The Cost of DDoS Security

An Executive Guide in designing a DDoS Protection strategy and the total costs involved

WHITE PAPER

Introduction

The threat of DDoS attacks looms large over every and all types of organization that relies on the Internet today to conduct their daily business. With today's DDoS attacks capable of easily taking down countries and ISPs, not to mention any business, DDoS detection and mitigation is now an inseparable part of every organization’s cybersecurity playbook and Business Continuity Planning (BCP). In this guide, we identify and break down the direct and indirect capital and operations costs involved in deploying and maintaining a DDoS detection and mitigation strategy that works.

Solutions which include hardware such as an on-premise-based DDoS appliance are usually accounted for as a capital expenditure (Capex), whereas ongoing subscription services such as a Cloud DDoS protection services are considered operating expenses (Opex). Depending on accounting and procurement processes, organizations will have a preference for one type over the other.

Types of Costs

Capex, or capital expenditure refers to upfront costs incurred for assets that will be used in the future. Capex corresponds to costs for the purchase of hardware such as servers and appliances, that usually have a lifespan of 3 to 5 years, depending on the depreciation value. With the Capex model, the business incurs the expense in the present with the aim of generating profit in the future.

Opex refers to the day-to-day operational expenses that support the business. These typically include the operating of the technology including internet bandwidth, human resources and training costs. Unlike Capex, Opex has no upfront costs and allows organizations to spread their expenses over a period of time. And since Opex corresponds to current costs, no future benefit to the business is accounted for in the Opex model.

Maintenance and Support includes the regular maintenance and warranty and support costs to ensure the technology remains reliable during its deployment.

Longevity Cost covers the costs associated with refreshing end-of-support technologies commonly associated with hardware reaching the end of its product life cycle.

As organizations weigh their options for DDoS protection, many of them realize that DDoS protection can come in a variety of formats, and they must consider which deployment type is best for them: DIY Protection, ISP Clean Pipe Service, or Third Party Security as a service provider?

DIY Protection

DIY protection attempts often involve static traffic thresholds and indiscriminate IP blacklisting. One of the main issues with these strategies is that legitimate users can get caught up in the blocking, even though these steps are supposed to prevent the denial of services to legitimate users.

Another drawback with DIY protection is that it is reactive as opposed to proactive approach. A DIY solution's configuration often has to be manually adjusted after the first wave of an attack has already hit. Though this may prevent similar future attacks, the successful first wave will likely have already caused significant downtime. With attackers constantly switching their attack methods, new configurations need to be repeatedly deployed in order to minimize downtimes caused by attacks using different vectors.

DIY protection is also only as good as a network's bandwidth, which typically does not offer much in the way of scalability, making network layer DDoS attacks almost impossible to stop.

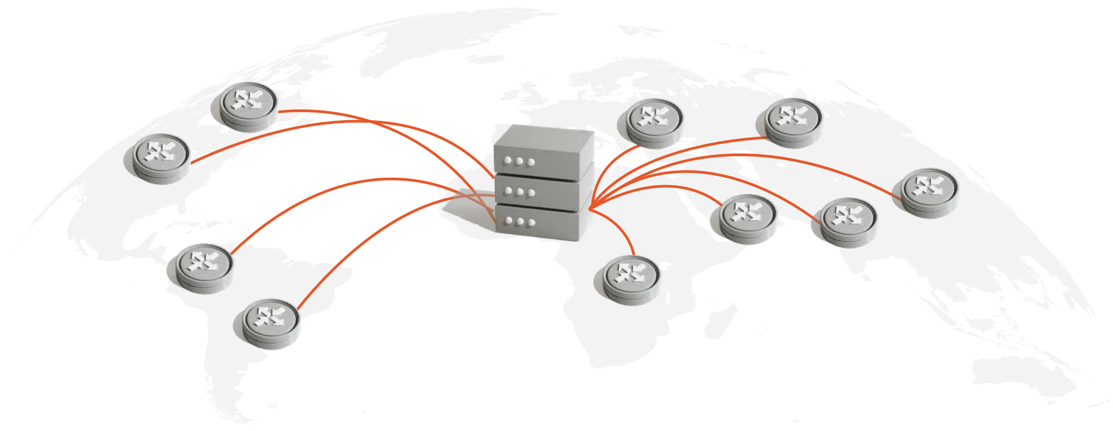
Costs associated with DIY

Capex Costs:

