EMA™ PRISM Report – DDoS Mitigation Solutions

Summary Report Spotlighting F5

March 2025

By **Christopher M. Steffen, CISSP, CISA;** VP of Research
Information Security, Risk, and Compliance Management
Enterprise Management Associates (EMA)

Table of Contents

1 Executive Summary
1 Understanding DDoS Mitigation
2 Solutions the EMA PRISM Report Evaluates
3 The EMA PRISM Report
4 EMA PRISM Evaluation Overview
4 Evaluated Categories
4 Product and Functionality
4 Integrations and Operability
4 Strength and Maturity
5 Product and Functionality
5 Integrations and Operability
5 Strength and Maturity
6 Evaluation Methodology
6 Solution Evaluation
7 On the EMA PRISM Report
8 Solution Profile: F5

Executive Summary

Welcome to the Enterprise Management Associates™ (EMA) PRISM report on DDoS mitigation solutions. EMA is an industry-leading analyst firm specializing in a wide range of technology areas, including cybersecurity. We are dedicated to providing comprehensive research, analysis, and insights to help organizations make informed decisions about their technology investments.

The EMA PRISM report is a broad overview of a particular product set in a larger technology space. It is designed to provide practitioners and business leaders with a starting point for solutions in a common vertical. It uses publicly available information and sentiments, as well as the expertise of EMA researchers, to create an easy to understand and digestible overview of significant vendors/solutions in a space. It is NOT meant to be a detailed or thorough examination of the solutions in that vertical, nor does it include all of the solutions in that vertical.

The information presented in this report acts as a starting point for decision-makers and practitioners to evaluate the vendors and solutions that best align with your organization's needs and requirements.

Understanding DDoS Mitigation

Distributed denial of service (DDoS) mitigation solutions are essential tools for protecting online services and infrastructure from DDoS attacks. These attacks overwhelm a target with a flood of malicious traffic, rendering it unavailable to legitimate users. DDoS mitigation solutions work by identifying and filtering this malicious traffic, allowing legitimate traffic to pass through. They employ various techniques, including traffic analysis, rate limiting, and traffic redirection, to distinguish between legitimate and malicious requests. Modern solutions often leverage cloud-based scrubbing centers and sophisticated algorithms to adapt to evolving attack vectors.

The importance of DDoS mitigation cannot be overstated. DDoS attacks can cripple businesses, disrupt critical services, and damage brand reputation. They can lead to financial losses, customer dissatisfaction, and regulatory penalties. With the increasing frequency and sophistication of DDoS attacks, having a robust mitigation strategy is crucial for any organization that relies on online presence. Effective mitigation ensures business continuity, protects sensitive data, and maintains a positive user experience, even under attack. It allows organizations to focus on their core business operations without fear of disruption from malicious actors. Investing in DDoS mitigation is a proactive measure that safeguards against potential disruptions and ensures the availability and resilience of online services.

Solutions the EMA PRISM Report Evaluates

This EMA PRISM report evaluates the following DDoS mitigation solutions:

- A10 Defend DDoS Protection
- Akamai Prolexic
- Allot Smart NetProtect
- Cloudflare DDoS Protection
- Corero SmartWall ONE
- F5 Distributed Cloud DDoS Mitigation
- Fastly DDoS Protection
- Fortinet FortiDDoS
- Gcore DDoS Protection
- Imperva DDoS Protection
- Link11 DDoS Protection
- Lumen DDoS Hyper
- NETSCOUT Arbor Cloud DDoS Protection Services
- Nexusguard Bastions
- NSFOCUS Anti-DDoS System (ADS)
- Radware DefenseProX
- Tencent Cloud Anti-DDoS Advanced
- Vercara UltraDDoS Protect
- Verizon DDoS Shield

Note: DDoS mitigation solutions provided by various cloud vendors to use in conjunction with instances located on their cloud infrastructure were not evaluated as part of this report. Their exclusion is not an assessment of their quality (all are excellent solutions), and organizations using those cloud providers as part of their environments should still consider them. Those solutions are:

- Amazon Web Services (AWS) Shield
- Google Cloud Armor
- Microsoft Azure DDoS Protection

The EMA PRISM Report

The security solutions landscape is constantly evolving, and organizations face a daunting challenge: selecting the optimal security solutions to safeguard their digital assets. With a myriad of vendors and products vying for attention, it can be difficult to discern the truly significant offerings. The Enterprise Management Associates (EMA) PRISM report is a novel approach designed to illuminate the path, providing a comprehensive and objective evaluation of security solutions.

