Check Point
SOFTWARE TECHNOLOGIES LTD.

DDoS RESPONSE GUIDE

HOW TO PROTECT YOURSELF FROM DDOS ATTACKS BEFORE, DURING, AND AFTER AN ATTACK

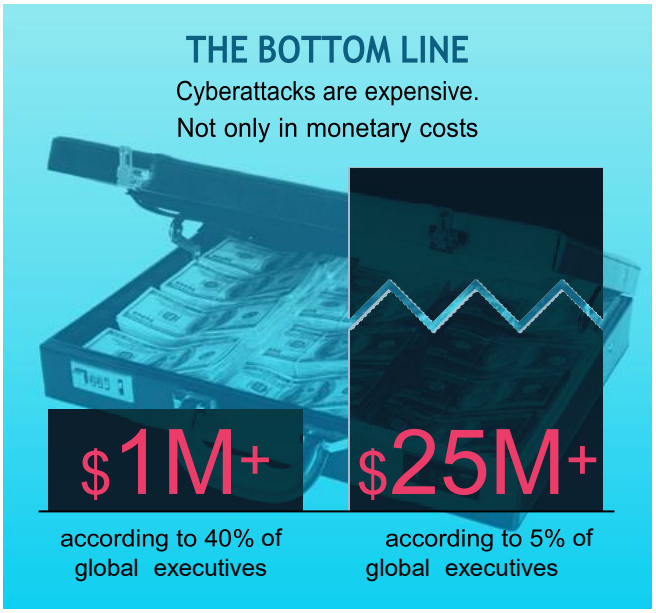
Check Point
SOFTWARE TECHNOLOGIES LTD.

INTRODUCTION

IT'S ALMOST AS INEVITABLE AS DEATH AND TAXES: SOMEWHERE, AT SOME POINT, YOU WILL BE THE TARGET OF A DDOS ATTACK.

DDoS attacks can flood your network with malicious traffic, bringing applications down and preventing legitimate users from accessing your services. They frequently result in lost sales, abandoned shopping carts, damage to reputation, and unhappy users. The reasons for DDoS attacks can vary from cybercrime to hacktivism to bad luck, but eventually someone will be out there to try and take you down.

The good news, however, is that there is plenty to be done about it. While you can't predict when an attack will happen, following the steps outlined in this guide will allow you to minimize the impact of the attack, recovery quickly, and ensure it doesn't happen again.



For more information: Tallying the Cost of a Cyberattack

The guide is divided into three parts:

- **BEFORE THE ATTACK**
  How to protect yourself before an attack.
  These steps can be taken even if you have never faced an attack before.

- **DURING AN ATTACK**
  What to do when you are attacked, and how to reduce its impact.

- **AFTER AN ATTACK**
  What to do after the attack is over, and how to make sure you are better prepared next time.

Check Point
SOFTWARE TECHNOLOGIES LTD.

PART I: PREPARING FOR AN ATTACK BEFORE IT HAPPENS

THE BEST TIME TO PREPARE FOR AN ATTACK IS BEFORE IT OCCURS. THESE STEPS WILL HELP YOU BE PREPARED IF ONE DOES OCCUR.

Step 1: Map Vulnerable Assets

The ancient Greeks said that knowing thyself is the beginning of wisdom. The same logic applies to protection against DDoS attacks. The first step to securing your assets against DDoS attacks is to know what assets there are to be secured. Begin by listing all external-facing assets which could be attacked. This list should include both physical and virtual assets:

- Physical locations & offices
- Data centers
- Servers
- Applications
- IP addresses and subnets
- Domains, sub-domains and specific FQDNs
- Mapping externally-facing assets will help you construct a threat surface and identify points of vulnerability

For more information: C-Suite Perspective: From Defense to Offense

Step 2: Assess Potential Damages

Determine what each asset is worth to properly allocate money/resources for protection. Keep in mind that some damages are direct, while other may be indirect. Some of the potential damages from a DDoS attack include:

