A10 Networks, Inc.
Form 10-K
March 11, 2015

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 10-K

(Mark One)

x ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2014

OR

¨ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

Commission file number: 001-36343

A10 NETWORKS, INC.
(Exact Name of Registrant as Specified in its Charter)

Delaware	20-1446869
(State or Other Jurisdiction of Incorporation or Organization)	(I.R.S. Employer Identification No.)

3 West Plumeria Drive, San Jose, California 95134
(Address of Principal Executive Offices, including zip code)

(408) 325-8668
(Registrant's Telephone Number, Including Area Code)

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange on Which Registered
Common Stock, $.00001 Par Value	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act:
None.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.
Yes ¨ No x

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act.
Yes ¨ No x

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was

required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes x No ¨

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes x No ¨

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant’s knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K, or any amendment to this Form 10-K. ¨

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of “large accelerated filer,” “accelerated filer” and “smaller reporting company” in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer	¨		Accelerated filer	¨
Non-accelerated filer	x	(Do not check if a smaller reporting company)	Smaller reporting company	¨

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Act). Yes ¨ No x

The aggregate market value of the registrant's common stock held by non-affiliates of the registrant as of June 30, 2014 (the last business day of the registrant's most recently completed second fiscal quarter) was approximately $465.2 million, based upon the closing sale price of such stock on the New York Stock Exchange. For purposes of this disclosure, shares of
common stock held or controlled by executive officers and directors of the registrant and by persons who hold more than 5% of the outstanding shares of common stock have been treated as shares held by affiliates. However, such treatment should not be construed as an admission that any such person is an “affiliate” of the registrant. The registrant has no non-voting
common equity.

As of February 27, 2015 the number of outstanding shares of the registrant’s common stock, par value $0.00001 per share, was 61,544,312.

DOCUMENTS INCORPORATED BY REFERENCE

As noted herein, the information called for by Part III is incorporated by reference to specified portions of the Registrant's definitive proxy statement to be filed in conjunction with the Registrant's 2015 Annual Meeting of Stockholders, which is expected to be filed not later than 120 days after the Registrant's fiscal year ended December 31, 2014.

A10 NETWORKS, INC.
ANNUAL REPORT ON FORM 10-K
FOR THE YEAR ENDED DECEMBER 31, 2014
TABLE OF CONTENTS

FORWARD LOOKING STATEMENTS

This Annual Report on Form 10-K contains forward looking statements made pursuant to the provisions of Section 21E of the Securities Exchange Act of 1934. These forward looking statements are based on management's current expectations and beliefs, including estimates and projections about our industry. The following discussion and analysis contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. The words “believe,” “may,” “will,” “potentially,” “estimate,” “continue,” “anticipate,” “intend,” “could,” “would,” “pro “expect,” and similar expressions that convey uncertainty of future events or outcomes are intended to identify forward-looking statements.

These forward-looking statements include, but are not limited to, statements concerning the following:

- our ability to maintain an adequate rate of revenue growth;
- our business plan and our ability to effectively manage our growth;
- costs associated with defending intellectual property infringement and other claims;
- our ability to attract and retain end-customers;
- our ability to further penetrate our existing customer base;
- our ability to displace existing products in established markets;
- our ability to expand our leadership position in next-generation application delivery and server load balancing solutions;
- our ability to timely and effectively scale and adapt our existing technology;
- our ability to innovate new products and bring them to market in a timely manner;
- our ability to expand internationally;
- the effects of increased competition in our market and our ability to compete effectively;
- the effects of seasonal trends on our results of operations;
- our expectations concerning relationships with third parties;
- the attraction and retention of qualified employees and key personnel;
- our ability to maintain, protect, and enhance our brand and intellectual property; and
- future acquisitions of or investments in complementary companies, products, services or technologies.

These forward-looking statements are subject to a number of risks, uncertainties, and assumptions, including those described in Item 1A Risk Factors and elsewhere in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment, and new risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties, and assumptions, the forward-looking events and circumstances discussed in this Annual Report on Form 10-K may not occur and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements.