PRISM, an acronym for **PR**oduct and Functionality, **I**ntegrations and Operability, and **S**trength and **M**aturity, offers a structured framework for assessing security vendors and their offerings. By examining these key dimensions, the PRISM report provides a nuanced understanding of a solution's capabilities, limitations, and potential impact on an organization's security posture.

The **Product and Functionality** section evaluates the core capabilities of a security solution. It assesses the solution's ability to deliver on reported features compared with other solutions and identifies solutions that offer robust protection against a wide range of cyber threats.

The **Integrations and Operability** section explores the solution's compatibility with existing security infrastructure and its ease of use. It evaluates the solution's ability to integrate seamlessly with other security tools, its user-friendliness, and its ability to provide meaningful analytics and reporting while identifying solutions that can enhance an organization's overall security posture without adding unnecessary complexity.

The **Strength and Maturity** section examines the vendor's financial stability, market reputation, and product innovation. It also assesses the solution's total cost of ownership, time to value, and its long-term vision and roadmap, highlighting vendors that are committed to delivering innovative and effective security solutions.

The EMA PRISM report is a powerful tool for organizations seeking to make informed decisions about their IT and security investments. The report empowers organizations to select the best solutions and tools to protect their critical assets and mitigate risk.

EMA PRISM Evaluation Overview

The EMA PRISM report combines public user sentiment and analyst analysis with vendor feedback to develop a quick-glance profile of a vendor and its product strengths in a segment of the industry.

The PRISM report scoring methodology is crafted to address various aspects of vendor offerings, found in Product and Functionality, Integrations and Operability, and Strength and Maturity. EMA understands that every organization has unique needs and hopes that the information gathered for this report will enable organizations to tailor their vendor selection to best align with their specific requirements.

Evaluated Categories

Product and Functionality

- Real-Time Attack Mitigation
- Anomaly Detection and Monitoring
- Performance Impact
- Scalability

Integrations and Operability

- Analytics & Reporting
- Integrations and Compatibility
- Ease of Use & Management
- •End-User Support

Strength and Maturity

- Vendor Strength
- Time to Value
- Total Cost of Ownership
- Strategy and Vision

Product and Functionality

Real-Time Attack Mitigation

This section evaluates the solution's ability to automatically and immediately respond to DDoS attacks.

Anomaly Detection and Monitoring

This section evaluates the solution's ability to identify unusual traffic patterns and potential DDoS attacks before they escalate.

Performance Impact

This section evaluates the impact of the DDoS mitigation solution on the performance of protected applications and services during both normal operations and under attack.

Scalability

This section evaluates the solution's ability to handle increasing traffic volumes and adapt to the growing demands of the protected infrastructure.

Integrations and Operability

Analytics & Reporting

This section evaluates the quality and comprehensiveness of the solution's analytics and reporting capabilities. This includes the ability to generate meaningful insights, customize dashboards, and integrate with other security tools.

Ease of Use & Management

This section evaluates the user-friendliness and efficiency of the solution's management interface. This includes the ease of configuration, the automation of tasks, and the overall user experience.

Integrations and Compatibility

This section evaluates the solution's ability to integrate with other security tools and platforms. This includes the availability of APIs, the compatibility with different technologies, and the ease of integration.

End-User Support

This section evaluates the quality of the vendor's customer support. This includes response time, technical expertise, and the availability of training and documentation.

Strength and Maturity

Vendor Strength

This section evaluates the vendor's financial stability, market reputation, and commitment to security. This includes the vendor's track record, customer satisfaction, and product innovation.

Total Cost of Ownership

This section evaluates the overall cost of acquiring, deploying, and maintaining the solution. This includes licensing costs, hardware requirements, and operational overhead.

Time to Value

This section evaluates the speed at which the solution can be deployed and deliver value. This includes the ease of deployment, the time to initial protection, and the return on investment.

Product Strategy and Vision

This section evaluates the vendor's long-term vision for the product and its alignment with industry trends. This includes the product roadmap, future development plans, and the commitment to addressing emerging threats.

Evaluation Methodology

All vendors are evaluated based on publicly available data. Publicly reviewed data includes, but is not limited to:

- Vendor documentation and public knowledgebase
- Media and news articles
- Social media posts by users of the product/solution
- Questions and answers on public help forums, including vendor help forums and third-party help forums, such as StackExchange

In addition to evaluation based on publicly available data, EMA offers all selected vendors the chance to provide feedback regarding their solution profile before final publication.

