MAZEBOLT

WHITEPAPER

DDoS Protection for AWS Hosted Applications

Learn industry best practices to build hybrid defense mechanisms that ensure DDoS protection for AWS hosted applications

Table of Contents

Index of Figures

Index of Tables

Proliferation of Cloud Application Adoption

Cloud adoption is becoming increasingly important for enterprises with CIOs and CTOs embracing it for business agility and competitive advantage. As a result, over the past decade, cloud adoption has witnessed phenomenal growth and risen from the status of `being adopted' to `the lifeline of enterprise architecture'. 451 Research says that 49% of organizations have adopted a cloud-first approach for deploying new applications. It predicts that the cloud computing market will reach $53.3 billion in 2021 – up from $28.1 billion in 2017.

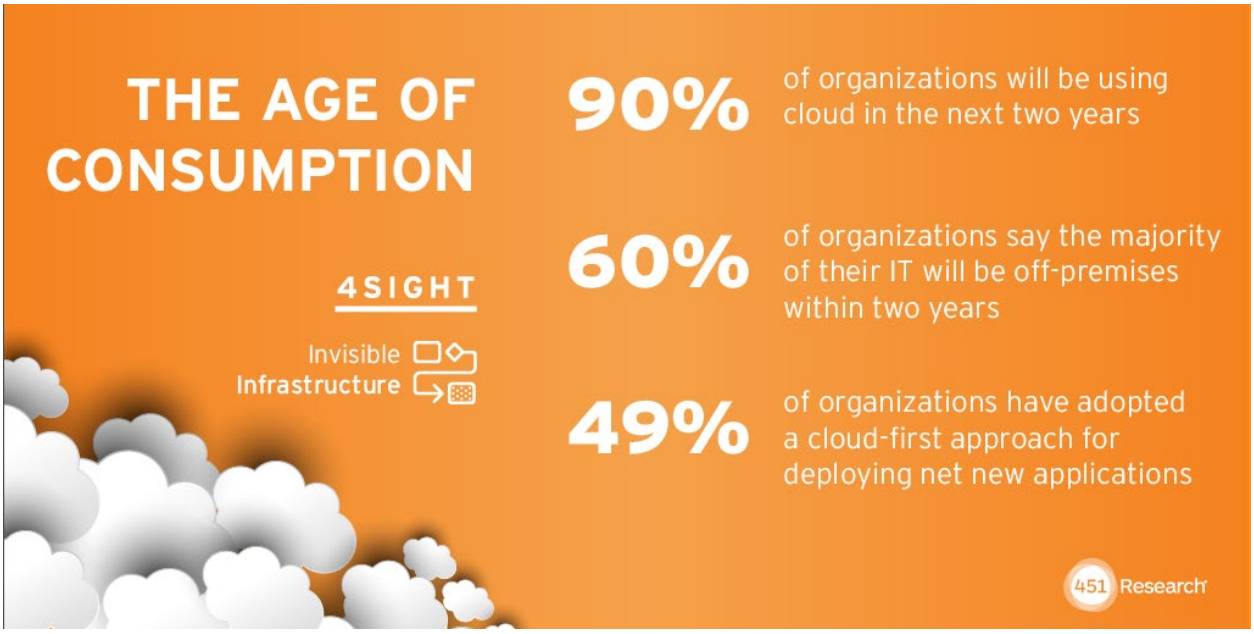


FIGURE 1: IMAGE SOURCE: 451 RESEARCH.COM

For CTOs, cloud adoption has already become the strategy. However, their challenges are related to the adoption process and the required steps within the same. Some critical decisive factors include **lift and shift,** on-premises versus cloud adoption, **hybrid, and multi-cloud adoption**. As far as enterprises are concerned there is no single universal rule regarding cloud adoption, and it remains unique to businesses and their specific existing applications as well as their strategic needs.

Broadly speaking, moving to the cloud helps enterprises to:

- Reduce IT overheads by nearly 50 percent
- Flexibility to scale IT operations up or down based on business requirements
- Improve IT to meet business needs by leveraging big-data and machine learning

Types of Cloud Computing

The three main types of cloud computing are:

Infrastructure as a Service which offers enterprises the flexibility to build the cloud strategy ground up. It provides networking, computers, and data storage to ensure maximum flexibility over IT resources.

Platform as a Service, as the name indicates, is a plug and play environment where the heavy-duty management of underlying infrastructure is taken away, and enterprises can focus on deployment, and management of applications.

Software as a Service is a preferred option for many enterprises that are looking to move to the cloud with the least amount of disruption. The service provider manages all the complexity and leaves the enterprise to only focus on how to run the business.