The forward-looking statements in this report speak only as of the time they are made and do not necessarily reflect our outlook at any other point in time. We undertake no obligation to update publicly any forward-looking statements, whether as a result of new information, future event, or for any other reason. However, readers should carefully review the risk factors set forth in other reports or documents we file from time to time with the Securities and Exchange Commission.

As used herein, “A10 Networks,” the “Company,” “we,” “our,” and similar terms include A10 Networks, Inc. and its subsidiaries, unless the context indicates otherwise.

PART I.

BUSINESS

Overview

We are a leading provider of advanced application networking technologies. Our solutions enable enterprises, service providers, Web giants and government organizations to accelerate, secure and optimize the performance of their data center applications and networks. Our products are built on our Advanced Core Operating System, or ACOS which is designed to enable our products to deliver substantially greater performance and security relative to prior generation application networking products. Our software based ACOS architecture also provides the flexibility that enables us to expand our business to offer additional products to solve a growing array of networking and security challenges arising from increased Internet cloud and mobile computing.

We currently offer three software based advanced application networking solutions. These are Application Delivery Controllers, or ADCs, to optimize data center performance; Carrier Grade Networking products, or CGN, to provide address and protocol translation services for service provider networks; and a Distributed Denial of Service Threat Protection System, or TPS, for network-wide security protection. We deliver these solutions both on optimized hardware appliances and as virtual appliances across our Thunder Series and AX Series product families.

Our ACOS platform architecture is optimized for modern 64-bit computer processors, or CPUs, which increasingly have multiple parallel processing cores that operate within a single CPU for higher efficiency and performance scalability. In order to maximize the capabilities of these increasingly dense multi-core CPUs, ACOS implements a proprietary shared memory architecture that provides all cores with simultaneous access to common memory. This shared memory architecture enables our products to utilize these multi-core CPUs efficiently and scale performance with increasing CPU cores. As a result, we believe our ACOS application networking platform enables us to provide our end-customers with products that can deliver superior price performance benefits over products that lack these capabilities. ACOS' high performance design enables our products to address a wide range of today's performance-driven networking challenges. For example, we have expanded our products' capabilities to defend against the rising volume of large scale, sophisticated cyber security threats, such as Distributed Denial of Service, or DDoS, and other increasingly sophisticated high volume network attacks. The flexible software design of ACOS enables our end-customers to deploy our products across a number of new models for Information Technology ("IT") operations, such as managed hosting of their network by a third party provider and Internet cloud-based applications and networks.

We sell our products globally to service providers and enterprises that depend on data center applications and networks to generate revenue and manage operations efficiently. Our high-touch sales force engages directly or through indirect distribution channels with our end-customers. We believe that a high-touch, customer-focused selling process is important before, during and after the sale of our products to maximize our sales success. Product fulfillment is generally done through our original equipment manufacturers or distribution channel partners.

For the years ended December 31, 2012, 2013 and 2014, our total revenue was $120.1 million, $141.7 million and $179.5 million, representing a compound annual growth rate of approximately 22% from 2012 to 2014. Our total revenue grew 18% from 2012 to 2013 and 27% from 2013 to 2014. For the years ended December 31, 2012, 2013 and 2014, our gross margin was 80%, 76% and 76%. We generated a net loss of $90.2 million, $27.1 million and $34.7 million for the years ended December 31, 2012, 2013 and 2014. Our net loss in 2012 and 2013 was affected by the settlement of, and legal expenses related to, our litigation with Brocade Communications Systems, Inc.

Trends Driving Continued Evolution of Application Networking

Commercial damage and customer dissatisfaction from poor website, data center application and network performance can have a lasting negative impact well beyond the expenses related directly to the downtime. To optimize data center application and network performance and avoid unforeseen downtime, organizations deploy application networking technology to ensure the performance and security of data center resources. These organizations must simultaneously address significant networking industry trends such as:

• Increased Adoption of Cloud Computing Applications. As organizations move their business critical applications to the cloud, they need application networking solutions optimized for cloud computing that can scale with the performance demands and security expectations of this growth.

