Choosing a DDoS Mitigation Strategy: How NDR Helps Identify and Contain DDoS Attempts

Key Takeaways

- Modern DDoS attacks are multi-vector, automated, and capable of record-breaking traffic volumes; traditional defenses alone are insufficient.
- A layered mitigation strategy (cloud, on-prem, WAF, automation) is critical for resilient protection across Layers 3–7.
- Detection speed determines impact, reactive, manual response models increase downtime risk.
- NDR strengthens DDoS defense through behavioral baselining, flow analytics, and anomaly detection.
- Real-time, automated containment reduces dwell time and prevents service disruption.
- Fidelis NDR delivers deep network visibility, encrypted traffic inspection, and context-driven correlation for accurate DDoS detection and response.

In today's digital battlefield, distributed denial-of-service (DDoS) attacks remain one of the most disruptive tactics used by threat actors. These attacks are not just about overwhelming servers they're about business downtime, customer dissatisfaction, and reputation loss.

A DDoS attack works by using multiple compromised systems, often a DDoS botnet, to flood a targeted server with malicious internet traffic, making an online service unavailable to legitimate users. With the increasing complexity of attack vectors, traditional DDoS mitigation strategies are no longer enough. Enterprises must adopt smarter, faster, and more adaptive ways to detect and mitigate DDoS attacks.

That's where Network Detection and Response (NDR) solutions step in. NDR doesn't just alert you to incoming attacks it actively monitors, correlates, and helps you contain them in real time. This blog explores how NDR platforms like Fidelis NDR enhance your DDoS protection strategy and what to consider when choosing the right DDoS mitigation approach for your organization.

What Is DDoS Mitigation and Why Does It Matter?

DDoS mitigation refers to a collection of processes and tools designed to detect, prevent, and respond to distributed denial-of-service attacks. These attacks flood a network, server, or application with internet traffic, exhausting server resources and making services unavailable.

Why DDoS Attacks Still Work:

- **Volume**
  Volumetric DDoS attacks can reach 3.8 Tbps, a record set in 2024, targeting bandwidth capacity.
- **Sophistication**
  Modern attacks strike multiple layers, including the application layer (Layer 7 DDoS mitigation) and protocol attacks at Layers 3–4.
- **Automation**
  Bots make attacks faster, smarter, and harder to block manually.

Without a proactive and layered mitigation plan, enterprises risk downtime, data loss, and long-

term reputational harm.

Types of DDoS Attacks

Understanding the types of DDoS attacks is essential before choosing a mitigation strategy. Most attacks fall into three categories:

1. **Volumetric Attacks** flood network bandwidth using techniques like UDP floods (which exploit the User Datagram Protocol's connectionless nature) and DNS amplification. These attacks aim to exhaust the capacity of your network infrastructure.
2. **Protocol Attacks** like SYN floods focus primarily on consuming the processing capacity of network equipment, firewalls, load balancers, and servers, by exploiting weaknesses in internet protocol handshakes rather than saturating bandwidth.
3. **Application Layer** DDoS Attacks target web servers at Layer 7, sending seemingly legitimate requests designed to exhaust server resources. They are harder to detect because attack traffic can mimic normal user behavior.

Types of DDoS Mitigation Strategies

Before we dive into NDR, it's important to understand the various types of DDoS mitigation strategies available:

1. Manual Mitigation

- Relies on security teams to detect and respond.
- Highly reactive, not scalable during multi-vector attacks.

2. Firewall and IPS/IDS Solutions

- Good for filtering known threats.
- Not always effective for volumetric attack mitigation or dynamic threats.
- IPS can help detect DDoS attacks, but often falls short in high-volume scenarios.

3. Web Application Firewalls (WAF)

- WAFs sit in front of web servers and filter malicious requests, allowing only legitimate traffic through.
- Particularly effective for application layer DDoS attacks targeting HTTP/HTTPS endpoints.

4. Cloud-Based DDoS Mitigation

- Routes legitimate traffic through scrubbing centers. Leverages content delivery networks (CDNs) to absorb volumetric attack traffic at scale.
- Scalable and effective for volumetric and burst attacks.
- May struggle with Layer 7 DDoS attacks or encrypted traffic.

