A10 Networks Recognized for

2021

Customer Value Leadership

Global DDoS
Mitigation Industry

Excellence in Best Practices

FROST & SULLIVAN

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. A10 Networks excels in many of the criteria in the Global DDoS Mitigation space.

Internal Efficiency Enhances Value Delivered to Customers

A10 Networks provides secure application services with multiple solutions for digital transformation and digital resiliency, covering on-premises, multi-cloud, and edge-cloud environments. The company has more than 800 employees, and is present in more than 117 countries, catering to 7,000+ customers around the globe, including Microsoft, Uber, NTT Communications, LinkedIn, UCLA, Samsung, GE Healthcare, and more.

> *"A10 has invested in strengthening processes and increasing efficiency over the years, and is now in a position to extend the accrued benefits to its customers. Its ability to scale and automate DDoS protection solutions reflects a commitment to its target market of those who operate large data centers, from service providers, gaming, large enterprises, universities, and more."*
>
> ***- Deepali Sathe, Senior Industry Analyst***

A10 Networks' DDoS mitigation solution Thunder TPS (Threat Protection System) was first released in 2014, and has since acquired many notable clients. With the core purpose of 'Enabling a secure and available digital world', A10 Networks' mission statement articulates its target market, 'We enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness'. This focused approach—to work with large service providers and data center operators in building their own DDoS scrubbing centers—results in effective designing of solutions, and sets clients expectations across its

multiple product lines. For instance, Leaseweb, a cloud computing and web services company based in the Netherlands, has 17,500 clients across the globe, and it relies on A10 Thunder TPS to secure its own global infrastructure against DDoS attacks. It also provides managed protection services to its customers using intelligent automation for faster responses.

A10 Networks competes with providers of legacy DDoS mitigation solutions that have been in the market for much longer. In addition to service providers, it has many enterprise clients across many verticals. The company leverages long term client engagements with many marquee and satisfied customers to strengthen its foothold in the market. For instance, one of the largest software companies in the world was already using other A10 products and being aware of its ability to scale, became one of the first customers for A10's independent DDoS mitigation offering. The DDoS protection solution, with artificial intelligence (AI) and machine learning (ML), was developed in response to specific demands in addition to existing DDoS mitigation capabilities integrated with other solutions such as application delivery and carrier grade networking (enabling IPv4 preservation and IPv6 migration). A10 is leveraging AI and ML to enhance its DDoS automation capabilities to add value from detection to reporting, for the last couple of years. Customers can use varying degrees of automation depending on their requirements, ranging from basic alerts to enabling service providers to offer enhanced DDoS protection capabilities to their clients. Another critical application where advanced technologies are deployed is in the prevention of zero day attacks, a significant differentiator for A10. This helps identify anomalous packets and automatically creates filters to enhance security for clients against previously unknown attacks. The current sophisticated DDoS attacks meant to bring down large systems are more likely to launch multiple disruptive mechanisms, such as a TCP flood attack and a UDP attack, at the same time. A10's DDoS mitigation solution effectively scales to provide protection against multi-vector attacks.

Advanced protection is becoming table stakes in a post Mirai (2016) era, demonstrated by recent reports by large organizations, including Microsoft Azure and AWS, successfully mitigating complex multi-terabit, multi-vector, DDoS attacks. A10 describes this as the "protected and not protected", with enterprises reliant on cloud services choosing those services that have the necessary advanced protection to ensure zero, or the least, disruption to ensure competitive advantage and expected levels of service for customer retention.

Synergies across its portfolio facilitate its 'land and expand' approach, and client engagements commencing with application delivery and carrier grade networking solutions are likely to extend to a DDoS protection solution when demands are met satisfactorily. This value based growth strategy is much more effective than acquiring new clients every time, and is cost effective for the customer, by benefiting from not having to on-board a new vendor, providing familiar administration to reduce training, and speeds overall deployment . A10 also relies on channel partners for sales, including OEM partners to extend its reach in the market. Its near decade old partnership with Ericsson[1] is a testament to A10 Networks' ability to scale and work with large customers. Its ability to scale is extremely relevant in use cases involving new technology such as the launch of 5G and the accelerating rise of IoT, which will increase the vulnerability of systems and threat surface. Mobile service providers such as T-Mobile, AT&T, Verizon and others require ultra-reliable, low latency features, and automation and scalability will

[1] https://www.lightreading.com/ericsson-to-resell-a10/d/d-id/701193

become paramount to effective DDoS mitigation. Another example is SK Telecom in South Korea that deployed A10 Thunder CFW, which provides multiple security functions including DDoS protection, to scale and secure its 5G network[2].

A10 offers the results of its threat intelligence report periodically to customers and the public at no extra cost to help them understand the nature of attacks that they face. The deep-dive into one different topic for each edition helps relevant companies to draw additional insights. The research intelligence also provides information about potential DDoS weapons, systems that have been compromised, botnets and their probable future impact, given the millions of Internet of Things (IoT) devices that can be compromised. Other internal changes such as the appointment of a new CEO, Dhrupad Trivedi in 2019, engineering investments, and subsequent rebranding were focused on further accelerating a new phase of growth. The company harnesses the expertise of its employees and enables an environment to ensure that their innovative ideas and relevant initiatives are leveraged to enhance customer value. The engineering and customer support teams work closely together to facilitate innovation that is relevant to customer requirements. A10 has invested in strengthening processes and increasing efficiency over the years, and is now in a position to extend the accrued benefits to its customers. Its ability to scale and automate DDoS protection solutions reflects a commitment to its target market of large service providers.