• Increased Network Complexity Due to Virtualization and Software Defined Networking Adoption. Application networking technologies need to adapt to software-oriented data center architectures, including virtualization and Software Defined Networking, or SDN.

• Rapid Growth of Internet-Connected Devices and the Exhaustion of the Existing IP Address Space. The rapid growth of mobile and other Internet-connected devices has overwhelmed the current Internet Protocol addressing scheme, IPv4. To support this rapid growth of Internet-connected devices, application networking technology will play an increasingly significant role in managing two Internet connection standards simultaneously, extending the viability of IPv4 and enabling end-customers to move to the IPv6 standard.

• Increasing Risk from Cyber Security Threats. Cybercriminals, foreign military intelligence organizations and amateur hackers are targeting the data centers of organizations of every type. Authentication, application security and encryption are necessary but insufficient defenses against increasingly sophisticated attacks. In one particular cyber threat, a DDoS attack, the perpetrator attempts to render the target network unavailable for its intended purpose by orchestrating coordinated attacks from massive worldwide networks of compromised computers, called botnets. DDoS attacks have become more frequent and sophisticated and can easily overwhelm an inadequately protected target network. As these and other types of attacks have become more frequent and sophisticated, organizations increasingly rely on application networking technologies for defense.

• Exponential Growth in Data Center Speeds. Organizations are enhancing the performance of their networks by increasing the data traffic speeds of their data center networks from the 1 and 10 Gigabit Ethernet rates in use over the last ten years to 40 Gigabit Ethernet currently and are now evolving to 100 Gigabit Ethernet. Organizations require high performance application networking technology to ensure data center application and network performance and security are maintained despite rapidly escalating data rates.

Need for Next-Generation High Performance Application Networking

In order to address these increasingly complex network challenges, a new generation of application-aware networking solutions is needed in order to look deeply into application content, modify content for performance optimization or security purposes, and forward the traffic at rapidly escalating network data rates. Next-generation application networking solutions require:

• Ability to Scale with High Speed Network Traffic. As the number of Internet-connected devices continues to increase rapidly and the speed of network traffic continues to accelerate, architectural limitations in first-generation application networking approaches prevent them from responding effectively due to their inability to scale performance effectively with newer multi-core processor architectures. Next-generation application networking technologies must be able to analyze application data intelligently as they move through faster networks to take full advantage of the increasing computing power of modern multi-core processors.

• Platform to Provide Broad Application Extensibility. First-generation approaches to application networking use rigid system architectures that have been unable to respond effectively to the escalating security threats and the rapidly changing requirements of modern applications and cloud computing. Next-generation application networking technology must be flexible and agile to address the increasing array of networking and application challenges.

• Sophisticated Security Functionality. Next-generation application networking technology should be capable of detecting and mitigating the effects of large-scale, sophisticated cyber security threats such as DDoS and other attacks at the application level of the network. In order to defend against the rising volume of these sophisticated cyber-attacks, which circumvent conventional network based security solutions, application networking solutions must have exceptional application content, inspection capabilities and processing speeds.

• Ability to Accommodate a Variety of IT Delivery Models. Enterprises are increasingly handling their information technology needs in a variety of ways, including operating their own conventional dedicated data centers, and outsourcing to managed IT hosting providers of cloud-based applications to multiple clients often known as Infrastructure-as-a-Service. Some application networking vendors offer products for only a subset of these IT delivery models, or provide inconsistent features and management across these products, which is unacceptable to customers using multiple IT delivery models. Organizations need consistent application networking features and functionality regardless of which IT model, or combination of models they use, and regardless of whether their networks are in virtual or physical forms.

• Predictable Operational Performance. As data center traffic grows, first-generation approaches have limitations that can cause unpredictable performance that cannot consistently meet expected service levels. Next-generation application networking needs to deliver appropriate levels of service at ever-increasing data traffic rates.