- Direct loss of revenue – if your website or application is generating revenue directly on a regular basis, then any loss of availability will cause a direct loss of revenue. For example, if your website generates $1 million a day, then every hour of downtime, on average, will cause over $40,000 in damages.
- Loss in productivity – for organizations which rely on online services, such as email, scheduling, storage, CRM or databases, any loss of availability to any of these services will directly result in loss of productivity.
- SLA obligations – for applications and services that are bound by service commitments, any downtime can lead to breach of SLA, resulting in refunding customers for lost services, granting service credits, and even potentially facing lawsuits.
- Damage to brand – availability and the digital experience is increasingly tied to a company's brand. Any loss of availability as a result of a cyberattack, can directly impact a company's brand and reputation
- Twenty percent of organization's report experiencing reputation loss following a cyberattack, according to Radware© 2019-2020 GLOBAL APPLICATION & NETWORK SECURITY REPORT.
- Loss of customers – one of the biggest potential damages of a successful DDoS attack is loss of customers. This can be either direct loss (i.e., of customer who choose to abandon you as a result of a cyberattack) or indirect (i.e., of potential customers who are unable to reach you and lost business opportunities).

When evaluating potential damage of a DDoS attack, assess vulnerable assets individually. A DDoS attack against a customer-facing e-commerce site will have a different impact than an attack against a field office.

After you assess the risk to each asset, prioritize them according to risk and potential damages. This allows you to prioritize protection and determine which type of protection is required.

Source: C-Suite Perspectives: Trends in the Cyberattack Landscape, Security Threats and Business Impacts

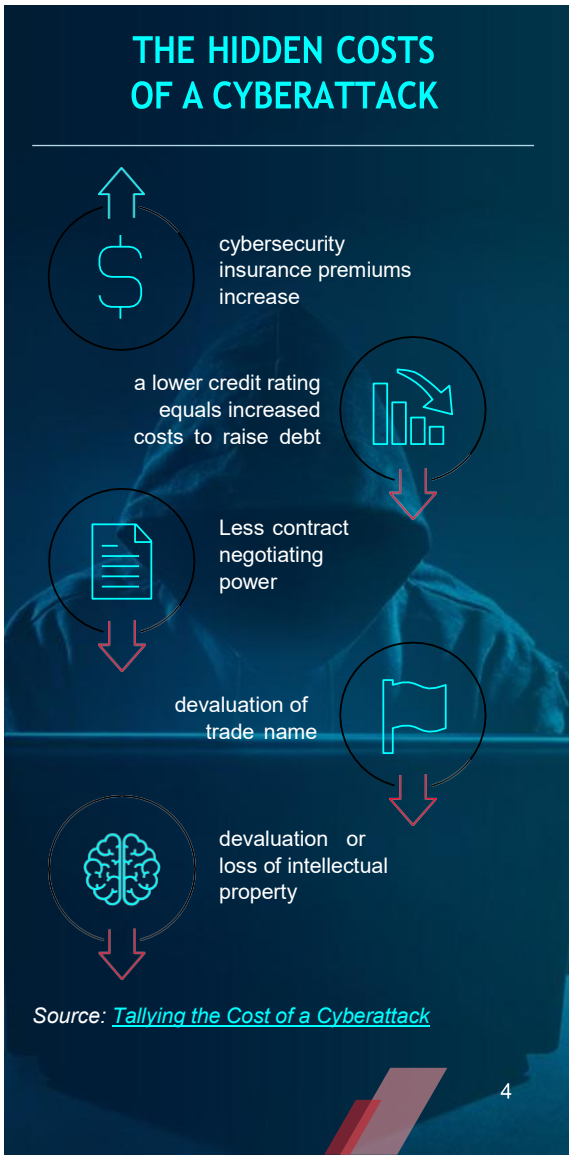
Step 3: Assign Responsibility

After you assign a monetary value to each asset, determine who is responsible for protecting them.

- Is DDoS the responsibility of the network administrator since it affects network performance?
- Is it the responsibility of application owner since it impacts application availability?
- Is it the responsibility of the business manager since it affects revenue?
- Is it the responsibility of the CISO because it is a type of cyberattack?