There are several large, medium and small enterprises, experiencing the benefits of cloud. In the recent past, Netflix is a classic example of cloud adoption for business growth. Netflix worked on detailing a cloud enabled, next-generation infrastructure. The journey was long, and it took the enterprise seven years to adopt cloud-native architecture. Today, even as the business grows, its IT infrastructure can scale to meet its needs, allowing its customers to experience **99% uptime while costs have been reduced to a fraction** of what it would have had to spend on on-premise infrastructure.

Challenges with Cloud Infrastructure – Gaps in Security

One of the key benefits cited for **cloud adoption is the anywhere anytime accessibility of secure data**. But how can enterprises reap the benefits of cloud technology while ensuring a secure environment for sensitive information? Data breaches, data loss, insecure access points, and DDoS attacks are some of the security vulnerabilities that accompany cloud adoption.

To delve deeper, requires looking at the various models of cloud adoption and the security challenges associated with each of them:

TABLE 1: SECURITY ISSUES WITH CLOUD ADOPTION

Security Issues with Cloud Adoption		
Software-as-a-service (SaaS)	Infrastructure-as-a-service (IaaS)	Private Cloud
● Lack of visibility into underlying data ● Data theft from malicious actors ● Incomplete control over secure data access ● Inability to prevent malicious insider data attacks ● **Advanced threats and attacks against the cloud application provider**	● Limited control of IT over cloud workloads ● Limited control over data accessibility ● Data theft from malicious actors ● **Advanced threats and attacks against the cloud application provider**	● Lack of consistent security controls spanning over traditional server and virtualized private cloud infrastructures ● Increasing complexity of infrastructure resulting in more time/effort for implementation and maintenance ● Incomplete visibility over security for a software-defined data center (e.g., virtual compute, network, storage) ● **Advanced threats and attacks**

Organizations should consider the recent evolution in attacks that extend beyond data as the center of risk. Malicious actors are conducting **hostile takeovers of computer resources** to mine cryptocurrency, and they are reusing those resources as an attack vector against other elements of the enterprise infrastructure and third parties.

When moving to the cloud, it is important to assess the enterprise ability to prevent theft and control access. Determining who can enter data into the cloud, tracking resource modifications to identify abnormal behaviors, securing and hardening orchestration tools, and adding network analysis of traffic as a potential signal of compromise are all quickly becoming standard measures in protecting cloud infrastructure deployments at scale.

Insidious DDoS Attacks on Cloud

As detailed in the earlier part of the whitepaper, cloud adoption comes with its own inherent security challenges. Keeping in mind the number of attacks as well as the malicious nature with which these attacks are conducted, DDoS as a security threat will require greater understanding.

Attackers typically look for a vulnerability in the overall network/software to disrupt services.

Some attacks deplete all the bandwidth or resources of the victims' systems.

Threat actors look for network vulnerabilities and use agents to launch attacks using spoofed IP's, resulting in denial of service. In the recent past, attackers have been using botnets to launch attacks. After establishing a botnet, the attacker directs the machines by sending updated instructions to each bot using remote control. A targeted IP address may receive requests from a multitude of bots, causing the targeted server or network to overflow capacity. This creates a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult. DDoS attacks affect all layers of the cloud, i.e. IaaS, PaaS or SaaS.

To summarize, DDoS attacks are currently a major threat, and are effective against cloud services. Even as cloud computing becomes more sophisticated, the attacks too grow more sophisticated and mitigation systems working on their own are always not completely effective. It is therefore necessary to build hybrid defense mechanisms which will be elaborated in the following chapters.

DDoS Protection for Cloud

DDoS mitigation using a cloud-based provider follows some distinct stages:

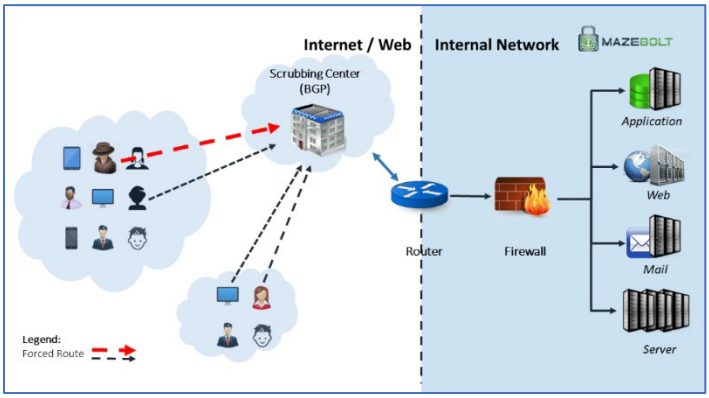
Detect – It is important for websites to distinguish legitimate traffic from illegitimate ones. For example, if there is a news published, the incoming traffic is obviously legitimate. The ability to scan and distinguish good traffic from bad is the first step

Respond – The mitigation system should respond to an incoming threat by segregating the bots from the good traffic and dropping the bots.

Routing – DDoS mitigation then routes the traffic by breaking it into manageable chunks preventing DDoS.

