Ongoing Vulnerability Testing for DDoS Protection

DDoS vulnerabilities remain the main reason DDoS attacks still succeed. Continuous DDoS testing and vulnerability identification proactively mitigates the risk of attack.

FROST & SULLIVAN VBOOK

CONTENTS

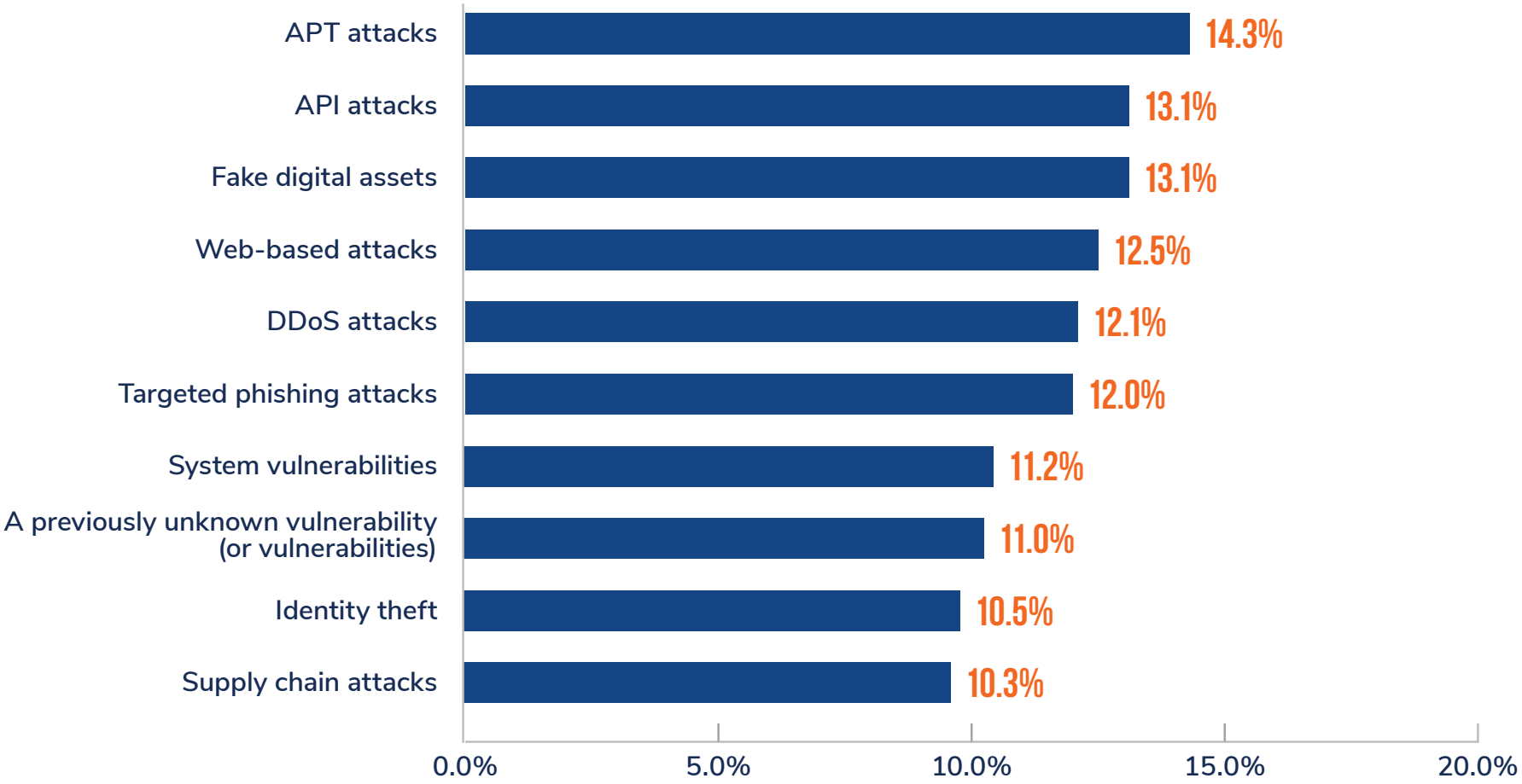
EXECUTIVE SUMMARY

- The surge in the frequency and sophistication of DDoS attacks can be attributed to:
  - Attackers understanding financial damages related to DDoS attacks and making extortion demands
  - The proliferation of Internet of Things (IoT) devices
  - The availability of affordable hacking toolkits, which now include some AI integration
  - Readily available DDoS-for-hire services
- Sophisticated DDoS attacks often outpace DDoS detection and mitigation solutions.
- Typically, intervention occurs after an attack begins and heavily relies on service level agreements (SLAs). This puts organizations at risk of incurring damaging downtime.
- Investing in proactive ongoing DDoS attack testing enhances overall cyber resilience and effectiveness.
- Organizations are realizing the need to add DDoS vulnerability management capabilities to supplement their current DDoS solutions.
- Industry compliance requirements create an urgent need for DDoS vulnerability testing for visibility and reporting.

Current Threat Landscape—Key Concerns

DDoS attacks continue to be one of the greatest security challenges.

Frost & Sullivan's Voice of the Enterprise Security Customer Survey 2023 shows that DDoS attacks are among the top 5 damaging cyberattacks that organizations experienced in 2023.



Why the Number of DDoS Attacks Is Increasing

The number of DDoS attacks continues to increase for several reasons:

- An inability of DDoS protection solutions (even premium solutions) to effectively thwart DDoS attacks automatically—primarily due to DDoS misconfigurations
- The wide range of motivations behind DDoS attacks, including service disruption, extortion, financial, or geopolitics
- The proliferation of IoT, connected devices, 5G, and ultra-fast networks, leading to an expanded attack surface
- The use of AI in orchestrating DDoS attacks, which adds another layer of complexity
- The lower entry barriers for launching DDoS attacks due to low-cost, matured toolkits and professional DDoS-as-a-Service
- DDoS extortion is an attractive method of financial gain for cybercriminals; they know how to inflict damage on even the best-protected systems