A surprising number of organizations don't have defined areas of responsibility regarding DDoS protection.

This can result in exposed assets because DDoS defenses "fall between the cracks."



Step 4: Set Up Detection Mechanisms

Once you've evaluated which assets require protection and assign responsibility, next establish detection and alert notifications when your organization is attacked. After all, you don't want your customers – or worse, your boss – to be the ones to tell you that your services and applications are offline.

Detection measures can be deployed either at the network or application level. Make sure these measures are configured so that they don't just detect attacks, but also alert you when something bad happens.

Step 5: Deploy a DDoS Protection Solution

Finally, after you've assessed your vulnerabilities and costs and established attack detection mechanisms, now is the time to deploy protection. This step is best accomplished before you are attacked, not when you're being assaulted.

DDoS protection is not a one-size-fits-all proposition, and there are many types of protection options based on the characteristics, risk and value of each individual asset.

On-demand cloud mitigation services are activated only once an attack is detected. They require the lowest overhead and are the lowest cost solution, but require traffic diversion for protection to activate. As a result, they are best suited for cost-sensitive customers and services that are not mission-critical, and customers who have never been (or are infrequently) attacked, but want a basic form of backup.

Always-on cloud services
Route all traffic through a cloud scrubbing center at all times. No diversion is required, but there is minor added latency to requests. This type of protection is best for mission-critical applications which cannot afford any downtime and organizations which are frequently attacked.

Hardware-based appliances provide advanced capabilities and fast-response of premise-based equipment. However, an appliance, on its own, is limited in its capacity. They are best used for service providers who are building their own scrubbing capabilities or in combination with a cloud service.

Hybrid DDoS protection combines the massive capacity of cloud services with the advanced capabilities and fast response of a hardware appliance. Hybrid protection is best for mission-critical and latency-sensitive services which require protection against volumetric, application-layer and encrypted traffic attacks and cannot afford any downtime at all.

PART II: DURING AN ATTACK

The steps in the first part of this guide outlined protective measures to take before you come under attack. However, there are also important measures you can take while you are under attack which will help minimize its impact – regardless of whether or not you already have DDoS protection deployed.

BY FOLLOWING THE STEPS OUTLINED BELOW YOU CAN MINIMIZE THE IMPACT OF AN ATTACK, ACCELERATE THE RECOVERY AND HELP PREVENT FUTURE ASSAULTS.

Step 1: Alert Key Stakeholders

It is often said that the first step in fixing a problem is recognizing that you have one. To that end, alert key stakeholders within the organization of the attack and steps that are being taken to mitigate it.

Examples of key stakeholders include the CISO, security operations center (SOC), IT director, operations managers, business managers of affected services, etc. Keep the alert concise but informative.

Key information should include:

- What is happening
- When the attack started
- Which assets (applications, services, servers, etc.) are being impacted
- Impact to users and customers
- What steps are being taken to mitigate the attack

Keep stakeholders informed as the attack develops and/or new information becomes available. Keeping key stakeholders informed avoids confusion, uncertainty, and panic and helps coordinate efforts to stop the attack.

Step 2: Notify Your Security Provider

You will also want to alert your security provider and initiate steps on their end to help mitigate the attack.

Your security provider could be your internet service provider (ISP), web hosting provider or a dedicated security service. Each vendor type has different capabilities and scope of service. Your ISP might help you minimize the amount of malicious network traffic reaching your network, whereas your web hosting provider might help you minimize application impact and scale your service accordingly. Likewise, security services will usually have dedicated tools for dealing with DDoS attacks.

Even if you don't already have a predefined agreement for service, or are not subscribed to their DDoS protection offering, you should nonetheless reach out to them to see how they can assist.

Step 3: Activate Countermeasures

If you have already have anti-DDoS countermeasures in place, activate them. One approach is to implement IP-based access control Lists (ACLs) to block all traffic coming from attack sources. This is accomplished at the network router level and can usually be accomplished by either your network team or your ISP. This is a useful approach if the attack is coming from a single source or a small number of attack sources. However, if the attack is coming from a large pool of IP address, this approach might not help.