For cloud technology, scrubbing centers are a preferred option. Attacking traffic is scrubbed near the source, not at the destination. They are essentially data cleansers – they **review traffic** going through them and **remove packets** that **do not adhere to the rules** defined. They are the first source of **defense** for volumetric attacks, which send an enormous number of packets in an attempt to overwhelm existing network resources and saturate bandwidth.

FIGURE 2: ILLUSTRATION OF A CLOUD SCRUBBING SERVICE



Advantages of Cloud Scrubbing:

- **Ability to scale and match**: The reason cloud scrubbing is used against large volumetric attacks is because of the **ability to scale and match** even some of the **largest floods** exceeding 10Tbps.
- **Uses BGP**: Scrubbing centers generally use the **Border Gateway Protocol (BGP).** BGP routes traffic according to **rulesets, policies and metrics**. It forces all traffic to go through the scrubbing center, where the incoming attack traffic is cleaned before being forwarded to the organizations' IT infrastructure.
- **DNS or IP Target protection:** Scrubbing centers **protect** organizations against attackers **targeting** the name (**DNS** name) of the organization or the **numerical IP address**.

Disadvantages of Scrubbing Centers:

- **Application Layer Attack:** A scrubbing center's advantage is analyzing large volumes of traffic however it is generally less able to recognize application-layer attacks. This is because most Application Layer (Layer 7) traffic is encrypted, as well as scrubbing centers being cautious of applying incorrect settings resulting in false positives. This means that the ability of a scrubbing service to effectively mitigate malicious Application Layer traffic is highly dependent on whether it has the relevant decryption keys i.e. "SSL Visibility". and professional services engagement.
- **Expensive:** Scrubbing centers can have expensive subscription fees, especially with regards to always on scrubbing.
- **Sophisticated Attacks:** Sophisticated multi-layer attacks require a granular capability for detecting and blocking attacks which scrubbing centers are not always efficient at adapting to.

DDoS protection for AWS hosted applications

AWS Shield is a managed **Distributed Denial of Service (DDoS) protection service** that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency There are two tiers of AWS Shield - Standard and Advanced.

All AWS customers benefit from the automatic protection of AWS Shield Standard, at no additional charge. AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target websites or applications. When enterprises use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, they receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

In addition to the network and transport layer protections that come with Standard, AWS Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with AWS WAF, a web application firewall. AWS Shield Advanced also gives **24x7 access to the AWS DDoS Response Team (DRT) and protection against DDoS related spikes** in the Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator and Amazon Route 53 charges.

Benefits

- Seamless integration and deployment
- Customizable protection
- Managed Protection and Attack Visibility
- Cost Efficient

One Step Further – DDoS Mitigation for AWS with MazeBolt

Experience indicates that even with a combination of different DDoS mitigations postures, **network vulnerability remains at around 48%, as the underlying network is continuously changing and is dynamic in nature.** This is because all existing DDoS Mitigation solutions are based on fixed configuration. **Due to continuous changes in networks and additions of new services & infrastructure, DDoS mitigation** is eroding over time. Potential DDoS vulnerabilities are continuously being added.

To simplify, DDoS mitigation needs to be configured for the underlying network it's protecting. No network is the same, therefore no mitigation configuration is the same**. And when a network changes, these changes need to have an associated update in the DDoS mitigation configuration.**

The only way to ensure your DDoS mitigation is configured properly is by gaining **continuous visibility** of your DDoS mitigation Gap. This visibility complements the inherent shortcomings of DDoS mitigation and allows your DDoS mitigation vendor to fix the ongoing erosion in your DDoS mitigation posture to secure the integrity of your online services.

MazeBolt's DDoS RADAR™ is the only product that advances **any DDoS mitigation posture** by bringing visibility into the DDoS vulnerabilities real-time 24x7 without disrupting the production environment. **DDoS RADAR™** enables Continuous Feedback layer by identifying DDoS vulnerabilities, giving feedback to threat intelligence to take corrective actions and once the vulnerabilities are closed, it revalidates the fixes. The process cuts DDoS Risks from ongoing 48% to under 2% ongoing.

#	Service Aspect	Traditional DDoS Testing	DDoS RADAR™ (1 Year)
1.	Detect DDoS Risks BEFORE Attacks	Limited	Complete
2.	Disruption to ongoing operations	Yes	Zero impact to ongoing operations
3.	Requires Maintenance window	Yes – 3 hrs per test or 6 hrs yearly	No
4.	Annual hours of DDoS testing	3 hrs x 2	167 hrs. / Month | 2,000 hrs. / Year
5.	# DDoS attack vectors	Up to 19(*)	100+
6.	Coverage (Web facing IP Addresses)	Up to 4	Tier 1 = 50 IPs
7.	Vulnerability Re-validation	Once a year (**)	Near real time
8.	End to End Service	No.	20 hrs Professional Services Included.
9.	Consulting and Remediation Services	No.	Up to 20 hrs / Year
10.	Proactive DDoS Security	No.	Yes.