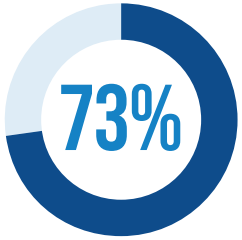
The Business Impact

DDoS attacks hurt a business in many ways, including:

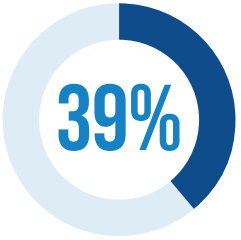
- Disruption of business continuity and the availability of services to customers, amounting to an average cost of $1.8 million per attack (Frost & Sullivan's report)
- Lost revenue, such as the cost of handling the DDoS attack, operational losses resolving the crisis, and the long-term business impact
- Increased regulatory scrutiny and fines following a successful attack are costly and burden organizations with endless reporting, audits and potential legal action
- Cyber insurance premium increases, rejection of claims related to damages, and even the inability to purchase cyber insurance at rates that make business sense
- Damage to the organization's reputation and trust, as downtime negatively affects the organization's customers, partners, and stakeholders
- Financial extortion attacks may continue until a ransom is paid to cybercriminals

What Drives Investment in DDoS Mitigation Solutions

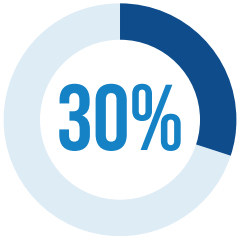
Frost & Sullivan's report indicates how many of the respondents to their survey were impacted by a DDoS attack:



were negatively impacted by a successful attack at least 11 times in 2023



were affected by the disruption of IT system availability



were affected by the loss of productivity

Investment in DDoS mitigation solutions is driven by:

- Companies across multiple verticals and sizes that have been targeted—the number of cybersecurity breaches is increasing globally, and DDoS attacks continue to succeed
- New regulatory compliance requirements for businesses operating in both the European Union and the United States
- Cyber insurance premiums are elastic and impacted by business continuity clauses
- The exponential rise in IoT, which has increased the DDoS attack surface

Companies Are Increasing Investment in DDoS Protection

According to Frost & Sullivan's survey, of respondents' current investment in network-based DDoS protection:

- **44%** use network-based DDoS protection
- **33%** are expected to add it during 2024

Of respondents' current investment in DDoS mitigation solutions to protect applications:

- **53%** use DDoS mitigation solutions to protect applications
- **39%** are expected to add it during 2024