Technology

Our Advanced Core Operating System Platform

ACOS Scalable Symmetrical Multi Processing Platform. ACOS is a scalable, flexible and agile software based platform for next-generation application networking. Our proprietary ACOS 64-bit shared memory architecture is critical for current and future performance and scalability requirements. Because ACOS is software based, we can use merchant silicon and industry standard x86 processors to increase our product development velocity, decrease our product development costs, and expand into new product markets. All of our products are built on our ACOS platform and leverage its performance optimization and security services.

ACOS is a symmetric multiprocessing operating system that was built from the ground up to leverage industry trends toward higher density, multi-core processor architectures.

• High Performance and Intelligent Network I/O Processing. In order to maximize the efficiency of high density, multi-core processors, we have developed a high performance intelligent network I/O technology that can balance application traffic flows equitably across processor cores. Our Flexible Traffic Accelerator logic can be implemented either as software running within a standard x86 processor or a Field Programmable Gate Array, or FPGA, semiconductor. Our Flexible Traffic Accelerator also performs certain hardware-based security checks for each packet and can discard suspicious traffic before it can impact system performance.

• Scalable and Efficient Memory Usage. To improve the performance of our multi-core processor architecture, we have developed a shared memory technology to allow all processors to share common memory and the state of the system simultaneously. As a result, we avoid the overhead associated with Inter-Processor Communication architectures deployed in first-generation approaches. We optimize memory to be visible to all cores simultaneously, while minimizing communication overhead and contention among processors for allocated memory space. Since all processors share a common memory pool, we can dynamically allocate memory space based upon the application processing requirements without constraints. Because configurations, policies and network databases are efficiently stored within a shared memory architecture, we can achieve greater performance and scalability from memory and processor resources.

• Optimized Application Networking. Once data has been processed and placed into a shared memory, then a processor can begin to apply ACOS common services and function-specific logic. To ensure that every processor can be utilized to perform every function, and thereby achieve greater system utilization, we have designed ACOS to use all processor cores symmetrically for all functions and services. The ACOS common services perform a set of key

operational functions, including configuration management, network I/O, aFleX scripting, Virtual Chassis System, or aVCS, aXAPI for management integration, Application Delivery Partitions, or ADP, virtualization to enable multi-tenancy, and common resource management such as buffer, system memory, timer management and other internal system management tasks. ACOS features a modular software design, which improves reliability by ensuring that modifications made to one module will not have unwanted side-effects on other system functions.

Other ACOS Technologies. ACOS incorporates a number of other technologies to provide a rich environment for developing Layer 4-7 application networking solutions, including:

• aFleX Scripting. aFleX scripting technology is based on industry-standard Tool Command Language and enables end-customers to write custom scripts to augment the application processing.

• ADP. ADP enables multi-tenancy in the ACOS common services so that multiple departments of an organization or multiple end-customers can share a physical/virtual appliance.

• aVCS. aVCS enables multiple physical/virtual appliances to be managed as a single chassis.

• aXAPI. aXAPI is an industry standard RESTful program interface to enable management integration for achieving automated management.

Our Products

We offer our end-customers a portfolio of software based solutions that are built upon ACOS. Our premium Thunder Series product family, launched in the second quarter of 2013, has three solutions to address end-customer needs, including ADC to optimize data center performance, CGN to provide network address and protocol translation services for service provider networks, and TPS for network-wide security protection. Our AX Series is our original product family that was launched in 2007 and includes ADC and CGN solutions.

Application Networking Solutions

We currently offer three software based solutions that are built on top of our software based ACOS application networking platform and are delivered primarily on our optimized hardware appliances:

Application Delivery Controller. Our ADC solution provides advanced server load balancing, including global server load balancing, high availability, aFleX scripting, aVCS, ADP virtualization delivery for multi-tenancy, Secure Sockets Layer, or SSL, acceleration, SSL intercept, caching and compression, web application firewall, domain name server application firewall and others. ADC solutions are typically deployed in front of a server farm within a data center, including web, application and database servers.

Carrier Grade Network Address Translation. Our CGN solution extends the life of increasingly scarce IPv4 address blocks and their associated infrastructure, and provides migration solutions to the IPv6 addressing standard. Our CGN solution is typically deployed in service provider networks to provide standards-compliant address and protocol translation services between varying types of IP addresses.