5. On-Premise DDoS Protection

- Offers low-latency defense.
- Requires significant infrastructure investment.

6. Hybrid Solutions

- Combines cloud scalability with on-premise speed.
- Ideal for enterprises needing best DDoS mitigation across layers.

But even with these in place, gaps remain. That's where NDR for DDoS protection becomes critical.

Why NDR Is a Game-Changer in DDoS Mitigation

Network Detection and Response (NDR) takes DDoS mitigation to a new level by using behavioral analytics, flow monitoring, and machine learning to identify abnormal patterns and neutralize threats before they escalate.

Key Advantages of NDR in DDoS Mitigation:

- **Behavioral Detection of DDoS Attempts:**
  NDR uses baseline network behavior to flag anomalies helping you detect DDoS attacks that signature-based tools may miss.
- **Flow Monitoring for Detecting DDoS Attacks:**
  NDR tracks and analyzes legitimate traffic flows, identifying patterns indicative of slow drip attacks or volumetric floods. This includes continuous traffic monitoring across your entire network, not just the perimeter.
- **Real-Time Response:**
  Enables automated DDoS mitigation actions like blocking malicious IPs, isolating network segments, or triggering alerts.
- **Proactive Defense:**
  Goes beyond detection to offer proactive DDoS mitigation, reducing future attack dwell time. NDR also strengthens your overall security posture by correlating DDoS threats with other attack signals across your digital infrastructure.

Fidelis NDR: A Smarter Shield Against DDoS

Fidelis NDR stands apart with its deep visibility across hybrid environments, encrypted traffic inspection, and advanced behavioral analytics. Its platform supports:

- **High-fidelity DDoS detection** through continuous deep session inspection.
- **Automated response workflows** to contain volumetric and application-layer DDoS threats.
- **Intelligent context correlation** to reduce false positives and highlight real DDoS events.

Whether you're facing credential stuffing, UDP floods, SYN floods, or HTTP layer abuse, Fidelis NDR delivers robust distributed denial-of-service protection without slowing down your operations.

Discover how Fidelis Network delivers real-time prevention, not just detection

- Stop attacks earlier in the kill chain
- Gain deep visibility into lateral movement
- Automate threat prevention at scale

Download the Whitepaper

How to Choose a DDoS Mitigation Strategy

Choosing the right strategy isn't just about tools – it's about alignment with your business, risk tolerance, and network architecture. Here's What to Consider:

1. Nature of Your Assets

- Are your assets primarily cloud-based or hybrid?
- If cloud-native, cloud-based DDoS mitigation might suffice.
- For sensitive workloads, consider on-premise or hybrid setups with NDR visibility.

2. Traffic Volume and Complexity

- High-volume businesses should prepare for volumetric DDoS attack mitigation.
- Application-heavy platforms should prioritize Layer 7 DDoS mitigation techniques and web application firewalls to filter malicious requests targeting web servers.

3. Current Detection Capabilities

- Can your team identify a DDoS attack before damage occurs?

- Most organizations lack automated detection methods, a key reason to add NDR for DDoS protection.

4. Response Time and Automation

- Manual response is no longer viable for modern threats.
- Automated DDoS mitigation via NDR is now essential for 24/7 defense. A documented DDoS response plan paired with automation ensures business continuity even during multi-vector attacks.

5. Integration with Existing Security Stack

- Does your DDoS mitigation solution integrate with SIEM, SOAR, or endpoint detection?
- NDR vs traditional DDoS solutions shows NDR often excels due to its context-rich detection.

6. Service Level Agreement (SLA) Requirements

- If your SLA requires high availability, ensure your DDoS mitigation system can respond fast enough to maintain uptime, especially during sudden volumetric surges.

DDoS Attack Detection Techniques You Should Know

Understanding the methods behind detection is key to choosing between multiple DDoS mitigation strategies:

- **Threshold-based detection:** Triggers alerts when bandwidth exceeds expected limits.
- **Signature-based detection:** Looks for known attack traffic patterns (limited against new threats).
- **Machine learning detection:** Leverages anomaly detection to spot illegitimate traffic.
- **Application-layer monitoring:** Monitors HTTP/HTTPS traffic for abuse.