The Gap Between Perception and Reality

Frost & Sullivan's Voice of the Enterprise Security Customer Survey 2023 found that:

- The **vast majority of organizations seem to be overconfident about their ability** to prevent cyberthreats and cyberattacks
- Most believe that they are not likely to be impacted by an attack in the next 12 months
  - **24%** said they have an **excellent** ability to prevent attacks
  - **47%** indicate that their ability to prevent cyberattacks is **very good**
- In reality, **most organizations are not secure**, as:
  - **59%** of organizations experienced between 11 and over 50 cyberattacks in 2023
  - **26%** experienced at least 1 to 10 attacks

Many Organizations Are Not Prepared

Frost & Sullivan finds that:

- Although many organizations have a DDoS protection solution in place, very few have a dedicated program for DDoS vulnerability testing in their strategies and deployment.
- This creates false confidence and overconfidence in current DDoS deployments.
- Organizations suffer from a lack of visibility into their true risk profile, leaving organizations at risk of DDoS attacks and often surprised when they have a damaging attack, whether on-premises or in the cloud.
- Many organizations follow traditional DDoS mitigation approaches:
  - They leave the mitigation responsibilities to either their cloud service providers (CSPs) or contracted principal vendors.
  - They believe that they invested enough in technologies to prevent DDoS attacks.
- However, many don't even know if such systems are enabled, configured, or will mitigate when a DDoS attack hits their online services.

Current DDoS Mitigation Approaches Are Unreliable

Each approach to DDoS mitigation has strengths and weaknesses, but all have one thing in common: without regular fine-tuning, security policies in protections will not be automated and vulnerabilities will creep in.

Scrubbing Centers

- Scrubbing centers offer robust defenses against volumetric DDoS attacks that are designed to protect upstream bandwidth.
- Scrubbing centers are often not truly multi-tenant when it comes to DDoS security policies, leaving a de-facto default policy in place for all.
- There are limitations of what can be mitigated in a scrubbing center due to the handling process of private SSL keys.

Content Delivery Networks (CDNs)

- CDNs are effective at blocking attacks aimed at the transport or network layers.
- However, they can face challenges when mitigating attacks targeting the application layer.
- The reliance on CDN caches for processing requests makes it harder to defend against Layer 7 attacks when faced with dynamic attacks.

continues on next page

Customer Premise Equipment (CPE)

- CPE-based solutions are great at detecting and responding to threats at both the network and application layers in real time, with no or little impact on latency.
- CPE requires that an upstream scrubbing center has mitigated most volumetric traffic, leaving internet links unsaturated.
- It often requires human intervention and heavy configuration to maximize the outcomes.

Web Application Firewalls (WAFs), Intrusion Prevention Systems (IPS), Firewalls, Load Balancers

- These can perform specific DDoS protection capabilities but are not designed specifically for these tasks—this makes them largely ineffective.
- For example, WAF can be utilized to defend against application layer DDoS attacks, but it fails to mitigate network-based attacks.
- IPS, firewalls, and load balancers are not designed to handle volumetric and application layer DDoS attacks.

Operational problems that cause organizations to be vulnerable to DDoS attacks include:

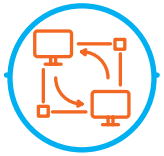
- The limitations of out-of-the-box solutions
- Lack of visibility and data to validate if solutions deployed are working
- Reactive reliance on SLAs with mitigation providers
- Degraded security and configuration drift over time
- The lack of identified vulnerabilities being patched on a regular basis

Out-of-the-Box (OOTB) DDoS Protections Are Less Effective

- Regardless of the deployment approach an organization takes—either a cloud-based mitigation service or CPE-based appliance—most organizations have de-facto OOTB protection for their DDoS defense strategy.
- While this deployment type offers some benefits, such as built-in security features, minimal intervention of the in-house team for configuration, and easy and quick set-ups, it comes with limitations.
- OOTB DDoS protections will not fully meet security requirements in more and more scenarios.

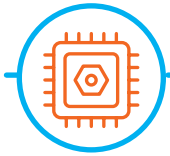
OOTB DDoS protections often come with generic settings built into mitigation devices or services normally designed to provide a baseline level of security for a wide range of users.