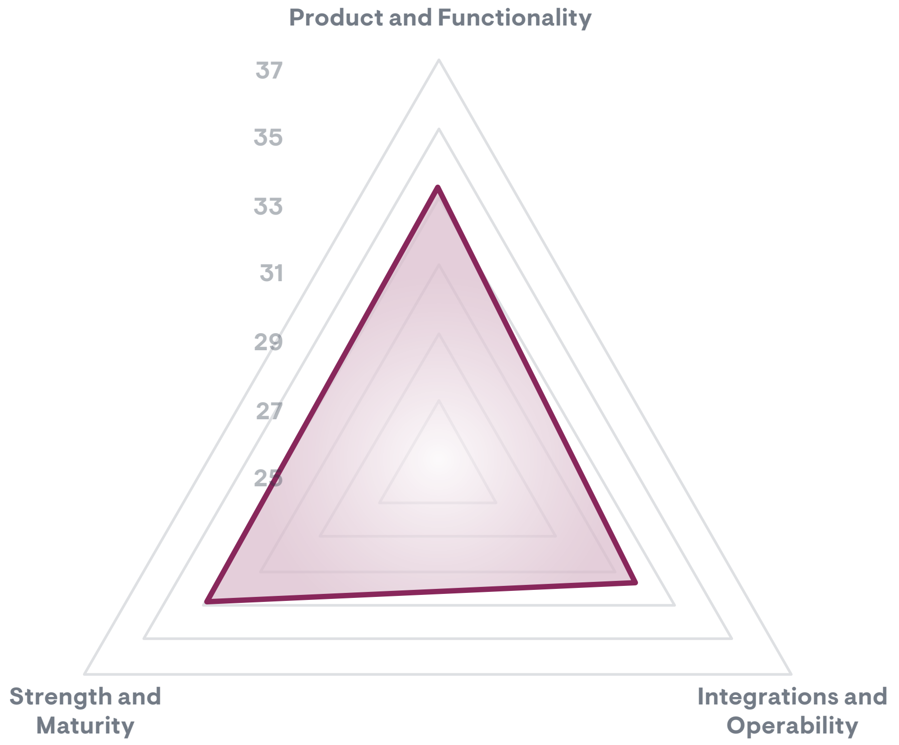
EMA evaluates all responses and scoring based on information within the last several years, utilizing the most up-to-date information possible. EMA evaluates each data point on a weighted scale, with some criteria weighing more heavily on final scoring.

Solution Evaluation

The EMA PRISM report showcases each vendor solution with a profile that highlights the evaluated categories of the solution, displayed on a spectrum chart. All points are rated on a weighted scale, with fractional points allowed. The overall vendor score is determined by taking the sum of all data points. An overview of the product and our findings will be included, as well as several bullet points highlighting the product's key differentiators.

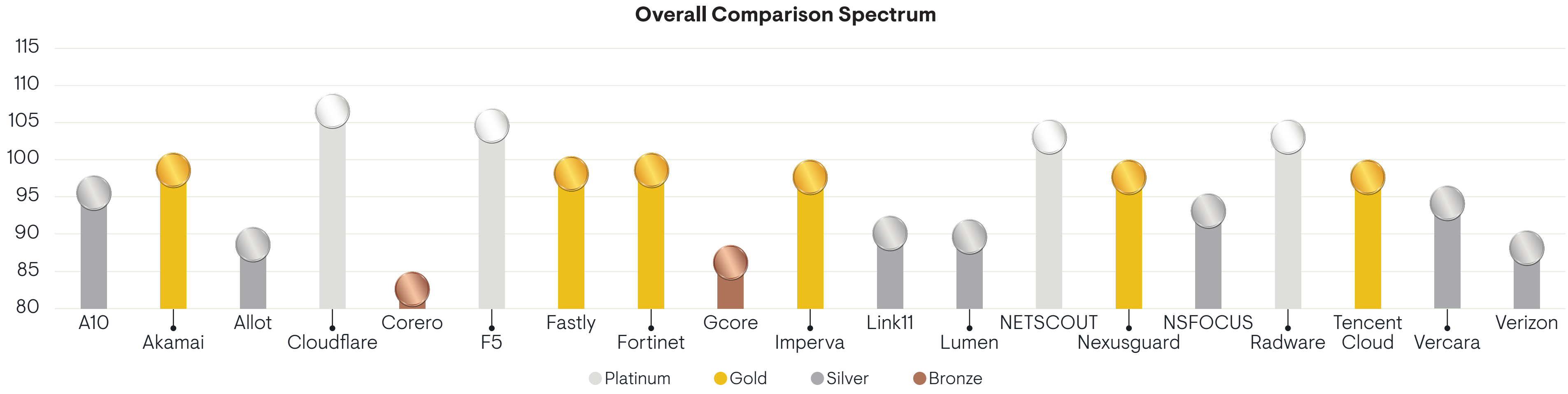
For the EMA PRISM report, each compared solution includes their overall spectrum score, as well as a category comparison spectrum.