If the target of the attack is an application or a web-based service, you could limit the number of concurrent application connections. This approach is known as rate-limiting and is frequently the favored approach by web hosting providers and CDNs. Note that this approach is prone to high degrees of false positives because it cannot distinguish between malicious and legitimate user traffic.

Dedicated DDoS protection tools will give you the widest coverage against DDoS attacks. DDoS protection measures can be deployed either as an appliance in your data center, as a cloud-based scrubbing service, or as a hybrid solution combining a hardware device and a cloud service.

Ideally, these countermeasures will initiate immediately when an attack is detected. However, in some cases, certain tools – such as out-of-path hardware devices or manually-activated, on-demand mitigation services – might require the customer to initiate them manually.

As mentioned previously, even without a dedicated security solution, most security services allow for emergency onboarding during an attack. This typically carries a hefty price, or an obligation to subscribe to the service later, however this might be necessary if you have no other option.

Step 4: Monitor Attack Progression

Throughout the attack, monitor the progression of the attack to see how it develops. This should include:

- What type of DDoS attack is it? Is it a network-level flood or an application-layer attack?
- What are the attack characteristics? How large is the attack, both in terms of bits-per-second and of packets-per-second?
- Is the attack coming from a single iP source or multiple sources? Can you identify them?
- How does the attack pattern look like? Is it a single sustained flood or is it a burst attack? Does it involve a single protocol or does it involve multiple attack vectors?
- Are the targets of the attack staying the same or are attackers changing their targets over time? Tracking attack progression will also help you tune your defenses to stop it.

Step 5: Assess Defense Performance

Finally, as the attack develops and countermeasures are activated, assess their effectiveness.

Your security vendor should provide a Service Level agreement (SLA) document which commits their service obligations. Ensure they're meeting their SLAs and whether there is an impact to your operations. If they're not, or not able to stop the attack whatsoever, now is the time to assess whether you need to make an emergency change to your service.

Check Point
SOFTWARE TECHNOLOGIES LTD.

PART III: AFTER THE ATTACK

RECOVERING FROM A DDOS ATTACK IS NOT SIMPLE, BUT ONCE AN ATTACK IS OVER, ASSESS THE IMPACT, EVALUATE YOUR DEFENSES AND PREPARE FOR THE NEXT TIME.

Step 1: Analyze the Attack

Once the attack is over, it's time to analyze it. Your service provider should provide most of this data. Internal network and application system logs should provide additional information. Key questions to ask will include:

- What assets were attacked? Did it target your entire network or specific servers/services?
- What were the attack characteristics? Was it a single sustained flood or did it employ sophisticated attack methods such as multi-vector attacks, dynamic IP spoofing or burst attacks?
- What attack protocols and patterns were used?
- What was the peak amount of network traffic, both in terms of data (bits per second) as well as requests (connections per seconds)?
- Did the attack impact the network layer and/or the application layer?
- Did the attack include encrypted traffic or protocols?
- How long did the attack last?

Gathering this information will help you get a full picture of what happened.

Step 2: Assess Damages

Now understand how the attack impacted you. This is key to understanding the "cost" of the attack, which influences how much you're willing to spend to prevent future assaults. Consider the following:

- Was the attack stopped or did it penetrate your defenses, either entirely or partially?
- Which services were impacted, to what extent and for how long?
- What was the net monetary damages (i.e., lost revenue, productivity time, etc.)?
- Were there any indirect damages, such as a devaluation or loss of intellectual property, increase in insurance premiums, damage to trade name, etc.?
- Did users experience any impact as a result of the attack, either due to the attack or due to defensive measures(false positives)?

Step 3: Identify Weak Spots

The next step after identifying damages is to identify any vulnerabilities in your defense.

- Did any attack/malicious traffic get through? If so, how much?
- Were there certain attack vectors that were more successful than others? More specifically, were certain attack patterns more successful than others?
- Were there any targeted resources (networks, servers, applications, etc.) that were impacted more than others? For example, were certain resources that were able to fend off the attack versus others?
- Did legitimate users experience any false positives? What was the ratio of legitimate traffic to malicious traffic that was stopped (or allowed to go through)?