Threat Protection System. Our TPS solution provides high volume, large scale detection and mitigation services to ensure that networks and server resources remain available even throughout a massive DDoS attack. TPS solutions are typically deployed at the perimeter of customer networks to protect their internal network resources from large-scale, volumetric cyber attacks, protocol attacks and resource attacks from distributed networks of compromised machines, or botnets.

With the release of our ACOS 4.0 software version we now have the ability to operate ADC and CGN solutions on the same platform, resulting in operational benefits for us and our customers. Our ACOS 4.0 release represents the most significant enhancement to our operating system since the introduction of the 64-bit ACOS release in 2009. The ACOS 4.0 enhanced feature set includes programmability, policy engine and telemetry support for our A10 Harmony architecture, an architecture that lays the foundation of a rapid services integration platform for enterprise, cloud, and service provider networks. An example is our Thunder Series integration and certification with Cisco Application Centric Architecture (ACI) for agile deployment and management of our advanced L4-7 services.

Product Families

We deliver these solutions as both physical and virtual appliances across our Thunder Series and AX Series product families.

Thunder Series. Our ADC, CGN and TPS solutions are available on our Thunder Series product family, including a range of physical appliances with throughput ranges from 5 gigabits per second, or Gbps, to 155 Gbps and a variety of other security and performance options available, as listed in the table below. Our vThunder virtual appliances operate on all major hypervisor platforms, including VMware, Microsoft, Citrix Xen and Linux KVM. Our vThunder virtual appliance is also available from cloud IaaS providers, including Amazon Web Services (AWS), and service providers offering our Pay-as-you-Go Licensing model.

AX Series. Our ADC and CGN solutions are available on our AX Series product family, including a range of physical appliances with throughput ranges from 7.5 Gbps to 115 Gbps and a variety of other security and performance options available.

Centralized Management Solution

Our aGalaxy multi-device network management solution enables a network administrator to manage multiple A10 devices. While full control of our appliances can be achieved effectively out-of-the-box, the benefit of central and automated management increases as more appliances are added. The user interface provides a quick, at-a-glance view of status using a standard web browser. aGalaxy is designed to provide lower operational costs, as staff are freed up from repetitive tasks, while also increasing precision and accuracy with centralized and automated tasks, reducing the potential for human error.

Support and Services

One of our founding principles is to provide superior customer and technical support. Our global support team is part of our engineering organization and is trained across all products and solutions. Our support team takes complete ownership of customer issues from the beginning to the end to achieve rapid response and a high quality resolution. We believe that our ability to provide consistent, high-quality customer service and technical support is a key factor in attracting and retaining end-customers of all sizes. Accordingly, we offer a broad range of support services that include installation, phone support, repair and replacement, software updates, online tools, consulting and training services.

All customers receive warranty support for 90 days and greater than 95% of our end-customers purchase one of our maintenance products which entitles them to the support provided by our global support team. We offer a variety of support offerings, primarily two maintenance product options – Basic Support and Gold Support. The average maintenance contract term is 18 months. We invoice our channel partners or end-customers directly for maintenance contracts, in advance, at the time of hardware purchase. We generally provide discounts to our end-customers when they commit to longer term contracts. All our maintenance contracts are non-cancellable and are renewed through the same channel as originally purchased. Updates of our software are provided to all end-customers with a current maintenance contract on a when-and-if-available basis. Additionally, we provide on-site technical support as part of certain maintenance contracts. We maintain technical support centers in the United States, Japan, China and the Netherlands.

We have a professional services team able to provide a full range of fee-based consulting services, including pre-sale network assessment, comprehensive network analysis and capacity planning, post-sale migration and implementation services, on-site installation and on-going support.