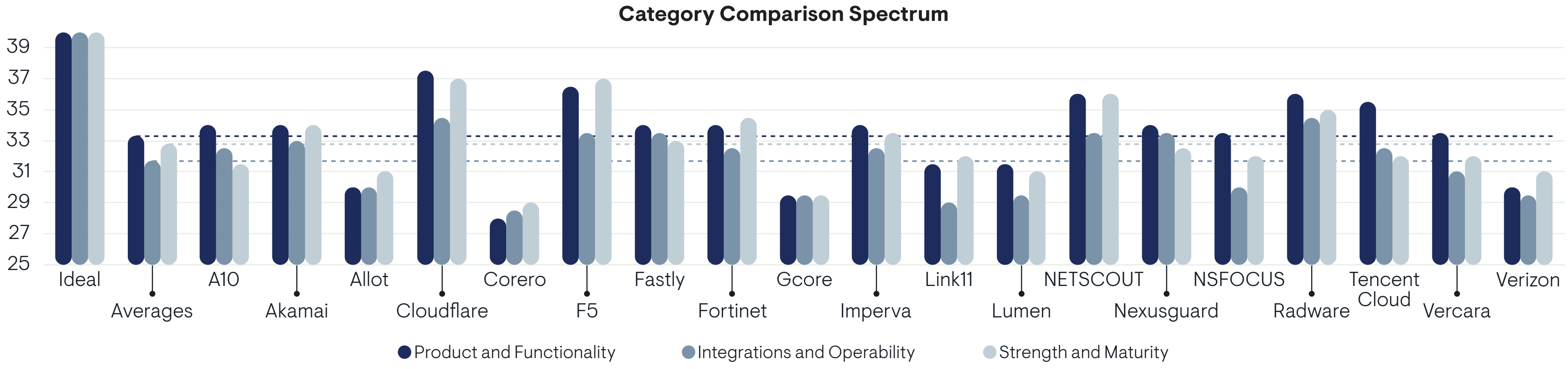
Product and Functionality	Platinum	40.00
Integrations and Operability	Platinum	40.00
Strength and Maturity	Platinum	40.00
Overall	**Platinum**	**120.00**



On the EMA PRISM Report

The EMA PRISM report defines the overall value of any solution as a spectrum of three characteristics: Product and Functionality, Integrations and Operability, and Strength and Maturity.