1. DDoS detection appliance taking into account the size of the network, number of ingress/ egress points and routers that need to be monitored.
2. DDoS mitigation appliance which could be either inline mitigation or scrubbing centre mitigation.
3. Router upgrade/ replacement cost.
4. Network infrastructure redesign cost

Example

i) A small internet service provider looking to acquire a traffic monitoring system to monitor up to 10 routers spread across different locations with an estimated volume of 500,000 flows per second (sampled) will cost between USD 30,000 to USD 60,000 upfront for the hardware.



ii) A unit of specialized DDoS mitigation appliances will cost between USD 20,000 to USD 50,000 for an enterprise-grade appliance with up to 10Gbps of capacity, or between USD 200,000 to USD 500,000 for a carrier grade appliance with up to 100Gbps of scrubbing capacity.

100G
USD 500,000
10G
USD 20,000

Opex Costs

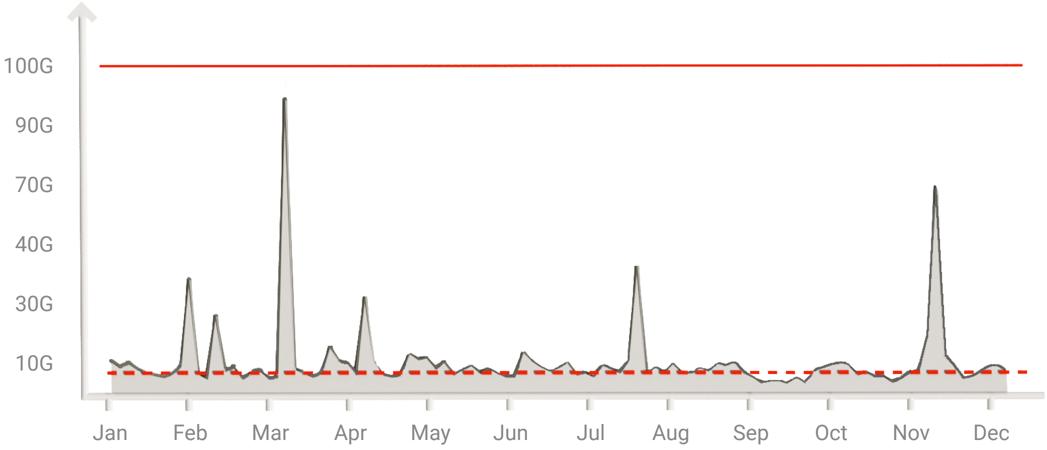
1. Capacity planning for additional bandwidth on top of the operational bandwidth.

2. Hiring and retaining skilled cybersecurity staff whose salaries are higher than those of other staff due to the global shortage of cybersecurity professionals.

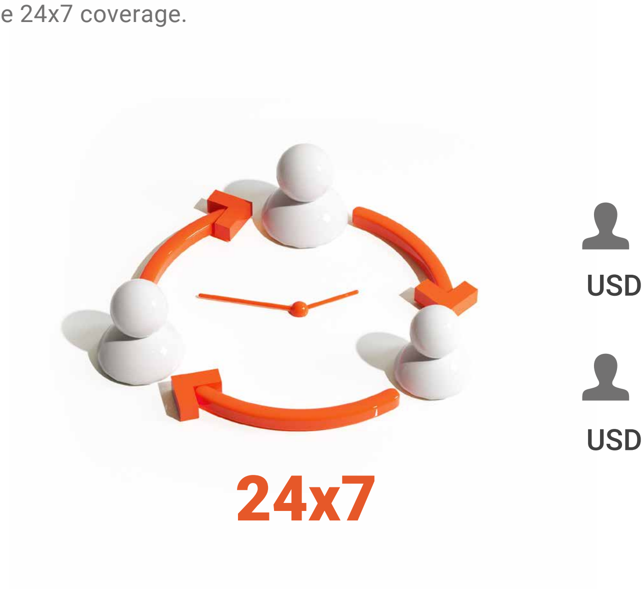
3. Continuous training costs to ensure employee training is kept up to date and stays relevant.