Table 2: Traditional DDoS Testing versus RADAR™

Benefits of DDoS RADAR™

- Anticipates DDoS exposures real-time before getting exploited

  Proactively identifies and closes DDoS vulnerabilities in real-time **to strengthen existing DDoS Mitigation defenses.**

- Keeps DDoS risk continuously and in real-time under 2% ongoing

  Through dashboards and reports. It provides a clear understanding of DDoS vulnerabilities from the initial validation, how they **were brought to under 2%,** and how they are continuously kept under 2%.

- Clear and concise dashboards and reporting

  Enterprises get **a clear report that shows the percentage of vulnerabilities open** in the underlying network. Percentage of detected vulnerabilities vs. percentage closed vulnerabilities. KPIs of monthly improvement and one dashboard that shows vulnerabilities open and fixed, across all data center sub-divisions or subsidiaries across the networks globally.

- Empowers in-house security staff & mitigation vendors

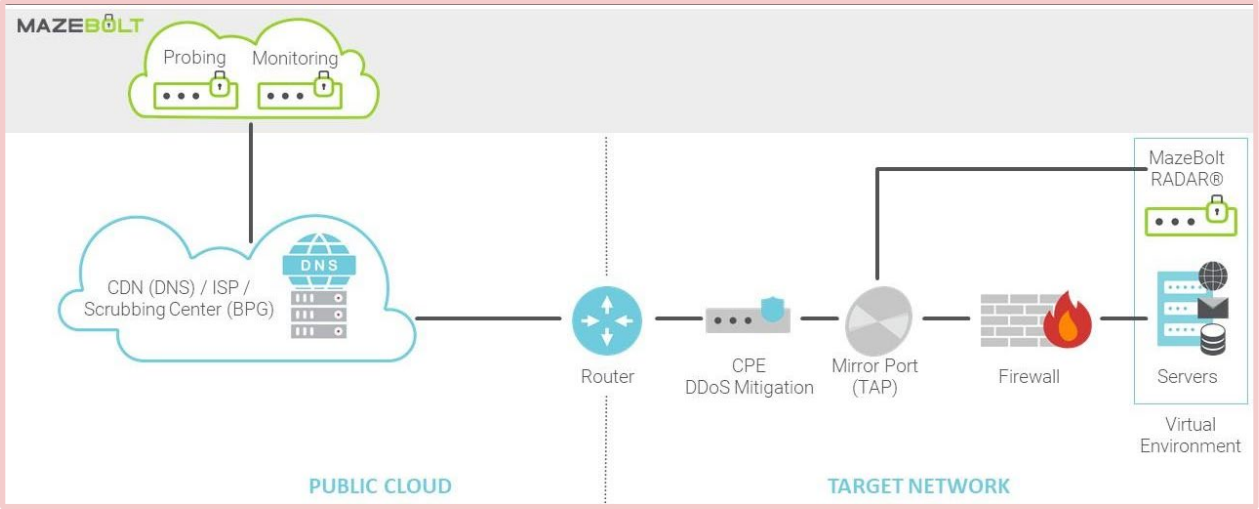
  In-house security staff can view exactly where the vulnerabilities are open in the network, and can easily communicate with their **DDoS Cloud vendor to immediately close the gap.** Once the Cloud vendor submits a report of closing the gap, with the help of DDoS RADAR™ the customer or vendor can re-validate immediately to ensure the vulnerability is closed

- Ensures that your network Is resilient to the latest, smart and sneakiest DDoS attacks

  DDoS RADAR™ has a library of DDoS Attack vectors and it is updated weekly as per the knowledge of new attack vectors that constantly evolve. This assures that all networks across the **global centers are validated against all the latest DDoS Attack vectors.**

MazeBolt helps mitigation to protect Cloud Applications

FIGURE 2: MAZEBOLT HELPS MITIGATION TO PROTECT CLOUD APPLICATIONS



About MazeBolt

MazeBolt is an innovation leader in cybersecurity and part of the DDoS mitigation space. Offering full DDoS risk detection and elimination and working with any mitigation system to provide end to end full coverage. Supporting organizations in avoiding downtime and closing DDoS vulnerabilities before an attack happens.

References

https://www.cloudflare.com/learning/ddos/ddos-mitigation/

https://itchronicles.com/cloud/the-evolution-of-cloud-computing-wheres-it-going-next/

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization

https://www.cdnetworks.com/cloud-security-blog/5-key-cloud-security-challenges/

https://www.gartner.com/smarterwithgartner/4-trends-impacting-cloud-adoption-in-2020/

https://www.sciencedirect.com/science/article/pii/S1877050915007541