Customers

We target organizations globally that depend on data center applications and networks to generate revenue and manage operations efficiently. Our end-customers operate in a variety of industries including telecommunications, technology, industrial, retail, financial and education. Since inception, our customer base has grown rapidly. As of December 31, 2014, we had sold our products to more than 3,900 customers across 71 countries. Our end-customers include three of the top four United States wireless carriers, seven of the top ten United States cable providers, and the top three wireless carriers in Japan, in addition to other global enterprises, Web giants and governmental organizations. Our business is geographically diversified with 48% of our total revenue from the United States, 26% from Japan and 26% from other geographic regions for the year ended December 31, 2014. During the years ended December 31, 2012, 2013 and 2014, purchases from our ten largest end-customers accounted for approximately 49%, 43% and 37% of our total revenue.

Two end-customers, NTT DoCoMo, Inc., a Japanese wireless provider, and Microsoft Corp., an enterprise customer, both purchasing through resellers, accounted for 13% and 10% of net revenue in the year ended December 31, 2013; no other end-customer accounted for more than 10% of our total revenue during the periods presented.

Backlog

As of December 31, 2014 and 2013, we had product backlog of approximately $4.0 million and $12.0 million. Backlog represents orders confirmed with a purchase order for products to be shipped generally within 90 days to customers with approved credit status. Orders are subject to cancellation, rescheduling by customers and product specification changes by customers. Although we believe that the backlog orders are firm, purchase orders may be canceled by the customer prior to shipment without significant penalty. For this reason, we believe that our product backlog at any given date is not a reliable indicator of future revenues.

Sales and Marketing

Sales. We sell our products globally to service providers and enterprises that depend on networks and data centers to generate revenue and manage operations efficiently. Our high-touch sales force engages directly or through indirect distribution channels with service providers and enterprises. Depending on size, geography, and complexity, some end-customer sales are originated and completed by our OEM and distribution channel partners with little or no direct engagement with our sales personnel. We fulfill nearly all orders globally through our distribution channel partners, which include distributors, value added resellers and system integrators.

For the year ended December 31, 2014, 85% of our revenue was generated through our distribution channel partners. In 2014, one distribution channel partner, Itochu Techno Solutions Corporation accounted for 13% of our total revenue. In 2013, two distribution channel partners, NEC Corporation and Adaptive Integration, accounted for 15% and 10% of our total revenue. In 2012, revenues from NEC Corporation accounted for 34% of our total revenue. We also work closely with OEM partners. We believe that our high-touch sales organization is unique given our deep focus on technology competence and partnership with our end-customers' network engineers and architects. We believe this sales approach allows us to leverage the benefits of the channel, such as expanding our market coverage, as well as maintain face-to-face relationships with our end-customers.

Our sales team is comprised of inside sales and field sales personnel who are organized by geography and maintain sales presence in 30 countries, including in the following countries and regions: United States, Western Europe, the Middle East, Japan, China, Taiwan, South Korea and Latin America. Our sales organization also includes sales engineers with deep technical domain expertise who are responsible for pre-sales technical support, solutions engineering for our end-customers, proof of concept work and technical training for our distribution channel partners. Our sales team is also comprised of a channel sales organization that is expanding our market reach through partners. We expect to continue to grow our sales headcount, including in geographies where we currently do not have a sales presence.

Marketing. Our marketing strategy is focused on building our brand and driving end-customer demand for our application networking products and services through channel marketing, direct marketing and corporate communications campaigns. Marketing activities include product and solution launches, demand generation, advertising, Website development, trade shows and conferences. We are also actively engaged in driving global thought leadership through industry analyst engagement, media outreach, blogs and social media, and speaking events.

Manufacturing

We outsource the manufacturing of our hardware products to original design manufacturers. This approach allows us to benefit from the scale and experience of our manufacturing partners to reduce our costs, overhead and inventory while allowing us to adjust more quickly to changing end-customer demand. Our manufacturers are Lanner Electronics Inc., or Lanner, and AEWIN Technologies Co., Ltd., or AEWIN. These companies manufacture and assemble our hardware products using design specifications, quality assurance programs and standards that we establish. Our manufacturers procure components and assemble our products based on our demand forecasts and purchase orders. These forecasts represent our estimates of future demand for our products based upon historical trends and analysis from our sales and product management functions as adjusted for overall market conditions. The component parts incorporated into our products are sourced either by our manufacturing partners or directly by us.