Example

i) The basis of any active DDoS Mitigation measures is to cater for enough capacity to take on the sudden surge of traffic during a DDoS attack. This can only be achieved by subscribing more band width on top of what the business needs. Depending on the cost of bandwidth locally, a 100Gbps burstable pipe with a minimum of 10Gbps committed consumption can cost between USD 4,000 to USD 20,000 per month, depending on the location and buyer negotiation power.



ii) The cost to hire one cybersecurity specialist will vary greatly depending on where they would reside, and ranges between USD 20,000 to USD 80,000 per annum excluding benefits and training costs in Asia, to USD 100,000 on average in the US. A team of at least 3 specialists is recommended to ensure 24x7 coverage.



in Asia

USD 20,000~80,000

in US

USD 100,000

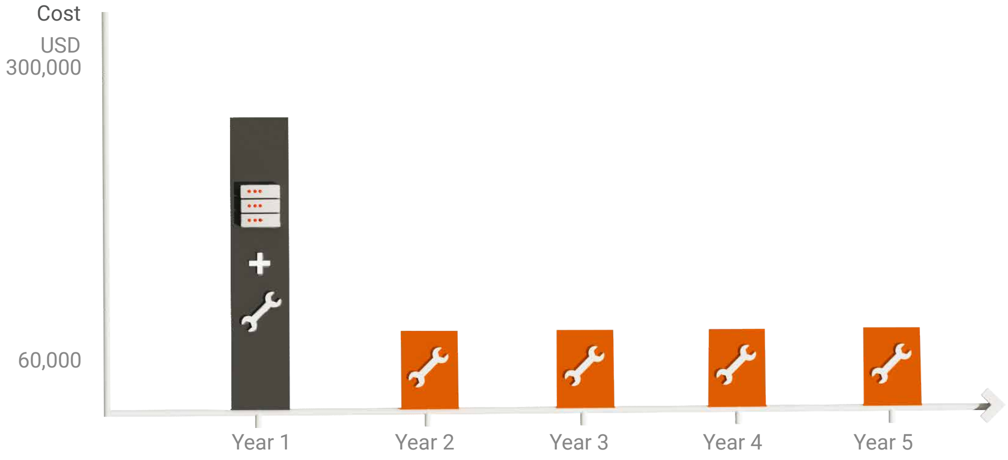
Maintenance Cost:

1. By standard industry practices, appliance Maintenance and Support costs are about 20% of the purchased price from the second year onwards.

2. Downtime and man-hour costs related to the planning and implementation of firmware updates.

Example

i) One of the most obvious costs associated with a DIY strategy is the yearly maintenance costs associated with the appliance purchased from the vendor, which ranges between 17% to 21%. A carrier grade appliance that costs USD 300,000 will mean a yearly maintenance agreement cost of USD 60,000.



Longevity Cost

1. Hardware appliances typically have a shelf life of 3 to 5 years before becoming obsolete, requiring mandatory replacement to prevent end-of-support. In general, most hardware depreciates its cost over 5 years.