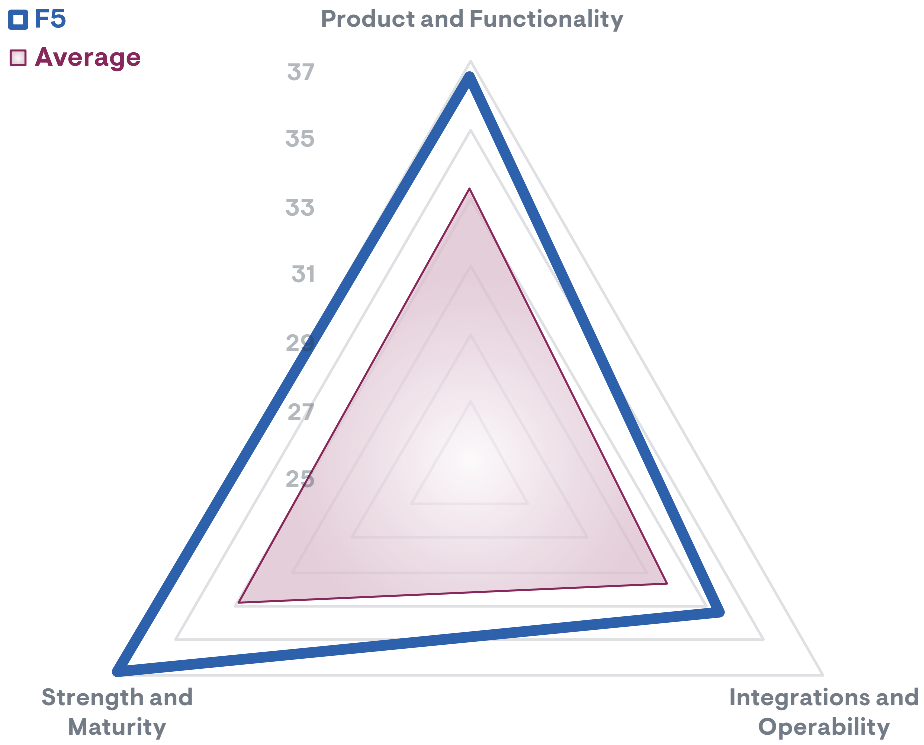


The F5 Distributed Cloud DDoS Mitigation is a robust solution designed to protect businesses from distributed denial of service attacks. This service leverages a global network to provide Layer 3 (L3) and Layer 7 (L7) attack mitigation, ensuring real-time protection against volumetric and application-layer threats. Its architecture provides unparalleled visibility and control over DDoS threats, integrating seamlessly with existing infrastructures to bolster resilience.

Product and Functionality	36.5	Platinum
Integrations and Operability	33.5	Gold
Strength and Maturity	37	Platinum
Overall Ranking	**107**	**Platinum**

Solution: **Distributed Cloud DDoS Mitigation**

Website:
https://www.f5.com/products/distributed-cloud-services/l3-and-l7-ddos-attack-mitigation



Key Capabilities

- Real-Time Attack Mitigation: This service neutralizes attacks instantaneously by employing automated responses and preestablished rules, ensuring that operations remain uninterrupted during an assault.
- Anomaly Detection and Monitoring: The service uses sophisticated algorithms to detect unusual traffic patterns and behaviors, enabling proactive identification of potential threats and fast response.
- Scalability: The architecture supports extensive scaling capabilities, managing spikes in traffic without service degradation, which is vital for businesses experiencing variable load patterns.

Key Differentiators

- Global Reach: With data centers and security nodes across multiple geographies, F5's solution mitigates attacks closer to their source, reducing latency and improving response time.
- Comprehensive Support for L3 and L7 Attacks: Unlike many solutions that focus solely on either Layer 3 or Layer 7 threats, F5 mitigates both, providing a holistic approach to DDoS security.
- Integrated Analytics & Reporting: The service includes advanced analytics capabilities that generate insightful reports on traffic behavior and attack vectors, helping businesses inform their security strategies.

Product and Functionality

The F5 Distributed Cloud DDoS Mitigation exemplifies maturity in both technology and vendor operations. It integrates advanced capabilities like real-time attack mitigation and anomaly detection into a cohesive platform designed for agility and resilience. The scalability of the solution allows customers to adapt to evolving traffic patterns without sacrificing performance. The comprehensive support for both L3 and L7 attacks is a strong feature, ensuring complete coverage against various threats. Moreover, F5's commitment to continuous improvement in response to the dynamic threat landscape further underscores the strength and maturity of the product.

Integrations and Operability

The ease of integration the F5 Distributed Cloud DDoS Mitigation offers stands out as a notable strength. Its compatibility with existing security ecosystems promotes efficient operability and seamless management of security protocols. The user-friendly interface simplifies administrative tasks, making it accessible even to those with limited technical expertise. Additionally, the analytics and reporting features provide significant insights, empowering organizations to fine-tune their defenses based on real data. Support from F5 ensures that users can leverage these capabilities effectively, underscoring the maturity of the product and its commitment to user satisfaction.

Strength and Maturity

F5's strong reputation and commitment to innovation support the Distributed Cloud DDoS Mitigation solution. With a clear strategy focused on evolving security needs, F5 has positioned this service as a cornerstone for organizations looking to enhance their cyber defenses. The low total cost of ownership, combined with rapid time to value, ensures a strong return on investment. This focus on long-term effectiveness and strategic growth solidifies F5's solution as a reliable choice for organizations seeking to mitigate DDoS threats efficiently and effectively.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com** 4496.030525-F5 Summary