By identifying weak spots, you should be able to understand what resources and/or services were impacted and why and which types of attacks were most effective. Another key element to look at is false positives. If your security solutions are deployed too broadly, this can lead to false positives. Identifying weak spots in your security allows you to address them in the next steps.

Step 4: Verify Security Vendor SLA

If you have a preexisting DDoS mitigation service in place, now is the time to check they met their SLA commitments. There are a number of key metrics that can verified and measured to ensure protection against DDoS attacks:

SLA METRIC	EXPLANATION
Time to Detect	How quickly was the DDoS attack detected from the time it began?
Time to Alert	How quickly did your security vendor alert you once they detected the attack?
Time to Initiate Diversion	How quickly was traffic diversion initiated once an attack was detected? (Note that this only applies to services based on an on-demand cloud service.)
Time to Mitigate	How quickly was the attack mitigated once it was detected?
Consistency of Mitigation	What was the ratio between malicious traffic that was allowed through versus malicious traffic that was blocked?
Service Availability	Were defenses available and online?

Any capable DDoS protection service will commit to all six of these metrics. A particularly important KPI is the 'time-to-detect' metric, since it measures how quickly the attack is detected, and thus, when does mitigation begin. Not including this metric effectively allows the DDoS service provider to define for themselves the time when mitigation should begin.

Another important metric is 'consistency of mitigation.' This metric tests the ratio of malicious traffic allowed through versus bad traffic that is stopped. Essentially, this measures the effectiveness of mitigation since it verifies that malicious traffic is actually being stopped and defense are not deployed ineffectively.

Step 5: Consider Upgrading Your DDoS Defenses

Once you have completed an assessment of the attack, the damages, any potential weak spots, and the effectiveness of your existing defenses, now is the time to evaluate if you should upgrade your protection?

An enterprise-grade DDoS protection service should provide you with technology, capacity and service guarantees to ensure full protection against any type of DDoS threat. Evaluate your analysis and ask yourself the following questions:

- Did my defenses stop the attack?
- Was all attack traffic stopped or did some get through?
- Were my users able to escape the impact of the attack, either directly or as false positives?
- Did my security vendor deliver all guaranteed services and meet contractual obligations?

If the answers to those questions is 'yes', then you are well protected. If the answer to one or more of these questions is 'no', you should consider alternatives.

Check Point
SOFTWARE TECHNOLOGIES LTD.

DDoS RESPONSE PLAN CHEAT SHEET

PHASE	ACTION ITEM	STATUS
BEFORE AN ATTACK	Map vulnerable assets	
	Assess potential damage	
	Assign responsibilities	
	Set up detection mechanisms	
	Deploy a DDoS protection solution	
DURING AN ATTACK	Alert key stakeholders	
	Notify your security provider	
	Activate countermeasures	
	Monitor attack progression	
	Assess DDoS mitigation performance	
AFTER AN ATTACK	Analyze the attack/ conduct a post mortem	
	Assess damages	
	Identify weak spots	
	Verify security vendor SLA	
	Consider upgrading your protection	

CHECK POINT DDOS PROTECTION

CHECK POINT PROVIDES COMPREHENSIVE PROTECTION FOR ANY TYPE OF ASSET AGAINST APPLICATION AND SERVICE DOWNTIME.

Check Point DDoS protections are based on its behavioral-based technologies and real-time attack signature algorithms, which can accurately detect and mitigate the largest, most sophisticated DDoS attacks. Check Point services can be deployed in any mode, including cloud-based protection (on-demand and always-on), appliance (physical or virtual), or hybrid (combining both cloud service and appliance), to suit any customer need or architecture.

Check Point services are complimented by a global scrubbing network with a worldwide footprint and massive capacity, managed and supported by its emergency response team (ERT) and backed by an industry-leading SLA. This helps ensure the service availability and business continuity of your services.

CONTACT US