Fidelis NDR blends these with deep traffic inspection and metadata correlation, improving accuracy and speed.

Common DDoS Mitigation Methods in Practice

Let's break down some effective methods:

- **Rate limiting:** Controls the number of requests from each source, protecting server resources from being overwhelmed by a single source or botnet node
- **Geo-blocking:** Stops traffic from high-risk regions.
- **Blackholing:** Redirects malicious traffic to a null route.
- **Scrubbing centers:** Clean incoming traffic before it reaches the network.
- **Network segmentation:** Contains impact by isolating systems.
- **Anomaly-based filtering:** Removes traffic that deviates from typical patterns.

These are strengthened when paired with an NDR platform like Fidelis that understands legitimate traffic context and user intent.

Fidelis NDR vs Traditional DDoS Mitigation

Feature Traditional DDoS Tools Fidelis NDR Detection Method Signature/Volume-Based Behavioral + Contextual Response Manual/Rule-Based Automated + Correlated Scope Network Perimeter Lateral Movement + Deep Visibility Encrypted Traffic Analysis Limited Built-in Deep Session Inspection False Positives Higher Reduced via Correlation Web Application Firewall Integration Siloed Native Stack Correlation Threat Detection Coverage Perimeter Only Entire Network + DNS Servers

Fidelis NDR combines Machine Learning driven detection with deep understanding of attacker behavior, giving you a tactical edge.

Final Thoughts: Strengthen Your DDoS Defense with Fidelis NDR

In the age of advanced DDoS attacks, mitigation is no longer just about buying bigger firewalls or offloading traffic to the cloud. It’s about smarter detection, faster response, and better visibility across every layer of your digital infrastructure.

Fidelis NDR delivers all that and more. By combining behavioral analytics, machine learning, and contextual visibility, it empowers your security team to identify and contain DDoS attempts before they turn into full-blown outages.

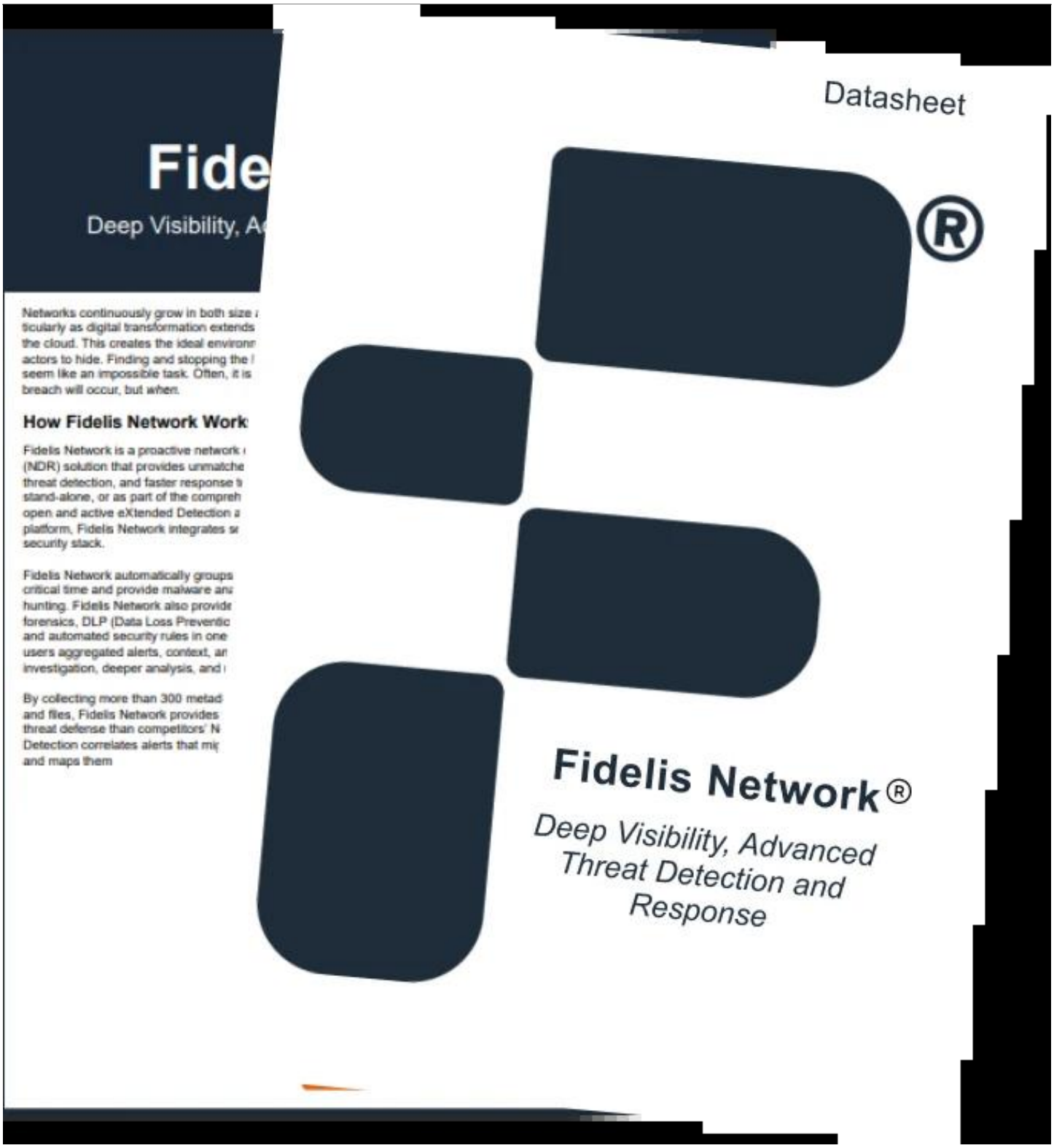
Whether you’re building out proactive DDoS mitigation, responding to a breach, or optimizing your network DDoS protection, Fidelis NDR has your back.