> *"A deep understanding of customer challenges in dealing with DDoS mitigation, and highly relevant solutions helped A10 enhance the customer experience. It continues to invest in innovative techniques to become the preferred option for large companies looking to mitigate DDoS attacks on a global scale and become a more recognized brand, rather than a best kept secret."*
>
> ***- Deepali Sathe, Senior Industry Analyst***

Solutions to Mitigate Tangible Business Challenges Inevitably Improve Customer Experience

A10 Networks started off as a provider of high performance and customized DDoS mitigation appliances to large organizations. In response to changing market requirements and customer demands, the company has evolved and now provides software versions of its DDoS protection solutions. In addition to providing DDoS protection to data center operators, such as large enterprises, gaming, education, and more, A10 also helps service providers that are building their own DDoS scrubbing centers. Leaseweb proactively protects its global infrastructure from DDoS attacks and minimizes false positives using A10's innovations in intelligent automation, analytics based insights and AI/ML. It has succeeded in achieving a high 98% mitigation of DDoS attacks[3] in its scrubbing centers, which in turn helped it lower operating costs, reduce support tickets, and enhance responsiveness when under attack.

The DDoS scrubbing center solution goes beyond basic services to include provider and subscriber portals, observability and management, customers can protect their customers and offer a SaaS offering with best-in-class mitigation.

The pandemic has changed the way organizations conduct business and the unprecedented increase in remote work has also led to a proliferation of risks and spotlighted the need for digital resiliency. While

[2] https://www.a10networks.com/wp-content/uploads/A10-CS-80201-EN.pdf
[3] https://www.a10networks.com/wp-content/uploads/A10-CS-80193-EN.pdf

no industry was left unaffected by the pandemic, the responses varied depending on each organization's level of digital transformation, resiliency and preparedness. For instance, the education sector, which has had to move to online delivery in a short span of time and was largely underprepared for the transition, is a key client segment. A10's proven DDoS protection capabilities led to multiple deals in the education sector globally. A university a Germany and another in Taiwan were converted to clients since the pandemic. The fact that 7 of the top 12 leading gaming companies indicate that A10 has significant presence in this industry —one that is highly susceptible to DDoS attacks – is a telling metric of how that industry perceives A10 capabilities, and in a relatively short time.

Given that a DDoS attack has the potential to significantly affect business continuity, a rapid response to contain an attack is critical. In addition to supporting customers 24/7/365, A10 differentiates by providing a dedicated support hotline to experts assigned to its DDoS security incident response team (DSIRT) for its Thunder TPS customers, above and beyond regular support services. In the event of disruption despite the presence of a DDoS solution, DSIRT helps to diagnose, interpret, and stop an attack. Most companies struggle with adequately staffing their IT and security teams and are unlikely to have experts to cater to many different devices and protocols, making this an important resource, especially in critical "wartime" moments when under attack. Similarly, the benefits of automation go beyond alerts, and highlighting anomalies to also include improving the productivity of the support staff. Manual intervention at scale is most likely to fail and the benefit of AI and ML automatically creating signatures for unknown attacks, and preventing zero day attacks enhances customer experience and satisfaction.

Customer feedback is actively sought and A10 introduces incremental enhancements in response to requests from clients. Some of A10's significant product enhancements include the aforementioned Zero-day Automated Protection (ZAP) which brings AI/ML techniques to pinpoint attacks automatically for customers, but other specific enhancements can specifically benefit certain verticals, for example the unique packet watermarking feature for gaming, or the subscriber portal, which helps service providers and MSSP clients to interact effectively with their customers to share data insights, is the result of its efforts to align to client requirements. Customers have cited enhanced network performance by 75%, a positive return on investment (ROI) within 3 months, product reliability, scalability, and a 50-74% reduction in OPEX among many others reasons for high satisfaction. A deep understanding of customer challenges in dealing with DDoS mitigation, modern automated protection techniques and highly relevant solutions have helped A10 greatly enhance customer experience. It continues to invest in efforts to become the preferred option for large companies looking to mitigate DDoS attacks on a global scale and become a more recognized brand.

Conclusion

A10 Networks has a clear vision and strategy in terms of its target market and is continuously striving to ensure that it develops capabilities that can help with specific DDoS mitigation requirements. Over the years, building on inputs from clients and on its own research, it has evolved into a DDoS mitigation provider that excels is adding value via automation and scalability for digital resiliency. The use of AI and ML to augment its offerings and future proofing solutions has led large organizations to work with A10. Helping clients deal with multi-vector, zero day, and other sophisticated attacks, A10 has established itself in the market as a leading contender.

For its strong overall performance, A10 Networks is recognized with Frost & Sullivan's 2021 Global Customer Value Leadership Award in the DDoS mitigation industry.

What You Need to Know about the Customer Value Leadership Recognition

Frost & Sullivan's Customer Value Leadership Award recognizes the company that offers products or services customers find superior for the overall price, performance, and quality.

Best Practices Award Analysis

For the Customer Value Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly own the company's product or service and have a positive experience throughout the life of the product or service

Customer Service Experience: Customer service is accessible, fast, stress-free, and high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

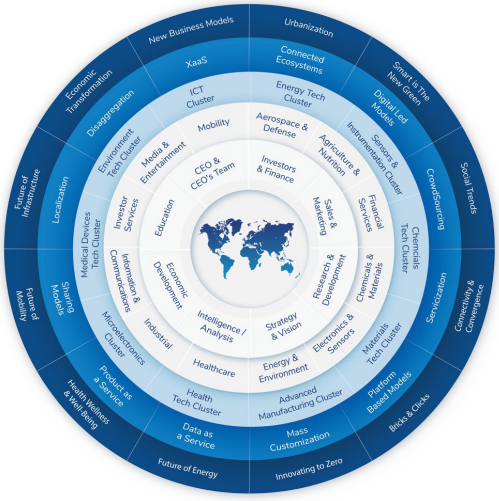
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)