They don't provide granular initial policy customizations to meet each organization's specific needs.



As a result, the solutions are less effective and can't provide automated DDoS mitigation.

They can be particularly ineffective when it comes to the differences between legitimate traffic spikes and DDoS attacks—potentially leading to false positives or negatives.



DDoS attacks are evolving constantly with new techniques and vectors. OOTB solutions may not be able to detect and mitigate new types of attacks if capabilities and policies are not updated or customized.

Customizing allows organizations to update thresholds and rules that align with their traffic patterns and risk profile.

Organizations Are Exposed by a Lack of Visibility and Heavy Reliance on SLAs

Many tools designed to reroute or filter DDoS traffic fail to provide detailed insights into their performance, making it challenging to identify vulnerabilities. This impedes the ability to automate DDoS protection, as protection can only be automated after the DDoS attack traffic is detected and blocked.

Most companies working with DDoS mitigation services rely on SLAs, which typically focus on incident response rather than automated proactive prevention.

SLAs often do not tangibly account for detailed metrics (like potential attack types, size, distribution, duration, attack surface, and time to detect and mitigate in real-time). These are crucial for proactive defense and consequently, organizations are stuck in a reactive position.

Some providers may exaggerate their capabilities by promoting “zero-second downtime SLAs.” Such promises can be misleading and provide a false sense of security because these SLAs often apply only to attacks that have been identified automatically, leaving organizations exposed to the more complex, unconfigured, or unknown threats.

Ongoing Maintenance of Security Policies Is Key

Most organizations don't actively manage their DDoS security policies, but as DDoS attacks evolve, defense policies must be fine-tuned. Security configurations require constant review to ensure policies don't drift over time and automated DDoS protection is still possible.

If security policies become outdated, this can create:

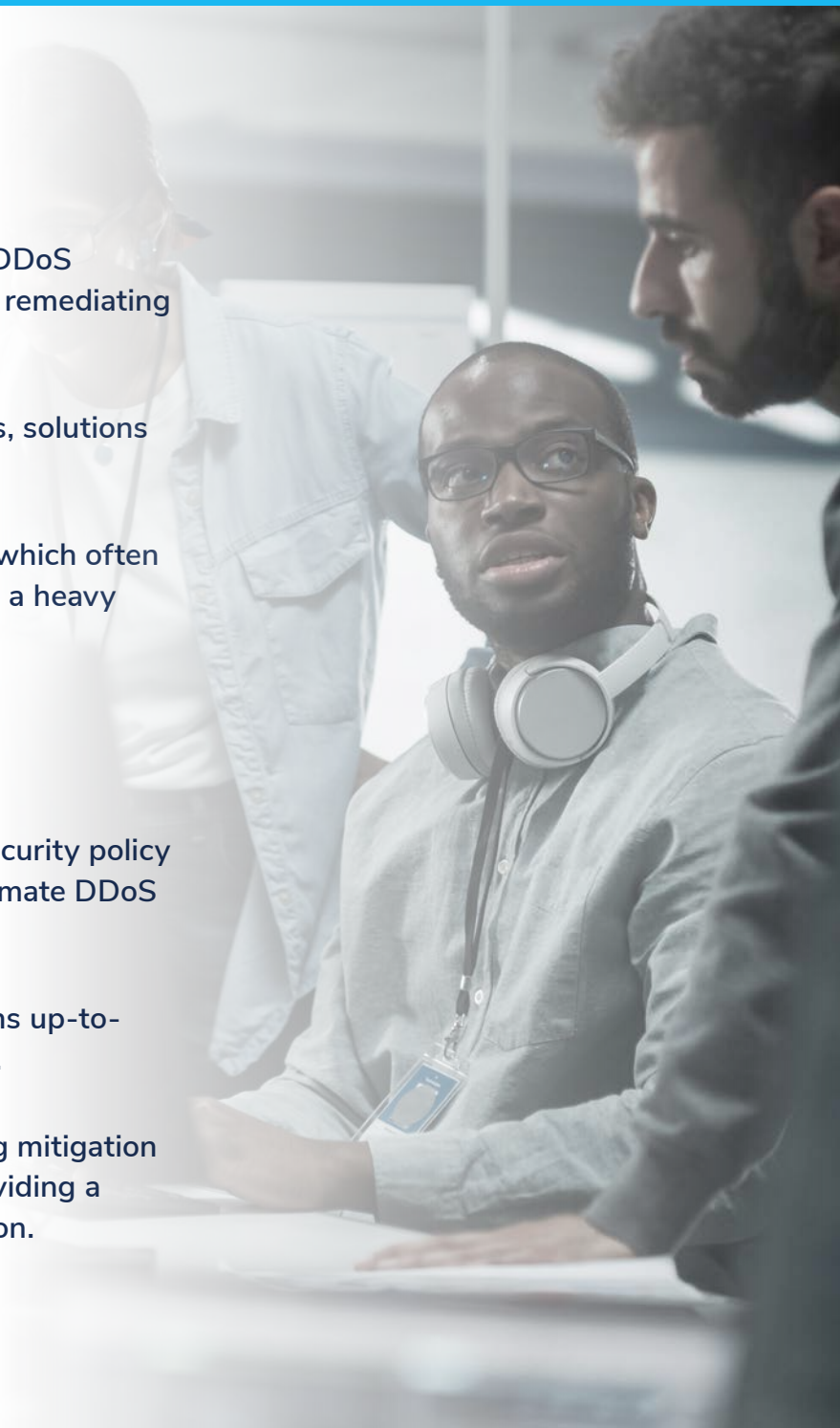
- New DDoS vulnerabilities
- Non-compliance with regulations and standards, which can have legal and financial ramifications and erode customer trust
- A false sense of security, which can lead to a damaging DDoS attack
- An inability to automate DDoS protection