See how Fidelis NDR identifies threats others miss—with unmatched context and speed

- Behavioral and threat-based detection
- Flow monitoring and session reconstruction
- Response automation with high-fidelity alerts

Get the Datasheet

See Fidelis Network in Action



Frequently Ask Questions

What is a volumetric DDoS attack?

A volumetric DDoS attack floods a network or server with an overwhelming volume of traffic, exhausting bandwidth and infrastructure resources. These attacks aim to make services unavailable by saturating the target's capacity, often via UDP floods or DNS amplification, measured in gigabits or terabits per second. According to Cloudflare's 2024 DDoS Threat Report, hyper-volumetric attacks have now exceeded 3.8 Tbps.

How to mitigate DDoS attacks effectively?

To mitigate attacks, organizations should adopt a layered approach that includes:

- Network Detection and Response (NDR) for behavioral detection and real-time response
- Rate limiting and geo-blocking to reduce attack surface
- Cloud-based DDoS mitigation services for scalable defense
- Web application firewalls to block malicious requests at the application layer
- Automated response workflows to block malicious traffic at speed
- A DDoS response plan that covers escalation, SLA obligations, and business continuity

The key is to combine proactive monitoring with automated and scalable mitigation strategies.

How does DDoS mitigation work?

DDoS mitigation works by identifying malicious traffic patterns and diverting or blocking them before they impact service availability. This involves:

- Traffic analysis using flow data and behavioral baselines
- Filtering or scrubbing incoming traffic
- Rate controls and anomaly detection to isolate abnormal behavior

Modern tools like Fidelis NDR add an intelligence layer to this process by detecting DDoS attempts early and automating the containment response.

Do IPS help detect DDoS attacks?

Yes, Intrusion Prevention Systems (IPS) can help detect DDoS attacks, particularly known patterns or signature-based threats. However, they may struggle with:

- Volumetric or multi-vector attacks
- Encrypted traffic
- Zero-day DDoS tactics

For comprehensive protection, IPS should be combined with NDR solutions that provide behavioral and context-aware detection.

How to identify a DDoS attack in progress?

You can identify a DDoS attack by monitoring for signs such as:

- Sudden traffic spikes without corresponding business activity
- Network latency or timeouts
- Unresponsive applications or services

Using flow monitoring, behavioral analytics, and tools like NDR, you can detect anomalies in traffic patterns and correlate them to DDoS attack behavior for early response.