on various parameters and immediately scales-up to observe any amount of load.

## Anomaly Detection Layer:

Traffic observed by the WAF layer is checked for abnormal behavior using sophisticated algorithms, and any requests exhibiting abnormal behavior are flagged for further action. Abnormal behavior is determined based on the request patterns, global threat score based on reputation, etc, and also rate limits set for the site. Action taken on these requests can vary, including alerts to the internal team.

# Industry's Only Comprehensive Unmetered Managed DDOS Protection for Your Applications

## Get Sophisticated Controls

Get control of rules that can be created for distributed denial of service attack prevention. Learn the past trends per IP/URI and set rate limits that meet your application needs.

Get the ability to write URI-specific rate limits at no additional cost.

## Get Immediate Actionable Alerts

Get notified if your site is under DDOS attack. Notification is sent to you when an attack starts and when the attack is completely mitigated. In case of stubborn attacks, notification is sent to experts who analyze the attack pattern of the site and write tailored-made rules to thwart sophisticated attacks.

## Get Complete Visibility

Get transparent visibility into attacks, trends, and how they were protected. Get specific reports on DDOS and determine the efficacy of protection first-hand.

Link References:


- https://www.infosecurity-magazine.com/blogs/ddos-attacks-stats-protection/
- https://www.spamhaus.org/statistics/botnet-cc/
- https://securityboulevard.com/2019/06/telegram-hit-by-powerful-ddos-attack-blames-china/

Indusface is a leading application security SaaS company that secures critical Web, Mobile, and API applications of 5000+ global customers using its award-winning fully managed platform that integrates web application scanner, web application firewall, DDoS & BOT Mitigation, CDN, and threat intelligence engine.

Indusface, funded by Tata Capital Growth Fund II, is the only vendor to receive 100% customer recommendation rating three years in a row and is a global customer choice in the Gartner Peer Insights™ Web Application and API Protection (WAAP) Report 2023. Indusface is also a "Great Place to Work" 2022 Winner in the Mid-Size category in India and is PCI, ISO27001, SOC 2, GDPR certified and has been the recipient of many prestigious start-up awards.

CONTACT US - +91 265 6133021 | +1 866 537 8234
EMAIL - sales@indusface.com