An Urgent Call for Continuous DDoS Testing and Vulnerability Identification

- A proactive DDoS mitigation approach with continuous attack testing and vulnerability identification and validation enables organizations to:
  - **Utilize a DDoS testing system that requires no maintenance window**—a requirement for 100% attack surface coverage
  - **Identify, validate, prioritize, and manage** the remediation of potential security vulnerabilities, misconfigurations, and configuration drift in current DDoS solutions
  - **Ensure that automated DDoS mitigation solutions** in place are configured correctly and can effectively handle various DDoS attack types
  - **Assess the effectiveness and efficiency of automated DDoS protection** by enabling fully automated DDoS protection strategies that adapt to evolving attack techniques and variations—ensuring organizations' resilience against known and emerging threats over time
  - **Maximize ROI on DDoS protection investments while avoiding downtime and associated regulatory and financial damages**
- Continuous DDoS vulnerability testing is **not going to replace current DDoS mitigation solutions** already in place.
- Integration with existing mitigation solutions enables organizations to have a **complete and effective approach** to protecting against the ever-changing DDoS attack surface.

KEY TAKEAWAYS

- Vulnerabilities in DDoS protection solutions lead to damaging DDoS attacks - and the only way to prevent this is by identifying and remediating proactively, prior to the start of an attack.
- Despite significant investment in DDoS protection technologies, solutions are only partially automated and remain reactive.
- Organizations rely on traditional out-of-the-box deployments, which often lack policy customization, use static configurations, and lead to a heavy reliance on reactive SLAs.
- Current mitigation approaches do not provide visibility into the effectiveness of deployed solutions (automated mitigation).
- Over time, changes in IT systems and online services lead to security policy drift that results in vulnerabilities and blocks the ability to automate DDoS protection.
- Continuous testing keeps automated DDoS protection solutions up-to-date and resilient against the evolving nature of DDoS threats.
- The integration of continuous vulnerability testing with existing mitigation solutions is a crucial evolution in DDoS defense strategies, providing a more effective approach to DDoS attack visibility and prevention.



Featured Vendor—MazeBolt

About MazeBolt

MazeBolt RADAR™ is a patented DDoS Vulnerability Management solution. Using thousands of non-disruptive DDoS attack simulations and without affecting online services, it can identify and enable the remediation of vulnerabilities in deployed DDoS defenses. RADAR enables organizations and governments to maintain the uninterrupted business continuity of online services. Using RADAR's patented technology, enterprises have unparalleled visibility into their DDoS protection solutions so they can be confident that damaging DDoS attacks can be prevented - before they happen.

Read more at www.mazebolt.com.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➜

FROST & SULLIVAN