We have agreements with both Lanner and AEWIN pursuant to which they manufacture, assemble, and test our products. The Lanner agreement has an initial one year term and the AEWIN agreement has an initial term of six years. Each agreement automatically renews for successive one-year terms unless either party gives notice that they do not want to renew the agreement. We do not have any long-term manufacturing contracts that guarantee us any fixed capacity or pricing. We perform quality assurance and testing at our San Jose, Taiwan and Japan distribution centers, as well as at our manufacturers' locations. We warehouse and deliver our products out of our San Jose warehouse. We also outsource warehousing and delivery to a third-party logistics provider in some regions.

Research and Development

Our research and development effort is focused on developing new products and on enhancing and improving our existing products, leveraging our ACOS platform. Our engineering team works closely with end-customers and technology partners to identify future needs. A majority of our research and development team is focused on software development, with substantial experience in networking, network management, application delivery, performance optimization, security, software quality engineering and automation.

We believe that innovation and timely development of new features and products is essential to meeting the needs of our end-customer and improving our competitive position. We supplement our own research and development effort with open source technologies and technologies that we license from third parties. We test our products thoroughly to certify and ensure interoperability with third-party hardware and software products.

Our engineering teams are located mainly in our headquarters in San Jose, California, Beijing, China and Taipei, Taiwan. For the years ended December 31, 2012, 2013 and 2014 our research and development expenses were $25.5 million, $33.3 million and $49.9 million, representing 21%, 24% and 28% of our total revenue.

Competition

We operate in the intensely competitive application networking market that is characterized by constant change and innovation. Changes in application delivery needs, cyber security threats, and the technology landscape result in evolving customer requirements to address application performance and security. In addition to server load-balancing and other functions normally associated with application delivery, our solutions have expanded our addressable market into DDoS production and CGN, where we compete with a number of companies not included among traditional ADC vendors. The agility and flexibility of the ACOS platform enables us to rapidly innovate and deploy solutions into adjacent markets to ADC. As a result, we believe the traditional definitions of our market do not encompass all of the features, functions and capabilities of our solutions, or accurately represent the addressable market.

The ADC, CGN and TPS markets are characterized by a set of identifiable participants. We do not consider any of these markets to include a single dominant company, nor do we consider the markets to be fragmented.

We believe that our main competitors fall into three categories:

• Companies that sell products in the traditional ADC market which includes companies that are well established in this market, such as F5 Networks, Inc., Brocade Communications Systems, Inc., Citrix Systems, Inc., and Radware Ltd.

• Companies that sell CGN products, products originally designed for other networking purposes, such as edge routers and security appliances from vendors such as Alcatel-Lucent USA Inc., Cisco Systems, Inc. and Juniper Networks, Inc.

• Companies that sell traditional TPS mitigation products. We are a new entrant into the DDoS market and first publicly launched our DDoS detection and mitigation solution, TPS, in January 2014. We believe our principle competitors in this market are Arbor Networks, Inc., a subsidiary of NetScout Systems, Inc., and Radware, Ltd.

We believe that the principal competitive factors in our markets include:

• Ability to innovate and respond to customer needs rapidly;

• Breadth and depth of product features and functionality;

• Level of customer satisfaction;

• Price performance and efficiency;

• Ability for products to scale with high speed network traffic;

• Flexible and agile design of products;

• Ability to detect and mitigate large-scale cyber security threats;

• Ability to accommodate any IT delivery model or combination of models, regardless of form factor;

• Brand awareness and reputation; and

• Strength of sales and marketing efforts

We compete primarily based on the quality and price of our products, the rich and comprehensive features and functionalities offered by our platform, our differentiated customer support offerings and our close and ongoing relationship with our end-customers. However, many of our competitors have substantially greater financial, technical and other resources, greater name recognition, larger sales and marketing budgets, broader distribution, and larger and more mature intellectual property portfolios.