2. With upgrades and changes to the new appliance comes the potential need to upgrade the systems around which the new appliance is operating such as interfaces, performance and compatibility

3. Migration costs need to be factored in for the decommissioning and migration of old to new hardware platforms.

4. Purchase costs including man hours and costs related to the tender exercise necessary to refresh the technology.

ISP Clean Pipe Services

With the rise of DDoS attacks, many Internet Service Providers (ISPs) have begun to offer anti-DDoS services often referred to as Clean Pipe. The crux of Clean Pipe protection is to let all incoming traffic pass through a scrubbing centre, where malicious traffic is identified and separated, permitting only legitimate traffic to reach the server.

Clean Pipe is a fairly popular protection method offered by many ISPs. In the past, ISPs commonly mitigate DDoS attacks using blackholing methods, where all traffic including legitimate traffic is dropped completely.

The strengths of ISP Clean Pipe are:

1. DDoS Protection can be activated as a value added service to a connectivity product from the ISP
2. No upgrades or equipment purchase is required
3. Scalable according to size of business (bandwidth size)
4. No longevity or maintenance costs

However, there are also some weaknesses with this method, namely:

1. ISPs typically do not have sufficient network capacity to protect against large DDoS attacks, often protecting only up to 20 Gbps. Protection is usually Layer 3/4 only, providing network protection and typically nothing more.
2. ISP-based solutions have limited in-house security expertise and tools that can be leveraged to respond to persistent and complex attacks that shift over time.
3. Many organizations purchase Internet connectivity from multiple ISPs, requiring them to also purchase a different Clean Pipe solution for each. While the cost of Clean Pipe solutions are low, the widely varying levels of services provided by different ISPs, such as dashboards and SLAs, adds not only complexity, but also incurs additional costs due to the management of multiple vendors.

Costs involved with ISP Clean Pipe Services

Should an organization satisfy the conditions required to benefit from an ISP Clean Pipe offering, and accept the limits of such a service, a clean pipe service could cost between 20% of the cost of the connectivity contract, or sometimes as much as the original contract itself, depending on the quality, features and the service level commitments that might or might not come with each service.

Third Party Security as a Service Providers

Security as a Service (SECaaS) can most easily be described as a cloud delivered model for outsourcing cybersecurity services. Much like Software as a Service (SaaS), SECaaS provides security services on a subscription basis hosted by cloud providers. SECaaS solutions have become increasingly popular for organizations and enterprises as a way to ease the burden of in-house security team's responsibilities, scale security needs as the business grows, and avoid the costs and maintenance of on-premise appliances.

Benefits of Security as a Service

1. Cost savings

One of the biggest benefits of a security as a service model is that it saves business money. A cloud delivered service is often pay-walled with several upgrade options so a business only pays for more services or extensions as and when they need them. Obviously, there are no longevity costs associated with this model

2. Manages the entire solution on your behalf as a service

SECaaS solutions can be scaled up or down as required and are provided on demand where and when you need them. This means that any uncertainty is removed when it comes to deployment or updates as everything is managed for you by the SECaaS provider and visible to you through a web-based dashboard.

3. Pure Opex model

SECaaS fully embraces the Opex model since it delivers a dependable stream of recurring monthly revenue that is beneficial to both their business operations and financial planning. They are also better able to leverage their expertise by providing a more consultative service to their customers, which is a win-win situation for both parties.

4. Fully managed service

Comprehensive and robust DDoS protection requires highly specialized skills and expertise. An accustomed SECaaS provider not only manages and monitors your protected assets but also provides a 24x7x365 security team capable of mitigating a multitude of DDoS threats, as well as new zero-day DDoS attacks.

Limitations of Security as a Service

Aside from the aforementioned benefits, SECaaS is however rather limited in scope in that it is often service specific, covering web services, custom applications and API etc. Therefore, for organizations seeking to protect their Operations Technology (OT) and other infrastructure, they would typically need to purchase multiple solutions, which introduces additional complexity and costs such as managing multiple vendors.

Cost of Engaging specialized security as a service providers

Delivered bespoked, customized managed security services can be truly effective for any organization that wishes to be well protected against cyber threats. The range of service available for each customer is limitless, as are the costs involved, which is usually subscription-based. There are also different pricing models to choose from - the more risk-averse users might opt for a solution that has lower monthly recurring costs, but are penalized with a much higher cost in the event of an event or incident. The less risk-averse user might also opt for a higher, more inclusive solution that covers the cost for any incidents. A good ballpark number to budget for such a type of solution would generally be between USD 50,000 per annum for a solution with limited coverage, to upper-end 5-figure monthly recurring fees for a more comprehensive solution.

Nexusguard’s Approach

Innovative Opex Model

DDoS Protection doesn’t have to be too complicated or expensive for your business. Nexusguard offers a fully managed security as-a-service, staffed with multilingual security experts who operate a round-the-clock SOC that protects your assets at a cost that makes financial sense.

Powered by built-in return on investment (ROI) and break-even point mechanisms, Nexusguard’s innovative Opex model absorbs all ongoing costs, replacing them with a simple monthly payment that makes complex cybersecurity protection both cost effective and more predictable for customers.

Structured and Transparent Costing

Nexusguard’s offerings are atypical to the common offerings in the market today. Despite this, our offerings are priced in the same familiar way that the market has grown accustomed to. It is structured to be simple, scalable and transparent;

Network Protection Costs - This is a flat, monthly recurring cost that a user pays to Nexusguard for an on-premise protection solution and includes the hardware, maintenance and 24x7 platform and service support necessary to protect the user’s infrastructure from attacks.

Cloud Protection Service Costs - Can be purchased as a standalone protection service that relies on the Nexusguard cloud, or as an add-on and supplement to the on-premise Network Protection to provide for an all-rounded protection. Like the Network Protection services - this is an outcome driven service and includes all that is necessary to deliver the desired outcome and is a fixed, monthly-recurring cost.

Managed Services - Allows a user to outsource the entire DDoS-related SOC duties to Nexusguard so that they can focus on their core business. With our Managed Services, the user pays a fixed monthly recurring fee that is based on the size of the deployment and covers all that an in-house SOC would be expected to deliver.

Specialized Cybersecurity Experts

Keeping staffing costs down is a key element in which Nexusguard excels when it comes to providing staffing and specialized cybersecurity skill sets. These costs are distributed across our entire client base, providing a shared service so that individual customers do not need to bear the cost alone.

You can also leverage Nexusguard’s SOC team of experts to provide you with continuous help and support with attack handling, incident management, reviewing security policies, round-the-clock monitoring of new attack vectors, escalations, and more.

Proprietary Cybersecurity Technology Stack

As a leading managed DDoS mitigation service provider, Nexusguard has built and owns its cybersecurity technology stack from the ground up apart from core network appliances such as routers and switches. This means that each of our scrubbing centers are infinitely scalable both horizontally and vertically. These scrubbing centers are strategically placed around the globe in nine countries.

Nexusguard's cybersecurity technology stack encompasses a wide range of tools, including:

- A comprehensive suite of mitigation tools to handle a multitude of cyber threats, including DDoS attacks
- A portal complete with visibility and analytics capabilities, allowing customers to view service status, DDoS attack information and more)
- Threat intelligence feeds: Up-to-the-minute data detailing constantly evolving attack patterns and indicators of compromise
- Network monitoring: software that logs and identifies network traffic, identifying suspicious events and escalating them for in-depth analysis
- Security orchestration, automation, and response (SOAR) platform: automation tools that help offload tasks involved in cybersecurity response, freeing up time for human analysts, thereby reducing response times
- Endpoint protection: software including device management and anti-DDoS tools to protect endpoint devices from attack

Nexusguard's core business revolves around building and continuously refining this toolset, the complexities of which are hidden from customers, who can simply enjoy a fully managed security as-a-service without having to worry about the heavy lifting involved, and at a cost that makes sound financial sense. Contact us to learn more.

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communications service providers to deliver DDoS protection solution as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

www.nexusguard.com

NEXUSGUARD®
DDoS Protection Made Simple